DIRECTORATE GENERAL FOR NEIGHBOURHOOD AND ENLARGEMENT NEGOTIATIONS – DG NEAR

Short term high quality studies to support activities under the Eastern Partnership Project

HiQSTEP

Study on the Harmonisation of the Digital Markets (HDM)

in the Eastern Partnership

ANNEX: TECHNICAL NOTES

First draft submitted:	20.4.2015
Final draft submitted:	8.6.2015
Final version submitted:	12.11.2015

[document requires further formatting]

This report has been prepared by the KANTOR Management Consultants - led Consortium. The findings, conclusions and interpretations expressed in this document are those of the Consortium alone and should in no way be taken to reflect the policies or opinions of the European Commission.

CONTENTS

1 APPLICABLE EU LEGAL FRAMEWORK 3

Network, information and cyber security 3

Electronic identification and trust services 4

eCustoms 4

eCommerce for SMEs 7

Digital skills 8

Telecom Rules 10

2 EU BEST PRACTICE 14

Network, Information and Cyber Security 14

eCustoms - Detailed description of the EU baseline 14

eCommerce – detailed description of the EU baseline 29

Digital Skills 40

Telecom Rules 51

3 ACHIEVEMENTS, GAPS AND ROADMAPS OF THE PARTNER COUNTRIES RELEVANT TO THEIR ASSOCIATION AGREEMENTS 90

Network, information and cyber security 90

Electronic identification and trust services 106

eCustoms 116

eCommerce for SMEs 121

Digital Skills 136

Telecom Rules 138

4 DETAILED STATE OF PLAY AND GAP ANALYSIS OF THE PARTNER COUNTRIES 150

Network, Information Security and Cybersecurity 150

Electronic identification and Trust Services 171

eCustoms 189

eCommerce for SMEs 235

Digital Skills 294

Telecom Rules 307

5 RELEVANT NATIONAL ORGANISATIONS AND INTERVIEWED PEOPLE 314

Information, network and cyber security 314

Electronic identification and trust services 320

eCommerce 323

eCustoms 328

Digital skills 333

Telecom rules 335

6 BIBLIOGRAPHY AND SOURCES 337

7 QUESTIONNAIRES 338

7.1 Network and Information Security and Cyber-security 338

7.2 Electronic identification and Trust Services 403

7.3 eCustoms 444

7.4 eCommerce 485

7.5 Digital skills 517

7.6 Telecom rules 549

1 APPLICABLE EU LEGAL FRAMEWORK

Network, information and cyber security

European Cyber-security Strategy. A Joint Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions (7.2.2013) including Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union.

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 (Framework Directive) on a common regulatory framework for electronic communications networks and services (Framework Directive) (as amended by Directive 2009/140/EC and Regulation 544/2009.

Directive on privacy and electronic communications: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector including such related and amending acts as: Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications [Official Journal L 173 of 26.06.2013] and Directive 95/46/EC of the European Parliament and of the Council (Data Protection Directive)).

Regulation No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.

Digital Agenda for Europe (DAE) - Communication from the Commission to the Council, The European Parliament, the European Economic and Social Committee and the Committee of the Regions, 19.05.2010.

Regulation No 910/2014 of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (including the preceding E-Signature Directive 1999/93/EC)

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

Baseline Capabilities of National/Governmental CERTs – Policy recommendations by ENISA (European Network and Information Security Agency), 2012.

ENISA Technical Guideline for Security Measures – guiding National Regulatory Authorities (NRAs) about security measures they should take into account when evaluating the compliance of public communications network and service providers with the Directive's Article 13a.

ENISA Technical Guideline for Incident Reporting – guiding National Regulatory Authorities (NRAs) about reporting in the form of (a) the annual summary of significant incidents and (b) ad hoc notification of incidents to other NRAs in case of cross-border.

Electronic identification and trust services

Regulation No 910/2014 of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (replacing the preceding E-Signature Directive 1999/93/EC).

Mandate M460 regarding the EU Standardisation initiatives/cross border tools.

Decision 2004/387/EC (Corrigenda) of the European Parliament of 21 April 2004 on interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC). Takes into account the Directive 95/46/EC of the European Parliament and of the Council (Data Protection Directive) and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

Interoperability of European public services, Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA).

European Interoperability reference Architecture and European Cartography of Interoperability solutions and (2) European federated Interoperability Repository (EFIR).

Directive 95/46/EC of the European Parliament and of the Council (Data Protection Directive).

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, part of the "Telecom Package"); amending acts: Directive 2002/58/EC, Directive 2006/24/EC, Directive 2009/136/EC.

Directive 2004/18/EC of the European Parliament and Council of 31.3.04 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts.

Directive 2006/123/EC of the European Parliament and Council of 12.12.06 on services in the internal market.

A Digital Agenda for Europe (DAE) (Communication from the Commission to the Council, The European Parliament, the European Economic and Social Committee and the Committee of the Regions, 19.05.2010).

Commission Implementing Decision of 3 April 2014 on the identification of ICT technical specifications eligible for referencing in public procurement (notified under document C(2014) 2120) (2014/188/EU; Official Journal of the European Union 5.4.2014).

eCustoms

Council Regulation (EEC) No 2913/92 - establishing the Community Customs Code

Regulation (EU) No 952/2013 - The Union Customs Code (UCC)

Commission Implementing Decision of 29 April 2014 establishing the Work Programme for the Union Customs Code

Decision N° 70/2008/EC - Decision on the paperless environment for customs and trade - 'Electronic Customs Decision'

Regulation (EC) n° 648/2005 - security amendment to the Community Customs Code. Pre-arrival and pre-departure information (in the form of summary declarations lodged before the goods are brought into or out of the Union customs territory) to be filed electronically and also envisages exchange and sharing of the information between the Member States administrations

REGULATION EC 1875/2006 – security amendment to the Customs Code

Regulation (EC) No 312/2009 - Economic Operators' Registration and Identification system

Regulation (EEC) No 2454/93 laying down provisions for the implementation of Council Regulation (EEC) No 2913/92 establishing the Community Customs Code

REGULATION (EC) No 450/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 April 2008 laying down the Community Customs Code (Modernised Customs Code)

Council Regulation (EEC) No 2658/87 of 23 July 1987 - The legal base of the TARIC on the tariff and statistical nomenclature and on the Common Customs Tariff (Official Journal L 256, 07/09/1987).

Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on the interoperable delivery of pan-European e-Government services to public administrations, businesses and citizens

Communication on EU Strategy and Action Plan for customs risk management: Tackling risks, strengthening supply chain security and facilitating trade (COM/2014/527). The Strategy and Action Plan annexed - 21 August 2014

Communication on Customs Risk Management and the Security of the Supply Chain (COM/2012/793) - 8 January 2013

Customs 2020 Regulation : Regulation (EU) No 1294/2013 of the European Parliament and of the Council of 11 December 2013 establishing an action programme for customs in the European Union for the period 2014-2020 (Customs 2020)

AWP 2014 - The Annual Work Programme constitutes the whole framework for the implementation of the programme. The Customs 2020 Committee provides its formal opinion on the AWP before its adoption by the Commission

Single Window at Community Level - WORKING DOCUMENT: TAXUD/1241/2005 – Rev. 5

REGULATION (EU) No 608/2013 of the European Parliament and of the Council of 12 June 2013 concerning customs enforcement of intellectual property rights and repealing Council Regulation (EC) No 1383/2003

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

Council Regulation (EEC) No 2913/92 - establishing the Community Customs Code

Regulation (EU) No 952/2013 - The Union Customs Code (UCC)

Commission Implementing Decision of 29 April 2014 establishing the Work Programme for the Union Customs Code

Decision N° 70/2008/EC - Decision on the paperless environment for customs and trade - 'Electronic Customs Decision'

Regulation (EC) n° 648/2005 - security amendment to the Community Customs Code. Pre-arrival and pre-departure information (in the form of summary declarations lodged before the goods are brought into or out of the Union customs territory) to be filed electronically and also envisages exchange and sharing of the information between the Member States administrations

REGULATION EC 1875/2006 – security amendment to the Customs Code

Regulation (EC) No 312/2009 - Economic Operators' Registration and Identification system

Regulation (EEC) No 2454/93 laying down provisions for the implementation of Council Regulation (EEC) No 2913/92 establishing the Community Customs Code

REGULATION (EC) No 450/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 April 2008 laying down the Community Customs Code (Modernised Customs Code)

Council Regulation (EEC) No 2658/87 of 23 July 1987 - The legal base of the TARIC on the tariff and statistical nomenclature and on the Common Customs Tariff (Official Journal L 256, 07/09/1987).

Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on the interoperable delivery of pan-European e-Government services to public administrations, businesses and citizens

Communication on EU Strategy and Action Plan for customs risk management: Tackling risks, strengthening supply chain security and facilitating trade (COM/2014/527). The Strategy and Action Plan annexed - 21 August 2014

Communication on Customs Risk Management and the Security of the Supply Chain (COM/2012/793) - 8 January 2013

Customs 2020 Regulation : Regulation (EU) No 1294/2013 of the European Parliament and of the Council of 11 December 2013 establishing an action programme for customs in the European Union for the period 2014-2020 (Customs 2020)

AWP 2014 - The Annual Work Programme constitutes the whole framework for the implementation of the programme. The Customs 2020 Committee provides its formal opinion on the AWP before its adoption by the Commission

Single Window at Community Level - WORKING DOCUMENT: TAXUD/1241/2005 – Rev. 5

REGULATION (EU) No 608/2013 of the European Parliament and of the Council of 12 June 2013 concerning customs enforcement of intellectual property rights and repealing Council Regulation (EC) No 1383/2003

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014

on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

eCommerce for SMEs

COM(2011) 942 - A coherent framework for building trust in the Digital Single Market for e-commerce and online services – Commission communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions

COM(2011) 206 final - Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, Single Market Act, Twelve levers to boost growth and strengthen confidence, "Working together to create new growth", 13.04.2011

COM(2010) 245 final/2 - Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A Digital Agenda for Europe, 26.08.2010

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178/1, 17.07.2000

Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 013/12, 19.01.2000

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201/37, 31.07.2002

Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, OJ L 217/18, 05.08.1998

Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC

Regulation (EU) No 815/2012 of 13 September 2012 laying down detailed rules for the application of Council Regulation (EU) No 904/2010, as regards special schemes for non established taxable persons supplying telecommunications, broadcasting or electronic services to non taxable persons

Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market

Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006

on services in the internal market, OJ L 376/36, 27.12.2006

Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 157/16, 30.4.2004; available at:

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167/10, 22.06.2001

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Directive 2010/45/EU on the common system of value added tax as regards the rules on invoicing

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market

Directive 2000/46/EC on electronic money institutions (issue means of payment in e-money)

Directive 2007/64/EC on payment services (any kind of e-payment)

DIRECTIVE 2013/11/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on alternative dispute resolution for consumer disputes

Regulation on Online Dispute Resolution (ODR) (PE-CONS 79/12 and PE-CONS 80/12)

Digital skills

Digital Agenda for Europe

- Pillar IV of the Digital Agenda for Europe defines Enhanced digital literacy, skills and inclusion ec.europa.eu/digital-agenda/en/our-goals/pillar-iv-enhancing-digital-literacy-skills-and –inclusion

The “Grand Coalition for Digital Jobs”

- This is the European Commission led multi-stakeholder partnership to tackle the lack of digital skills in Europe and the thousands of unfilled ICT-related vacancies across all industry sectors. ec.europa.eu/digital-agenda/en/grand-coalition-digital-jobs

The National and Local Coalitions for Digital Jobs

- These are multi-stakeholder partnerships developed in Member States to enhance digital skills at national, regional or local level. ec.europa.eu/digital-agenda/en/national-local-coalitions

The Digital Skills Strategy for the 21st Century is described on ec.europa.eu/enterprise/sectors/ict/Digital Skills//index_en.htm

The reference documents for the Digital Skills strategy are the following;

- Filling the gaps: Digital Skills and Education for Digital Jobs
- www.filling-the-gaps.eu/Report.pdf
- E-Leadership: Digital Skills for Competition and Innovation Report

- ec.europa.eu/enterprise/sectors/ict/files/eskills/vision_final_report_en.pdf
- Towards a European Quality Label for ICT Industry Training and Certification Report
- ec.europa.eu/enterprise/sectors/ict/files/eskills/quarterly_final_report_en.pdf
- Digital Skills Manifesto with contributions from leading figures in government, education, policy, research and industry
- ec.europa.eu/DocsRoom/documents/7039
- Digital Skills and ICT Professionalism in Europe
- ec.europa.eu/enterprise/sectors/ict/files/eskills/ict_professionalism_report_en.pdf
- Digital Skills: Cloud Computing, Cyber-security and Green IT Report
- ec.europa.eu/enterprise/sectors/ict/files/eskills_and_cloud_computing_final_report_en.pdf
- European e-Competences Framework CEN ICT Skills Workshop
- www.cen.eu/work/areas/pages/default.aspx
- Digital Skills: Financial and Fiscal Incentives Report
- ec.europa.eu/enterprise/sectors/ict//files/Digital Skills_and_incentives_en.pdf
- European Exchange Mechanism for Digital Skills Development Report
- ec.europa.eu/enterprise/sectors/ict//files/eskills/exchange_mecs_eskills_final_report_en.pdf

Employment Package of 2012

This is a set of policy documents looking at how EU unemployment policies intersect with a number of other policy areas in support of smart, sustainable and inclusive growth. It identifies the EU's biggest job potential areas and the most effective ways for EU countries to create more jobs. ec.europa.eu/social/main.jsp?catId=1039

e-CF: A common European framework for ICT Professionals in all industry sectors.

The European e-Competence Framework (e-CF) provides a reference of 40 competences as required at the ICT workplace, using a common language for competences, skills and proficiency levels that can be understood across Europe. The framework definition is downloadable on:

www.ecompetences.eu/wp-content/uploads/2014/02/European-e-Competence-Framework-3.0_CEN_CWA_16234-12014.pdf

The user guide for the application of the e-CF is downloadable on;

www.ecompetences.eu/wp-content/uploads/2014/02/User-goide-for-the_-application-of-the-e-CF-3.0_CEN_CWA_16234-12014.pdf

Opening up Education Initiative

The main goal of this initiative is to stimulate ways of learning and teaching through ICT and digital content, mainly through the development of the Open Education

Resources (OER). Among its actions the most important one is to change the role of digital technologies at school.

www.openeducationeuropa.eu/en/initiative

http://europa.eu/rapid/press-release_IP-13-859_en.htm

Initiatives linked to Opening up Education will be funded with support from Erasmus+, the new EU programme for education, training, youth and sport, and Horizon 2020, the new research and innovation programme, as well as the EU structural funds.

http://ec.europa.eu/programmes/erasmus-plus/discover/index_en.htm

http://ec.europa.eu/programmes/horizon2020/en/what-horizon-2020

Open Educational Resources (OER)

The EU-funded Open Education Europa portal provides access to the many resources available.

http://openeducationeuropa.eu/

In addition, large scale pilot projects such as Open Discovery Space, co-funded by the Commission, are working with teachers to create and make better use of OER.

http://opendiscoveryspace.eu/

Telecom Rules

The EU legal and regulatory framework for electronic communications

"EU Aquis"

The opening-up of the telecommunications market to competition has acted as a catalyst on a sector previously reserved for national incumbent monopolies. To keep up with these changes, Europe's decision-making bodies have adopted legislation in tune with technological progress and market requirements. These developments have given rise to the adoption of a new regulatory framework on electronic communications, the main aim of which is to strengthen competition by making market entry easier and by stimulating investment in the sector. The European Union`s legislation liberalising national electronic communications market was first adopted by all EU Member States in 1998. Since the beginning of the 21st century, several improvements of the EU framework have been made to ensure competition, investment and the creation of a single market in this area. This was done by means of legal directives that are mandatory for transposition in to the EU Members States` legislation. Depending on the date of their issuance, these additions are often referred to as "The 2003 and 2009 European Union regulatory frameworks".

The collective name, EU 2002 regulatory framework, encompasses the five following directives:

- Directive 19/2002/19/EC, "The Access Directive"[1] – deals especially with the access

[1] DIRECTIVE 2002/19/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 March 2002

on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) as amended by Directive 2009/140/EC (unofficially consolidated version)

obligation that the national regulatory authority can impose on the SMP operators, which means the SMP operators can be obliged to provide access to their networks and services, ensuring non-discrimination, transparency and cost-orientation

- Directive 2002/20/EC, "The Authorisation Directive"[2] – facilitates market entry by requiring a general authorisation regime, which means that everybody can provide electronic communications services without the need for a licence or the need to pay inappropriate fees
- Directive 2002/21/EC, "The Framework Directive"[3] – sets the legal environment required for the independent national regulatory authorities to perform regular market analyses and adopt appropriate remedies when competition is insufficient
- Directive 2002/22/EC, "The Universal Service Directive"[4] – contains several provisions to ensure consumer protection, especially the requirement to ensure that a basic level of electronic communications service is available on the whole territory of the country and for every end-user, even in cases when it would not be provided under normal market conditions
- Directive 2002/58/EC, "The Privacy Directive"[5]– deals with the protection of personal data in electronic communications

Often added to this list is another legal act, Decision 2002/676/EC, "The Radio Spectrum Decision" which deals with the regulatory framework for radio spectrum policy in the EU.

In December 2009, the European Union (aiming to improve the regulatory environment, customer protection and market competition), amended some of the provisions of the abovementioned framework.

The two Directives and one Regulation are known under the collective name of the EU 2009 amendments:

---

http://www3.ebu.ch/files/live/sites/ebu/files/Knowledge/Media%20Law/Reference%20Texts/EU%20-%20Telecom/REF%20EU-DIR2002.19.EC.pdf

[2] DIRECTIVE 2002/20/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) as amended by Directive 2009/140/EC (unofficially consolidated version)
http://www3.ebu.ch/files/live/sites/ebu/files/Knowledge/Media%20Law/Reference%20Texts/EU%20-%20Telecom/REF%20EU-Dir2002.20.EC.pdf

[3] DIRECTIVE 2002/21/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) as amended by Directive 2009/140/EC and Regulation 544/2009 (unofficially consolidated version)
http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/140framework_5.pdf

[4] DIRECTIVE 2002/22/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 March 2002

on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0022&from=en

[5] DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)as amended by Directive 2006/24/EC and Directive 2009/136/EC (unofficially consolidated version)
http://www3.ebu.ch/files/live/sites/ebu/files/Knowledge/Media%20Law/Reference%20Texts/EU%20-%20Telecom/REF%20EU-DIR2002.58.EC.pdf

- Directive 2009/136/EC, "The Citizen`s Rights Directive"[6]– provides more protection for the rights of consumers of electronic communications services and amends Directive 2002/22/EC, Directive 2002/58/EC, and Regulation (EC) No. 2006/2004
- Directive 2009/140/EC, "The Better Regulation Directive" [7] – deals with the independence of the NRAs and the overall regulatory environment and amends Directive 2002/21/EC, Directive 2002/19/EC and Directive 2002/20/EC
- Regulation 1211/2009 establishing the Body of European Regulators for Electronic Communications (BEREC)[8] - The main task of BEREC is to advise and assist the European Commission in developing the internal market, and to form a link between national regulatory authorities (NRAs) and the Commission

In addition, the European Commission issued on 7 May 2009 Recommendation No. 2009/396/EC[9] on the Regulatory Treatment of Fixed and Mobile Termination Rates in the EU.

Another important part of the regulatory framework is the Commission Recommendation 2007/879/EC [10] on relevant product and service markets within the electronic communications sector susceptible to ex-ante regulation in accordance with Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services. In the 2007 document, the European Commission lists the 7 relevant markets where it recommends exercising market analysis and stipulates the methodology to be used when identifying other relevant markets.

---

[6] DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal

data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0136&from=en

[7] DIRECTIVE 2009/140/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009

amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0140&from=en

[8] REGULATION (EC) No 1211/2009 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009R1211&from=EN

[9] COMMISSION RECOMMENDATION of 7 May 2009 on the Regulatory Treatment of Fixed and Mobile Termination Rates in the EU. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:124:0067:0074:EN:PDF

[10] COMMISSION RECOMMENDATION of 17 December 2007 on relevant product and service markets within the electronic communications sector susceptible to ex ante regulation in accordance with Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:344:0065:0069:en:PDF

In 2014, a revised recommendation was issued[11] which removed 2 of the 7 markets and redefined another 2 markets to take account of market and technology developments.

In order to encourage innovation and increase productivity, employment and competitiveness, and ultimately to create economic growth and achieve the goals of the Europe 2020 Strategy, on 11th September 2013 the European Commission has adopted the Commission Recommendation on consistent non-discrimination obligations and costing methodologies to promote competition and enhance the broadband investment environment[12]. The recommendation aims to create an environment that is both competitive and investment-attractive for the development of high-speed broadband internet.

[11] COMMISSION RECOMMENDATION of 9.10.2014 on relevant product and service markets within the electronic communications sector susceptible to ex ante regulation in accordance with Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services. https://ec.europa.eu/digital-agenda/en/news/commission-recommendation-relevant-product-and-service-markets-within-electronic-communications

[12] COMMISSION RECOMMENDATION of 11.9.2013 on consistent non-discrimination obligations and costing methodologies to promote competition and enhance the broadband investment environment http://ec.europa.eu/smart-regulation/impact/ia_carried_out/docs/ia_2013/c_2013_5761_en.pdf

2 EU BEST PRACTICE

Network, Information and Cyber Security

Box 1: Developing Cyber Security Strategies – ENISA Good Practice Guide on National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace.

Box 2: Three lessons learned from cooperation between CERTs and law enforcement agencies.

eCustoms - Detailed description of the EU baseline

1. Legal framework

N	Benchmark	EU baseline
1.1	Common criteria and priority areas for risk assessment	The EU establishes an equivalent level of protection in customs controls for goods brought into or out of the customs territory of the Community. In order to achieve this objective, an equivalent level of customs controls in the Community is established to ensure a harmonised application of customs controls by the Member States, which have principal responsibility for applying these controls. Rules concerning a Community Risk Management Framework laid down in Regulation (EC) 648/2005. The conditions under which information provided by economic operators to customs may be disclosed to other authorities in the same Member State, other Member States, to the Commission, or to authorities in third countries is clearly specified. Customs and other competent authorities, such as veterinary and police authorities, may communicate data received, in connection with the entry, exit, transit, transfer and end-use of goods that do not have Community status moved between third countries to the customs territory of the Community.
1.2	Risk Information Form (RIF)	The RIF is an electronic declaration and automated system for the implementation of risk management and for the electronic exchange of data between customs offices of entry, import, export and exit. The function of the RIF is to exchange risk information dealing with routine control concerns. A RIF should raise the awareness of the customs offices concerned with regard to a potential irregularity. A RIF can be prepared following a finding of an irregularity (for example a misdeclaration or finding of counterfeit or undeclared CITES goods). The RIF

		could give information on the technique used to find the irregularity, for example the result of a physical examination or a classification decision. The RIF can be used to support targeting and risk analysis in a simple and effective manner at the external frontier. The first phase of the RMF, the electronic Risk Information Form (RIF) system, was launched in April 2005. The second phase involves an upgrade of the RIF system to include new user requirements arising from the practical experience gained by the users of the system. The next phase will involve enhancing the RIF system to permit the secure electronic transmission and management of common Community risk profiles, requiring mandatory control action by Member States. These risk profiles will relate to priority control areas as required under the rules concerning a Community Risk Management Framework laid down in Regulation (EC) 648/2005 and the corresponding implementing provisions. An example of the use of the RIF is the dissemination by the Commission to all Member States and Candidate Countries risk analysis centres, information regarding the protection measures relating to avian influenza in Thailand. EU customs have been given detailed information to include in their risk assessment strategies to support their controls in the fight against the possible illegal importation of prohibited poultry products from Thailand.
1.3	Authorised economic operators status	The common EU procedure (Regulation (EC) 648/2005) is used to determine the rules: — for granting the status of authorised economic operator — for granting authorisations for the use of simplifications The customs authorities in all Member States recognise the status of authorised economic operator. The other Member States should allow the use of simplifications by authorised economic operators if they meet all the specific requirements for use of the particular simplifications. In considering a request to use simplifications, the other Member States need not repeat the evaluation of the operator's control systems, financial solvency or compliance record, which will already have been completed by the Member State that granted the operator the status of authorised economic operator. However, they should ensure that any other specific requirements for use of the particular simplification are met. (The model was developed and tested

		in a pilot case COMPACT). The use of simplifications in other Member States may also be coordinated by agreement between the customs authorities concerned.
1.4	Interoperating of systems of identification and registration for economic operators with the authorised economic operators system	System of identification and registration for economic operators interoperating with the authorised economic operators system and enabling those economic operators to register only once for all their interactions with customs authorities throughout the Community, taking into account existing Community or national systems (Decision 70/2008/EC)
1.5	Provisions for the paperless environment for customs and trade	Paperless environment for customs and trade is defined in the Electronic Customs Decision (DECISION No 70/2008/EC). Council Regulation (EEC) No 2913/92 of 12 October 1992 establishing the Community Customs Code requires the use of data processing techniques for lodging summary declarations and for the electronic exchange of data between customs authorities, with a view to basing customs controls on automated risk analysis systems. The objectives of the electronic customs systems shall be achieved by the following means: • the harmonised exchange of information on the basis of internationally accepted data models and message formats; • offering to economic operators of a wide range of electronic customs services enabling those operators to interact in the same way with the customs authorities of any Member State The Community promotes the interoperability of electronic customs systems with the customs systems of third countries or of international organisations and the accessibility of electronic customs systems to economic operators in third countries, with a view to creating a paperless environment at international level where provided for under international agreements and subject to proper financial arrangements. Electronic customs systems shall consist of Community components and national components. Member States shall, in cooperation with the Commission, make operational the following electronic customs systems: • Systems for import and export interoperating with the

		system for transit and enabling the seamless flow of data from one customs system to another throughout the Community; • A system of identification and registration for economic operators interoperating with the authorised economic operators system and enabling those economic operators to register only once for all their interactions with customs authorities throughout the Community, taking into account existing Community or national systems; • A system for the authorisation procedure, including the information and consultation process, the management of certificates for authorised economic operators and the registration of those certificates in a data base accessible by customs authorities.

2. Infrastructure

N	Benchmark	EU baseline
2.1	Single Electronic Access Points (SEAP)	Decision 70-2008-EC defines the general requirements for implementation of electronic interfaces for economic operators enabling them to conduct all customs-related business, even if several Member States are involved, with the customs authorities of the Member State where they are established. Single Electronic Access Point (SEAP) provides the framework environment where traders can be connected in order to interact with EU Customs (e.g. to submit an application, a document or a declaration). The components contributing to the implementation of SEAP will be realised in the context of the development of new systems and providing interoperability between the national customs systems (SEAP is not a system by itself).
2.2	Interoperating systems for import, export and transit	Systems for import and export interoperate with the system for transit and enable the seamless flow of data from one customs system to another throughout the Community (Decision 70-2008-EC) The electronic customs systems of the Community and the Member States provide the exchange of data between the customs authorities of the Member States and between those authorities and economic operators, the Commission, and other administrations or official agencies involved in the

		international movement of goods.
2.3	Automated Import System	The objective of the Automated Import System is to ensure that import operations started in one Member State can be completed in another Member State without re-submission of the same information. This includes the exchange of electronic messages related to the different stages of the operations amongst the various actors (customs, traders and other governmental administrations). The first phase of the implementation, Import Control System (ICS), is aimed to provide for the handling of pre-arrival declarations (under security and safety amendment Regulation (EC) 648/2005) and the link of the information with risk analysis. The ICS system Phase 1 is fully operational since 01/01/2011 in all Member States and, within 2013, the error rate was stabilised around 0.12%.
2.4	Automated Export System (AES)	The objective of the Automated Export System (AES) is to ensure that export operations started in one Member State can be finalised in another Member State without re-submission of the same information. This includes the exchange of electronic messages related to the different stages of the operations amongst the various actors. The current AES service assures the central clearance approach with the full control of the conclusion of export operations via the electronic exchange of export/exit information between customs offices of export and customs offices of exit, and electronic handling of exit summary declarations (Export Control System phase 1, 2 and AES full deployment). The current UCC Automated Export System project is divided into 3 phases: Export Control System (ECS) phase 1 - exit "fiscal" control - provides for the full control of the conclusion of export operations via the electronic exchange of export/exit information between customs offices of export and customs offices of exit ECS phase 2 - exit "security" control - provides for the electronic handling of exit summary declarations under the security amendment Regulation (EC) 648/2005 and will, inter alia, require additional information to be included in export declarations for safety and security purposes. AES - full deployment - will build on and contain the functionalities of ECS Phases 1 and 2 and, in particular, will

		introduce the central clearance approach. The AES aims at automation of the completion of the export procedures and exit formalities covering common, national and external domains. Current ECS Phase 2 already covers the handling of export movements and exit summary declarations, enables electronic lodgement of the declarations.
2.5	New Computerised Transit System (NCTS), NCTS – TIR	Fully computerised and operational customs system working in all Member States. It allows for the temporary suspension of duties, taxes and commercial policy measures that are applicable at import, thereby allowing customs clearance formalities to take place at the destination rather than at the point of entry into the customs territory. The New Computerised Transit System (NCTS), being the first and currently only fully computerised and operational customs system working in all Member States (as well as in EFTA countries - Iceland, Norway, Liechtenstein, and Switzerland) is to be updated in its features as required by Regulation (EC) 648/2005 and its implementing provisions. One of the main adjustments will be the incorporation of the data elements as required by the regulation. The EU member states currently implement the UCC Transit System including NCTS project. The scope of the project consist of two components: Adaptation of the NCTS to the new requirements of the UCC; Implementation of the processes related to the use of an electronic transport document as a transit declaration. The objective of this system (currently in the pilot phase) is to provide full control of the European leg of TIR movements and to facilitate the termination/discharge of TIR operations within the Community by replacing the return of Voucher No 2 with the sending of NCTS messages.
2.6	Integrated tariff environment and interconnection between the tariff related IT systems	The European Community has created the Binding Tariff Information (BTI) system as a tool to assist economic operators to obtain the correct tariff classification for goods they intend to import or export. Interconnection between the already existing tariff related IT systems aims to achieve re-use of data and functionality of one system to another (e.g. descriptions of Combined Nomenclature (CN) codes owned by the CN system are to be re-used by Integrated Tariff of the European Communities (TARIC)) and to harmonise the interfaces of the different

		inter-related tariff systems with the Member States without redundancy of data (Council Regulation (EEC) No 2658/87). The UCC Binding Tariff Information project will implement the changes introduced by the UCC, namely the validity period of a BTI will be reduced from 6 to 3 years; the processes will be aligned to the standard decision processes; and the BTI will be binding on the holder as well. As a result, BTI holders will be obliged to include the BTI reference in their customs declaration and the customs authorities will have to control this obligation. It will be carried out via central monitoring of the BTI usage (through the Surveillance system covering all customs declarations). Whereas the BTI is currently only binding upon the customs, the UCC makes the BTI also binding upon the holder as against customs. Thus, the holder has to inform the customs authorities that he holds a BTI decision for the declared goods. For the customs authorities this raises the issue of proper control of traders with regard to this new obligation. It also provides the possibility for traders to submit their BTI applications and receive the BTI decisions electronically via an EU harmonised trader interface.
2.7	Single Point for Entry or Exit of Data (SPEED) portal	SPEED has been designed to ensure the confidentiality, privacy and integrity of the CCN/CSI network, shielding it from the 'outside world'. It includes high-security hardware and software components to defend against, monitor and log all possible threats facing the CCN network. The CCN/CSI operational infrastructure consists of a closed and secured network infrastructure that is provided by the European Commission to facilitate the exchange of information between the National Administrations of the Customs and Taxation area. An examples of use of SPEED (and SPEED 2) is data exchange for New Computerised Transit System (NCTS) between the EU and countries which are not a candidate for EU membership (e.g. Ukraine, Russian Federation, Albania); From 2014 (3 years), DG Taxud will replace existing legacy communications infrastructure with a cost-effective, flexible platform based on industry standards and a services oriented architecture. The new network, to be called Common Communication Network 2 (CCN2), will provide mission-critical interoperability and communications links between the 28 EU member states' customs and tax operations and the multiple systems in operation across the region.

		DG Taxud's Common Communication Network (CCN) is the gateway for all tax and customs applications in the EU, supporting areas of taxation between member states, including VAT, excise duties, transit and import. In 2011 the CCN handled more than 1.2 billion data exchanges for EU countries. The CCN allows exchange of messages for NCTS, ECS, ICS, EOS, EBTI, SURVEILLANCE and SMS systems.
2.8	Uniform user management & digital signatures	The EU best practice is the Direct trader access to European Information System (EIS) through use of the Uniform user management & digital signature (UUM&DS). The UUM&DS Project aims to implement a system that allows traders to access electronic EU-wide services, including central services, in line with the security policies, legal provisions and operational responsibilities. Therefore the new system shall offer unified access to traders to: A number of supporting IT systems such as UCC (Union Customs Code) Customs Decisions, EOS-AEO (Economic Operators System – Authorised Economic Operators sub-system), COPIS (Anti-Counterfeiting and Anti-Piracy System), UCC BTI (Binding Tariff Information) usage and decision; Central services for electronic submission of declarations that will be forwarded to the competent national authority. The legal basis for the Uniform user management & digital signature is defined in the Article 6(1) and 16 of Regulation (EU) No 952/2013 laying down the Union Customs Code and the UCC Work Program (Section II: 4.Direct trader access to the European Information Systems (Uniform user management & digital signature)). The UUM&DS Project has been initiated aiming at enabling the provision of a unique interface to a number of central services implemented by the EC for traders, therefore, effectively addressing the lack of harmonized interfaces for Trade and the redundant implementations of services of common functionality at Member States level. UUM&DS enabling the provision of a unique interface on an EU-basis to Customs European Information System for traders will contribute to reducing trader interfaces from 28 to 1. In addition, provision of direct access capabilities (and central development and operation of EIS) would mean that MS Customs administrations will not implement functionality

	(or systems) offering those same services 28 times over. The MASP project UUM&DS shall enable direct unified access for trader users (EO users) to a number of central Customs EIS, by federating Member States Identity and Access Management (IAM) systems, as traders users are currently connected to national IT systems. The UUM&DS Project has been initiated aiming at enabling the provision of a unique interface to a number of central services implemented by the EC for traders, therefore, effectively addressing the lack of harmonized interfaces for Trade and the redundant implementations of services of common functionality at the Member States-level.

3. Services

N	Benchmark	EU baseline
3.1	Registered Exporters System	In the EU, the REX system (which is currently under development) aims to make up-to-date and complete information available on Registered Exporters established in non-EU countries (Generalised System of Preferences beneficiary countries) exporting goods to the EU under preferential trade arrangements. Current legal provision is the Consolidated Regulation (EU) 2454/1993 and some provision of Regulation (EU) 1063/2010 and 530/2013. Exporters should be registered with the competent authorities of the beneficiary countries in order to be entitled to make out statements on origin if the total value of originating products in a consignment exceeds EUR 6.000. In addition, the registration of exporters will facilitate targeted ex-post controls. In order to register exporters, each beneficiary country should use the REX established by the European Commission. Through the system, put in place for the benefit of administrations and Economic Operators in the EU and in beneficiary countries, the Economic Operators should be able to check – before declaring goods for release for free circulation – that their supplier is a registered exporter in the concerned beneficiary country. Similarly, EU Economic Operators should be registered with the competent authorities in the Member States for the purpose of bilateral cumulation of origin and splitting of consignments to be sent to beneficiary countries. The main purpose of the system is to replace the current

		paper-based certification process by an IT-supported self-certification process. A central database will contain the registered exporters. Therefore, the REX will also offer the opportunity to Member States to enhance their national systems for Custom Declarations with an automated verification of the REX number from the declarations against that central database. It is expected to cover exporters from more than 80 GSP countries.
3.2	Economic Operators Registration and Identification system	Economic Operators Registration and Identification (EORI) number is an identification number, unique in the European Community, assigned by a Member State customs authority or designated authority or authorities to economic operators and to other persons in accordance with the rules laid down in Chapter 6 of the Regulation (EC) No 312/2009. The EORI system is established in order to implement the security measures introduced by Regulation (EEC) No 2913/92, as amended by Regulation (EC) No 648/2005 of the European Parliament and of the Council. An EORI number means a number, unique throughout the European Community, assigned by a customs authority or designated authority or authorities in a Member State to economic operators and other persons. The provisions on the EORI number neither limit nor undermine the rights and obligations derived from rules governing the requirement to register for, and obtain, any identification number which may be required in individual Member States in fields other than customs, such as taxation or statistics. By registering, for customs purposes, in one Member State operators are able to obtain an EORI number that is valid throughout the Community. Holders must use the EORI number in all communications with any EC customs authorities where a customs identifier is required. Economic operators not established in the customs territory of the Community should be registered if they perform one of the following main activities: • lodge in the Community a summary (e.g. a summary declaration for temporary storage) • lodge in the Community an exit or entry summary declaration; • operate a temporary storage facility; • apply for an Authorised Economic Operator certificate. Customs authorities in the EU have easy and reliable access to operators' registration and identification data. In order to

		ensure this, a central electronic system has been developed for storing data on the registration of economic operators and other persons and for exchanging data on Economic Operators Registration and Identification numbers between customs authorities. This central system holds that are currently stored in each national system in the Member States (Regulation (EC) No 312/2009). The European Commission is responsible for storage of the EORI data at central level and collection of the national EORI data provided by the Member States to the central repository. Member States should upload on a regular basis to the central system data concerning economic operators and other persons whenever new EORI numbers are assigned or changes in that data occur. Once the EORI number has been granted, this unique number must be used in all customs transactions and activities throughout the Community whenever an identifier is required.
3.3	Authorised Economic Operators mutual recognition	The legal basis for the status of the Authorised Economic Operator is laid down in the Regulation (EC) No 648/2005. Authorised economic operators benefit from facilitations with regard to customs controls relating to security and safety and/or from simplifications based on the criteria for granting the status that are recognised in all Member States. Economic Operators' System – Authorised Economic Operator subsystem (EOS-AEO) is an existing and operational information system that interconnects the authorities of the EU Member States and DG TAXUD. The EAP countries can consider negotiating AEO Mutual Recognition Agreement with the EU and the following IT implementation of the Agreement. The AEO Mutual Recognition (AEO MR) project aims to ensure the exchange of AEO data among Member States, DG TAXUD and third countries in a uniform way to increase security and facilitation. The economic operator benefits from reduced physical and document based controls and priority treatment. The data exchange framework jointly developed by the USA and DG TAXUD has been proposed as a global standard for Mutual Recognition within the WCO. The AEO Mutual Recognition adaptations prior to UCC have been successfully completed in 2013. It assured the development and deployment of a standard interface for AEO

		data exchange with partner countries, the update of the EOS system-to-system interface to allow the AEO data received from partner countries to be disseminated to the EU Member States and the validation of the partner counties' AEO status in the EU transaction systems, based on the adopted user requirements. Decisions of the Joint Customs Co-operation Committee regarding Mutual Recognition of the Authorised Economic Operator Programme in the EU and enterprises registration programs have been concluded with several countries such as the Peoples' Republic of China, Japan, Switzerland and Norway.
3.4	Summary electronic declaration for pre-arrival and pre-departure information	The Regulation (EC) 648/2005 defines the legal requirements for a summary declaration for goods brought into the customs territory of the Community. In order to allow for appropriate risk-based controls, the requirements are established of pre-arrival or pre-departure information for all goods brought into or out of the customs territory of the Community, except for goods passing through by air or ship without a stop within this territory. Such information should be available before the goods are brought into or out of the customs territory of the Community. Different timeframes and rules may be set according to the type of goods, of transport or of economic operator or where international agreements provide for special security arrangements. In order to avoid security loopholes, this requirement is also introduced with regard to goods brought into or out of a free zone. The summary declaration shall be lodged before the goods are brought into the customs territory of the Community. The summary declaration shall be lodged by the person who brings the goods, or who assumes responsibility for the carriage of the goods into the customs territory of the Community. Common data set and format for the summary declaration are defined, containing the particulars necessary for risk analysis and the proper application of customs controls, primarily for security and safety purposes. Customs authorities may accept, instead of the lodging of the summary declaration, the lodging of a notification and access to the summary declaration data in the economic operator's computer system. Customs authorities may allow the customs declaration to be lodged at a customs office of import different from the

		customs office of entry, provided that this office immediately communicates or makes available electronically the necessary particulars to the customs office of entry. Customs authorities may accept paper-based summary declarations in exceptional circumstances, provided that they apply the same level of risk management as that applied to summary declarations made using a data processing technique. Where the customs office of export is different from the customs office of exit, the customs office of export shall immediately communicate or make available electronically the necessary particulars to the customs office of exit. The customs declaration shall contain at least the particulars necessary for the summary declaration referred to in Article 182d(1) of the Regulation (EC) 648/2005. Customs authorities may allow the summary declaration to be lodged at another customs office, provided that this office immediately communicates or makes available electronically the necessary particulars to the customs office of exit. The summary declaration shall be made using a data processing technique. Commercial, port or transport information may be used, provided that it contains the necessary particulars
3.5	Information systems interconnection for lodging Summary Declarations and their communication to other countries systems	Risk-related information on import and export goods is shared between the competent authorities of the Member States and the Commission. A common, secure infrastructure is in process to be defined, enabling the competent authorities to access, transfer and exchange this information in a timely and effective manner. In order to harmonize processes and the data exchange with trade, to evolve towards a best-practice approach as well as to ensure the seamless execution with previous and subsequent processes, the processes and data requirements for the external domain, which are to be defined and agreed upon on EU-level, are to be implemented nationally. At the EU level, the future development of common infrastructures is handled by the ***UCC Notification of Arrival, Presentation Notification and Temporary Storage project***. The scope of this project is harmonisation of data exchange between trade and customs for the Entry Summary Declaration, Notification of Arrival, clarification of the use, function (legal/technical) and the content of the Presentation Notification, of the process and the content of the Temporary

		Storage Declaration and Customs Declaration across the Member States on the inbound trade flow. The project starts in Q2 2015 and will extend the existing infrastructures. The implementation processes, as well as the deadlines, are to be defined by the Member States.
3.6	EU Single Window	The objective of the EU Customs Single Window program is to enable Economic Operators to electronically lodge, and only once, all the information required by customs and non-customs legislation for EU cross-border movements of goods. A Customs SW is focused on Customs formalities and involves stakeholders dealing with cross-border movement of goods. The envisaged national single windows will be connected to one another and will be supported by the Single Electronic Access Point (SEAP). Given the complexity of the SW concept as such, the EU Customs Single Window program foresees several implementation steps, first of which consists in automated validation of supporting documents to the customs declaration. The European Union Single Window – Common Veterinary Entry Document (EU SWCVED) is the first project of the EU Single Window Programme. The EU Single Window Programme aims at facilitating clearance of goods at customs by providing an IT back office tool for a single IT entry point through which economic operators provide documents required for customs clearance. As such, the need to present the supporting paper documents to the Customs Declaration could be reduced and this would speed up the customs clearance process with higher quality. The concept requires the supporting Customs Declaration documents to be made available electronically, which already is the case for the Common Veterinary Entry Document (CVED). The aim of the EU SW-CVED Phase 1 is to provide for automated validity checks of the CVED submitted with customs declarations. This project consists in interconnecting the MS Customs Systems and the DG SANCO TRACES system which holds the CVED.
3.7	System for management of electronic trade certificates	National administrations or agencies deliver certificates required for import or export authorisation in electronic format. A common and secure system for the authorisation procedure, including the information and consultation process, the management of certificates for authorised economic operators and the registration of those certificates

		in a data base accessible by customs authorities.
3.8	The electronic customs systems of the Community and the Member States	The UCC Customs Decisions project aims to harmonise the processes related to the application for a customs decision, the decision taking and the decision management by standardisation and electronic managing of application/authorisations data across the EU. It introduces paperless environment for customs and trade. This project sets the basic framework and major deadlines for the electronic Customs projects. The UCC Customs Decisions system will allow the electronic processing and central storage of the applications and authorisations and publication of the list of holders on the Internet. The central storage of applications and authorisations will allow the consultation and validation of Customs Decisions by the movement systems and customs authorities in the Member States. The IT system will facilitate the necessary consultations between Member States' customs authorities during the decision taking period and the management of the authorisations process. The Customs Decisions system will be implemented with the external trader access, the Direct trader access to European Information System. The objective of the Customs Decisions external trader access system is to provide a uniform access to customs decisions-related services to the economic operators, by offering them a single user interface across all Member States to apply for and manage their customs decisions vis-à-vis customs.
3.9	Anti-Counterfeiting and Anti-Piracy System	Anti-Counterfeiting and Anti-Piracy System (COPIS) is intended to enhance intellectual property rights (IPR) protection by improving the cooperation and sharing of information between right-holders and Member States' Customs Administrations and between all the Customs offices of the Member States. To protect themselves against IPR infringements, right holders can ask the intervention of Customs in order to take measures against goods infringing certain IPR. A single information system is accessible by all Member States, thereby simplifying and reducing the workload of Customs administrations and of the EU Commission and improving the cooperation in the area of IPR enforcement. The current legal provision is Regulation (EU) No 608/2013 of the European Parliament and of the Council of 12 June 2013 concerning customs enforcement of intellectual property

		rights. The COPIS system is an EU-wide information exchange system for all customs operations and is addressing inter alia counterfeiting and piracy by facilitating the information exchange. The development of the new release took place throughout 2013. The COPIS 1.2.0 Central System Operation was deployed in operation on 01.01.2014. Most of the EU member states have proceeded with a Light Client Development to satisfy legal requirements at first, and then, to develop a system-to-system connection between the national application and the common system COPIS (eCustoms program).

eCommerce – detailed description of the EU baseline

1. Internet security & privacy

N	Benchmark	EU baseline
1.1	Allowance to process user traffic data by the provider of a electronic communication service	Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of an electronic communications service may process the data to the extent and for the duration necessary for such services or marketing; if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time. The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes of subscriber billing and, prior to obtaining consent, for the purposes of marketing electronic communications services or the provision of value added services (Directive 2002/58/EC on privacy and electronic communications Article 6).
1.2	Specific liability regime for	The ECD introduced a specific liability regime for three categories of services: mere conduit operators, caching

	intermediary service providers	providers and hosting services (Directive 2000/31/EC on electronic commerce Articles 12-15). **Mere conduit.** Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider does not initiate the transmission, does not select the receiver of the transmission; and, does not select or modify the information contained in the transmission. **Caching.** Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on some conditions such as the provider does not modify the information and others. **Hosting.** Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages is not aware of facts or circumstances from which the illegal activity or information is apparent; or the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.
1.3	No general obligation for providers to monitor transmitted or stored information	Member States shall not impose a general obligation on providers, when providing the services of transmission, caching and hosting, to monitor the information which they transmit or store, or a general obligation actively to seek facts or circumstances indicating illegal activity. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements (Directive 2000/31/EC on electronic commerce

		Article 15).
1.4	Authorised recording of communications and the related traffic data in the course of lawful business practice / confidentiality of the communication	According to the Article 5 of the Directive 2002/58/EC on privacy and electronic communications, the national legislation of the Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so. However, this requirement shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication. The use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information about the purposes of the processing. Subscriber or user should be offered the right to refuse such processing by the data controller.

Consumer rights

N	Benchmark	EU baseline
2.1	Online trustmarks for retail websites	Digital Agenda for Europe – Europe 2020 strategy / Action 17: Stakeholder platform for EU online trustmarks. The Commission set up a stakeholder platform to discuss the issues surrounding online trustmarks in 2012 and to pilot a study on trustmarks. The final product of this platform was the study "EU online Trustmarks – Building Digital Confidence in Europe", published by the Commission in 2013. The Commission is exploring the usefulness and benefits of the EU-wide trustmark schemes to reassure consumers on the reliability of accredited traders. The aim is to encourage the establishment of pan-EU price-comparison websites. Such certified sites will help consumers to make informed decisions when using online retail services. The Commission

		will further elaborate different policy options for EU-wide trustmark schemes and the effectiveness of cooperation platforms in the governance of such trustmark systems. Article 23 eIDAS by 1 July 2015 implementing act to provide for specifications with regard to the form, and in particular the presentation, composition, size and design of the EU trust mark for qualified trust services. (Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market –eIDAS)
2.2	Minimum general information to be provided by information society service provider	Information society service provider shall render easily, directly and permanently accessible to the recipients of the service and competent authorities, at least the following information: the name of the service provider, geographical address, e-mail address, registration number if registered in a trade or similar public register. This information is important and may even be vital for customers claiming their rights. The country of origin of the web trader can have major consequences, for example, for their right of withdrawal. Moreover, Article 5 (Directive 2000/31/EC on electronic commerce) requires the online service provider to establish an effective direct communication channel with its customers. It imposes the obligation on the service provider to render "easily, directly and permanently accessible" to both recipients of services and the competent authorities "the details of the service provider, including its electronic e-mail address, which allow it to be contacted rapidly and communicated with in a direct and effective manner" (Directive 2000/31/EC on electronic commerce Article 5).
2.3	Transparency requirement of commercial communications information to be provided	This requirement emphasises the need for transparency when advertisements are displayed on the Internet. It obliges the Member States to ensure that online commercial communications (including promotional offers, discounts, premiums, promotional competitions or games) meet certain transparency requirements. Both the commercial communication and the natural or legal person responsible for it must be clearly identifiable, and any conditions attached to the offers, discounts etc. must be easily accessible. For example, advertising originating from the operator of an online marketplace and displayed by a search operator must always disclose both the identity of the online marketplace operator and the fact that the trademarked goods advertised are being sold through that online marketplace (Directive 2000/31/EC

		on electronic commerce Article 6).
2.4	Minimum pre-contractual information required for distance contracts and off-premises contracts	Pre-contractual information. Before the consumer is bound by a distance or off- premises contract, or any corresponding offer, the trader shall provide the consumer with the information required in a clear and comprehensible manner: **Information requirements** for all consumer contracts include information in relation to the product/service, address and identity of the seller, price, additional charges, payment mechanism, delivery details, complaints policy, cooling-off period (where applicable) and after-sales services, and others. **Transparency of terms**. Contract terms must be in plain, intelligible and legible language. Moreover, pricing must be transparent and express consent to ancillary charges must be sought (that is, any online tick boxes must be opt-in, not opt-out). **Obligation to pay**. If a distance contract to be concluded by electronic means places the consumer under an obligation to pay, the trader shall make the consumer aware in a clear and prominent manner, and directly before the consumer places his order. The formal requirements for distance contract also include: **Delivery restrictions** applied and which **means of payment** are accepted **Requirements for concluding a distance contract by telephone** **Requirements for confirmation of the contract concluded** on a durable medium within a reasonable time after the conclusion of the distance contract (Directive 2011/83/EC on Consumer Rights)
2.5	Consumer Protection Cooperation Network between government agencies of EU Member States	The Consumer Protection Cooperation (CPC) Network brings together the public authorities in all the EU Member States (and other EEA countries) who are responsible for the enforcement of EU consumer protection laws. Thanks to the CPC Network established in 2007, a national authority in the EU country where consumer interests are harmed can call on their counterpart in the Member State where the trader is located and ask for action to stop the infringement. Enforcement authorities can also alert each other to malpractices they have spotted which may spread to other countries.

		In 2013 the Commission co-funded projects that strengthen the online enforcement capacities of the CPC Network. One central element of the CPC Network is the CPC-System, the common IT-tool used by the authorities for the exchange of information. It is an electronic database maintained by the European Commission and designed to provide a secure system for the exchange of information between competent authorities in the Member States for the performance of their mutual assistance obligation under the Consumer Protection Cooperation Regulation (Directive 2011/83/EC on Consumer Rights).
2.6	Non obstruction to out-of-court dispute settlement	Member States shall ensure that, in the event of disagreement between an information society service provider and the recipient of the service, their legislation does not hamper the use of out-of-court schemes, available under national law, for dispute settlement, including appropriate electronic means. Member States shall encourage bodies responsible for the out-of-court settlement of, in particular, consumer disputes to operate in a way which provides adequate procedural guarantees for the parties concerned (Directive 2000/31/EC on electronic commerce Article 17).
2.7	Online Dispute Resolution system for consumers for eCommerce transactions	The action aims at exploring initiatives on consumer Alternative Dispute Resolution in the EU with a view to adopting directive on Alternative Dispute Resolution (ADR) and a regulation on Online Dispute Resolution (ODR) and proposing an EU-wide Online Dispute Resolution system for cross-border eCommerce transactions by 2012 (Directive 2013/11/EU on alternative dispute resolution for consumer disputes). The ADR system is supplemented by an ODR mechanism involving the setting up of a European online dispute resolution platform (an interactive website free of charge in all languages of the Union Accessible through "Your Europe" portal: http://europa.eu/youreurope/). The ODR Regulation entered into force on 9 July 2013 and shall apply as of 9 January 2016. Through this website, parties can initiate ADR in relation to disputes concerning online transactions. National ADR entities will receive the complaint electronically and seek to resolve the dispute through ADR, using the ODR platform exclusively if they wish. Today, more than 750 ADR schemes exist in EU Member States. Existing national ADR schemes should be able to continue to operate within the new framework.

2.8	Requirements for sending of unsolicited commercial communication	This requirement preserves the possibility for Member States to either prohibit or allow the sending of unsolicited commercial communications ("spams") by e-mail. Those Member States permitting unsolicited commercial communication must ensure that such communication is clearly and unambiguously identifiable, and that service providers respect the opt-out registers to which natural persons not wishing to receive such commercial communications can sign up (Directive 2000/31/EC on electronic commerce Article 7).
2.9	Limitation of rate for communication by telephone	This provision ensures that where the trader operates a telephone line for the purpose of contacting him by telephone in relation to the contract concluded, the consumer, when contacting the trader is not bound to pay more than the basic rate (Directive 2011/83/EC on Consumer Rights).

Competition

N	Benchmark	EU baseline
3.1	Free movement of information society services	The Internal Market clause aims to ensure the free movement of information society services between the Member States. Each Member State must ensure that information society services provided by a service provider established on its territory comply with the national provisions applicable in the Member State in question which fall within the coordinated field. It may not, for reasons falling within the coordinated field, restrict the freedom to provide information society services from another Member State (Directive 2000/31/EC on electronic commerce Article 3).
3.2	Principle excluding prior authorisation to pursuit the activity of an information society service provider	The EC Directive on electronic commerce defines the principle excluding prior authorisation to pursuit the activity of an information society service provider. The Community legal framework ensures that the taking up and pursuit of the activity of an information society service provider may not be made subject to prior authorisation or any other requirement having equivalent effect. This principle shall be without prejudice to authorisation schemes of the Member States which are not specifically and exclusively targeted at information society services, or which are covered by legislation, such as a framework for general authorisations and individual licences in the field of telecommunications services. (Directive 2000/31/EC on electronic commerce

		Article 4)
3.3	Mini One-Stop-Shop for exchanges of data on VAT	The introduction of the mini One Stop Shop (OSS) for exchange of data on VAT in 2015 is another priority action indicated by the Commission in the Communication on the future of VAT. Furthermore, on 13 September 2012 a Commission Implementing Regulation which determines the necessary technical details for exchanges of data under the mini OSS was adopted under the "Comitology" procedure (Regulation (EU) No 815/2012 - non established taxable persons supplying telecommunications, broadcasting or electronic services to non taxable persons). Finally, as regards the broadening of the mini OSS concept to, amongst others, distance sales of goods, this can only be envisaged once the Commission has assessed whether the mini OSS (to be implemented by 2015) works properly.

E-payments

N	Benchmark	EU baseline
4.1	Legal framework in the area of eCommerce payments and rules on the fees for the use of means of payment	Next to ever growing payments with credit or debit cards, the rise of eCommerce and the increasing popularity of smart phones has enabled new ways of making payments. The benefits of better market integration in this field at European level are substantial. The European Commission published the Green Paper on an integrated European market for card, internet and mobile payments (January 2012). The Commission announced legislative actions as a follow-up to the Green Paper i.e. revision of the Payment Services Directive (Directive 2007/64/EC) and legislative initiative on multilateral interchange fees for card-based payment transactions. The aim of the present proposal is to help to develop an EU-wide market for payments, which will enable consumers, retailers and other undertakings to enjoy the full benefits of the EU internal market including eCommerce, in line with Europe 2020 and the Digital Agenda. Rules on the fees for the use of certain means of payment (e.g. credit or debit cards, electronic valets) prohibit traders from charging consumers, in respect of the use of a given means of payment, fees that exceed the cost borne by the trader for the use of such mean (Directive 2011/83/EC on

		Consumer Rights).
4.2	Equal treatment between paper and electronic invoices	Because of the huge advantages it offers in terms of efficiency for companies, the European Commission supports several initiatives to promote e-Invoicing in Europe for businesses and public authorities. The Commission adopted the Communication, 'Reaping the benefits of e-Invoicing for Europe' in 2010. It identifies a set of actions to support the uptake of e-invoicing by ensuring legal certainty and promoting the development of interoperable e-invoicing solutions based on a common standard, paying particular attention to the needs of small and medium-sized enterprises. Directive 2010/45/EU on the common system of value added tax as regards the rules on invoicing sets out new VAT rules regarding e-Invoicing and removes obstacles to the uptake of e-invoicing by creating equal treatment between paper and e-invoices, while also ensuring that no additional requirements are imposed on paper invoices. There is market fragmentation in technologies related to e-invoicing because of the diversity of data and usage requirements, and different approaches to their implementation. Because no existing e-Invoicing format has achieved dominance, market players need to support multiple formats, which requires substantial mapping and conversion exercises. The key challenge is to define a single and clear semantic data model. A common data model will facilitate semantic interoperability and ensure technology neutrality. The European Committee for Standardization (CEN), which is funded by the Commission, runs a number of activities on e-invoicing implementation issues.

E-logistics

N	Benchmark	EU baseline
5.1	Equal validity of electronic contracting and contract concluded offline	The EC Directive on electronic commerce (2000/31/EC) defines the fundamental principles of equal validity of electronic contracting and contract concluded offline. **Treatment of contracts.** Contracts concluded by electronic means should have the same validity as contracts concluded offline by "traditional" means (equivalence principle). This applies to all stages and acts of the contractual process, such as the contractual offer, the negotiation and the conclusion of

		the contract by electronic means. Legal provisions obliging hand-written contracts, for example, are no longer allowed. But the principle only covers legal requirements and not practical obstacles such as cases where the conclusion of a contract requires the physical presence of parties, e.g. must be signed before a notary. Article 9 of the ECD has been complemented by the Electronic Signatures Directive which regulates the legal recognition of e-signatures. **Information to be provided**. Online traders must provide the consumer with specific information prior to the order being placed and, in particular: the steps to follow to conclude a contract, the filing of the contract by the service provider, the technical means for identifying and correcting input errors prior to the placing of the order, the languages offered for the conclusion of the contract. In addition, online service providers must make available any relevant codes of conduct, contract terms and general conditions. Consumers should not only be able to store the contract terms and general conditions, but they must also be able to reproduce (print) them. **Placing of the order**. Article 11 of the ECD harmonises the placing of the order in B2C contracts. The online contract has to be concluded through an "order" placed by the consumer, followed by an electronic "acknowledgment" of the online trader without undue delay. The "order" and the "acknowledgement" are deemed to be received when the involved contracting parties are able to access them. In addition, the online trader has to provide the consumer with the technical means allowing him/her to identify and correct input errors prior to the placing of the order. (Directive 2000/31/EC on electronic commerce Articles 9-11).
5.2	Passing of risk - rules on the conditions for the risk of loss of or damage to the goods	These rules define the conditions for the risk of loss of or damage to the goods and responsibilities of the trader, the consumer, a third party indicated by the consumer, or the carrier. Delivery of goods within a minimum of 30 days from execution of sale contract; seller bears risk of loss/damage until goods are received by consumer; automatic right of refund within 7 days of non-delivery. Remedies. Standardisation of the remedies available to consumers for damaged or faulty goods. Consumers will be entitled to replacement or repair in the first instance and a refund or discount only where specific circumstances apply. (Directive 2011/83/EC on Consumer Rights)

5.3	Rights on delivery of goods	The rules on delivery define the requirements for time of delivery. Unless the parties have agreed otherwise on the time of delivery, the trader shall deliver the goods by transferring the physical possession or control of the goods to the consumer without undue delay, but not later than 30 days from the conclusion of the contract. It also clearly defines the conditions when the trader fails to fulfil his obligations to deliver the goods at the time agreed, additional period of time and the right of the consumer to terminate the contract and get reimbursement of all sums paid under the contract (Directive 2011/83/EC on Consumer Rights).

Digital Skills

National Coalitions

EU member state	Enablers/ key organisations	Description
Latvia	Memorandum of cooperation on "Digital Skills partnership" has been signed by representatives of governmental sector, non-governmental organizations and industry representatives – Latvian Information and Communications Technology Association (LIKTA, representing ICT industry with more than 220 members employing more than 25000 ICT specialists), Ministry of Environmental Protection and Regional Development, Ministry of Economics, Ministry of Education and Science, Ministry of Welfare, Latvian Chamber of Commerce and Industry (representing entrepreneurs from various sectors with more than 1000 members and employing more than 70 thousand employees), Latvian Open Technology Association and Latvian Internet	**A National Coalition for Digital Skills and jobs in Latvia** has been established in March 2013. The cooperation will comply with the priority axes defined in such European Union and Latvian policy development documents as Latvia 2030, the National Development Plan for Latvia 2014-2020, Digital Agenda for Europe, the Grand Coalition for Digital jobs initiative and LIKTA Charter By signing the memorandum, government, non-governmental organizations and entrepreneurs agreed to cooperate in four main areas: •**ICT training for the labour market needs:** *ICT training in accordance with labour market demands involves a closer cooperation of higher education and vocational training institutions with industry associations, in order to train qualified ICT specialists as well as support for further training to improve competitiveness of the existing labour force. Likewise, cooperation includes commitment to lifelong learning and training activities as well as promotion of a unified European qualification and certification scheme;* •**Youth involvement in ICT:** *An important issue across Europe is how to attract young professionals to the ICT industry. EU forecasts shows that the lack of ICT specialists in Europe in 2015 could reach up to 700 000 specialists. Therefore, one of the goals of signed memorandum is to attract young adults to ICT industry. It implies promotion of math and science in schools, alteration of IT lessons syllabus, support for vocational education programs for youngsters by providing practical approach to learning cutting-edge technologies, as well as advertising campaigns and other industry oriented events;* •**Modern and interactive learning process:** *In order to attract students to ICT industry, it is important to raise the interest to technology already in schools, therefore, modern and interactive learning process and digital content is one of the focal points of the memorandum: development, application and free access of diverse digital content and learning materials, including in Latvian, as well as digital supplements for existing printed learning materials;* •**General awareness raising about importance of digital literacy and ICT skills:** *Thinking about the development of*

	Association.	*information society, it is critical to educate people about the necessity of digital literacy and e-inclusion. Informative annual campaign "Digital Skills week" has already become an important tradition and this year it was held for the fourth year in a row. With a commitment to continue Digital Skills week tradition, the goal of cooperation is to inform different societal groups – small, micro and medium enterprises, government and public sector workers, teachers and parents, children and youngsters – about the Digital Skills and ICT solutions, effective use of e-services as well as about customized training programs for seniors.* ***Achievements:*** 1,000s of training programmes for young, unemployed, employees, teachers, seniors.

EU member state	Enablers/ key organisations	Description
Lithuania	A National Coalition has been established by socially responsible businesses, developing ICT skills in Lithuania and promoting a safe use of the Internet as well as public and private electronic services in order to improve Lithuanian people's quality of life and to raise competitiveness in Europe and in the world. The Ministry of Transport and Communications of the Republic of Lithuania is in charge of the development of information society and coordinates the programme Digital Agenda for Lithuania and the implementation of the EU Digital Agenda Strategies in Lithuania. The Ministry of Education and Science of the Republic of Lithuania seeks to adapt education to the needs of the information society of Lithuania and to develop possibilities for a lifelong learning in cyberspace.	Institutions, companies and organizations agreed to form the National Digital Coalition for the Promotion of Digital Skills for Jobs in Lithuania mission to increase employment and to achieve a more effective use of digital potential and cooperate in implementing information society development programme 2014–2020 Digital Agenda for Lithuania. **OBJECTIVES** **1. To substantially reduce the shortage of IT professionals, to improve the conditions for the private and public sector employees as well as all inhabitants to learn and continuously improve the necessary ICT skills for job, the establishment of IT business and development of the digital market:** • **To (re)skill the ICT professionals according to market requirements and to encourage professionals from other fields to specialize in ICT.** • **To promote e-leadership, ICT start-ups and the use of new digital opportunities in multifarious Lithuanian economy fields.** • **To promote a more efficient use of available ICT infrastructure and existing services.** • **To promote the development and use of open educational resources, to encourage institutions, companies and organizations to develop and provide Internet courses.** **2. To attract more young people to choose ICT and other science studies and professions, to ensure the acquisition of digital skills also when learning other professions:** • **To continuously improve general education, higher education and vocational training programmes according to the labour market requirements.** • **To seek that the professionals that are being trained had necessary ICT skills required by the labour market.** • **To reinforce the framework of digital skills training by cooperation between the representatives of business, education and other organizations.** • **To include ICT training to the system of non-formal youth education.** **3. To raise public awareness of the importance of digital skills and competences:** • **To involve the society in the dissemination activities**

		of digital skills and competences. • **To constantly keep the Lithuanian society informed about the importance of digital skills and competences.** • **Reaching every resident of Lithuania, jointly organize public informational campaigns and regional activities.** **Resources:** All partners of the National Digital Coalition of Lithuania cooperate in order to execute projects related to the main objectives of the Coalition and to organise public events to promote the activities of the Coalition outside the country. **Achievements:** ICT training for young, fast-track preparation of IT specialists, political support

EU member state	Enablers/ key organisations	Description
Malta	eSkills Malta Foundation, now a National Coalition, is a multi-stakeholder partnership between the industry, the education authorities and Government committed to improve the variety, quality and quantity of ICT competences for economic growth.	The eSkills Malta Foundation was launched in February 2014 and has been recognized as a National Coalition for Digital Jobs. It covers the following terms of reference: • **Advise Government and stakeholders on policy matters regarding skills related to ICT** • **Instigate further reform in the ICT educational offerings and contribute to capacity-building in the ICT education community.** • **Contribute to the expansion of ICT educational programmes and related formative initiative** • **Lead an ICT professionalism development programme.** • **Champion campaigns and promote the Maltese eSkills potential locally and internationally.**

EU member state	Enablers/ key organisations	Description
Greece	This National Coalition has 9 Greek Coalition partners: *Ministry of Education, Lifelong Learning and Religious Affairs, Ministry of Labour and Social Security, Ministry of Competitiveness, Development and Shipping, Ministry of Administrative Reform and E-Governance, Ministry of Infrastructure, Transport and Networks, General Secretariat of Mass Media, General Secretariat of Gender Equality, General Secretariat of Youth, Federation of Hellenic ICT Enterprises*	The Greek Coalition for the Digital Economy was launched in May 2014 and is aimed at young people and potential entrepreneurs. In particular, the Greek Coalition will design targeted policies and actions in order to boost employment in the IT sector, especially for the young people; to promote ICT and web entrepreneurship; to encourage training programmes via a life-long learning approach; and to augment awareness about the importance of digital literacy and ICT skills. The 9 Greek Coalition partners commit to developing an Action Plan during 2014 and to include more partners in the near future (ICT businesses, universities, SMEs associations, public and private employment agencies, etc.). The coalition builds on the "Women & Girls Go Digital in Greece" initiative, which brought together 21 Greek and other European partners (government, universities, businesses etc.) to enhance women's digital skills and their role in the technology sector.

EU member state	Enablers/ key organisations	Description
Bulgaria	Digital National Alliance (DNA) - Bulgaria (National Coalition) Launched in June 2014, the Digital National Alliance (DNA) has been recognised as the National Coalition for Digital Jobs in Bulgaria. The main aim of the DNA is to	The Digital National Alliance stands for diverse initiatives that aim at: • Ensuring that more Bulgarian people have digital skills • Addressing the mismatch between business needs and education requirements • Supporting the Bulgarian young talents in the Global Digital Worldwide Stage • Facilitating young people to access digital technologies and use them to communicate and co-create with people across Europe • Helping young people to find new job opportunities. Resources:

	ultimately get more young people trained on digital skills. There are 37 members of the DNA, including national and municipal government, educational institutes and industry	**Each partner of the DNA pledged to deploy specific activities to support the National Coalition (e.g. trainings, awareness raising events, job fairs, incubator initiatives...)** **More detailed information on these initiatives are available on http://digitalalliance.bg/en/happening** Achievements: **Awareness raising, coding, ICT training, soft skills training.**

EU member state	Enablers/ key organisations	Description
Italy	The "Coalition for Italian-skills" (which is a National Coalition participates in the Grand Coalition for Digital Jobs EU Commission) is an initiative sponsored by the Agency for Digital Italy (AGID) with the aim of improving digital skills. **The organization of the Coalition** AGID is responsible for organizing the activities of the Coalition and promotes and supports the projects carried out by the various components. AGID also establish a Technical and Scientific Committee, with the task of verifying that the various initiatives have the requirements of coherence, relevance and effectiveness required by the Coalition, and to assist in the AGID monitoring the evolution of the projects and provide guidance to improve its effectiveness. Nominations for the members of the Technical and Scientific Committee, who will lend their activities free of charge, can be received by January 31 to; competenzedigitali@agid.gov.it	Examples of expected results; ★ citizens acquire greater " awareness Digital " and greater ability to use digital services and to participate in their design / engineering ★ workers and those looking for work will improve their ability to use digital skills in the work context ★ entrepreneurs and managers will increase their ability to identify and exploit the opportunities offered by ICT , for example in design of products and services ★ companies will increase their ability to innovate and "think digital " ★ the public sector can engage citizens with more skills Digital to offer increasingly advanced services

EU member state	Enablers/ key organisations	Description
Poland	Under the patronage of President Bronisław Komorowski the initiative of the Ministry of Administration and	The agreement is an informal association of the good will of the institutions, organizations and companies that identify with its objectives and intend to work towards their implementation. It will seek synergies between existing initiatives; inspire new projects, focusing on good practices, to promote them in different environments - even distant subjects digitization. By increasing awareness of the benefits and risks but will promote

	Digitization. **Broad Alliance for Digital Skills Development**, (a National Coalition) which The aim is to inspire and support activities to the general public; - digital education, effective use of digital technology - acceptance of the changes caused by the constant development	access to knowledge and information, the dissemination of digital participation and acquiring the skills needed in all stages of life and areas of social activity and employment. **Projects include:** - Developing digital literacy and computing for older women to reduce disparities in the level of knowledge - "Water Forest and Nature" - an educational portal, bringing together environmental data results in an interesting tool for teachers - A report describing the most interesting social projects including crowdfunding and e-philanthropy, citizen journalism, e-learning, knowledge resources building projects or maps created by the community **Achievements:** - 136,600 people trained - 76 initiatives started

Examples of practices, enablers and initiatives in EU member states

Other Best Practices and Local Coalitions

EU member state	Enablers/ key organisations	Description
United Kingdom	**The Tech Partnership is a growing network of employers, collaborating to create the skills to accelerate the growth of the digital economy.** Its leadership includes the CEOs of major companies in the tech industry, heads of technology from companies across the economy, and small company representation. www.thetechpartnership.com	The Partnership's strategy Taking forward the work of e-skills UK, its strategy is to: • **Inspire new talent**: inspiring young people, particularly girls, about technology education and careers • **Create new jobs**: accelerating the flow of talented people from all backgrounds into technology careers, with a particular focus on apprentices and graduates • **Develop new skills**: making it easier for employers to develop strategic digital skills, for example cyber security, big data, mobile, e-commerce and the Internet of Things • **Raise standards**: setting industry standards, accrediting and promoting education and training that meets them. The Partnership's aims Its aims are that, by 2020: • There will be a 50:50 gender balance in young people entering tech careers, expanding the pool of talent coming into the sector • Digital careers will be in the top quartile of desirable jobs

		in the view of 16-21 year olds • The number of tech apprenticeships will be doubled, giving the nation a new pipeline of home grown talent to support the growth of the digital economy

EU member state	Enablers/ key organisations	Description
UK (Scotland)	Scottish Local Coalition was launched in March 2014 by setting up the Skills Investment plan which aims to review future skills and employment demands, in order to help the sector respond to and embrace the ICT skills challenges that exist in a dynamic and rapidly evolving sector.	The Scottish Government is committed to Scotland being a world class digital nation by 2020.Digital Skills are critical to achieving this vision which is why Scotland's First Minister personally launched Scotland's industry guided Skills Investment Plan (SIP) for the ICT & Digital Technologies sector and announced additional funding of £6.6 million for digital skills. Delivering the Skills Investment Plan for Scotland's ICT and digital technologies sector has been facilitated by Skills Development Scotland, working in partnership with key skills groups and industry stakeholders. Partnership is central to this approach; The Digital Scotland – Business Excellence Partnership was created to ensure a strategic and co-ordinated approach between our public agencies and with industry.

EU member state	Enablers/ key organisations	Description
UK (Northern Ireland)	The Sector Skills Agreement (SCC) in Northern Ireland – a Local Coalition partnership between e-skills UK and Momentum e-skills UK »	**e-skills UK**, as the Sector Skills Council (SCC) for the IT and Telecoms industry, was the voice of employers for all IT-related strategic skills issues in Northern Ireland and across the UK. In Northern Ireland, e-skills UK was responsible for strategic development of the SSA, all authoritative research on IT related skills issues including Labour Market Intelligence, the development and currency of all IT related skills frameworks and industry standards such as the National Occupational Standards. **Momentum** » Momentum is the trade association for ICT companies in Northern Ireland. It was established to represent those with a common interest in promoting and developing the industry both locally and internationally. » Momentum's membership comprises over 160 ICT companies in Northern Ireland. The vast majority are very small companies and they supply products and services to all industry sectors.

Telecom Rules

Examples of practices already implemented in EU member states

This annex contains extracts from the report – “Benchmarking Electronic Communications Markets in EaP countries” (Version December 2014) ENPI / 2012 / 307-572

The major source of information for this EaP Benchmarking report was a special series of questionnaires distributed among the state bodies responsible for the regulation of electronic communication markets in the countries of the Eastern Partnership and selected EU Members States including Czech Republic, Lithuania, Poland, Romania, Slovakia and Sweden.

Where no relevant information was included in the EaP benchmarking report, other tables have been prepared from separate analysis.

LEADERSHIP ENABLERS – EU EXAMPLES

Framework Directive: Separation of policy, regulatory and operational functions in the electronic communications sector.

EU member state	Responsible organisations	Functions *(extracts from the EaP benchmarking report December 2014)*
Czech Republic	• The Czech Telecommunication Office (CTU) • The Ministry of Industry and Trade (MIT) • The Office for Personal Data Protection (OPDP)	*The CTU is a central administration body in the area of electronic communications and postal services - the independent NRA. The MIT is responsible for the creation of state policy in the area of electronic communications. The OPDP ensures the protection of personal data in the area of electronic communications.* *Shared competences between the CTU and the MIT: the CTU ensures number management - arranging numbering plans, drawing up rules for creating addresses and names - except Internet addresses - and changing them, granting, amending and withdrawing authorisations to utilise numbers, and recording and inspecting the utilisation of numbers. The numbering plans are determined by an implementing legal regulation, which is issued by the Ministry of Industry and Trade. The Ministry decides upon the approval and the final version of the regulation. The CTU and the Ministry of Industry and Trade cooperate on this issue within an internal working group.* *Shared competences between the OPDP and the CTU: the CTU covers only part of the protection of traffic and localisation data and communications confidentiality. Protection of personal data is in the responsibility of the Office for Personal Data Protection.*
Lithuania	• The Communications Regulatory Authority (RRT) • The Ministry of Transport and Communications • The State Data Protection Inspectorate	*The RRT is the most important body in the area of electronic communications regulation – the independent NRA. The Ministry of Transport and Communications, along with the Government, is the policy-making body in the area of ICT. The State Data Protection Inspectorate performs the supervision of private life violability of electronic communication users (natural and legal persons) according to the Lithuanian Law on Electronic Communications. It carries out data management and performs inspections of privacy protection, and handles consumer complaints related to data protection in the field of electronic communications. The Inspection also supervises data protection and usage legitimacy.*
Poland	• The Office of Electronic Communication (UKE) • The Ministry of Administration and Digitisation • The National Centre for Accreditation (NCA) • The National Broadcasting Council	*The President of the UKE is the relevant national regulatory authority responsible for electronic communications – the independent NRA. The Ministry of Administration and Digitisation plays a leading role in the development of the National Table of Frequency Allocations or the National Numbering Plan. In addition, in certain areas the UKE cooperates with other regulators, e.g. with the NCA or the National Broadcasting Council.*

Romania	• National Authority for Management and Regulation in Communications (ANCOM)	*An independent NRA in the area of electronic communication has been established in 2002. The National Authority for Management and Regulation in Communications (ANCOM), is the body that protects the interests of the communications users in the country, by prompting competition in the communications market, ensuring the management of scarce resources and encouraging innovation and efficient investments in infrastructure.*
Slovakia	• Regulatory Authority for Electronic Communications and Postal Services (RÚ) • The Ministry of Transport, Construction and Regional Development of the Slovak Republic	*The RU is the Slovak independent NRA in the area of electronic communications. RU was established in 2014 after a merger with Postal services Regulatory Authority. The Ministry of Transport, Construction and Regional Development of the Slovak Republic elaborates a proposal of the national table of the frequency spectrum, elaborates a proposal of the national electronic communications policy and other strategic documents in the electronic communications sector, and submits them to the Government of the Slovak Republic.*
Sweden	• The Ministry of Enterprise, Energy and Communications • The Swedish Post and Telecom Authority (PTS)	*The Ministry of Enterprise, Energy and Communications is the national policy-maker in various spheres, including electronic communications. The PTS is the independent NRA, responsible for the monitoring of the electronic communications and postal sectors in Sweden. The PTS elaborates an annual report to the abovementioned sector ministry.* *As the electronic communications regulatory legislation of the EU Members states is aligned with the recommendations of the 2003 and 2009 EU regulatory frameworks, the NRAs in the area were established and are deemed independent.*

Framework Directive: Requirement for transparency and public consultation before introducing new policy or regulatory measures

EU member state	Description *(extracts from the EaP benchmarking report December 2014)*
Czech Republic	*In discharging its authority, the Czech NRA will consult on the drafts of measures of a general nature and the decisions on price, decisions having a significant effect on the relevant market and any other action to be taken by the CTU, where the Telecommunications Act provides that consultations must be held (this is not the case of dispute resolutions). Anyone whose rights, obligations or interests may be directly affected by the proposed measure may express his opinion concerning the proposed measure or may present written comments to the NRA within 1 month of the date of making the draft measure public. If there is any danger of delay, the NRA may reduce this period adequately, but it should never be shorter than 5 working days.*
Lithuania	*There is a formal public consultation procedure before the decision of the NRA becomes binding. To provide comments and proposals, a reasonable time period is set which may not be less than 28 calendar days, if legal acts do not set a different time frame. In exceptional circumstances and on a substantiated basis, a shorter timeframe for public consultation may be set. Dispute resolution at the meeting is public, except for the cases when RRT is seeking to protect state, RRT or commercial secrets or seeking to ensure the persons' right to his private life, decides to resolve the dispute in a closed meeting.*
Poland	*There is a consultation procedure in place before the decision of the Polish NRA becomes binding for the concerned parties. The parties should submit their comments to the NRA within 30 days.*
Romania	*ANCOM submits to public consultation all the draft decisions that may have a significant impact on the electronic communications market. The deadline for submitting comments and suggestions on the drafts under public consultation is of minimum 30 days from the date of publishing the document on the ANCOM Internet page. Where the decisions must be adopted under the emergency regime, this term may be shorter than 30 days, but not shorter than 10 days.*
Slovakia	*A consultation procedure about the draft decisions of the NRA exists. The concerned parties are given a period of 30 days to provide their comments. This period can be prolonged to 60 days in the case of a complicated measure or a reasoned delay. The NRA is then given 1 month to evaluate the comments.*
Sweden	*The legislation stipulates that the timeframe given for consultation should be reasonable, without specifying the exact duration.*

Universal Services and ePrivacy Directives: Clear mandate for the regulator to protect users' rights and freedoms

EU member state	Description *(extracts from the EaP benchmarking report December 2014)*
Czech Republic	*The maximum commitment period for contracts is regulated. If the undertaking that is providing publicly available electronic communication services or ensuring connection to the public communications network is entering into a fixed-term contract with a consumer, the initial time period of the contract regarding this service cannot exceed 24 months. The undertaking is also obliged to allow the consumer to enter into a contract for a period not exceeding 12 months. This limitation does not preclude the possibility of signing the contract for a longer period if the consumer asks for such a contract. The contractual penalties for early termination are not regulated at the moment, but the new draft law which is in the process of approval deals with this issue. The undertaking should, at least 1 month before the effective date of any change to the substantial contractual conditions or change to other provisions which represent a worsening of those conditions for the subscriber, notify verifiably the subscriber about that change and should also inform him of his right to terminate the contract without incurring any sanctions if he does not accept the new conditions. In 2014, an amendment to the Act No 127/2005 Coll. on Electronic Communications and on Amendment to Certain Related Acts (Electronic Communications Act) is in legislative procedure which comprehends inter alia some changes relating to obligation of an undertaking´s providing a publicly available electronic communications service or ensuring connection to the public communications network, to inform the subscriber of an amendment to the contract. The European Commission is informed about this case via the EU Pilot (no. 6992/14/CNCT).*
Lithuania	*It is established that the provider must ensure that the initial time period of a contract, concluded with the user for a fixed period of time, is no longer than 24 months. The provider must also ensure that service users have the possibility to conclude the contract for a time period no longer than 12 months. Contractual penalties for premature termination are not regulatory limited. The possibility of terminating a contract in cases of service changes is stipulated by Lithuanian regulations.*
Poland	*The Polish NRA is currently working on the approach potentially to define the maximum commitment period for contracts between ICT service providers and consumers. For the time being it should be assumed that it is not applied in practice and its possible introduction depends on the interpretation of amended provisions of the Telecommunications Act. Under the last amendment to the Telecommunications Act, two scenarios are possible depending on the interpretation chosen by the UKE. Either the regulation will prevent telecommunications service providers from concluding initial contracts for the provision of a particular telecommunications service with subscribers for a period longer than 24 months or, the regulation prevents the conclusion of contracts for the provision of telecommunications services for a period exceeding 24 months, irrespective of the fact if this is the first or subsequent contract.* *Depending on the interpretation followed by the UKE, the first possibility is that a maximum commitment period for contracts will be regulated exclusively in relation to the first contract for the provision of telecommunications services concluded with a particular provider of telecommunications services for a particular service which may not exceed 24 months. The second possibility is that a maximum commitment period for contracts will be regulated in such a way that each contract may not exceed 24 months.* *In the event of concluding an agreement for the provision of telecommunications services, including connection to a public telecommunications network, associated with an allowance granted to the*

	subscriber, any claim resulting from unilateral termination of an agreement by the subscriber or a service provider due to the subscriber's fault prior to the termination date fixed in an agreement, may not exceed the value of an allowance granted to the subscriber reduced by its proportional value for the period from concluding the agreement to its termination date. The claim will not apply if the agreement is terminated by the consumer before the services are provided, unless telecommunications terminal equipment is subject to the allowance. *A provider of publicly available telecommunications services will inform the subscriber of his/her right to terminate the agreement if he/she does not access these modifications, without the obligation to pay any contractual penalties. The above also refers to a situation where a modification to an agreement results from a modification to the terms and condition of service provision.*
Romania	*Contracts concluded with consumers can only have an initial contractual period of no more than 24 months. Also, providers have to offer consumers contracts with a minimum commitment period of 12 months. In the country there are no regulatory limited contractual penalties for early termination. Current Romanian regulation stipulates condition for contract cancelation without penalty in case of changes in service conditions.*
Slovakia	*According to Slovak regulations, when a subscriber, who is a natural person, commits himself to use a certain public service of an undertaking for a certain minimum period, the duration of such a period at the initial conclusion of the contract to provide a public service should not exceed 24 months. At the same time, the undertaking will be obliged to offer the user the possibility to conclude a contract to provide public services with a maximum duration of 12 months. Without prejudice to the minimum period of the contract to provide public services, the undertaking will be obliged to ensure that the contractual conditions and procedures for the contract termination do not discourage the subscriber to change the service provider. Contractual penalties in cases of early termination are subject to agreement between the ICT service provider and the consumer. The subscriber has the right to withdraw from the contract of the provision of public services without sanctions in several cases defined by law. The first case is if he does not accept the substantial modification of the contractual conditions, and the second case is when, despite repeated complaint, the operator does not provide the services under the contract or the services are not of the expected quality.*
Sweden	*The maximum commitment period for contracts in this area is regulated to 24 months. The contractual penalties for early contract termination are not specifically regulated for the ICT sector. However, penalties are still limited through common tort law and by rules against unreasonable contract terms. There is the possibility to terminate the contract if there are changes in service conditions.*

POLICY ENABLERS – EU EXAMPLES

Universal Services Directive: Clear, competitively neutral policy for the provision of a defined set of services to any person requesting it, including internet access at affordable prices

EU member state	Functions *(extracts from the EaP benchmarking report December 2014)*
Czech Republic	*The provision of public pay phones, access for disabled persons to PATS and special price plans are included in the scope of universal service. The connection and access at a fixed point to the public network, directories and directory enquiry services and complementary services are out of the scope of the universal service obligation, as they are considered to be available in the market under normal commercial conditions. The designation of the universal service provider has been completed through a tender procedure for the provision of the universal service at national level. The designation mechanism ensured in the tender procedure rules that no operator was a priori, excluded both from being designated with regard to the possibility of providing the different elements separately, and in its provision at regional level. Currently, the incumbent (O2 Czech Republic) is designated with the obligation to provide public payphone services until 31 December 2014, access for disabled persons to PATS until 15 July 2015, and special price plans until 2 July 2014.* *Net costs from the universal service provision are compensated from the state budget. No maximum or minimum funding caps have been implemented. There are no minimum and maximum data rates provided under the universal service scope in the Czech Republic.* *The universal service provider must fulfil the quality parameter values and performance targets of the universal service. These quality parameters are set out by Decree on the determination of the quality parameters of universal service and the limit values thereof, and by the Measure of General Nature laying down the content, form and method of publishing information about the results of the universal service provision. No additional international standards for universal service are applied.*
Lithuania	*In Lithuania, the universal service provider has to provide access to a network of electronic communications, provided at a fixed location for natural and legal persons; local and long distance calls as well as international calls for natural and legal persons; public payphone services; directory enquiry services, and guarantee the provision of universal services for disabled customers. In 2014 TEO LT, AB is providing the universal service. Prices of universal services should not be higher than the fixed price cap. Prices of universal services cannot be differentiated geographically. The operator, having the SMP in the market of access to the public network of electronic communications, provided at a fixed location, has to provide universal services. The NRA periodically invites interested parties to provide universal services without compensation.* *The net cost of universal services could be compensated from the net cost compensation fund, by increasing the prices of universal services or by combining the two methods. No minimum or maximum funding caps have been applied regarding the financing of the universal service. Services providers of electronic communication services that have operated for less than 24 months or whose revenues from public telephone services are below EUR 577,143, are exempt from payments to the net cost compensation fund.* *In Lithuania, the Quality of Service standard of the universal service is stipulated in the Specification of requirements for universal service quality, approved by the Order of the RRT Director, who implements "The Universal Service Directive" and takes into consideration the ETSI recommendation, ETSI EG 201 769-1.*
Poland	*The situation concerning universal service is more complicated in Poland. During the period from 8 May 2006 until 8 May 2011 when Telekomunikacja Polska S.A. was obliged to provide a universal service to the entire national territory, it failed to deliver this obligation fully. Therefore, regulatory*

	tools in the form of a universal service obligation provided by a designated undertaking proved ineffective. The provisions of European law allow for a flexible approach to the USO. Universal service comprises a set of services, including inter alia connection to the network, subscription, and national as well as international telephone calls which are provided by different telecommunications undertakings. Universal service is, therefore, provided by different telecommunications undertakings under the commercial/market terms. Only where the market mechanism fails to satisfy users' needs in the entire or part of the national territory with respect to universal service or particular elements thereof, an obligation should be imposed, i.e. an undertaking or undertakings should be designated which are not in a position to refuse or resign from the provision of universal service or particular elements thereof. Taking these aspects into account and having regard for the current situation in the telecommunications market in Poland, users' needs, and the efficiency of the regulatory tool in the form of the obligation to provide universal service by a designated undertaking, the President of the UKE has taken steps to elaborate a new universal service model. *Under the new universal service model, the regulator has been entrusted with the power to designate such an undertaking or undertakings only if this is necessary, in particular taking account of real end users' needs in different areas of the country (i.e. where the market alone, based on self-regulation and taking account of the principles of effective competition, fails to provide universal service). Therefore, the decision on the need to design an undertaking obliged to provide universal service rests on the President of the UKE. Currently, the President of the UKE is analysing the market in the above-mentioned scope, particularly in terms of availability, quality and price affordability of the services of which the universal service comprises.* *If this analysis proves that it is necessary to launch proceedings to designate the undertaking or undertakings obliged to provide universal service, the analysis conducted by the President of the UKE will have a decisive role when making a decision on the need to designate an undertaking obliged to provide universal service, including definition of material and territorial scope.*
Romania	
Slovakia	*After the market liberalisation, the RU imposed an obligation related to providing universal services to disabled users, network access, phone books, and public payphones and information services. The RU does not monitor the data rates provided under the universal service obligation.* *The designation of the universal service provider took place on the basis of public consultations. The fixed incumbent, Slovak Telekom, remained the designated provider. No operator was a priori excluded from the designation procedure. However, the interest to provide universal service was rather low. The duration of the designation was set for an unlimited period.* *The net costs of universal service are funded from sector resources (contributions from undertakings operating in the market of electronic communications). For compensation of the net costs of universal service, the undertaking operating public networks or public services is obliged to contribute if an annual share of revenues in the national market of the public network or public services is equal to or greater than 0.2 %. The revenues from the provision of retransmission services are not included in the revenues. No minimum or maximum funding cap has been applied.* *The quality of universal service is based on several indices, including the time limit of the initial connection, the fault rate per subscriber line, the fault repair time, the response time of the directory enquiry service, the ratio of fully functional coin and card operated public pay telephones, and bill correctness complaints. No international standards concerning the quality of universal service are applied. Quality of universal service shall be based on the following indices:* *a) Time limit of initial connection,* *b) Fault rate per subscriber line,* *c) Fault repair time,* *d) Response time of telephone directory enquiry service,* *e) A ratio of fully functional coin and card operated public pay telephones,* *f) Bill correctness complaints.*

Sweden	*No universal service obligation is imposed as the operators provide sufficient service for the most part. In cases where no service is available, the situation is handled either through procurement or by instructing an operator (which is under a specific licensing condition) to provide 4G coverage at a specified site.*

Commission Recommendation on Broadband Investment: Clear policy towards increased effectiveness of broadband competition and for enhancing investment in infrastructure for high speed broadband services

EU member state	**Wholesale broadband access[13]** *[This type of access involves non-physical or virtual network access including 'bitstream' access at a fixed location. This market is situated downstream from the physical access (see right hand column), in that wholesale broadband access can be constructed using the physical elements input combined with other elements]*	**Wholesale physical infrastructure access[14]** *[This type of access involves (physical) network infrastructure access (including shared or fully unbundled access) at a fixed location. The market may include all types of physical infrastructure (ducts, manholes, poles, street cabinets, masts, towers, metallic loops, fibres, internal or external building trunking and cabling distribution) and associated supporting plant (e.g. buildings, power supplies and support systems etc.)]*	**Next Generation Access[15]** *[This type of network technology is generally included in the wholesale markets in the first two columns, so that any SMP operator has top provide access under regulated conditions to its NGA infrastructure.]*
Czech Republic	*Via market analysis, the regulator has identified 1 SMP operator which has to follow these obligations:* • *Transparency obligation including the publication of Reference offer* • *Access obligation* • *Non-discrimination obligation* • *Accounting separation* *The form of access is IP*	*Via market analysis, the regulator has identified 1 SMP operator. The following obligations were imposed on the company:* • *access obligation* • *transparency obligation including the publication of Reference offer and provision of information to the wholesale access customers if the SMP chooses to replace the*	*All 3 fibre scenarios, FTTH, FTTB and FTTC are included in the scope of the definition of the wholesale infrastructure access market. Fibre access is the fastest growing type of access in the wholesale markets and also in the related retail markets; it now has more than 10 % of the retail market share. In the wholesale market, fibre has more than 20 % of market share. The SMP operator has only 5% market*

[13] From Section 3.2 and Table 42 in the EaP Benchmarking Report Dec 2014

[14] From Section 3.2 and Table 40 in the EaP Benchmarking Report Dec 2014

[15] From Section 4.9.2 and Table 44 in the EaP Benchmarking Report Dec 2014

	level (from 2006)	*subscriber copper lines with optical fibres locally* • *non discrimination* • *accounting separation (separately for copper and fibre)* • *price control*	*share in the FTTx segment.*
Lithuania	*Via market analysis the regulator has imposed the following remedies on the 1 identified SMP;* • *obligation to provide access* • *non-discrimination* • *transparency* • *price control and cost accounting* • *accounting separation* *The form of access is DSL (from 2003)*	*Via market analysis, the regulator has indentified 1 SMP and has imposed the following remedies:* • *access obligation* • *price control and cost accounting* • *non-discriminatory pricing* • *transparency* • *accounting separation*	*Fibre, LAN and STP/UTP unbundling and access to dark fibre are regulated in the wholesale infrastructure access market. One operator is found having SMP and specific remedies were imposed on it.*
Poland	*The form of access is IP DSLAM/MSAN/OLT level, ATM level and managed and unmanaged IP level (from 2006)*		*In market analysis of both the wholesale broadband access and the wholesale infrastructure access markets, the VDSL2 and FTTH rollouts of the SMP operator are particularly taken into account.*
Slovakia	*The form of access is IP level bitstream at national level (from 2009). The price regulation is based on retail minus methodology.*	*Via market analysis, the regulator has identified 1 SMP operator and has imposed the following remedies;* • *access obligation* • *publication of a reference offer* • *price control and cost accounting* • *non-discriminatory pricing* • *transparency* *accounting*	*The SMP in the wholesale infrastructure market is obliged to provide FTTx access at ODF (P2P and point to multipoint - VULA), and to publish a reference offer. In the wholesale broadband access market, the SMP is obliged to provide FTTx access and to publish the reference offer on FTTx. In the present, because of dismissal of decisions on the wholesale broadband access market there is no fibre within the market definition as it was not deployed significantly in 2009 and only DSL infrastructure was included in the market definition*

Sweden	*The form of access is Level2 bitstream access (from 2007)*	*Via market analysis, the regulator has identified 1 SMP operator and has imposed the following remedies;* • *access obligation* • *publication of a reference offer* • *cost orientation using LRIC*	*The wholesale infrastructure access market has been defined to include both copper and fibre, and access to both LLU and dark fibre is mandated in the decision. Both are also subject to cost orientation according to the LRIC model.*

Radio Spectrum Policy Programme: Clear policy and regulations ensuring the harmonised availability and efficient use of spectrum, taking account of the market needs and the optimal use of scarce resources

EU member state	Description *(extracts from the EaP benchmarking report December 2014)*
Czech Republic	*Frequency allocation and preparation and approval of the national frequency plan are primarily the responsibility of the Ministry of Trade and Industry, which cooperates with the NRA - CTU. The assignment of frequencies is performed by the Spectrum management department of the CTU. The frequency assignment methods used are beauty contest and financial bidding (auction). CTU in the Radio Spectrum Utilisation Plan (RSUP) determines the way and conditions of radio spectrum utilisation by radiocommunication services. The Plan is based on Plan of Frequency Bands Allocation and consists of common part and parts for particular frequency bands.* *Spectrum trading is in Czech Republic allowed but under certain conditions. Legal framework for spectrum trading is regulated at national level according to the Act No. 127/2005 Coll., on electronic communications and on amendment to certain related acts (the Electronic Communications Act, hereinafter only Act). The relevant rules in the Act are based on Framework Directive 2002/21/EC and Authorisation Directive 2002/20/EC, both amended by Directive 2009/140/EC. Restrictions for the SMP are that tradability of spectrum rights assigned in auction 2013 is restricted for 7 years.* *On the basis of the Act No. 127/2005 Coll., the holders of authorization to use of radio frequencies shall pay the annual fees for the use of radio frequencies. The method of calculation of the charges for the use of radio frequencies and numbers are set down in Government decree No. 154/2005, as amended. The spectrum fees are paid by both commercial subjects and governmental bodies. The fees form a part of state budget.* *Czech Republic used in 2013 frequency allocation through the simultaneous multiple round auctions. During the auction some of the rules must be met as in 1800 MHz band Spectrum Cap 2x23 MHz in order to reserve the contiguous block 2x15.8 MHz for a newcomer (i.e. 2x9 MHz available for existing operators). In 900 MHz frequency band 2x10 MHz band must be reserved for a possible newcomer. Spectrum Cap applied also in the 2.6 GHz as max. of 2x20 MHz in the FDD band, 15 MHz in the TDD band. In the future, CTU will assign vacant frequencies through the auction of 1800 and 2600 MHz bands.*
Lithuania	*The NRA is responsible for the allocation and assignment of frequencies, and also for the preparation of the national frequency allocation plan. Frequencies are assigned using the beauty contest method. Frequency fees must be paid by operators as commercial subjects. Spectrum fee is calculated on cost of spectrum management and monitoring. Spectrum fee is received by the state budget. Under consideration is reallocation of broadcasting form 694- 790 MHz band.* *In Lithuania, NRA used auctions as the method of frequency assignment for 800 MHz in 2013 and 2.5 GHz in 2014. The SMRA as an auction format has been used with the reserved price 25 000LTL (7240 EUR) -1 000 000 LTL (289 620 EUR) per 5MHz block. One frequency band 450-470 remains unlicensed. In Lithuania, spectrum trading is allowed expect spectrum for broadcasting and governmental usage.*
Poland	*The final act of the national frequency allocation table is issued by the Council of Ministers of the Republic of Poland. The governmental bodies that have the largest responsibility are the Ministry of Administration and Digitalisation, the Ministry of the Interior, the Ministry of National Defence and the Office of Electronic Communications (NRA). The preparation and approval of the national frequency plan is the responsibility of the NRA. The assignment of frequencies for civil purposes is within the authority of the NRA, while for military purposes there is a special authority, the NARFA POL. In Poland, frequencies were so far assigned only using the method of beauty contest. The first auction is planned to be organised in 2013.*
Romania	*The NRA is responsible for frequency allocation and assignment. Together with relevant ministry ANCOM is responsible for preparation and approval of the national frequency plan. There has been 1 block in 800 MHz and 8 blocks in 2600MHz band which remain unawarded. In Romania, the NRA have already used auction as the method of frequency assignment for certain frequencies in*

	September 2012 for the 800, 900, 1800 and 2600 MHz bands. *The format of auction which was used in Romania was multiround ascending. During the auction, 1 bidder could acquire usage rights below 1GHz with the width 2x20 MHz.* *The minimum price (reserve price) has been set according to Government Decision no.605/13.06.2012 as follows: in 800 MHz band in the amount of EUR 35 million/2x5 MHz; in 900 MHz band in the amount of EUR 40 million/2x5 MHz; in 1800 MHz band in the amount of EUR 10 million/2x5 MHz; in 2600 MHz band in the amount of EUR 4 million/2x5 MHz and EUR 3 million/1x15 MHz. The use of auction as a form of frequency assignment will be used in the future.* *The spectrum trading is allowed according to Art. 35 of the GEO, No. 111/2011. The usage rights may be transferred to a third party, in total or in part, only based on the prior ANCOM approval. The transfer of the usage rights shall not result in competition constraints, hindering or distortion. In cases where the use of radio frequencies is harmonised at the European level, the transfer of the usage rights must not lead to changing the usage destination of the frequencies that are subject to the licence in such a way as to breach this harmonised usage. In case of a partial transfer of the rights in 800 MHz, 900 MHz, 1800 MHz and 2600 MHz, the licence holder may only transfer 5 MHz blocks, with all the obligations associated with or, for the TDD operation mode in 2600 MHz, only in compact unpaired blocks of 15 MHz.* *The spectrum fees are paid on year-to-year basis and calculation are based on a number of parameters (frequency range, number of blocks, radio channel, number of transmitters, e.i.r.p. etc.), according to ANCOM President's Decision no.551/2012, with the subsequent amendments and completions. The spectrum fees are received by NRA and the Parliament approves their budget.*
Slovakia	*In Slovakia, the RU cooperates with the Ministry of Transport, Construction and Regional Development in elaboration of the draft of the national table of the frequency spectrum, preparing the plan of use of the frequency spectrum, assigning frequencies and laying down conditions for the use of frequencies and coordinating and checking the use of the frequency spectrum. In Slovakia is frequency trading between market participants allowed. The only restriction used during the auction is spectrum cap of 20 MHz for 800 MHz and 40 MHz for 1800 MHz. For one block of 2x5 MHz the reserve price in 800MHz was set in the amount if 19 000 EUR, in 1800 MHz 2 200 000 EUR and in 2600MHz was the price 1 100 000 EUR. The next auction is planned for frequency assignment in 2015.* *The last auction in 2013 was realized to use frequencies from the 800 MHz, 1800 MHz, and 2600 MHz frequency bands together as one amount where SMPs gain the following frequencies. WIFI 2400 MHz band stayed unlicensed.*
Sweden	*In Sweden, frequencies are allocated and assigned by the NRA, which also elaborates the national frequency plan. Frequencies are assigned using the methodologies of beauty contest and financial bidding.*

STRATEGY ENABLERS – EU EXAMPLES

Framework Directive: Clear procedures for the identification, definition and analysis of relevant markets that are subject to ex-ante regulation in order to determine SMP

EU member state	**Regulation applied to market analysis** ***(extracts from the EaP benchmarking report December 2014)***	**Frequency of analysing markets** ***(extracts from the EaP benchmarking report December 2014)***
Czech Republic	*Adoption of EC recommended relevant markets* *Three criteria test*	*1 – 3 years from imposing a remedy*
Lithuania	*Adoption of EC recommended relevant markets, Three criteria test*	*Every 3 years*
Poland	*Adoption of EC recommended relevant markets, Three criteria test*	*Every 2 – 3 years*
Romania	*Adoption of EC recommended relevant markets*	*N/A*
Slovakia	*Adoption of EC recommended relevant markets*	*Every 3 years*
Sweden	*Adoption of EC recommended relevant markets, Three criteria test, SMP identified by a set of factors including market share*	*Every 3 years*

Framework Directive: Rights of way: simple, efficient, transparent procedures, applied without discrimination or delay

EU member state	Legal basis	Fees	Notes
UK	*Any electronic communications provider has rights to install and maintain apparatus on public or private land (Under the Communications Act 2003, the Electronic Communications Code confers rights -"code powers")*	*Administrative fee: Operators granted code powers must pay a one-off application fee of around €12,000 and an annual fee of €1,200* *For each project, fees are payable to the local government authority with a maximum fee for an application of around €130) and for the grant of a permit of around €300.*	*Under regulatory rules, requests for rights of way are considered more favourably for network operators who will share infrastructure with other operators.* *Another regulatory guideline shows how an operator must provide a bond or guarantee to meet any costs or damages arising from the exercise of the rights of way, for example in relation to any damage caused or the cost of removing equipment.*
Spain	*Operators of public communications networks can make use of public property if that is necessary to establish their networks. They can also make use of private property in what is strictly indispensable to set up the public network and in case there are no other alternatives which are economically viable.* *Public administrations must grant access rights to their property to operators deploying public electronic communications networks under neutral transparent and non-discriminatory conditions. No exclusive or preferential rights can be granted and no tender procedures can be used to award rights of ways in public land.* *Procedures must be public, simple, fast and transparent.* *Public administrations must facilitate such deployment and may not impose disproportionate restrictions or mandate technological solutions. They must also offer physical space for operators to install their infrastructure, Any regional/local regulations*	*The fees for rights of way are generally defined by the municipalities.* *A local tax can be levied of up to 4% of the total cost of constructions and installations within the municipality.*	*The regulator has set a non-binding view on the methodologies used by municipalities to tax mobile network operators for the use of local public property.* *There are no guarantees required at national level, although some local conditions may apply.*

	that may affect the deployment of electronic communications networks must be notified to the ministry prior to adoption, and can be vetoed. *Deployment of public networks in private land is not subject to any requirement for a previous licence or authorisation. If the competent administration does not respond within 2 months the plan is considered approved. The operator must in any event declare that the deployment complies with applicable regulations.*		
Netherlands	*The operator has to notify the owner of the private or public property.* *For public property, municipalities can set rules regarding the timing and operation of the works before accepting the request for right of way.* *If the operator can't agree with the owner of the private or public property within six weeks, The regulator can take a binding decision within eight weeks during which the right of way is suspended.*	*Right to compensation is restricted to compensation of the costs of any damages or required maintenance and the costs to return the property in its original condition.*	*No guarantees or bonds are required from the operators*
Greece	*Rights of way are granted to providers of public electronic communications networks, subject to a decision of the respective municipality.* *Rights of way apply equally to public and private properties. Property owners may be compensated.* *Where the owner (or the authorised property user) and the communications network provider cannot agree, the parties may ask the local Court of Arbitration to settle the dispute, and subsequently the Regional High Court for final decision if necessary.*	*The amount of compensation (a one-off payment) for the rights of way is set by the respective municipality, according to the procedure established in the Law.*	*In individual cases, the municipality may decide on a specific deposit amount as a guarantee for particularly high fees for rights of way*
Portugal	*Private use communications network operators are merely entitled to request rights of way over public domain. Public communications network providers are entitled to request the use of both private property and public property.* *The application procedures are defined by the municipalities. Such procedures must be swift, transparent, adequately publicised and non-discriminatory.*	*Fees based on a percentage (up to 0.25%) of the total value of bill of all end-user clients living in the relevant municipality – excluding any amounts that are for services other than electronic communications. No other fee may be imposed on operators.*	*Operators can pass the fees for rights of way onto their subscribers. The regulator defines the procedures for the collection and delivery of municipal fees for rights of way.*

Note: This table was compiled by analysis of the relevant websites

Authorisation Directive: A general authorisation procedure with simple notification for market participants and restricting the need for individual licences to specific, objectively justified cases

EU member state	Description *(extracts from the EaP benchmarking report December 2014)*
Czech Republic	*Market entry in the Czech Republic is simply subject to notification. Any natural person or legal entity wishing to carry out a communications activity representing an electronic communications business is obliged to notify the Czech NRA of that fact in writing beforehand. All the particulars of the notification are specified in the Electronic Communications Act, e. g. submission of a document proving that the person has no debts to the Czech Republic in taxes, social insurance and health insurance. The notification should be performed before commencement of a communications activity which represents an electronic communications business. The obligation for foreign companies settled in the area of EU to register into the Czech Commercial register is no longer in effect. Within one week of receiving the notification, the CTU will issue, to the person referred to above, a certificate to the effect that such person submitted the proper notification.* *A mandatory administrative fee of approx. EUR 39 is levied as a one-off fee for issuing the certificate proving the valid notification of the new communications activity. Also, an administrative fee of approx. EUR 20 is levied as a one-off fee for issuing the certificate proving the valid notification of changes of the previously notified communications activity. There is a one-off administrative fee of approx. EUR 195 collected for the authorisation to use numbers. Annual fees for the rights resulting from the Authorisation to Use Numbers can be found in the Government Regulation on the determination of the amounts and the method of calculation of the charges for the use of radio frequencies and numbers.*
Lithuania	*Market entry is subject to a simple authorisation regime by way of notification. An undertaking intending to engage in electronic communications activities has to notify the RRT of the commencement of its activities. The RRT enters the undertaking onto the list of electronic communications network and service providers within 7 days from the date of receipt of an accurate notification which complies with requirements.* *In Lithuania, no licensing regime is applied for number allocation. The numbers, with the exception of numbers provided in the National Numbering Plan as service numbers and the numbers assigned to providers of non-telecommunications services for provision of non-telecommunications services, are allocated to legal or natural persons who have the right to engage in the provision of the public fixed telephone network and/or the provision of public fixed telephone services (they were entered onto the list of electronic communication service providers). The person has to submit the completed application to the RRT, and the RRT, by issuing the RRT Director's order, allocates numbers from the database administered by the RRT, for an unlimited period of time. The RRT issues orders granting the right to use the name of Lithuania in internet domain names by way of a simple authorisation. Applicants, who intend to receive an authorisation from the RRT to use the name of Lithuania in domain names, are subject to no specific limitations (or any licensing procedure). The RRT issues authorisations within 10 days from the date of the receipt of the application by the natural or legal person if they meet the specific requirements set out in Rules on the Use of the Name of Lithuania in Internet Domain Names. The authorisation procedure on frequency assignment is dependent on frequency band; there are three scenarios used - individual licensing, general authorisation, and light licensing (general authorisation + obligation to register a radio station in the database).* *Undertakings engaged in the provision of electronic communication networks and services, and whose annual turnover exceeds EUR 288 572, are subject to monthly fees payable to the RRT for the supervision of compliance with General Terms and Conditions for Engaging in Electronic Communication Activities. No fees are paid to the RRT by undertakings, which have the right to engage in electronic communication activities, for the allocation of numbers. However, they have to pay monthly fees for the supervision of number use and compliance with the number allocation*

	conditions. Monthly fees are paid for the supervision of compliance with the Terms and Conditions of allocation of frequencies/channels. *Since 1 January 2015 RRT, as an EU member, will have to implement the new EC Recommendation 2014/710/EU on relevant product and service markets within the electronic communications sector susceptible to ex ante regulation in accordance with Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services.*
Poland	*In Poland, according to the Telecommunications act, the market entry is only subject to registration which is free of charge.* *The Polish NRA collects an annual telecommunications fee, which is paid by undertakings with revenues exceeding EUR 940,000. In addition, an annual fee for the right to use numbering and an annual fee for the right to use frequency resources are also levied.*
Romania	*In Romania, everybody can provide electronic communication services without the need for a licence or the need to pay inappropriate fees. There are no limitations for electronic communications market entry. There are three tariffs as a fees paid by the undertakings:* • *The monitoring tariff, owed by all the authorised providers of electronic communications networks or services and postal services whose turnover or revenues exclusively obtained from these activities exceed EUR 100,000* • *Second is the tariff for the use of spectrum, owed by all the holders of licences for the use of radio frequencies and holders of broadcasting licences* • *The last one is the tariff for the use of numbering resources, owed by all the holders of Licences for the use of Numbering Resources.*
Slovakia	*In Slovakia, market entry depends on the service that a new entrant wants to provide. If the new entrant wants to provide services without specific authorisation (e. g. WIFI ISPs), he has to notify the RU of his intention to provide such services. If the new entrant wants to provide services with specific authorisation (specific frequency, number assignment, etc.), he has to pass the specific authorisation criteria. There are several barriers to market entry still pertaining. Among them is ownership of the infrastructure, access to the scarce resources such as the frequencies, time barriers to build the network and economic barriers such as access to financial sources, permissions or interconnection agreements.* *The Slovak NRA collects annual number usage fees, another annual administrative fee which stands at 0.08 % of revenue, a quarterly payment for the right to use frequencies, and a one-off fee for the assignment of frequencies.*
Sweden	*In Sweden, entry to the electronic communications market is subject to notification.*

RESOURCES ENABLERS – EU EXAMPLES

Framework Directive: Adequate human and financial resources to carry out effective independent regulatory function

EU member state	Number of employees of the NRA[16]	NRA budget 2014 (Euro)[17]	Financing of NRA *(extracts from the EaP benchmarking report December 2014)*
Czech Republic	*444*	*23,892,046*	*The Czech NRA is an independent financial entity and has a separate budgetary section in the State Budget of the Czech Republic. The CTU´s mandatory expenditure and revenue limits are set by the Ministry of Finance. The budget surplus has to be transferred to the State Budget and the CTU is wholly financed from public sources (state budget).*
Lithuania	*163*	*6,372,000*	*The Lithuanian NRA (RRT) is financed from the state budget as well as a separate budget of its own, comprising revenues from services provided and work performed. The objects and scope of such services and work, as well as the procedure of payment, are established by the RRT on the basis of its costs.*
Poland	*642*	*22,320,077 (not including EU funds)*	*The Polish NRA is also wholly financed from the state budget. The fees collected by the UKE, consisting of the annual telecommunications fees, the annual fees for the right to use numbering and the annual fees for the right to use frequencies, are the income of the state budget.*
Romania	*N/A*	*N/A*	*The Romanian NRA, (ANCOM)'s financing is ensured from the following sources:* • *the monitoring tariff, owed by all the authorised providers of electronic communications networks or services and postal services whose turnover or revenues exclusively obtained from these activities exceed EUR 100,000,* • *the tariff for the use of spectrum, owed by all the holders of licences for the use of radio, frequencies and holders of broadcasting licences,* • *the tariff for the use of numbering resources, owed by all the holders of Licences for the Use of Numbering Resources.*
Slovakia	*158*	*4,635, 000*	*In Slovakia, the NRA is financed through administrative charges. The budget of the NRA is separated, but financially connected to state budget through a separate budgetary section of the Ministry of Finance. The Office imposes administrative charges on undertakings providing networks or services based on the general authorisation, charges for the right to use numbers and charges for the right to use frequencies.*
Sweden	*270*	*35,933,000*	*The Swedish NRA (PTS) has a separate annual budget. It is funded mostly by administrative charges, covering around 90 % of the budget, but also by state funds, covering the rest. The PTS also has appropriations from the national budget for security measures and services for people with disabilities, of approximately EUR 45, 342,000 million.*

[16] *From table 13 of EaP Benchmarking Report Dec 2014*

[17] *From table 11 of EaP Benchmarking Report Dec 2014*

Commission Recommendation on Broadband Investment: Access by investors to sources of capital for investment in broadband infrastructure

EU member state	Description *These links provide full details of state funding (at the European or Member State level or both) for provided for specific investment projects in electronic communications infrastructure*
Lithuania	*See* http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_N497_2007 http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_34166 http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_N183_2009 http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_36132
Poland	*See:* http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_35949 http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_34708 http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_34932 http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_35027 http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_34665 http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_33386 http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_33473 http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_33222 http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_33438
Romania	*See:* http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_37558
Slovakia	*See* http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_33151
Sweden	*See* http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_35913 http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_32037 http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_33221 http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_N30_2010

IMPLEMENTATION ENABLERS – EU EXAMPLES

Framework Directive: Clear mechanisms to appeal regulatory decisions

EU member state	Description *(extracts from the EaP benchmarking report December 2014)*
Czech Republic	*The appeals procedure in public law decisions, which encompasses the imposition of fees according to the Electronic Communications Act, and the decision in the case of universal service etc., is based on the principle of cassation. The court, which carries out the judicial review, can revoke the decision of the NRA as unlawful or for procedural faults, and can return the matter for a new proceeding and a new decision. The NRA is bound by this judgment in subsequent proceedings. In private law disputes, the Chairman of the Council should resolve disputes between persons performing telecommunications activities. This is not actually a review of the decisions issued by the NRA, rather a proceeding, in which the courts in the civil proceedings discuss again and factually decide disputes about which the NRA has previously made a decision. According to the Code of Civil Procedure, if the court reaches the conclusion that the decision made by the NRA about a dispute or other legal matter should be different, the court will produce a judgment on the case itself. This court judgment supersedes the decision of the NRA.*
Lithuania	*The parties in the dispute between end users and undertakings have the right to appeal to the court with a request to resolve their dispute in substance within 30 days from the date of the adoption of the regulator (RRT)'s decision on dispute resolution. The parties in the dispute between undertakings may appeal to the court with a request to resolve their dispute in substance within 14 days starting from the day the RRT adopted the decision, whereby the dispute is substantially resolved. In case RRT decision is appealed against at court, dispute is further being resolved in court and RRT decision does not come into force.*
Poland	*It is possible to appeal against the decision of the President of the NRA about the designation of SMPs, application of regulatory obligations, imposing of penalties etc. to the court of competition and consumer protection. However, it must be noted that the appeal should be filed through the President of the NRA who is able to repeal, or amend his/her decision in whole or in part, if he/she recognises that the appeal is justified.*
Romania	*The decisions adopted by the regulator (ANCOM) may be appealed only in the Administrative Division of the Bucharest Court of Appeal, also due to the fact that the appeal body must have the necessary expertise in the electronic communications field. The SMPs have the opportunity to ask the court for the annulment or temporary suspension of the NRA's decisions. A decision of the NRA which is being appealed is not automatically suspended. The telecom operators have the opportunity to ask the court for the annulment or temporary suspension of the NRA's decision.*
Slovakia	*A period of 15 days is given to appeal against the decision from the delivery of a decision by the NRA. After receiving the appeal, the body of first instance has a period of 30 days to withdraw the measure or submit it to the body of second instance (the chair of the NRA) with a proposal of the final decision (the decision on appeal). It is not possible to appeal against the decision on appeal. The undertaking in question has the legal right to bring the action to the Supreme Court of the SR. The final decision is then made by the Supreme Court, who can confirm or annul the decision made by the NRA.*
Sweden	*All decisions of the NRA can be appealed in a court of law, except regulations, and follow a standard appeal procedure.*

Access Directive: For operators found to have SMP under the market analysis procedures carried out in accordance with the Framework Directive, the regulator shall impose proportionate regulatory obligations with regard to:

- access to, and use of, specific network facilities
- price controls on access and interconnection charges, including obligations for cost orientation
- transparency, non-discrimination and accounting separation

EU member state	**Description** ***(extracts from the EaP benchmarking report December 2014)***
Czech Republic	*According to the 2007 EC recommendation, the Czech NRA performs market analysis in 7 relevant markets.* *In Market no. 1 - Access to the public telephone network at a fixed location for residential and non-residential customers, 1 SMP operator has been identified and the following obligations imposed;:* • *Carrier selection and carrier pre-selection* • *Accounting separation* *In Market no. 2 - Call origination on the public telephone network provided at a fixed location, 1 SMP operator has been identified and the following obligations imposed:* • *Transparency obligation including publication of Reference offer* • *Access obligation* • *Non- discrimination obligation* • *Accounting separation* • *Price control* *In Market no. 3 - Call termination on individual public telephone networks provided at a fixed location, 25 SMP operators have been identified. The incumbent operator has the following obligations:* • *Transparency obligation including publication of Reference offer* • *Access obligation* • *Non-discrimination obligation* • *Accounting separation* • *Price control* *The NRA has applied the following remedies on the other SMPs in Market no. 3:* • *Transparency obligation (without reference offer)* • *Non-discrimination obligation* *In Market no. 4 - Wholesale (physical) network infrastructure access (including shared or fully unbundled access) at a fixed location, 1 SMP operator has been identified and the following obligations imposed;:* • *Access obligation* • *Transparency obligation including the publication of Reference offer and provision of information to the wholesale access customers if the SMP chooses to replace the subscriber copper lines with optical fibres locally* • *Non discrimination* • *Accounting separation (separately for copper and fibre)* • *Price control* *In Market no. 5 - Wholesale broadband access, 1 SMP operator has been identified and the following obligations imposed:* • *Transparency obligation including the publication of Reference offer* • *Access obligation* • *Non-discrimination obligation* • *Accounting separation* *In Market no. 6 - Wholesale terminating segments of leased lines, 1 SMP operator has been identified but only for leased lines up to and equalling 2 Mbps, including Ethernet leased lines. The*

	regulator has imposed these remedies: • *Transparency obligation including the publication of Reference offer* • *Access obligation* • *Non-discrimination obligation* • *Accounting separation* *In the last analysed Market no. 7 - Voice call termination on individual mobile networks, 4 SMP operators have been identified. 3 SMPs have to follow these obligations:* • *Transparency obligation including the publication of Reference offer* • *Access obligation* • *Non-discrimination obligation* • *Accounting separation* • *Price control* *On the remaining SMP, the following reduced obligations were imposed:* • *Transparency obligation (without reference offer)* • *Non-discrimination obligation* • *Access obligation* • *Price control* *The NRA is exercising price control on 4 relevant markets. This uses mainly pure bottom-up LRIC modelling (wholesale markets for call origination and call termination. For the wholesale market for infrastructure access, monthly prices are based on LRIC and the one-off prices are based on Activity Based Costing.*
Lithuania	*The Lithuanian NRA, the RRT, performs market analyses and imposes remedies in 16 relevant markets according to the 2003 Recommendation of the EC.* *In Market no. 1 - Fixed Access to the public telephone network for residential customers, 1 SMP operator has been identified and the following obligations imposed:* • *Obligation to provide CS/CPS services* • *Obligation to provide wholesale line rental (WLR) service* • *Cost accounting and price control* • *Accounting separation and price control* *For WLR service these obligation are imposed - non-discrimination, transparency, price control and cost accounting, accounting separation.* *In Market no. 2 - Fixed Access to the public telephone network for non-residential customers,1 SMP operator has been identified and the following obligations imposed:* • *Obligation to provide CS/CPS services* • *Obligation to provide wholesale line rental (WLR) service* • *Cost accounting and price control* • *Accounting separation* *For WLR service these obligation are imposed - non-discrimination, transparency, price control and cost accounting, accounting separation.* *In Market no. 3 –Market with minimum set of the leased lines, 1 SMP operator has been identified and the following obligations imposed:* • *obligation to provide public information related to minimum set of leased lines* • *price control and cost accounting* • *accounting separation* • *non-discriminatory pricing* *In Market no. 4 - Call origination on the public telephone network provided at a fixed location, 1 SMP operator has been identified and the following obligations imposed:* • *price control and cost accounting* • *obligation to provide access* • *accounting separation* • *non-discriminatory pricing*

	• *transparency* *In Market no. 5 –Call termination on individual public telephone networks provided at a fixed location , 8 SMP operator has been identified and the following obligations imposed on 1 SMP operator:* • *price control and cost accounting* • *obligation to provide access* • *transparency* • *accounting separation* • *non-discriminatory pricing* *On the other 7 SMPs, the following obligations have been imposed:* • *obligation to provide access* • *price control* *In Market no. 6 –Wholesale (physical) network infrastructure access (including shared and fully unbundled access) at fixed location, 1 SMP operator has been identified and the following obligations imposed:* • *price control and cost accounting* • *non-discriminatory pricing* • *transparency* • *accounting separation* *In Market no. 7 - Wholesale broadband access, 1 SMP operator has been identified and the following obligations imposed:* • *obligation to provide access* • *non-discrimination* • *transparency* • *price control and cost accounting* • *accounting separation* *In Market no. 8 - Wholesale terminating segments of leased lines, 1 SMP operator has been identified and the following obligations imposed:* • *obligation to provide access* • *non-discrimination* • *transparency* • *price control and cost accounting* • *accounting separation* *In Market no. 9 - Wholesale trunk segments of leased lines, 1 SMP operator has been identified and the following obligations imposed:* • *obligation to provide access* • *non-discrimination* • *transparency* • *price control and cost accounting* • *accounting separation* *In Market no. 10 - Voice call termination on individual mobile networks, 3 SMP operators have been identified and the following obligations imposed:* • *obligation to provide access* • *non-discrimination* • *transparency* • *price control* *In Market no. 11 - Broadcasting transmission services, to deliver broadcast content to end users, 2 SMP operators have been identified and the following obligations imposed:* • *obligation to provide access* • *non-discrimination* • *transparency* • *price control and cost accounting* • *accounting separation*

	The Lithuanian NRA exercises price control on all 11 markets. The most common cost accounting methodology used is the FDC. On Markets no. 9 and 15, the benchmarking method is used so far, but the BU-LRAIC method is being implemented. On Markets no. 8 and 10, the Lithuanian NRA uses a hybrid LRAIC model, which is a combination of BU and TD LRAIC methods.
Poland	*The Polish NRA performs market analysis and imposed remedies in 18 relevant markets according to the 2003 Recommendation of the EC.* *In Market no. 1 - Fixed Access to the public telephone network for residential customers, 1 SMP operator has been identified and the following obligations imposed;* • *Obligation to refrain from distorting the market entry of other undertakings* • *Non-discrimination obligation* • *Obligation to refrain from providing end-users with unnecessary services* • *Transparency obligation* • *Obligation to refrain from limiting competition by fixing prices of providing telecommunication services at below costs* *In Market no. 2 - Access to the public telephone network at a fixed location for non-residential customers, 1 SMP operator has been identified and the following obligations imposed;* • *Obligation to refrain from distorting the market entry of other undertakings* • *Non-discrimination obligation* • *Obligation to refrain from providing end-users with unnecessary services* • *Transparency obligation* • *Obligation to refrain from limiting competition by fixing prices of providing telecommunication services at below costs* *In Market no. 3 - The national market for publicly available local and/or national telephone services provided at a fixed location for residential customers, 1 SMP operator has been identified and the following obligations imposed;* • *Obligation to refrain from fixing inflated prices for services* • *Obligation to refrain from distorting the market entry of other undertakings* • *Obligation to refrain from limiting competitiveness by fixing prices at below costs* • *Non-discrimination obligation* • *Obligation to refrain from enforcing end-users to use unnecessary services* • *Accounting separation obligation* • *Price control – using cost oriented prices according to the cost calculation description approved by the President of the UKE* • *Transparency obligation* *In Market no. 4 - Publicly available international telephone services provided at a fixed location for residential customers, 1 SMP operator has been identified and the following obligations imposed;* • *Obligation to refrain from fixing inflated prices for services* • *Obligation to refrain from distorting the market entry of other undertakings* • *Obligation to refrain from limiting competitiveness by fixing prices at below costs* • *Non-discrimination obligation* • *Obligation to refrain from enforcing end-users to use unnecessary services* • *Accounting separation obligation* • *Price control – using cost oriented prices according to the cost calculation description approved by the President of the UKE* • *Transparency obligation* *In Market no. 5 - The national market for publicly available local and/or national telephone services provided at a fixed location for non-residential customer, 1 SMP operator has been identified and the following obligations imposed;* • *Obligation to refrain from fixing inflated prices for services* • *Obligation to refrain from distorting the market entry of other undertakings* • *Obligation to refrain from limiting competitiveness by fixing prices at below costs* • *Non-discrimination obligation* • *Obligation to refrain from enforcing end-users to use unnecessary services*

- *Accounting separation obligation*
- *Price control – using cost oriented prices according to the cost calculation description approved by the President of the UKE*
- *Transparency obligation*

In Market no. 6 - The national market for publicly available international telephone services provided at a fixed location for non-residential customers, 1 SMP operator has been identified and the following obligations imposed;

- *Obligation to refrain from fixing inflated prices for services*
- *Obligation to refrain from distorting the market entry of other undertakings*
- *Obligation to refrain from limiting competitiveness by fixing prices at below costs*
- *Non-discrimination obligation*
- *Obligation to refrain from enforcing end-users to use unnecessary services*
- *Accounting separation obligation*
- *Price control – using cost oriented prices according to the cost calculation description approved by the President of the UKE*
- *Transparency obligation*

In Market no. 7 - The national market for the provision of partial or entire minimum set of leased lines which comprises the specified types of leased lines up to and including 2 Mb/sec, 1 SMP operator has been identified and the following obligations imposed;

- *Obligation to provide a partial or entire minimum set of leased lines according to principles of non-discrimination and transparency*
- *Obligation to refrain from fixing inflated prices for services*
- *Obligation to refrain from distorting the market entry of other undertakings*
- *Obligation to refrain from limiting competitiveness by fixing prices at below costs*
- *Non-discrimination obligation*
- *Accounting separation obligation*
- *Price control – using cost oriented prices according to the cost calculation description approved by the President of the UKE*
- *Transparency obligation*

In Market no. 8 - The wholesale national market of call origination on the public telephone network provided at a fixed location, 1 SMP operator has been identified and the following obligations imposed;

- *Obligation to provide network access*
- *Obligation of non-discrimination*
- *Obligation of transparency*
- *Obligation of accounting separation*
- *Obligation of price control*

In Market no. 9 - The wholesale market for call termination on the individual public telephone fixed network, 37 SMP operators have been identified, and the following obligations imposed. The obligations differ slightly between the operators, but the general ones are the following:

- *Obligation to provide network access*
- *Obligation of non-discrimination*
- *Obligation of transparency*
- *Obligation of cost orientation*
- *Obligation of non-excessive pricing*

In Market no. 10 - Transit services in the fixed public telephone network, the NRA has not identified any SMPs.

In Market no. 11 - Wholesale (physical) network infrastructure access (including shared or fully unbundled access) at a fixed location, 1 SMP operator has been identified and the following obligations imposed;

- *Obligation to provide network access*
- *Obligation of non-discrimination*
- *Obligation of transparency*
- *Obligation of accounting separation*
- *Obligation of price control*

	In Market no. 12 - Wholesale broadband access, 1 SMP operator has been identified and the following obligations imposed; *In the first group, these obligations were applied:* • *Obligation to provide network access* • *Obligation of non-discrimination* • *Obligation of transparency* • *Obligation of accounting separation* • *Obligation of price control* *In the second group, these remedies were imposed:* • *Obligation to provide network access* • *Obligation of non-discrimination* • *Obligation of transparency* *In the third group, this obligation was imposed:* • *Obligation to provide network access* *In Market no. 13 - Wholesale terminating segments of leased lines, 1 SMP operator has been identified and the following obligations imposed;* • *Obligation to provide network access* • *Obligation of non-discrimination* • *Obligation of transparency* • *Obligation of accounting separation* • *Obligation of price control* *In Market no. 14 - National market for wholesale trunk segments of leased lines, 1 SMP operator has been identified and the following obligations imposed;* • *Obligation to provide network access* • *Obligation of non-discrimination* • *Obligation of transparency* • *Obligation of accounting separation* • *Obligation of price control* *In this Market, the obligation of accounting separation will be imposed in the whole territory of Poland. Obligations of access, transparency and price control will be imposed in the territory of Poland excluding routes between areas listed in the decision. The obligation of non-discrimination, within the scope of physical access, will be imposed in the territory of Poland, excluding routes between areas listed in the decision.* *In Market no. 15 - Access and call origination on public mobile telephone networks, the NRA has not identified any SMPs.* *In Market no. 16 - The wholesale market of voice call termination on the public mobile telephone network, 8 SMP operators have been identified, and the following obligations imposed:* • *Obligation to provide network access* • *Obligation of non-discrimination* • *Obligation of transparency* • *Obligation of price control* *In Market no. 17 - The national market for international roaming services on public mobile telephone networks, the NRA has not identified any SMPs and thus remedies are not applied.* *In Market no. 18 - Broadcasting transmission, to deliver broadcast content to end users, 1 SMP operator has been identified and the following obligations imposed;* • *Obligation to provide network access* • *Obligation of non-discrimination* • *Obligation of transparency* • *Obligation of cost orientation of prices*
Slovakia	*The Slovak regulator performs market analysis in 7 relevant markets according to the 2007 EC recommendation.*

	In Market no. 1 - Access to the public telephone network at a fixed location for residential and non-residential customers, 1 SMP operator has been identified with the following obligations imposed: • *Prohibition of inappropriate preference for a particular group of end-users* • *Prohibition of unjustified bundling of services for the provision of other services and/or goods if provision of such services and/or goods can be performed separately* *In Market no. 2 - Call origination on the public telephone network provided at a fixed location, 1 SMP operator has been identified with the following obligations imposed:* • *Transparency of access* • *Non-discriminatory approach to access* • *Access to specific network facilities (obligation to provide CS/CPS, WLR)* • *Accounting separation* • *Price control (BU LRIC-PURE model + mark-up for origination rates)* *In Market no. 3 - Call termination on individual public telephone networks provided at a fixed location, 13 SMP operators have been identified and the following obligations have been imposed:* • *Transparency of access* • *Non-discriminatory approach to access* • *Access to specific network facilities* • *Price regulation: The regulator has imposed the maximum level of FTR based on BU LRIC-PURE model to all SMP operators in a Price decision* *In Market no. 4 - Wholesale (physical) network infrastructure access (including share of fully unbundling access) at a fixed location, 1 SMP operator has been identified with the following obligations imposed:* • *Transparency of access* • *Non-discriminatory approach to access* • *Accounting separation* • *Access to specific network facilities* • *Regulation of prices for access and co-location* *In Market no. 5 - Wholesale broadband access, 1 SMP operator has been identified with the following obligations imposed:* • *Transparency of access* • *Non-discriminatory approach to access* • *Accounting separation* • *Access to specific network facilities* • *Regulation of prices* *In Market no. 6 - Wholesale terminating segments of leased lines, 1 SMP operator in the segment of speed up to 2 Mbps. In the segment of speed above 2 Mbps there is effective competition. The following obligations imposed in the segment up to 2Mbps;* • *Transparency of access* • *Non-discriminatory approach to access* • *Accounting separation* • *Access to specific network facilities* • *Regulation of prices for terminating leased lines and for co-location* *In Market no. 7 - Voice call termination on individual mobile networks, 3 SMP operators have been identified and the following obligations have been imposed:* • *Transparency of access* • *Non-discriminatory approach to access* • *Access to specific network facilities* • *Regulation of prices: RU has imposed the maximum level of MTR based on BU LRIC-PURE model to all SMP operators in a price decision* *The Slovak NRA applies price control on 6 markets. On the call origination and termination markets they apply pure bottom-up LRIC. In the wholesale market for infrastructure access they apply mainly BU-LRIC except for co-location which uses LRAIC and Activity Based Costing. The*

	wholesale market for leased lines uses fully allocated historic cost, except for co-location which uses LRAIC and ABC
Sweden	*The Swedish NRA performs market analysis in the 7 relevant markets indicated by the EC 2007 Recommendation.* *In Market no. 1 - Access to the public telephone network at a fixed location for residential and non-residential customers, 1 SMP operator has been identified with the following obligations imposed:* • *Obligation to provide wholesale line rental* • *Price control and cost accounting procedures* • *Non-discrimination obligation* *In Market no. 2 - Call origination on the public telephone network provided at a fixed location, 1 SMP operator has been identified with the following obligations imposed:* • *Transparency of access* • *Price control – cost orientation* • *Non-discrimination* *In Market no. 3 - Call termination on individual public telephone networks provided at a fixed location, 24 SMP operators have been identified and the following obligations imposed:* • *Transparency of access* • *Specific obligation for the incumbent,, is the cost orientation of price, other operators shall keep a fair and reasonable price* *In Market no. 4 - Wholesale (physical) network infrastructure access at a fixed location, 1 SMP operator has been identified with the following obligations imposed:* • *Access obligation* • *Transparency* • *Non-discrimination* • *Accounting separation* • *Cost based pricing* *In Market no. 5 - Wholesale broadband access, 1 SMP operator has been identified with the following obligations imposed:* • *Access obligation* • *Transparency* • *Non-discrimination* • *Accounting separation* • *Cost based pricing* *In Market no. 6 - Wholesale terminating segments of leased lines, 1 SMP operator has been identified with the following obligations imposed:* • *Access obligation* • *Transparency* • *Non-discrimination* • *Accounting separation* • *Cost based pricing* *In Market no. 7 - Voice call termination on individual mobile networks, SMP operators have been identified and the following obligations have been imposed:* • *Access obligation* • *Transparency* • *Non-discrimination* • *Accounting separation* • *Cost based pricing* *The regulator applies price control on 2 markets. For wholesale broadband access, a BU-LRIC model is used, and for wholesale leased lines, historic cost accounting and fully distributed costs are used.*

Universal Services Directive: Introduction of number portability and the single European Emergency Call number 112

EU member state	**Fixed number portability** ***(extracts from the EaP benchmarking report December 2014 and CEPT Implementation Report on NP[18])***	**Mobile number portability** ***(extracts from the EaP benchmarking report December 2014 and CEPT Implementation report on NP)***	**Emergency call number 112 (extracts from EC Working Document on Implementation of the European Emergency Number[19]**
Czech Republic	*Since 2003* *4 business days* *Complies with 11 out of 12 NP best practices*	*Since 2006* *4 business days* *Complies with 11 out of 12 NP best practices*	*112 is the Single emergency number in Denmark, Finland, Malta, Romania, the* *Netherlands and Sweden.* *In Member States where 112 is not the single emergency number above 50% of the calls were directed to 112 in Bulgaria, Estonia, Ireland, Lithuania, Luxembourg, and Spain.* *Most member states have alternative means to voice as measures to provide access to emergency services: SMS as an alternative means of access to emergency services is available in 18 Member states Austria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Greece, Ireland, Italy, Latvia, Luxembourg, Malta, Portugal, Slovenia, Spain, Sweden, United Kingdom.*
Poland	*Since 2004* *24 hours max* *Complies with 11 out of 12 NP best practices*	*Since 2006* *24 hours max* *Complies with 12 out of 12 NP best practices*	
Romania	*Since 2008* *3.8 days* *Complies with 11 out of 12 NP best practices*	*Since 2008* *2.8 days* *Complies with 11 out of 12 NP best practices*	
Slovakia	*Since 2005* *4 days max* *Complies with 9 out of 12 NP best practices*	*Since 2005* *4 days max* *Complies with 9 out of 12 NP best practices*	
Sweden	*Since 1999* *Average of 9 days* *Complies with 12 out of 12 NP best practices*	*Since 2001* *Average of 9 days* *Complies with 12 out of 12 NP best practices*	

[18] http://www.cept.org/files/5466/documents/Number%20Portability%20Impementation%20in%20Europe%20-%20based%20on%20a%20survey%20of%20CEPT%20member%20countries%20-%20March%202014.pdf

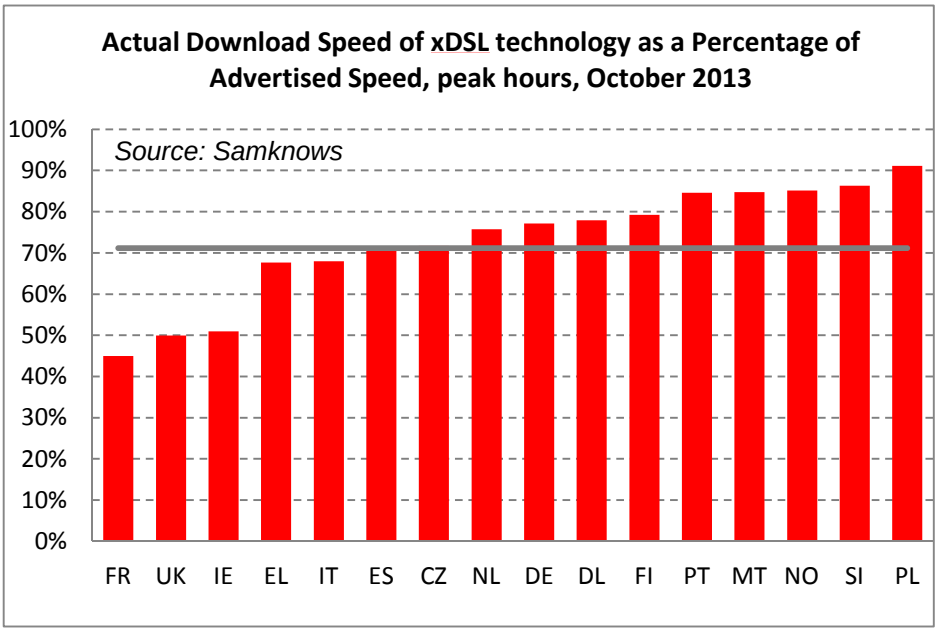
[19] http://ec.europa.eu/digital-agenda/en/news/implementation-european-emergency-number-112-%E2%80%93-results-seventh-data-gathering-round

Universal Services Directive: Effective measures for ensuring quality of service in a broadband environment, taking account also the context of net-neutrality

EU member state	Description
EU level	*In May 2010 the European Commission published its five year plan for the digital economy 'A Digital Agenda for Europe'. One of the seven goals of the Digital Agenda is to provide fast internet access (approximating to a download speed of 30 Mbps or more) to all Europeans before the end of the decade. The Digital Agenda does not define a speed for basic broadband. Most national broadband targets aim for basic broadband speeds within the next few years, although speeds are not always defined. Several member states have chosen to include basic broadband services within the scope of their universal service obligation. The following examples show the broadband coverage targets set in selected countries.* *A few Member States have decided to extend their universal service obligations to include basic broadband (from 144kbps up to 1 and 4 Mbps). This is the case in Belgium, Croatia, Finland, Latvia (only for disabled users), Malta, Romania, and Spain; in preparation in Slovenia.*
Czech Republic	*100% of households covered with >=30Mbps by 2020* *50% with 100Mbps by 2020*
Lithuania	*2015: 20% of households subscribed to at least 100Mbps* *2015: 80% of households covered with >=30Mbps* *2020: 50% of households subscribed to at least 100Mbps* *2020: 95% of households covered with >=30Mbps*
Poland	*100% of households covered with >=30Mbps by 2020*
Slovakia	*100% of households covered with >=30Mbps by 2020*
Sweden	*2013: 55% with 100 Mbps* *90% of households covered with >=30Mbps by 2020*
All	*EU research in 201220 showed that, on average, EU consumers receive 74% of the advertised headline speed they have paid for. xDSL based services achieved only 63.3% of the advertised headline download speed, compared to 91.4% for cable and 84.4% for FTTx. There are significant differences in the European national markets, most likely due to advertising practices.* *In 2013, the updated research[21] showed that;* *The actual download speed is 75.6% of the advertised speed;* • *Both advertised and actual speeds have increased since 2012. The average advertised download speed across all countries was 38.50 Mbps during peak hours, compared to 30.37 Mbps of actual speed;* • *Average actual download speeds have has increased by almost 10Mbps since March 2012;* • *Differences are small in cable, large in xDSL: xDSL based services achieved only 63.8% of the advertised headline download speed, compared to 89.5% for cable and 82.7% for FTTx Results are based on peak time performance, which is defined as weekdays 7:00pm to 11:00pm*

[20] http://ec.europa.eu/digital-agenda/en/news/quality-broadband-services-eu-march-2012

[21] http://ec.europa.eu/digital-agenda/en/news/quality-broadband-services-eu-samknows-study-internet-speeds-second-report

	(inclusive). 

Commission Recommendation 2009/396/EC on the Regulatory Treatment of Fixed and Mobile Termination Rates in the EU: Adopt measures to impose price control and cost-accounting on the markets for wholesale voice call termination on individual public telephone networks based on the costs incurred by an efficient operator, using current cost and a bottom-up modelling approach with long-run incremental costs (LRIC) as the relevant cost methodology.

EU member state	**Description** **Mobile termination rates (Eurocents/ minute)** **(Source: BEREC January 2014 Snapshot "Integrated Report on Mobile Termination Rates, Fixed Termination Rates & SMS Termination Rates" BoR (14) 85**	
Market	<u>Mobile call termination rates (Eurocents/min)</u> 34 country weighted average is **1.1316** (EU28 +Switzerland, Iceland, FYR Macedonia, Norway, Serbia, Vatican)	<u>Fixed call termination rates (Eurocents/min)</u> Layer 1 = local level service provision (average = **0.41**) Layer 2 = regional level service provision (single transit) (average = **0.47**) Layer 3 = national level service provision (or double transit) (average = **0.64**)
Czech Republic	*T-Mobile (market share 39.14%)* ***1.0128*** *Telefónica (market share 37.34%)* ***1.0128*** *Vodafone (market share 23.41%* ***1.0128*** *Air Telecom (market share 0.11%* ***1.0128***	*Telefónica Czech Republic a.s.* *Layer 1: 1.1254 (peak) 0.5627 (off peak)* ***0.8440*** *(total)* *Layer 2: 1.2754 (peak) 0.6377 (off peak)* ***0.9566*** *(total)*
Lithuania	*Bitė Lietuva (market share 22.41%)* ***1.0426*** *Tele2 (market share 40.99%)* ***1.0426***	*TEO LT, AB* *Layer 3: 0.6111 (peak) 0.6110 (off peak)*

	Omnitel (market share 34.70%) ***1.0426***	***0.6111****(total)*
Poland	*T-Mobile Polska (market share 29.30%)* ***1.0250*** *Polkomtel (market share 25.65%)* ***1.0250*** *PTK Centertel (market share 27.60%)* ***1.0250*** *P4 (Market share 16,10%)* ***1.0250***	*TPSA* *Layer 1: 0.6572 (peak) 0.3298 (off peak)* ***0.4935*** *(total)* *Layer 2: 0.7823 (peak) 0.3900 (off peak)* ***0.5861*** *(total)* *Layer 3: 1.1506 (peak) 0.5753 (off peak)* ***0.8630*** *(total)*
Slovakia	*Orange (market share 45.48%)* ***1.2260*** *Slovak Telekom (market share 29.96%)* ***1.2260*** *Telefónica (market share 24.56%)* ***1.2260***	*Slovak Telekom* *Layer 1: 0.1234 (peak) 0.1234 (off peak)* ***0.1234*** *(total)* *Layer 2: 0.1234 (peak) 0.1234 (off peak)* ***0.1234*** *(total)* *Layer 3: 0.1234 (peak) 0.1234 (off peak)* ***0.1234*** *(total)*
Sweden	*TeliaSonera (market share 41.04%)* ***1.0161*** *Tele2 (market share 32.05%)* ***1.0161*** *Telenor (market share 16.87%)* ***1.0161*** *Hi3G (market share 10.04%)* ***1.0161***	*TeliaSonera* *Layer: 1 0.0745 (peak) 0.0745 (off peak)* ***0.0745*** *(total)* *Layer: 2 0.1208 (peak) 0.1208 (off peak)* ***0.1208*** *(total)*

LEGAL ENABLERS – EU EXAMPLES

All defined EU Directives in the 2009 package: Clear date defined for alignment of primary legislation

EU member state	**Description** ***(extracts from the EaP benchmarking report December 2014)***
Czech Republic	*The Electronic Communications Law was introduced in 2005 as Act No. 127/2005 Coll. on Electronic Communications and on Amendment to Certain Related Acts. In the Act, the 2003 EU regulatory framework was transposed into national legislation. The 2009 EU framework was transposed into Czech law through the Act. No. 468/2011 Coll. amending Act No. 127/2005. Other EU regulatory frameworks concerning information society and electronic communications have also been considered.*
Lithuania	*The Electronic Communications Law was introduced on 1 May 2004. The 2003 and 2009 EU regulatory frameworks were considered and are transposed into current legislation. Other EU regulatory frameworks concerning the information society were also considered in national legislation, namely in the areas of electronic signature and data protection. In May 2014 new requirements for time marking services started to be applicable. Revision of Lithuanian legal acts was started in order to align them with new regulation of electronic identification and trust services such as e-Signature Directive 1999/93/EC which is repealed with effect from 1 July 2016- Regulation (EU) No 910/2014 of the European Parliament and the Council of 23 July 2014 electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.*
Poland	*Poland introduced the Electronic Communications Law in 2004, transposing the 2003 EU regulatory framework into national legislation. The 2009 EU framework was considered in the current legislation. Other EU frameworks in the area of electronic communications have not been considered.*
Romania	*The Electronic communication law dates from 2002. Following the adoption of the 2009 framework, Romania brought in 2011 a current version of Electronic communication law through incorporating Government Emergency Ordinance No. 111/2011 on electronic communications, with the subsequent amendments and completions.*
Slovakia	*In 2013 a new Act no. 402 on the Regulatory Authority for Electronic Communications and Postal Services and on the Transport Authority and on Amendment of Particular Acts was adopted which incorporates the EU 2009 regulatory framework. Before that Electronic Communications Law was introduced in 2011 (and cancelled the previous one that had been in force since 2004). The 2003 EU regulatory framework was transposed into national law in effect by 1 January 2004. During the preparation of the current legislation, the 2009 EU regulatory framework, as well as other regulatory frameworks (on e-commerce, electronic signature and data protection), were considered and transposed.*
Sweden	*The Electronic Communications Law was introduced in 2003. The 2003 and 2009 EU regulatory frameworks were transposed into national legislation, as well as other regulatory directives in the area of electronic communications.*

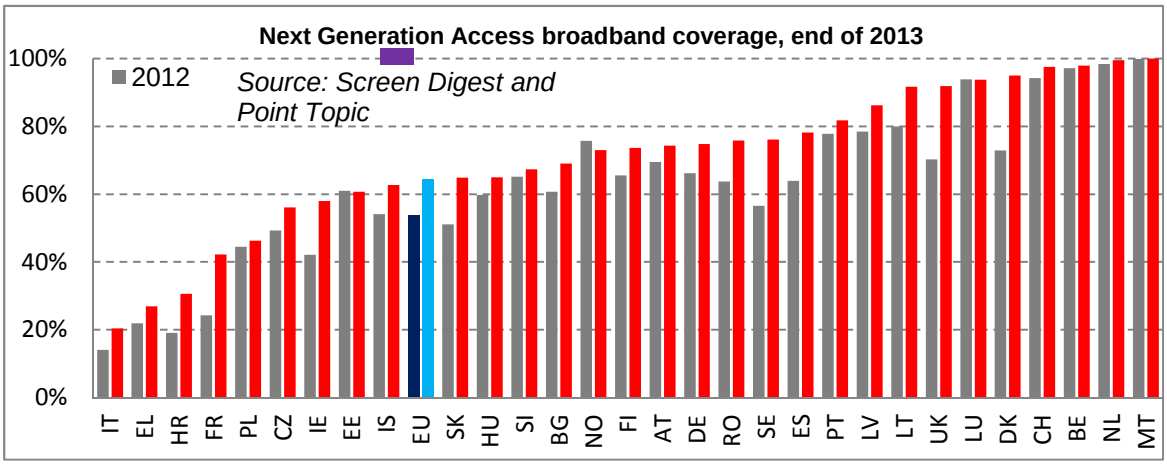
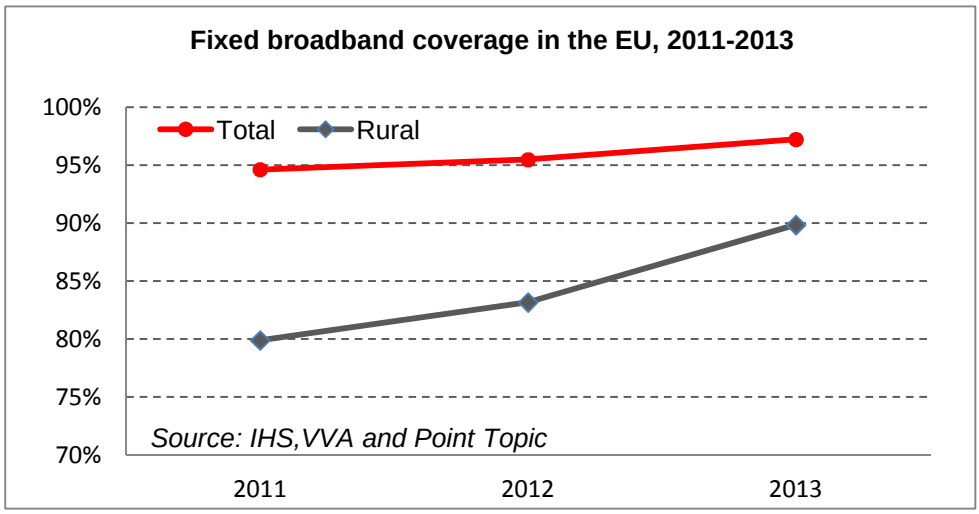
European recommendations and decisions on spectrum and broadband: Clear date defined for alignment of primary legislation

EU member state	Description *(extracts from the EaP benchmarking report December 2014)*
Czech Republic	*Frequency allocation and preparation and approval of the national frequency plan are primarily the responsibility of the Ministry of Trade and Industry, which cooperates with the NRA - CTU. The assignment of frequencies is performed by the Spectrum management department of the CTU. The frequency assignment methods used are beauty contest and financial bidding (auction). CTU in the Radio Spectrum Utilisation Plan (RSUP) determines the way and conditions of radio spectrum utilisation by radiocommunication services. The Plan is based on Plan of Frequency Bands Allocation and consists of common part and parts for particular frequency bands.* *Spectrum trading is allowed but under certain conditions. Legal framework for spectrum trading is regulated at national level according to the Act No. 127/2005 Coll., on electronic communications and on amendment to certain related acts (the Electronic Communications Act, hereinafter only Act). The relevant rules in the Act are based on Framework Directive 2002/21/EC and Authorisation Directive 2002/20/EC, both amended by Directive 2009/140/EC. Restrictions for the SMP are that tradability of spectrum rights assigned in auction 2013 is restricted for 7 years.* *On the basis of the Act No. 127/2005 Coll., the holders of authorization to use of radio frequencies shall pay the annual fees for the use of radio frequencies. The method of calculation of the charges for the use of radio frequencies and numbers are set down in Government decree No. 154/2005, as amended. The spectrum fees are paid by both commercial subjects and governmental bodies. The fees form a part of state budget.* *Czech Republic used in 2013 frequency allocation through the simultaneous multiple round auctions. During the auction some of the rules must be met as in 1800 MHz band Spectrum Cap 2x23 MHz in order to reserve the contiguous block 2x15.8 MHz for a newcomer (i.e. 2x9 MHz available for existing operators). In 900 MHz frequency band 2x10 MHz band must be reserved for a possible newcomer. Spectrum Cap applied also in the 2.6 GHz as max. of 2x20 MHz in the FDD band, 15 MHz in the TDD band. In the future, CTU will assign vacant frequencies through the auction of 1800 and 2600 MHz bands.*
Lithuania	*The NRA is responsible for the allocation and assignment of frequencies, and also for the preparation of the national frequency allocation plan. Frequencies are assigned using the beauty contest method. Frequency fees must be paid by operators as commercial subjects. Spectrum fee is calculated on cost of spectrum management and monitoring. Spectrum fee is received by the state budget. Under consideration is reallocation of broadcasting form 694- 790 MHz band.* *In Lithuania, NRA used auctions as the method of frequency assignment for 800 MHz in 2013 and 2.5 GHz in 2014. The SMRA as an auction format has been used with the reserved price 25 000LTL (7240 EUR) -1 000 000 LTL (289 620 EUR) per 5MHz block. One frequency band 450-470 remains unlicensed. In Lithuania, spectrum trading is allowed expect spectrum for broadcasting and governmental usage.*
Poland	*The final act of the national frequency allocation table is issued by the Council of Ministers of the Republic of Poland. The governmental bodies that have the largest responsibility are the Ministry of Administration and Digitalisation, the Ministry of the Interior, the Ministry of National Defence and the Office of Electronic Communications (NRA). The preparation and approval of the national frequency plan is the responsibility of the NRA. The assignment of frequencies for civil purposes is*

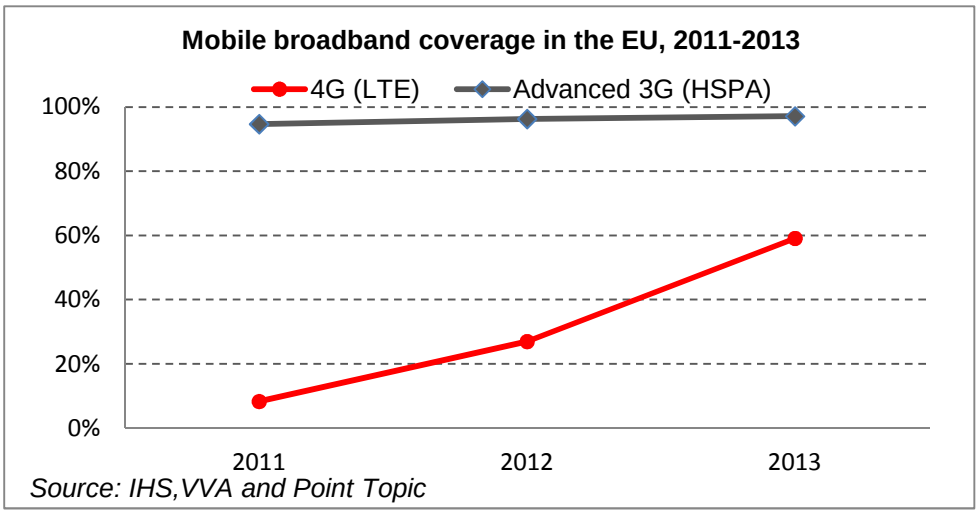
	within the authority of the NRA, while for military purposes there is a special authority, the NARFA POL. In Poland, frequencies were so far assigned only using the method of beauty contest. The first auction is planned to be organised in 2013.
Romania	*The regulator (ANACOM) is responsible for frequency allocation and assignment. Together with relevant ministry ANCOM is responsible for preparation and approval of the national frequency plan. There has been 1 block in 800 MHz and 8 blocks in 2600MHz band which remain un-awarded. ANACOM have already used auction as the method of frequency assignment for certain frequencies in September 2012 for the 800, 900, 1800 and 2600 MHz bands.* *The format of auction was multi-round ascending. During the auction, 1 bidder could acquire usage rights below 1GHz with the width 2x20 MHz.* *The minimum price (reserve price) has been set according to Government Decision no.605/13.06.2012 as follows: in 800 MHz band in the amount of EUR 35 million/2x5 MHz; in 900 MHz band in the amount of EUR 40 million/2x5 MHz; in 1800 MHz band in the amount of EUR 10 million/2x5 MHz; in2600 MHz band in the amount of EUR 4 million/2x5 MHz and EUR 3 million/1x15 MHz. The use of auction as a form of frequency assignment will be used in the future.* *The spectrum trading is allowed according to Art. 35 of the GEO, No. 111/2011. The usage rights may be transferred to a third party, in total or in part, only based on the prior ANCOM approval. The transfer of the usage rights shall not result in competition constraints, hindering or distortion. In cases where the use of radio frequencies is harmonised at the European level, the transfer of the usage rights must not lead to changing the usage destination of the frequencies that are subject to the licence in such a way as to breach this harmonised usage. In case of a partial transfer of the rights in 800 MHz, 900 MHz, 1800 MHz and 2600 MHz, the licence holder may only transfer 5 MHz blocks, with all the obligations associated with or, for the TDD operation mode in 2600 MHz, only in compact unpaired blocks of 15 MHz.* *The spectrum fees are paid on year-to-year basis and calculation are based on a number of parameters (frequency range, number of blocks, radio channel, number of transmitters, e.i.r.p. etc.), according to ANCOM President's Decision no.551/2012, with the subsequent amendments and completions. The spectrum fees are received by NRA and the Parliament approves their budget.*
Slovakia	*In Slovakia, the regulator cooperates with the Ministry of Transport, Construction and Regional Development in elaboration of the draft of the national table of the frequency spectrum, preparing the plan of use of the frequency spectrum, assigning frequencies and laying down conditions for the use of frequencies and coordinating and checking the use of the frequency spectrum. In Slovakia is frequency trading between market participants allowed. The only restriction used during the auction is spectrum cap of 20 MHz for 800 MHz and 40 MHz for 1800 MHz. For one block of 2x5 MHz the reserve price in 800MHz was set in the amount if 19 000 EUR, in 1800 MHz 2 200 000 EUR and in 2600MHz was the price 1 100 000 EUR. The next auction is planned for frequency assignment in 2015.* *The last auction in 2013 was realized to use frequencies from the 800 MHz, 1800 MHz, and 2600 MHz frequency bands together as one amount where SMPs gain the following frequencies. WIFI 2400 MHz band stayed unlicensed.*

INFRASTRUCTURE ENABLERS: EU EXAMPLES

"Digital Agenda" targets: Clearly defined targets for achievement of universal fast broadband access and take-up

EU member state	Description *(Extracts from EU digital scorecard 2014[22])*
All	***Access targets:*** • ***EU Basic broadband for all by 2013: achieved 100% in 2013*** • ***Fast broadband (>30Mbps) for all by 2020: achieved 62% in 2013***  

[22] https://ec.europa.eu/digital-agenda/en/news/scoreboard-2014-progress-report-digital-agenda-targets-2014

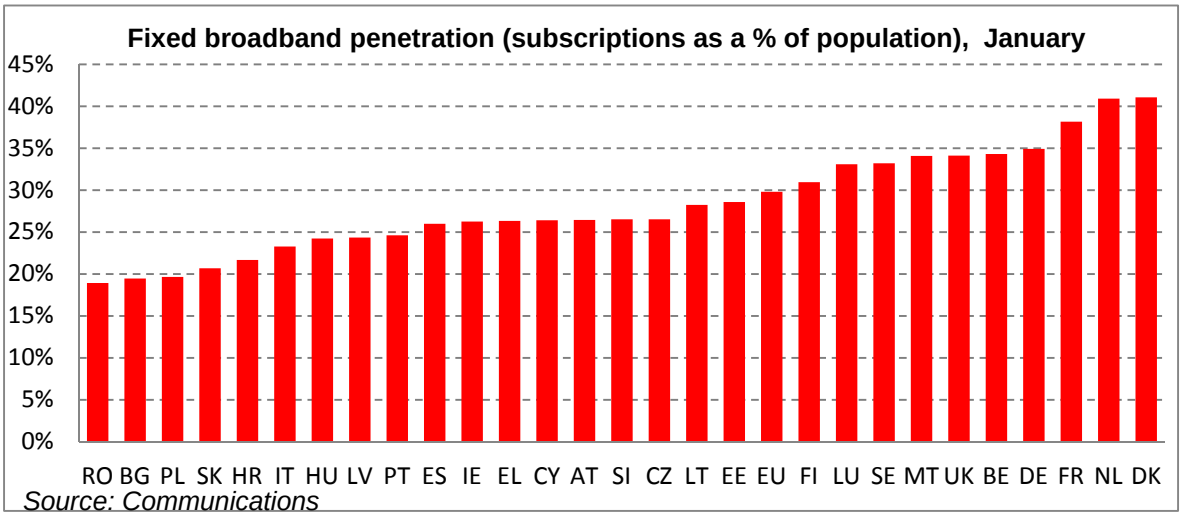
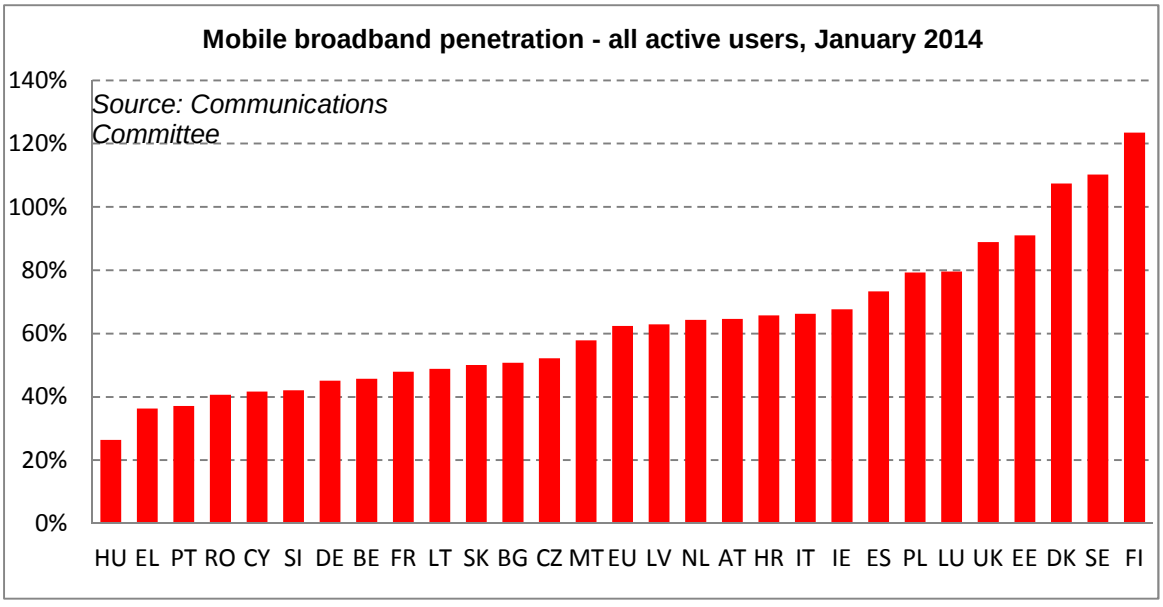


Source: IHS,VVA and Point Topic

SERVICES ENABLERS: EU EXAMPLES

Penetration (take-up) of fixed broadband services: Actual achievement (latest results)

Penetration (take-up) of mobile broadband services: Actual achievement (latest results)

EU member state	Description *(Extracts from EU digital scorecard 2014[23])*
All	 *Source: Communications Committee* 

[23] https://ec.europa.eu/digital-agenda/en/news/scoreboard-2014-progress-report-digital-agenda-targets-2014

3 ACHIEVEMENTS, GAPS AND ROADMAPS OF THE PARTNER COUNTRIES RELEVANT TO THEIR ASSOCIATION AGREEMENTS

Mapping of achievements, gaps and actions per country for the Partner Countries that have signed an Association Agreements of the DCFTA with the EU.

Network, information and cyber security

Georgia – achievements, gaps and recommendations relevant to the Association Agreement

Achievements according to the related topics of the country's Association Agreement / DCFTA	Major gaps	Main recommended actions (priority areas for cooperation)
- Article 14 Protection of personal data: The Parties agree to cooperate in order to ensure a high level of protection of personal data in accordance with the EU, Council of Europe and international legal instruments and standards referred to in Annex I to this Agreement. Annex I "Each Party shall, in the context of the implementation of this or other Agreements, ensure a legal level of data protection which at least corresponds to that set out in ***Directive 95/46/EC*** of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, as well as the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed on 28 January 1981 (ETS No. 108) and the Additional Protocol thereto, regarding Supervisory Authorities and Transborder Data Flows, signed on 8 November 2001 (ETS No. 181). Where relevant, each party shall take into account Council ***Framework Decision 2008/977/JHA*** of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, and Recommendation No R (87)15 of 17 September 1987 of the Committee of Ministers of the Council of Europe Regulating the Use of Personal Data in the Police Sector." ***- Article 118 Data processing***: 2. Each Party shall adopt adequate safeguards for the protection of privacy and fundamental rights, and freedom of individuals, in particular with regard to the transfer of personal data. ***- Chapter 8 Cooperation in the field of information society, Article 324:*** The Parties shall promote cooperation on the development of the Information Society to benefit citizens and businesses through the widespread availability of information and communication technologies (ICT) and through better quality of services at affordable prices. Cooperation will cover, inter alia, (a) exchange of information and best practices on the implementation of national information society initiatives, including, inter alia, those aiming at improving network security, developing public online services; ***Article 325*** Cooperation will cover, inter alia, the exchange of information and best practices on the implementation of national information society initiatives, including, inter alia, those aiming at promoting broadband access, improving network security and developing public online services***;*** ***- Annex XV-B Rules applicable to telecommunication services:*** Within three years, Georgia will carry out approximation of its legislation the Directive 2002/58/EC of the		

European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009. The approximation will include: implementing regulation to ensure protection of fundamental rights and freedoms, in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and ensuring the free movement of such data and of electronic communication equipment and services; ***- Article 111 Confidentiality of information***: Each Party shall ensure the confidentiality of electronic communications and related traffic data by means of a public communication network and publicly available electronic communication services without restricting trade in services. ***- Article 17 The fight against organised crime and corruption***: The Parties shall cooperate on combating and preventing criminal and illegal activities, in particular transnational activities, organised or otherwise, such as, *inter alia*, (g) ***cybercrime***. - Aspects of ***Framework Directive (Directive 2002/21/EC*** (Articles 13a and 13b) on a common regulatory framework for electronic communications networks and services) – establishes a common regulatory framework for the security and integrity of electronic communications networks and services.		
Progress in aligning with AA provisions, e.g. ***Article 14 Protection of personal data, Article 118 Data processing Chapter 8 Cooperation in the field of information society, Article 111Confidentiality of information***	- Protection of personal data and privacy - Confidentiality of electronic data	- Further align with ***Directive 2002/58/EC*** (as amended by Directive 2009/136/EC) to ensure protection of fundamental rights and freedoms, in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and ensuring the free movement of such data and of electronic communication equipment and services (before 2018) - Ensure alignment with a Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union (COM/2013/048 final - 2013/0027) - Ensure alignment with a Proposal for a Directive of 2010 (COM (2010) 517 final) on attacks against information systems - Continue cooperation under the Twinning programme to implement best EU policies and practices in

		Network and information security

Georgia - additional gaps and recommendations

Main achievements according to the EU baseline	Major gaps	Main recommended actions (priority areas for cooperation)
- Aspects of the ***Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*** (7/2/2013) and a *Proposal for a Directive* of the European Parliament and of the Council (part of a Joint Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions of 7.2.2013) – setting out principles for cyber security; presenting an EU's comprehensive vision on how best to prevent and respond to cyber disruptions and attacks; demonstrating a clear mandate to ensure that the digital economy can safely grow and the European values of freedom and democracy are protected; defining measures to ensure a high common level of network and information security across the Union; proposing to establish legally binding common minimum requirements for NIS at national level including the designation of national competent authorities for NIS, establishment of a well-functioning CERT, adoption of a national NIS strategy and a national NIS cooperation plan. Aspects (Articles 13a and 13b in page 55) of the Framework Directive (Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services as amended by ***Directive 2009/140/EC*** and ***Regulation 544/2009***) contain security risk management and incident reporting requirements for electronic communications operators ***- Policy recommendations of the European Network and Information Security Agency (ENISA)*** – make critical information infrastructure (CII) an integral part of a national social and economic policy agenda; helps empower CERTs with more authority to require telecom service providers and ISPs to implement security measures and changes; defines security measures and incident reporting procedures. - Aspects of the ***Commission's Communication on Critical Information Infrastructure protection (CIIP)*** – defines policy measures and criteria for European critical information infrastructure for being prepared to prevent, detect, respond and mitigate disruptions, as well as to recover from them; makes international cooperation an integral part of the overall CIIP policy. - Aspects of the ***Regulation No 910/2014 on electronic identification and trust services*** for electronic transactions in the EU internal market: establishing minimum security requirements applicable to trust services **-** Aspects of the ***Commission's Communications on CIIP***: COM(2009) 149 and COM(2011) 163		
- Good progress in aligning with the provisions of the ***Cybercrime***	- Legal and regulatory framework - National cyber security law	- Fully align with the above EU legislation, especially with ***Cybersecurity Strategy of the European Union: An Open, Safe***

Convention	and strategy - Transparency in reporting on security incidents - Public awareness raising - CERT services including Cyber attack simulation - Protection of personal data and privacy - Public/Private sector critical infrastructures	***and Secure Cyberspace*** (7/2/2013) and a ***Proposal for a Directive*** and other relevant laws and regulations, ***Commission's Communication on Critical Information Infrastructure Protection (CIIP)***

Moldova – achievements, gaps and recommendations relevant to the Association Agreement

Achievements according to the related topics of the country's Association Agreement / DCFTA	Major gaps	Main recommended actions (priority areas for cooperation)
- Article 13 Protection of personal data: The Parties agree to cooperate in order to ensure a high level of protection of personal data in accordance with EU, Council of Europe and international legal instruments and standards. Any processing of personal data shall be subject to the legal provisions referred to in Annex I to this Agreement, which reads as follows: 1. The Parties shall, in the context of the implementation of this or other Agreements, ensure a legal level of data protection which at least corresponds to that set out in ***Directive 95/46/EC*** of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, ***Council Framework Decision 2008/977/JHA*** of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, as well as the ***Convention for the Protection of*** **Individuals with regard to Automatic Processing of Personal Data**, signed on 28 January 1981 (ETS No 108) and its ***Additional Protocol, regarding Supervisory Authorities and Transborder Data Flows***, signed on 8 November 2001 (ETS No 181). Where relevant, the Parties shall take into account ***Recommendation No. R (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe Regulating the Use of Personal Data in the Police Sector***. 2. In addition, the following principles shall apply: (a) both the transferring authority and the receiving authority shall take every reasonable step to ensure, as appropriate, the rectification, erasure or blocking of personal data where the processing does not comply with the provisions of Article 13 of this Agreement, in particular because those data are not adequate, relevant, or accurate, or because they are excessive in relation to the purpose of processing. This includes the notification of any rectification, erasure or blocking to the other		

Party; (b) upon request, the receiving authority shall inform the transferring authority of the use of the transferred data and of the results obtained there from; (c) personal data may only be transferred to the competent authorities. Further transfer to other authorities requires the prior authorisation of the transferring authority; (d) the transferring and the receiving authorities are under an obligation to make a written record of the communication and receipt of personal data. ***- Chapter 8 Cooperation in the field of information society, Article 102, and Annex XXVIII-B Rules applicable to telecommunication services***: Within three years, Moldova will carry out approximation of its legislation the ***Directive 2002/58/EC*** of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (***Directive on privacy and electronic communications***) as amended by ***Directive 2009/136/EC*** of the European Parliament and of the Council of 25 November 2009. The approximation will include: implementing regulation to ensure protection of fundamental rights and freedoms, in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and ensuring the free movement of such data and of electronic communication equipment and services. ***- Chapter 8 Cooperation in the field of information society, Article*** *99* Cooperation on exchanging information and best practices on, inter alia, initiatives aiming at promoting broadband access, improving network security and developing public services online; ***- Article 238*** **Confidentiality of information:** Each Party shall ensure the confidentiality of electronic communications and related traffic data by means of a public communication network and publicly available electronic communication services without restricting trade in services. ***- Article 197*** **Customs cooperation:** (d) exchange, where appropriate, information and data subject to respect of the confidentiality of data and standards and regulations on protection of personal data. ***- Article 245*** **Data processing** 2. Each Party shall adopt adequate safeguards for the protection of privacy and fundamental rights and freedoms of individuals, in particular with regard to the transfer of personal data. ***- Article 16*** **Preventing and combating organised crime, corruption and other illegal activities**: The Parties shall cooperate on preventing and combating all forms of criminal and illegal activities, organised or otherwise, including those of a transnational character, such as: cyber crime.		
- Progress in aligning with some AA provisions, e.g. ***Article 13 Protection of personal data, Chapter 8 Cooperation in the field of information society, Article 238 Confidentiality of information, Article 245***	- Protection of personal data and privacy - Confidentiality of electronic data	- Further align with Directive 2002/58/EC (as amended by Directive 2009/136/EC) to ensure protection of fundamental rights and freedoms, in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and ensuring the free movement of such data and of electronic communication equipment and services

Data processing		(before 2018) - Ensure alignment with a Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union (COM/2013/048 final - 2013/0027) - Ensure alignment with a Proposal for a Directive of 2010 (COM (2010) 517 final) on attacks against information systems

Moldova - additional gaps and recommendations

Main achievements according to the EU baseline	Major gaps	Main recommended actions (priority areas for cooperation)
- Aspects of the ***Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*** (7/2/2013) and a *Proposal for a Directive* of the European Parliament and of the Council (part of a Joint Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions of 7.2.2013) – setting out principles for cyber security; presenting an EU's comprehensive vision on how best to prevent and respond to cyber disruptions and attacks; demonstrating a clear mandate to ensure that the digital economy can safely grow and the European values of freedom and democracy are protected; defining measures to ensure a high common level of network and information security across the Union; proposing to establish legally binding common minimum requirements for NIS at national level including the designation of national competent authorities for NIS, establishment of a well-functioning CERT, adoption of a national NIS strategy and a national NIS cooperation plan. - Aspects (Articles 13a and 13b in page 55) of the Framework Directive (Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services as amended by ***Directive 2009/140/EC*** and ***Regulation 544/2009***) contain security risk management and incident reporting requirements for electronic communications operators. ***- Policy recommendations of the European Network and Information Security Agency (ENISA)*** – make critical information infrastructure (CII) an integral part of a national social and economic policy agenda; helps empower CERTs with more authority to require telecom service providers and ISPs to implement security measures and changes; defines security measures and incident reporting procedures. - Aspects of the ***Regulation No 910/2014 on electronic identification and trust services*** for electronic transactions in the EU internal market: establishing minimum security requirements applicable to trust services. ***-*** Aspects of the ***Commission's Communication on Critical Information Infrastructure***		

protection (CIIP) – defines policy measures and criteria for European critical information infrastructure for being prepared to prevent, detect, respond and mitigate disruptions, as well as to recover from them; makes international cooperation an integral part of the overall CIIP policy. **-** Aspects of the ***Commission's Communications on CIIP***: COM(2009) 149 and COM(2011) 163.		
- Good progress in aligning with the provisions of the ***Cybercrime Convention***	- Legal and regulatory framework - National cyber security law and strategy - Transparency in reporting on security incidents - Public awareness raising - CERT services including Cyber attack simulation - Protection of personal data and privacy - Public/Private sector critical infrastructures	- Fully align with the above EU legislation, especially with ***Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*** (7/2/2013) and a ***Proposal for a Directive*** and other relevant laws and regulations, ***Commission's Communication on Critical Information Infrastructure Protection (CIIP)***

Ukraine – achievements, gaps and recommendations relevant to the Association Agreement

Achievements according to the related topics of the country's Association Agreement / DCFTA	Major gaps	Main recommended actions (priority areas for cooperation)
- ***Article 15 Protection of personal data***: The Parties agree to cooperate in order to ensure an adequate level of protection of personal data in accordance with the highest European and international standards, including the relevant Council of Europe instruments. Cooperation on personal data protection may include, inter alia, the exchange of information and of experts. **-** ***Article 122 Confidentiality of information*****:** Each Party shall ensure the confidentiality of electronic communication and related traffic data by means of a public electronic communication network and publicly available electronic communication services without		

restricting trade in services.

- *Article 129 Data processing*: 1. Each Party shall permit a financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier. 2. Each Party shall adopt adequate safeguards for the protection of privacy and fundamental rights and the freedom of individuals, in particular with regard to the transfer of personal data.

- *Chapter 14 Information society, Article 389*: The Parties shall step up cooperation on the development of the Information Society to benefit citizens and businesses through the widespread availability of Information and Communication Technology (ICT) and through better quality of services at affordable prices. This cooperation will also facilitate the access to the markets for electronic communication services, encouraging competition and investment in the sector. ***Article 390***: Cooperation shall aim at implementing national Information Society strategies, developing of a comprehensive regulatory framework for electronic communications, and increasing Ukraine's participation in the ICT research activities of the EU. Cooperation shall cover, inter alia, (a) improvement of network security and more widespread use of ICT by citizens, business and administrations by developing local content for the Internet and introducing online services, in particular e-business, e-government, e-health and e-learning. ***Article 394***: The Parties shall promote gradual approximation to the EU law and regulatory framework in the sphere of information society and electronic communication.

- *Annex XLIII to Title VI, Article 9 Confidentiality*: Information communicated or acquired in any form under this Annex shall be covered by professional secrecy and protected in the same way as similar information is protected by Ukrainian law and by the corresponding provisions applicable to the EU institutions. Such information may not be communicated to persons other than those in the EU institutions, in the Member States or in Ukraine whose functions require them to know it, nor may it be used for purposes other than to ensure effective protection of the Parties' financial interests. Article 10 ***Data protection*:** 1. The communication of personal data shall only take place if such communication is necessary for the implementation of this Agreement by the competent authorities of Ukraine or the EU as the case may be. When communicating, processing or treating personal data in a particular case, in line with Article 15 the competent authorities of Ukraine shall abide by the relevant legislation of Ukraine, and the EU Authorities shall abide by the provisions of the ***Regulation (EC) No 45/2001*** of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the EU institutions and bodies and on the free movement of such data. 2. In particular, the standards of the ***Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data***, signed on 28 January 1981 (ETS No. 108) and of the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows, signed on 8 November 2001 (ETS No. 181) shall apply to such communication. 3. In addition, the following principles shall apply: (a) both the communicating authority and the receiving authority shall take every reasonable step to ensure as appropriate the rectification, erasure or blocking of personal data where the processing does not comply with the provisions of this Article, in particular because those data are not adequate, relevant, accurate, or they are excessive in relation to the purpose of processing. This includes the notification of any rectification, erasure or blocking to the other Party; (b) upon request, the receiving authority shall inform the communicating authority of the use of the communicated data and of the results obtained there from; (c) personal data may only be

communicated to the competent authorities. Further communication to other bodies requires the prior consent of the communicating authority; (d) the communicating and the receiving authorities are under an obligation to make a written record of the communication and receipt of personal data. ***- Protocol II on mutual administrative assistance in customs matters, Article 10 Information exchange and confidentiality*:** 1. Any information communicated in whatsoever form pursuant to this Protocol shall be of a confidential or restricted nature, depending on the rules applicable in each of the Parties. It shall be covered by the obligation of official secrecy and shall enjoy the protection extended to similar information under the relevant laws of the Party that received it and the corresponding provisions applying to the authorities of the EU Party. 2. Personal data may be exchanged only where the Party which may receive them undertakes to afford such data an adequate level of protection in accordance with the standards and legal instruments referred to in Article 15 of Title III Justice, Freedom and Security of this Agreement. 3. The use, in judicial or administrative proceedings instituted in respect of breaches of customs legislation, of information obtained under this Protocol, is considered to be for the purposes of this Protocol. Therefore, the Parties may, in their records of evidence, reports and testimonies and in proceedings and charges brought before the courts, use as evidence information obtained and documents consulted in accordance with the provisions of this Protocol. The competent authority which supplied that information or gave access to those documents shall be notified of such use. 4. Information obtained shall be used solely for the purposes of this Protocol. Where one of the Parties wishes to use such information for other purposes, it shall obtain the prior written consent of the authority which provided the information. Such use shall then be subject to any restrictions laid down by that authority. ***- Article 22 Fight against crime and corruption***: The Parties shall cooperate in combating and preventing illegal activities, organised or otherwise, including in cyber crime.		
- Some progress in aligning with AA provisions, e.g. ***Chapter 14 Information society, Article 15 Protection of personal data, Article 122 Confidentiality of information, Article 129 Data processing***	- Protection of personal data and privacy - Confidentiality of electronic data	- Fully align with the above AA provisions

Ukraine - additional gaps and recommendations

Main achievements according to the EU baseline	Major gaps	Main recommended actions (priority areas for cooperation)
- Aspects of the ***Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*** (7/2/2013) and a *Proposal for a Directive* of the European Parliament and of the Council (part of a Joint Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions of 7.2.2013) – setting out principles for cyber security; presenting an EU's comprehensive		

vision on how best to prevent and respond to cyber disruptions and attacks; demonstrating a clear mandate to ensure that the digital economy can safely grow and the European values of freedom and democracy are protected; defining measures to ensure a high common level of network and information security across the Union; proposing to establish legally binding common minimum requirements for NIS at national level including the designation of national competent authorities for NIS, establishment of a well-functioning CERT, adoption of a national NIS strategy and a national NIS cooperation plan. - Aspects (Articles 13a and 13b in page 55) of the ***Framework Directive*** (Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services as amended by ***Directive 2009/140/EC*** and ***Regulation 544/2009***) contain security risk management and incident reporting requirements for electronic communications operators ***- Policy recommendations of the European Network and Information Security Agency (ENISA)*** – make critical information infrastructure (CII) an integral part of a national social and economic policy agenda; helps empower CERTs with more authority to require telecom service providers and ISPs to implement security measures and changes; defines security measures and incident reporting procedures. - Aspects of the ***Regulation No 910/2014 on electronic identification and trust services*** for electronic transactions in the EU internal market: establishing minimum security requirements applicable to trust services. **-** Aspects of the ***Commission's Communication on Critical Information Infrastructure Protection (CIIP)*** – defines policy measures and criteria for European critical information infrastructure for being prepared to prevent, detect, respond and mitigate disruptions, as well as to recover from them; makes international cooperation an integral part of the overall CIIP policy. **-** Aspects of the ***Commission's Communications on CIIP***: COM(2009) 149 and COM(2011) 163		
- Progress in aligning with the provisions of the ***Cybercrime Convention***	- Legal and regulatory framework - National cyber security law and strategy - Transparency in reporting on security incidents - Public awareness raising - CERT services including Cyber attack simulation - Protection of	- Fully align with the above EU legislation, especially with ***Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*** (7/2/2013) and a ***Proposal for a Directive*** and other relevant laws and regulations, ***Commission's Communication on Critical Information Infrastructure Protection (CIIP)***

	personal data and privacy - Public/Private sector critical infrastructures	

For other Partner countries

Armenia – achievements, gaps and recommendations

Main achievements according to the EU baseline	Major gaps	Main recommended actions (priority areas for cooperation)
- Aspects of the ***Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*** (7/2/2013) and a ***Proposal for a Directive*** of the European Parliament and of the Council (part of a Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 7.2.2013) – setting out principles for cyber security; presenting an EU's comprehensive vision on how best to prevent and respond to cyber disruptions and attacks; demonstrating a clear mandate to ensure that the digital economy can safely grow and the European values of freedom and democracy are protected; defining measures to ensure a high common level of network and information security; proposing to establish legally binding common minimum requirements for NIS at national level including the designation of national competent authorities for NIS, establishment of a well-functioning CERT, adoption of a national NIS strategy and a national NIS cooperation plan. Aspects (Articles 13a and 13b in page 55) of the ***Framework Directive*** (Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services as amended by ***Directive 2009/140/EC*** and ***Regulation 544/2009***) contain security risk management and incident reporting requirements for electronic communications operators. - Aspects of ***Policy recommendations of the European Network and Information Security Agency (ENISA)*** – make critical information infrastructure (CII) an integral part of a national social and economic policy agenda; helps empower CERTs with more authority to require telecom service providers and ISPs to implement security measures and changes; defines security measures and incident reporting procedures. ***- Directive 2002/58/EC*** of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (***Directive on privacy and electronic communications***) as amended by ***Directive 2009/136/EC*** of the European Parliament and of the Council of 25 November 2009. ***- Directive 95/46/EC*** of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, ***Council Framework Decision 2008/977/JHA*** of 27 November 2008 on the protection of personal data processed		

in the framework of police and judicial cooperation in criminal matters. ***- Convention for the Protection of Individuals*** with regard to Automatic Processing of Personal Data, signed on 28 January 1981 (ETS No 108) including ***Additional Protocol, regarding Supervisory Authorities and Transborder Data Flows***, signed on 8 November 2001 (ETS No 181). ***- Recommendation No. R (87) 15*** of 17 September 1987 of the Committee of Ministers of the Council of Europe ***Regulating the Use of Personal Data in the Police Sector***. ***- Regulation (EC) No 45/2001*** of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the EU institutions and bodies and on the free movement of such data. 2. In particular, the standards of the ***Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data***, signed on 28 January 1981 (ETS No. 108) and of the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows, signed on 8 November 2001 (ETS No. 181). - Aspects of the ***Regulation No 910/2014 on electronic identification and trust services*** for electronic transactions in the EU internal market: establishing minimum security requirements applicable to trust services. - Aspects of the ***Commission's Communication on Critical Information Infrastructure protection (CIIP)*** – defines policy measures and criteria for European critical information infrastructure for being prepared to prevent, detect, respond and mitigate disruptions, as well as to recover from them; makes international cooperation an integral part of the overall CIIP policy. - Aspects of the Commission's ***Communications on Critical Information Infrastructure Protection (CIIP)***: COM(2009) 149 and COM(2011) 163.		
- Progress in aligning with European standards (including ***Cybercrime Convention)***, e.g. in the area of personal data protection and reporting on security incidents (part of a draft Personal Data Protection law)	- Legal and regulatory framework - National cyber security law and strategy - Transparency in reporting on security incidents - Public awareness raising - Establishment of national/government CERT services and related services, including Cyber attack simulation - Protection of	- Align as closely as feasible with the above EU legislation, especially with ***Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*** (7/2/2013) and a ***Proposal for a Directive*** and other relevant laws and regulations, ***Commission's Communication on Critical Information Infrastructure Protection (CIIP), Directive 2002/58/EC, Directive 95/46/EC***

	personal data and privacy - Public/Private sector critical infrastructures	

Azerbaijan – achievements, gaps and recommendations

Main achievements according to the EU baseline	Major gaps	Main recommended actions (priority areas for cooperation)
- Aspects of the ***Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*** (7/2/2013) and a ***Proposal for a Directive*** of the European Parliament and of the Council (part of a Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 7.2.2013) – setting out principles for cyber security; presenting an EU's comprehensive vision on how best to prevent and respond to cyber disruptions and attacks; demonstrating a clear mandate to ensure that the digital economy can safely grow and the European values of freedom and democracy are protected; defining measures to ensure a high common level of network and information security; proposing to establish legally binding common minimum requirements for NIS at national level including the designation of national competent authorities for NIS, establishment of a well-functioning CERT, adoption of a national NIS strategy and a national NIS cooperation plan. Aspects (Articles 13a and 13b in page 55) of the ***Framework Directive*** (Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services as amended by ***Directive 2009/140/EC*** and ***Regulation 544/2009***) contain security risk management and incident reporting requirements for electronic communications operators. - Aspects of ***Policy recommendations of the European Network and Information Security Agency (ENISA)*** – make critical information infrastructure (CII) an integral part of a national social and economic policy agenda; helps empower CERTs with more authority to require telecom service providers and ISPs to implement security measures and changes; defines security measures and incident reporting procedures. ***- Directive 2002/58/EC*** of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (***Directive on privacy and electronic communications***) as amended by ***Directive 2009/136/EC*** of the European Parliament and of the Council of 25 November 2009. ***- Directive 95/46/EC*** of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, ***Council Framework Decision 2008/977/JHA*** of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. ***- Convention for the Protection of Individuals*** with regard to Automatic Processing of Personal Data, signed on 28 January 1981 (ETS No 108) including ***Additional Protocol,***		

regarding Supervisory Authorities and Transborder Data Flows, signed on 8 November 2001 (ETS No 181). ***- Recommendation No. R (87) 15*** of 17 September 1987 of the Committee of Ministers of the Council of Europe ***Regulating the Use of Personal Data in the Police Sector***. ***- Regulation (EC) No 45/2001*** of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the EU institutions and bodies and on the free movement of such data. 2. In particular, the standards of the ***Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data***, signed on 28 January 1981 (ETS No. 108) and of the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows, signed on 8 November 2001 (ETS No. 181) - Aspects of the ***Regulation No 910/2014 on electronic identification and trust services*** for electronic transactions in the EU internal market: establishing minimum security requirements applicable to trust services - Aspects of the ***Commission's Communication on Critical Information Infrastructure protection (CIIP)*** – defines policy measures and criteria for European critical information infrastructure for being prepared to prevent, detect, respond and mitigate disruptions, as well as to recover from them; makes international cooperation an integral part of the overall CIIP policy. - Aspects of the Commission's ***Communications on Critical Information Infrastructure Protection (CIIP)***: COM(2009) 149 and COM(2011) 163.		
- Progress in aligning with the provisions of the ***Cybercrime Convention***	- Legal and regulatory framework - National cyber security law and strategy - Transparency in reporting on security incidents - Public awareness raising - CERT services including Cyber attack simulation - Protection of personal data and privacy - Public/Private sector critical infrastructures	- Align as closely as feasible with the above EU legislation, especially with ***Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*** (7/2/2013) and a ***Proposal for a Directive*** and other relevant laws and regulations, ***Commission's Communication on Critical Information Infrastructure Protection (CIIP), Directive 2002/58/EC, Directive 95/46/EC***

Belarus – achievements, gaps and recommendations

Main achievements according to the EU baseline	Major gaps	Main recommended actions (priority areas for cooperation)
- ***Cybercrime Convention of the Council of Europe*** - Aspects of the ***Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*** (7/2/2013) and a ***Proposal for a Directive*** of the European Parliament and of the Council (part of a Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 7.2.2013) – setting out principles for cyber security; presenting an EU's comprehensive vision on how best to prevent and respond to cyber disruptions and attacks; demonstrating a clear mandate to ensure that the digital economy can safely grow and the European values of freedom and democracy are protected; defining measures to ensure a high common level of network and information security; proposing to establish legally binding common minimum requirements for NIS at national level including the designation of national competent authorities for NIS, establishment of a well-functioning CERT, adoption of a national NIS strategy and a national NIS cooperation plan. Aspects (Articles 13a and 13b in page 55) of the ***Framework Directive*** (Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services as amended by ***Directive 2009/140/EC*** and ***Regulation 544/2009***) contain security risk management and incident reporting requirements for electronic communications operators. - Aspects of ***Policy recommendations of the European Network and Information Security Agency (ENISA)*** – make critical information infrastructure (CII) an integral part of a national social and economic policy agenda; helps empower CERTs with more authority to require telecom service providers and ISPs to implement security measures and changes; defines security measures and incident reporting procedures. ***- Directive 2002/58/EC*** of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (***Directive on privacy and electronic communications***) as amended by ***Directive 2009/136/EC*** of the European Parliament and of the Council of 25 November 2009. ***- Directive 95/46/EC*** of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, ***Council Framework Decision 2008/977/JHA*** of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. ***- Convention for the Protection of Individuals*** with regard to Automatic Processing of Personal Data, signed on 28 January 1981 (ETS No 108) including ***Additional Protocol, regarding Supervisory Authorities and Transborder Data Flows***, signed on 8 November 2001 (ETS No 181). ***- Recommendation No. R (87) 15*** of 17 September 1987 of the Committee of Ministers of the Council of Europe ***Regulating the Use of Personal Data in the Police Sector***.		

- Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the EU institutions and bodies and on the free movement of such data. 2. In particular, the standards of the ***Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data***, signed on 28 January 1981 (ETS No. 108) and of the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows, signed on 8 November 2001 (ETS No. 181). - Aspects of the ***Regulation No 910/2014 on electronic identification and trust services*** for electronic transactions in the EU internal market: establishing minimum security requirements applicable to trust services - Aspects of the ***Commission's Communication on Critical Information Infrastructure protection (CIIP)*** – defines policy measures and criteria for European critical information infrastructure for being prepared to prevent, detect, respond and mitigate disruptions, as well as to recover from them; makes international cooperation an integral part of the overall CIIP policy. - Aspects of the Commission's ***Communications on Critical Information Infrastructure Protection (CIIP)***: COM(2009) 149 and COM(2011) 163.		
N/a	- Cybercrime Convention - Legal and regulatory framework - National cyber security law and strategy - Transparency in reporting on security incidents - Public awareness raising - CERT services including Cyber attack simulation - Protection of personal data and privacy - Public/Private sector critical infrastructures	Ratify Cybercrime Convention and start aligning national legislation with the Convention's provisions - Align as closely as feasible with the above EU legislation, especially with ***Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*** (7/2/2013) and a ***Proposal for a Directive*** and other relevant laws and regulations, ***Commission's Communication on Critical Information Infrastructure Protection (CIIP), Directive 2002/58/EC, Directive 95/46/EC***

Electronic identification and trust services

Georgia – achievements, gaps and recommendations relevant to the Association Agreement

Achievements according to the related topics of the country's Association Agreement / DCFTA	Major gaps	Main recommended actions (priority areas for cooperation)
Article 110 Cross-border provision of electronic communication services*:** Neither Party may require a service supplier of the other Party to set up an establishment, to establish any form of presence, or to be resident, in its territory as a condition for the cross-border supply of a service. ***Article 128 Cooperation in electronic commerce*:** 1. The Parties shall maintain a dialogue on regulatory issues raised by electronic commerce, which will inter alia address, inter alia, the recognition of certificates of electronic signatures issued to the public and the facilitation of cross-border certification services. ***Article 325 Cooperation in the field of information society**:* Cooperation will cover, inter alia, (a) exchange of information and best practices on the implementation of national information society initiatives, including those aiming at developing public online services. ***Article 141 Public procurement: 1. The Parties recognise the contribution of transparent, non-discriminatory, competitive and open tendering to sustainable economic development and set as their objective the effective, reciprocal and gradual opening of their respective procurement markets. 2. This Chapter envisages mutual access to public procurement markets on the basis of the principle of national treatment at national, regional and local level for public contracts and concessions in the traditional sector as well as in the utilities sector. It provides for a gradual approximation of the public procurement legislation in Georgia with the Union public procurement *acquis* based on the principles governing public procurement in the Union and the terms and definitions set out in ***Directive 2004/18/EC*** of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts ***(Directive 2004/18/EC***) and ***Directive 2004/17/EC*** of the European Parliament and of the Council of 31 March 2004).		
Good pprogress in implementing various aspects of the above AA provisions, e.g. ***Article 325 Cooperation in the field of information society***	- Legal and regulatory framework	- Fully align with the above AA provisions

Georgia - additional gaps and recommendations

Main achievements according to the EU baseline	*Major gaps*	*Main recommended actions (priority areas for cooperation)*

Aspects of: **- *Regulation No 910/2014*** of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (including the preceding ***E-Signature Directive 1999/93/EC***) **- *Mandate M460*** *(*regarding the EU Standardisation initiatives/cross border tools) **- *Decision 2004/387/EC*** (Corrigenda) of the European Parliament of 21 April 2004 on interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC), Interoperability of European public services **- *Decision No 922/2009/EC*** of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA) **- *Directive 2002/58/EC*** of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, part of the "Telecom Package" **- *A Digital Agenda for Europe (DAE)*** **- *Large Scale Pilots*** (especially STORK (Secure identity across borders linked)		
- Good progress in implementing ***Directive 2002/58/EC*** - Progress in aligning with ***A Digital Agenda for Europe (DAE)***	- Legal and regulatory framework - Cross-border recognition of certificates of certification services and electronic signatures	- Fully align with the above EU legislation, especially with ***Regulation No 910/2014*** of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (eIDAS regulation) - Fully align national e-government policies with ***Digital Agenda for Europe (DAE)*** - Fully align with ***Decision 2004/387/EC*** and ***E-Signature Directive 1999/93/EC*** - Participate in ***STORK large-scale project*** - Adopt EU good practices

Moldova – achievements, gaps and recommendations relevant to the Association Agreement

Achievements according to the related topics of the country's Association Agreement / DCFTA	Major gaps	Main recommended actions (priority areas for cooperation)
Article 245 **Data processing:** 1.Each Party shall permit a financial service supplier of the		

other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier. 2. Each Party shall adopt adequate safeguards for the protection of privacy and fundamental rights and freedoms of individuals, in particular with regard to the transfer of personal data.

Sub-section 5, Electronic communication networks and services. Article 237 **Cross-border provision of electronic communication services:** Neither Party may require a service supplier of the other Party to set up an establishment, to establish any form of presence, or to be resident in its territory as a condition for the cross-border supply of a service; ***Article 238*** **Confidentiality of information:** Each Party shall ensure the confidentiality of electronic communications and related traffic data by means of a public communication network and publicly available electronic communication services without restricting trade in services.

Annex XXVIII-B Rules applicable to telecommunication services: Within one year of the entry into force of this Agreement, Moldova will implement the following provisions of the ***Directive 1999/93/EC*** of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures: (a) adopting a policy and legislation to create a framework for the use of electronic signatures ensuring their basic legal recognition and admissibility as evidence in legal proceedings and (b) establishment of a mandatory supervision system of certification service providers issuing qualified certificates.

Chapter 18 Information society, Article 98*:* The Parties shall strengthen cooperation on the development of the Information Society to benefit citizens and businesses through the widespread availability of Information and Communication Technology (ICT) and through better quality of services at affordable prices. That cooperation should aim at facilitating access to electronic communications markets, encouraging competition and investment in the sector, and promoting the development of public services online. ***Article 99*** Cooperation may cover the following subjects: (a) exchange of information and best practices on the implementation of national Information Society strategies, including, inter alia, initiatives aiming at promoting broadband access, improving network security and developing public services online; (b) exchange of information, best practices and experience to promote the development of a comprehensive regulatory framework for electronic communications, and in particular to strengthen the administrative capacity of the national administration in Information and Communication Technologies, as well as of the independent regulator, to foster a better use of spectrum resources and to promote interoperability of networks in the Republic of Moldova and with the EU; (c) encouraging and promoting the implementation of ICT tools for a better governance, e-learning and research, public healthcare, digitisation of cultural heritage, development of e — content and electronic commerce; and (d) enhancing the level of security of personal data and the protection of privacy in electronic communications.

Article 255 Cooperation in electronic commerce**:** 1. The Parties shall maintain a dialogue on regulatory issues raised by electronic commerce, which will inter alia address, inter alia, the recognition of certificates of electronic signatures issued to the public and the facilitation of cross-border certification services.

Chapter 8 Public procurement, Article 268 Objectives**:** 1.The Parties recognise the contribution of transparent, non-discriminatory, competitive and open tendering to

sustainable economic development and set as their objective the effective, reciprocal and gradual opening of their respective procurement markets. 2. This Chapter envisages mutual access to public procurement markets on the basis of the principle of national treatment at national, regional and local level for public contracts and concessions in the public sector as well as in the utilities sector. It provides for a gradual approximation of the public procurement legislation in the Republic of Moldova with the Union *acquis* on public procurement, accompanied with an institutional reform and the creation of an efficient public procurement system based on the principles governing public procurement in the Union and the terms and definitions set out in ***Directive 2004/18/EC*** of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts and ***Directive 2004/17/EC*** of the European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors.		
- Good progress in implementing various aspects of the above AA provisions, e.g. ***Chapter 18 Information society, Article 245 Data processing, Article 238 Confidentiality of information***	- Legal and regulatory framework	- Fully align with the above AA provisions

Moldova - additional gaps and recommendations

Main achievements according to the EU baseline	*Major gaps*	*Main recommended actions (priority areas for cooperation)*
Aspects of: **- *Regulation No 910/2014*** of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (including the preceding ***E-Signature Directive 1999/93/EC***) **- *Mandate M460*** *(*regarding the EU Standardisation initiatives/cross border tools) **- *Decision 2004/387/EC*** (Corrigenda) of the European Parliament of 21 April 2004 on interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC), Interoperability of European public services **- *Decision No 922/2009/EC*** of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA) **- *Directive 2002/58/EC*** of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, part of the "Telecom Package" **- *A Digital Agenda for Europe (DAE)*** **- *Large Scale Pilots*** (especially STORK (Secure identity across borders linked)		

- Good progress in aligning with ***Digital Agenda for Europe*** - Progress in implementing aspects of ***Directive 2002/58/EC, Decision 2004/387/EC***	- Legal and regulatory framework - Cross-border recognition of certificates of certification services and electronic signatures	- Fully align with the above EU legislation, especially with ***Regulation No 910/2014*** of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (eIDAS regulation) - Fully align national e-government policies with ***Digital Agenda for Europe (DAE)*** - Fully align with ***Decision 2004/387/EC*** and ***E-Signature Directive 1999/93/EC*** - Participate in ***STORK large-scale project*** - Adopt EU good practices

Ukraine – achievements, gaps and recommendations relevant to the Association Agreement

Achievements according to the related topics of the country's Association Agreement / DCFTA	Major gaps	Main recommended actions (priority areas for cooperation)
Article 129 Data processing**:** 1. Each Party shall permit a financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier. 2. Each Party shall adopt adequate safeguards for the protection of privacy and fundamental rights and the freedom of individuals, in particular with regard to the transfer of personal data. ***Chapter 14 Information society, Article 389****:* The Parties shall step up cooperation on the development of the Information Society to benefit citizens and businesses through the widespread availability of Information and Communication Technology (ICT) and through better quality of services at affordable prices. ***Article 390****:* Cooperation shall aim at implementing national Information Society strategies, developing of a comprehensive regulatory framework for electronic communications, and increasing Ukraine's participation in the ICT research activities of the EU. ***Article 391****:* Cooperation shall cover the following subjects: (a) promotion of broadband access, improvement of network security and more widespread use of ICT by citizens, business and administrations by developing local content for the Internet and introducing online services, in particular e-business, e-government, e-health and e-learning; (b) coordination of electronic communication policies with a view to making optimal use of the radio spectrum and interoperability of networks in Ukraine and the EU.		

Article 121 Cross-border provision of electronic communication services**:** The Parties shall not adopt or maintain any measure restricting the cross-border provision of electronic communication services. ***Article 122 Confidentiality of information*****:** Each Party shall ensure the confidentiality of electronic communication and related traffic data by means of a public electronic communication network and publicly available electronic communication services without restricting trade in services. ***Section 6 Electronic commerce, Article 140 Regulatory aspects of electronic commerce*****:** 1. The Parties shall maintain a dialogue on regulatory issues raised by electronic commerce, which will inter alia address the following issues: (a) the recognition of certificates of electronic signatures issued to the public and the facilitation of cross-border certification services ***Chapter 8 Public procurement, Article 148 Objectives:*** The Parties recognise the contribution of transparent, non-discriminatory, competitive and open tendering to sustainable economic development and set as their objective the effective, reciprocal and gradual opening of their respective procurement markets. This Chapter envisages mutual access to public procurement markets on the basis of the principle of national treatment at national, regional and local level for public contracts and concessions in the traditional sector as well as in the utilities sector. It provides for the progressive approximation of the public procurement legislation in Ukraine with the EU public procurement *acquis*, accompanied with an institutional reform and the creation of an efficient public procurement system based on the principles governing public procurement in the EU Party and the terms and definitions set out in ***Directive 2004/18/E***C of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts and ***Directive 2004/17/EC*** of the European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors.		
- Progress in implementing various aspects of the above AA provisions, e.g.***Chapter 14 Information society***	- Legal and regulatory framework	- Fully align with the above AA provisions

Ukraine - additional gaps and recommendations

Main achievements according to the EU baseline	***Major gaps***	***Main recommended actions (priority areas for cooperation)***
Aspects of: **- *Regulation No 910/2014*** of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (including the preceding ***E-Signature Directive 1999/93/EC***) **- *Mandate M460*** *(*regarding the EU Standardisation initiatives/cross border tools)		

- *Decision 2004/387/EC* (Corrigenda) of the European Parliament of 21 April 2004 on interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC), Interoperability of European public services **- *Decision No 922/2009/EC*** of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA) **- *Directive 2002/58/EC*** of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, part of the "Telecom Package" **- *A Digital Agenda for Europe (DAE)*** **- *Large Scale Pilots*** (especially STORK (Secure identity across borders linked)		
- Progress in implementing various aspects of the above provisions, e.g. ***Directive 2002/58/EC***	- Legal and regulatory framework - Cross-border recognition of certificates of certification services and electronic signatures	- Fully align with the above EU legislation, especially with ***Regulation No 910/2014*** of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (eIDAS regulation) - Fully align national e-government policies with ***Digital Agenda for Europe (DAE)*** - Fully align with ***Decision 2004/387/EC*** and ***E-Signature Directive 1999/93/EC*** - Participate in ***STORK large-scale project*** - Implement mobile eID/TS solutions including mobile digital signature - Adopt EU good practices

Armenia – achievements, gaps and recommendations

Main achievements according to the EU baseline	Major gaps	Main recommended actions (priority areas for cooperation)
Aspects of: **- *Regulation No 910/2014*** of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (including the preceding ***E-Signature Directive 1999/93/EC***)		

- *Mandate M460* *(*regarding the EU Standardisation initiatives/cross border tools) **- *Decision 2004/387/EC*** (Corrigenda) of the European Parliament of 21 April 2004 on interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC), Interoperability of European public services **- *Decision No 922/2009/EC*** of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA) **- *Directive 2002/58/EC*** of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, part of the "Telecom Package" **- *A Digital Agenda for Europe (DAE)*** **- *Large Scale Pilots*** (especially STORK (Secure identity across borders linked)		
N/a	- Legal and regulatory framework - Cross-border recognition of certificates of certification services and electronic signatures	- Align as closely as possible with the above EU legislation, especially with with ***Regulation No 910/2014*** of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (eIDAS regulation) - Align national e-government policies as closely as possible with ***Digital Agenda for Europe (DAE)*** - Align as closely as possible with ***Decision 2004/387/EC*** and ***E-Signature Directive 1999/93/EC*** - Participate in ***STORK large-scale project*** - Adopt EU good practices - Implement mobile eID/TS solutions including mobile digital signature

Azerbaijan – achievements, gaps and recommendations

Main achievements according to the EU	Major gaps	Main recommended actions (priority areas for cooperation)

baseline		
Aspects of: **- *Regulation No 910/2014*** of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (including the preceding ***E-Signature Directive 1999/93/EC***) **- *Mandate M460*** *(*regarding the EU Standardisation initiatives/cross border tools) **- *Decision 2004/387/EC*** (Corrigenda) of the European Parliament of 21 April 2004 on interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC), Interoperability of European public services **- *Decision No 922/2009/EC*** of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA) **- *Directive 2002/58/EC*** of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, part of the "Telecom Package" **- *A Digital Agenda for Europe (DAE)*** **- *Large Scale Pilots*** (especially STORK (Secure identity across borders linked)		
N/a	- Legal and regulatory framework - Cross-border recognition of certificates of certification services and electronic signatures	- Align as closely as possible with the above EU legislation, especially with with ***Regulation No 910/2014*** of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (eIDAS regulation) - Align national e-government policies as closely as possible with ***Digital Agenda for Europe (DAE)*** - Align as closely as possible with ***Decision 2004/387/EC*** and ***E-Signature Directive 1999/93/EC*** - Participate in ***STORK large-scale project*** - Adopt EU good practices

Belarus – achievements, gaps and recommendations

Main achievements according to the EU baseline	Major gaps	Main recommended actions (priority areas for

		cooperation)
Aspects of: **- *Regulation No 910/2014*** of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (including the preceding ***E-Signature Directive 1999/93/EC***) **- *Mandate M460*** *(*regarding the EU Standardisation initiatives/cross border tools) **- *Decision 2004/387/EC*** (Corrigenda) of the European Parliament of 21 April 2004 on interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC), Interoperability of European public services **- *Decision No 922/2009/EC*** of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA) **- *Directive 2002/58/EC*** of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, part of the "Telecom Package" **- *A Digital Agenda for Europe (DAE)*** **- *Large Scale Pilots*** (especially STORK (Secure identity across borders linked)		
N/a	- Legal and regulatory framework - Cross-border recognition of certificates of certification services and electronic signatures	- Align as closely as possible with the above EU legislation, especially with with ***Regulation No 910/2014*** of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (eIDAS regulation) - Align national e-government policies as closely as possible with ***Digital Agenda for Europe (DAE)*** - Align as closely as possible with ***Decision 2004/387/EC*** and ***E-Signature Directive 1999/93/EC*** - Participate in ***STORK large-scale project*** - Adopt EU good practices - Implement mobile eID/TS solutions including mobile digital signature

eCustoms

Georgia

Achievements, gaps and recommendations relevant to the Association Agreement

Achievements according to the related topics of the country's Association Agreement	Major gaps	Main recommended actions (priority areas for cooperation)
Association Agreement between the European Union and Georgia • Title IV: "Trade and trade-related matters", Chapter 5 "Customs and trade facilitation" (Articles 66-75) • Title VI "Other Cooperation Policies", Chapter 8 "Cooperation in the field of Information Society" (Articles 324-327) • Annex XIII – Approximation of customs legislation • Annex XV-B "Rules Applicable To Telecommunication Services" Timetable: the approximation with the provisions of the above mentioned Regulation, with some exceptions, shall be carried out within four years following the entry into force of this Agreement.		
Council Regulation (EEC) No 2913/92 establishing the Community Customs Code Paperless environment for customs and trade Implementation of a paperless environment has already been launched. The automation of customs operations in Georgia is organised through two independent and fragmentally integrated information systems Data exchange is provided between different agencies within Georgia. Currently, Georgian Customs exchanges electronic information with the customs authorities of two countries:	Not all relevant public organisations within Georgia participate in the paperless environment. Currently, Georgian Customs exchanges electronic information only with the customs authorities of two countries: the Turkey and Ukraine.	Secure, integrated, interoperable and accessible electronic customs systems have to be set up for the exchange of data contained in customs declarations, documents accompanying customs declarations and certificates and the exchange of other relevant information. The electronic customs systems shall provide for the exchange of data between the customs authorities of Georgia and the Member States and between those authorities and economic operators, the Commission, other administrations or official agencies involved in the international movement of goods.

the Turkey and Ukraine.		
Regulation (EU) No 608/2013 concerning customs enforcement of intellectual property rights Anti-Counterfeiting and Anti-Piracy System The approximation with the provisions of the above mentioned Regulation, with the exception of Article 26, shall be carried out within three years following the entry into force of this Agreement.	Therefore, a national information system on IPR has not yet been created and no information exchange has been undertaken with internationally or with EU centralised Anti-Counterfeiting and Anti-Piracy System. An IPR oriented National Anti-Fraud system has not been implemented. In Georgia there is no electronic service in place that provide traders with the possibility to submit a claim asking the intervention of Customs in order to take measures against goods infringing certain IP rights.	Create a national Anti-Fraud Information System with an electronic service that provides economic operators and citizens with the possibility to submit a claim asking the intervention of Customs in order to take measures against goods infringing certain intellectual property rights. Connect the national Anti-Fraud Information System with the EU centralised Anti-Counterfeiting and Anti-Piracy System. Conclude agreements, define formats of information sharing and connect the national Anti-Fraud Information System with the similar systems of the Region.
Authorised Economic Operator (AEO) status AEO status implementation is part of the strategy, as part of the Association Agreement between the European Union and Georgia. The Customs authorities do not currently apply common criteria and harmonised requirements for granting the status of authorised economic operators, allowing the use of simplifications by authorised economic operators.	Recognition of the status of AEOs registered in the EU member states or other countries has not been yet implemented.	Implement the status of the authorised Economic Operator compliant with the EU requirements (part of the Association Agreement between the European Union and Georgia's implementation plan). Promote incentives of the authorised Economic Operator status

Moldova

Achievements, gaps and recommendations relevant to the Association Agreement

Achievements according to the related topics of the country's Association Agreement	Major gaps	Main recommended actions (priority areas for cooperation)
EU-Moldova Association Agreement: • Title IV "Economic and other Sectoral Cooperation" o Chapter 18 "Information Society" • Title V "Trade and trade related matters" o CHAPTER 5 - Customs and trade facilitation • ANNEX XXVI – Approximation of customs legislation • Annex XXVIII-B "Rules Applicable To Telecommunication Services"		
Council Regulation (EEC) No 2913/92 of 12 October 1992 establishing the Community Customs Code Timetable: The approximation with the provisions of the above mentioned Regulation shall be carried out by the Republic of Moldova within three years following the entry into force of this Agreement Paperless environment for customs and trade As from March 2013, Moldovan customs implemented electronic export declaration and the share of eExport submissions grew by 42% by January 2015. As from September 2014, an electronic import declaration has been also been implemented. At present a number of projects are	None	None

being implemented which will permit electronic exchange of information within the public sector. The Customs Service participates in this process. The Government has adopted the Government Decision no.656/2012 on Interoperability framework [24] and is currently implementing the technical layer of interoperability (pilot project) in accordance with Government Decision no.404 of 2.06.2014. National legal provisions are defined for secure, integrated, interoperable and accessible electronic customs systems for the exchange of data contained in customs declarations, documents accompanying customs declarations, certificates and the exchange of other relevant information. Appropriate system applications are in the process of implementation.		
Regulation (EU) No 608/2013 of the European Parliament and of the Council of 12 June 2013 concerning customs enforcement of intellectual property rights Timetable: The approximation with the provisions of that Regulation shall be carried out by the Republic of Moldova within	There is no electronic service providing traders with the possibility to submit a claim asking the intervention of Customs in order to take measures against goods infringing certain intellectual property rights.	Create the national Anti-Fraud Information System with an electronic service that provides economic operators and citizens with the possibility to submit a claim asking the intervention of Customs in order to take measures against goods infringing certain intellectual property rights. Connect the national Anti-Fraud Information System with the

[24] http://egov.md/images/normative/Moldova_Interoperability_Framework_Program.pdf

one year following the entry into force of this Agreement. Anti-Counterfeiting and Anti-Piracy System An Anti-Counterfeiting and Anti-Piracy System has not been established.		EU centralised Anti-Counterfeiting and Anti-Piracy System. Conclude agreements, define formats of information sharing and connect the national Anti-Fraud Information System with the similar systems of the Region.

Ukraine

Achievements, gaps and recommendations relevant to the Association Agreement

Achievements according to the related topics of the country's DCFTA	Major gaps	Main recommended actions (priority areas for cooperation)
EU-Ukraine Association Agreement • Title V "Economic and Sector Cooperation", Chapter 14 "Information Society" • Title IV "Trade and Trade-related Matters", Chapter 6 "Establishment, trade in services and electronic commerce", Section 5 "Regulatory framework" (page 54/2144), Sub-section 5 "Electronic communications" • Appendix XVII-3 "Rules Applicable to Telecommunication Services"		
Council Regulation (EEC) No 2913/92 - establishing the Community Customs Code Paperless environment for customs and trade A unified Automated Information System assures a paperless environment and exchanges of data with many state bodies. 92 % of tax declarations are paperless. National legal provisions are defined for secure, integrated, interoperable and accessible electronic customs systems for the exchange of data contained	Data exchange between other State bodies and the Customs Service is very limited.	None

in customs declarations, documents accompanying customs declarations, certificates and the exchange of other relevant information		

eCommerce for SMEs

Georgia

Achievements, gaps and recommendations relevant to the Association Agreement

Achievements according to the related topics of the country's Association Agreement	Major gaps	Main recommended actions (priority areas for cooperation)
Association Agreement between the European Union and Georgia • Title IV: "Trade and trade-related matters", in Chapter 6 "Establishment, trade in services and electronic commerce" (starts in page 33/740), in Section 5 "Regulatory Framework" (starts in page 41 of 740), see Sub-Section 5 "Electronic communication networks and services" (pages 46-50 of 740, articles 104-113) • Title VI "Other Cooperation Policies", Chapter 8 "Cooperation in the field of Information Society" (Articles 324-327) • Annex XV-B "Rules Applicable To Telecommunication Services" Timetable: the approximation with the provisions of the above mentioned Regulation, with some exceptions, shall be carried out within 6 years following the entry into force of this Agreement.		
Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market Legal framework in the area of eCommerce payments	The national legislation does not define the requirements for eCommerce payments and does not define the rules on the fees for the use of means of electronic payment.	Make payments online more attractive to consumers and increase the competitiveness of SMEs. Develop the regulations on the fees for the use of certain means of payment and prohibit traders from charging consumers, in respect of the use of a given means of payment, fees that exceed the cost borne by the trader for the use of such mean.
Directive 2002/58/EC of the	National Legislation does	Amend the national

European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector Authorised recording of communications and the related traffic data in the course of lawful business practice / confidentiality of the communication	not specify any obligation of information service providers to monitor transmitted information. The only obligation set in the consumer's rights protection decree by GNCC puts an obligation to the providers of hosting and registrars on the provisioning of legal content i.e. the provider of such services shall monitor the content and take it down in case it violates the law including copyrights. This general regulation on hosting and web-service providers to monitor legality of the content placed has not been yet applied and is considered to be amended.	legislation with provisions about the specific liability regimes for three categories of online service providers: transmission conduit operators, caching providers and hosting services providers. The legislation should be amended to define the degree of liability of the service provider for the information transmitted in a communication network of information provided by a recipient of the service. The liability of service provider should be defined for the automatic, intermediate and temporary storage of that information, performed for making more efficient the information's onward transmission to other recipients of the service upon their request. Liability of the hosting service providers should be defined for the information stored at the request of a recipient of the service, with some clearly defined liability exceptions (does not have actual knowledge of illegal activity or information, and others).
Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector Allowance to process user traffic data by the provider of an electronic communication service The Law on Protection of	Being precise on personal data, the national legislation does not explicitly define the rules of processing of user traffic data by providers of an electronic communication service for the purposes of marketing electronic communications services or for the provision of value added services.	Assure to users their rights to manage online privacy. Amend the national legislation with the rules of processing of user traffic data by the provider of an electronic communication service for the purposes of marketing electronic communications services or for the provision of value added services. The

Personal Data prohibits retention of user specific personal data. Implementation of the law is monitored by the Personal Data Protection Inspector's office. Decree of Georgian National Communications Commission of March 16, 2006 on protection of consumers' rights in the field of electronic communications obliges communication service providers to retain data for certain period for billing and interconnection purposes. Such data shall be possessed by an operator for the period defined by the Georgian National Communications Commission. Retention of any data beyond time and purpose limits, including metadata is prohibited.		legislation should indicate if the service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing.

Moldova

Achievements, gaps and recommendations relevant to the Association Agreement

Achievements according to the related topics of the country's Association Agreement	Major gaps	Main recommended actions (priority areas for cooperation)
EU-Moldova Association Agreement: • Title IV "Economic and other Sectoral Cooperation", see Chapter 18 "Information Society" • Title V "Trade and Trade-related Matters", in Chapter 6 "Establishment, Trade in Services and Electronic Commerce" o Section 5 "Regulatory Framework" Sub-Section 5 "Electronic communication networks and services" • Title VI "Other Cooperation Policies", Chapter 8 "Cooperation in the field of Information Society"		

• ANNEX XXVI – Approximation of customs legislation • Annex XXVIII-B "Rules Applicable To Telecommunication Services" • ANNEX XXVIII-A – Rules applicable to financial services		
Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market • Free movement of information society services The subjects of eCommerce can be physical and legal entities, including foreign ones, regardless of the type of ownership and organisational - legal form, as well as the state as a legal entity. Participation in e-commerce, unless otherwise provided by contract or by law, cannot serve as a basis for establishing additional requirements, procedures or restrictions on entrepreneurial activity (Law N284 “On electronic commerce” Art 7). By this, the country’s legislation does not restrict the freedom to provide eCommerce services by a provider from another country.	None	None
• Principle excluding prior authorisation to pursuit the activity of an information society	None	None

service provider The legal framework of the country ensure that the taking up and pursuit of the activity of an information society service provider, including eCommerce activities, may not be made subject to prior authorisation or any other requirement having equivalent effect. The legislation restricts starting of eCommerce activities by a condition of getting prior authorisation in some particular sectors or for some products. This complies with the Directive 2000/31/EC		
• Minimum general information to be provided by information society service provider eCommerce service providers are obliged to provide to other subjects of eCommerce interaction, as well as to state control bodies, appropriate access to reliable information about themselves in electronic form in the Moldovan language, and if necessary, in other languages (Law No.284 of 22.07.2004 "On electronic commerce", Art 11).	None	None
• Transparency requirement of commercial communications information to be provided The Law N1227 "On advertisement" does not	However, the legislation is not explicit about the specific requirements to the different types of commercial communications on the Internet such as promotional offers,	Amend the legislation with the requirements emphasising the need for transparency when advertisements are displayed on the Internet for the types of the online commercial

specify any requirements to the advertisement on the Internet. The Law No.284 of 22.07.2004 "On electronic commerce" Art 11(2) defines requirements for outgoing advertisement from the eCommerce service provider about clear information about goods, works or services, prices and tariffs and their conditions of sale, execution or provision. The requirements emphasising the need for transparency when advertisements are displayed on the Internet are generally provisioned in the legislation.	premiums, promotional competitions or games.	communications such as promotional offers, discounts, premiums, promotional competitions or games.
• Requirements for sending of unsolicited commercial communication The national legislation clearly defines the requirements applied to sending of unsolicited commercial communications by e-mail. Sending commercial messages by e-mail (unsolicited commercial communication) is prohibited, except in cases where the recipient previously agreed to receive such communications (Law N284 "On electronic commerce" Art 17). Any person has the right to opt out of receiving commercial messages. This ensure that communication is clearly and unambiguously identifiable, legal or natural person sending unsolicited	None	None

commercial communication is clearly indicated, conditions of promotions & discounts are described.		
• Equal validity of electronic contracting and contract concluded offline The legal force of an electronic contract is equivalent to a contract drawn up in writing and signed by the parties, including those certified by the seal of the parties. An electronic contract on the probative value equivalent to a written contract. The legislation explicitly describes the cases when a contract cannot be signed in electronic format. Also, the provisions indicates requirements which are compulsory to include in electronic contract activity (Law N284 "On electronic commerce" Art 20). Nevertheless, the provisions of this legislative act are planned to be revised. There are at least three centres in the country, which offer the electronic signature, so most of the persons have to use at least three different types of electronic signatures depending of the document that is signed. The legal framework requires application of a timestamp and it needs to be revised.	Currently, it is not possible to submit contracts concluded online to some authorities.	Mechanisms to verify transactions also need to be revised, as it is not duly finalised.
• Specific liability regime for intermediary service	The current national legislation (Law No.241 "On	Increase the transparency of rules for provision of

providers The approximation of the Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce will be conducted by June 2017.	electronic communications") does not define the overall degree of liability of the eCommerce intermediary service providers for the information transmitted in a communication network of information provided by a recipient of the service. It does not explicitly define specific liability regimes for three categories of online service providers.	cross border eCommerce services by SMEs. Amend the national legislation with provisions about the specific liability regimes for three categories of online service providers: transmission conduit operators, caching providers and hosting services providers.
• No general obligation for providers to monitor transmitted or stored information Intermediary service providers in eCommerce are not required to monitor and verify the accuracy of the transmitted, received and stored electronic documents and e-mails, as well as their compliance with the law, unless otherwise provided by the contract concluded with the participants of eCommerce, or the law (Art 12, Law No.284 of 22.07.2004 "On electronic commerce"). This is in accordance with the Directive 2000/31/EC on electronic commerce Article 15.	None	None
• Non obstruction to out-of-court dispute settlement Directive 2000/31/EC will be approximated by June 2016. The country has not yet deployed an online dispute resolution platform through which parties can initiate	The country's legislation does not define the mechanisms of dispute resolution, in the event of disagreement between an information society service provider and the recipient of the service (Law N241 "On electronic communication",	Facilitate dispute resolution for cross-border purchases. Amend the national legislation allowing the use of out-of-court schemes for dispute settlement regarding provision of eCommerce services, including by appropriate

alternative dispute resolution in relation to disputes concerning online transactions.	law No.284 of 22.07.2004 "On electronic commerce"). The legislation does not include prerequisites for the use of out-of-court schemes for dispute settlement.	electronic means.
Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market Timetable: that Directive's provisions shall be implemented within three years Equal treatment between paper and electronic invoices The national legal framework stipulates that the handwritten signature is equivalent with the electronic one.	However, there is no mechanism in place to verify that the invoice was signed by authorised person. The legal framework requires on certain occasions to apply the stamp, even if documents are signed electronically they have to be printed put and stamped. Infrastructure is required to be implemented. The secondary acts (including the technical provisions) to implement the Law no.91 of 29.05.2014 on eSignature and eDocument will be elaborated and adopted in 2015. It is not clear who has the mandate to monitor and verify application of the electronic signature. Launched on February 11, 2014, the eInvoice service[25] represents a software solution designed for the economic agents from Moldova in terms of bills and invoices' development and electronic circulation. For eInvoice service, the user must be in possession of a digital (mobile) signature issued by an accredited certification centre. There is no defined framework of a common	Reduce costs and delays of international eCommerce transactions. Define national technical standards by promoting the development of interoperable e-invoicing solutions based on common with the EU standards, paying particular attention to the needs of small and medium-sized enterprises. Define a single and clear semantic data model & a common eInvoicing format compatible with the EU best practices to facilitate semantic interoperability, ensure technology neutrality, facilitate the uptake of e-invoicing for eCommerce transactions for SMEs.

[25] http://egov.md/index.php/en/for-business/e-invoice#.VRE4lTSsVQc

	national data model of eInvoicing format.	
Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. Timetable: those provisions of that Directive shall be implemented within three years of the entry into force of this Agreement. • Allowance to process user traffic data by the provider of an electronic communication service Intermediary service providers in eCommerce are not required to monitor and verify the accuracy of the transmitted, received and stored electronic documents and e-mails, as well as their compliance with the law, unless otherwise provided by the contract concluded with the participants of eCommerce, or the law (Art 12, Law No.284 of 22.07.2004 "On electronic commerce"). This is in accordance with the Directive 2000/31/EC on electronic commerce Article 15.	None	None

Ukraine

Achievements, gaps and recommendations relevant to the DCFTA

Achievements according to the related topics of the	Major gaps	Main recommended actions (priority areas for

country's DCFTA		cooperation)
EU-Ukraine Association Agreement • Title V "Economic and Sector Cooperation", see Chapter 14 "Information Society" • Title IV "Trade and Trade-related Matters", in Chapter 6 "Establishment, trade in services and electronic commerce", Section 5 "Regulatory framework" (page 54/2144), Sub-section 5 "Electronic communications" • Appendix XVII-3 "Rules Applicable to Telecommunication Services"		
Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) • Free movement of information society services The national legislation does not explicitly restrict the freedom to provide eCommerce services compliant to the national laws by a lawful service provider established in another country.	None	None
• Principle excluding prior authorisation to pursuit the activity of an information society service provider Ukraine's legislation does not explicitly define the principle excluding prior authorisation to pursuit the activity of eCommerce service provider. The regulation of authorisations for eCommerce activities falls under the overall legal framework. These principles do not prejudice the	This is partially compliant with the EC Directive on electronic commerce that defines the principle excluding prior authorisation to pursuit the activity of an information society service provider (Directive 2000/31/EC on electronic commerce Article 4).	None

authorisation schemes of Ukraine which are not specifically and exclusively targeted at information society services, or which are covered by legislation.		
• Minimum general information to be provided by information society service provider The Law "On advertising" regulates the requirements on minimum general information to be indicated by information society service provider. This is compliant with the requirements of the Directive 2000/31/EC on electronic commerce Article 5.	None	None
• Transparency requirement of commercial communications information to be provided The national legislation (Law "On advertising") does not impose that advertisements on the Internet indicate natural (for legal persons there is a legal requirement) responsible for commercial communication and any conditions attached to the offers.	Does not assure transparency of commercial communications.	Amend the legislation by requirements that advertisements on the Internet indicates natural person responsible for commercial communication and any conditions attached to the offers.
• Requirements for sending of unsolicited commercial communication The national legislation prohibits the sending of unsolicited commercial	None	None

communications by e-mail (Government Resolution № 295”On rules providing telecom services”). The EU best practice in this domain preserves the possibility to either prohibit or allow the sending of unsolicited commercials by e-mail. Compliant with the requirements of the Directive 2000/31/EC on electronic commerce Article 7.		
• Equal validity of electronic contracting and contract concluded offline The national legislation does not explicitly establish the equal validity of electronic contracting and contract concluded offline together with defining the specific requirements to electronic contracts.	The EC Directive on electronic commerce (Directive 2000/31/EC on electronic commerce Articles 9-11) requires the fundamental principles of equal validity of electronic contracting and contract concluded offline, and not only for eCommerce.	extend possibilities of cross-border trade by facilitating conclusion of contracts. Amended the national legislation to assure the same validity of the contracts concluded by electronic means and contracts concluded offline by "traditional" means. Amend the legislation with requires that online traders provide the consumer with specific information prior to the order being placed. This should include information on steps to follow to conclude an electronic contract, the filing of the contract by the service provider, the technical means for identifying and correcting input errors prior to the placing of the order, the languages offered for the conclusion of the contract, availability of any relevant codes of conduct. Amend the legislation with requirements regarding placing of orders for electronic contracts. The

		online contract has to be concluded through an "order" placed by the consumer, followed by an electronic "acknowledgment" of the online trader without undue delay. The "order" and the "acknowledgement" are deemed to be received when the involved contracting parties are able to access them. Trader also has to provide the consumer with the technical means allowing him/her to identify and correct input errors prior to the placing of the order.
• Specific liability regime for intermediary service providers Ukraine's Parliament will consider in the second reading the draft law "On Electronic Commerce". The draft law describes the basic principles of the market regulation, the rights and obligations of the online vendors and their customers, differentiates responsibilities of good's sellers, service providers of intermediate character such as internet access, hosting, and domain name registrars.	The current national legislation does not provide the specific liability regime for transmission conduit operators, caching providers and hosting services providers.	Increase the transparency of rules for provision of cross border eCommerce services by SMEs. Amend the national legislation with provisions about the specific liability regimes for three categories of online service providers: transmission conduit operators, caching providers and hosting services providers. The legislation should be amended to define the degree of liability of the service provider for the information transmitted in a communication network of information provided by a recipient of the service. The liability of service provider should be defined for the automatic, intermediate and temporary storage of that information, performed for making more efficient the information's onward

		transmission to other recipients of the service upon their request. Liability of the hosting service providers should be defined for the information stored at the request of a recipient of the service, with some clearly defined liability exceptions (does not have actual knowledge of illegal activity or information, and others).
• No general obligation for providers to monitor transmitted or stored information The Security Service of Ukraine (SSU) has the right to monitor transmitted or stored information. All providers and operators are required to provide lawful interception and link up to the SSU's systems. The national legislation defines the requirements on information services providers to monitor information transmitted in order to detect illegal activities and to inform the competent public authorities. This is compliant with the general provisions of the Directive 2000/31/EC on electronic commerce Article 15.	None	None
• Non obstruction to out-of-court dispute settlement Some basic principles will be reflected in the draft of the Law on eCommerce.	The national legislation currently does not define the use of out-of-court schemes for dispute settlement regarding provision of eCommerce services, including by	Amend the national legislation allowing the use of out-of-court schemes for dispute settlement regarding provision of eCommerce services, including by appropriate

	appropriate electronic means.	electronic means.

Digital Skills

There are no specific requirements defined in the Association Agreements with Georgia, Moldova and Ukraine regarding Digital Skills.

Armenia - achievements, gaps and recommendations

Main achievements according to the EU baseline	Major gaps	Main recommended actions (priority areas for cooperation)
ICT for better education		
	Policy context, measuring the digital skills gap, initiatives to create growth and jobs, best practices	Measurement of the digital skills gap, formation of “National Coalition for Digital Jobs”

Azerbaijan - achievements, gaps and recommendations

Main achievements according to the EU baseline	Major gaps	Main recommended actions (priority areas for cooperation)
ICT for better education		
	Policy context, measuring the digital skills gap, initiatives to create growth and jobs, best practices	Measurement of the digital skills gap, formation of “National Coalition for Digital Jobs”

Belarus - achievements, gaps and recommendations

Main achievements according to the EU baseline	Major gaps	Main recommended actions (priority areas for cooperation)
ICT for better education, Initiatives to create growth and jobs		
	Policy context, measuring	Measurement of the digital

	the digital skills gap, best practices	skills gap, formation of “National Coalition for Digital Jobs”

Georgia - achievements, gaps and recommendations

Main achievements according to the EU baseline	Major gaps	Main recommended actions (priority areas for cooperation)
ICT for better education		
	Policy context, measuring the digital skills gap, initiatives to create growth and jobs, best practices	Measurement of the digital skills gap, formation of “National Coalition for Digital Jobs”

Moldova - achievements, gaps and recommendations

Main achievements according to the EU baseline	Major gaps	Main recommended actions (priority areas for cooperation)
ICT for better education		
	Policy context, measuring the digital skills gap, initiatives to create growth and jobs, best practices	Measurement of the digital skills gap, formation of “National Coalition for Digital Jobs”

Ukraine - achievements, gaps and recommendations

Main achievements according to the EU baseline	Major gaps	Main recommended actions (priority areas for cooperation)
ICT for better education, initiatives to create growth and jobs		
	Policy context, measuring the digital skills gap, best practices	Measurement of the digital skills gap, formation of “National Coalition for Digital Jobs”

Telecom Rules

Georgia – achievements, gaps and recommendations relevant to the Association Agreement

Achievements according to the related topics of the country's Association Agreement	Major gaps	Main recommended actions (priority areas for cooperation)
Directive 2002/21/EC (Framework Directive) as amended by Directive 2009/140/EC	Rights of way Definitions of broadband and infrastructure markets	Implement simple, efficient, transparent procedures, applied without discrimination or delay Implement COMMISSION RECOMMENDATION of 9.10.2014 on relevant product and service markets within the electronic communications sector
Directive 2002/20/EC (Authorisation Directive) as amended by Directive 2009/140/EC	None	None
Directive 2002/19/EC (Access Directive) as amended by Directive 2009/140/EC	Wholesale broadband safeguards for Next Generation Access	Implement the specific requirements of COMMISSION RECOMMENDATION of 11.9.2013 on consistent non-discrimination obligations and costing methodologies to promote competition and enhance the broadband investment environment
Directive 2002/22/EC (Universal Services Directive) as amended by Directive 2009/136/EC	Implementing regulation on Universal Service obligations (USO), including the establishment of mechanisms for costing and financing	Implement the specific requirements from the Universal Service Directive relating to broadband quality
Decision 676/2002/EC on a regulatory framework for	None	None

radio spectrum policy		
Directive 2002/58/EC (Directive on privacy and electronic communications) as amended by Directive 2009/136/EC	None	None

Note: The above table refers only to the topics of the EU/ Georgia Association agreement. Georgia has largely implemented the basic requirements. There are a number of other priority areas for cooperation recommended that relate specifically to the additional EU Baseline requirements defined in this study, in particular for Leadership, policy, strategy and resources, investment and infrastructure.

Georgia - additional gaps and recommendations

Additional topics of the EU baseline	Major gaps	Main recommended actions (priority areas for cooperation)
Leadership, policy, strategy and resources, investment and infrastructure	Broadband infrastructure funding and state aid rules	Implement state aid rules for broadband investment in line with EU
	Universal broadband targets	Formulate “Digital Agenda” targets for universal high-speed broadband access

Moldova - achievements, gaps and recommendations relevant to the Association Agreement

Achievements according to the related topics of the country’s Association Agreement / DCFTA	Major gaps	Main recommended actions (priority areas for cooperation)
Directive 2002/21/EC (Framework Directive) as amended by Directive 2009/140/EC	Rights of way Definitions of broadband and infrastructure markets	Implement simple, efficient, transparent procedures, applied without discrimination or delay Implement COMMISSION RECOMMENDATION of 9.10.2014 on relevant product and service markets within the electronic

		communications sector
Directive 2002/20/EC (Authorisation Directive) as amended by Directive 2009/140/EC	None	None
Directive 2002/19/EC (Access Directive) as amended by Directive 2009/140/EC	Wholesale broadband safeguards for Next Generation Access	Implement the specific requirements of COMMISSION RECOMMENDATION of 11.9.2013 on consistent non-discrimination obligations and costing methodologies to promote competition and enhance the broadband investment environment
Directive 2002/22/EC (Universal Services Directive) as amended by Directive 2009/136/EC	The single European emergency number 112 has not yet been implemented	Implement the specific requirements from the Universal Service Directive relating to broadband quality
Decision 676/2002/EC on a regulatory framework for radio spectrum policy	None	None
Directive 2002/58/EC (Directive on privacy and electronic communications) as amended by Directive 2009/136/EC	None	None
Commission Directive 2002/77/EC on competition in the markets for electronic communications networks and services	None	None
Directive 2000/31/EC (Directive on electronic commerce)	None	None

Note: The above table refers only to the topics of the EU/ Moldova Association agreement. Moldova has largely implemented the basic requirements. There are a number of other priority areas for

cooperation recommended that relate specifically to the additional EU Baseline requirements defined in this study, in particular for Leadership, policy, strategy and resources, investment and infrastructure.

Moldova – additional gaps and recommendations

Additional topics of the EU baseline	Major gaps	Main recommended actions (priority areas for cooperation)
Leadership, policy, strategy and resources, investment and infrastructure	Broadband infrastructure funding and state aid rules	Implement state aid rules for broadband investment in line with EU
	Universal broadband targets	Formulate “Digital Agenda” targets for universal high-speed broadband access

Ukraine - achievements, gaps and recommendations relevant to the DCFTA

Achievements according to the related topics of the country’s DCFTA	Major gaps	Main recommended actions (priority areas for cooperation)
Directive 2002/21/EC (Framework Directive) as amended by Directive 2009/140/EC	-Strengthening the independence and administrative capacity of the national regulator in the field of electronic communications, –Establishing public consultation procedures for new regulatory measures, –Establishing effective mechanisms for appeal against the decisions of the national regulator in the field of electronic communications, –Defining the relevant product and service markets in the electronic communications sector that are susceptible to ex ante regulation and analyse those	Defining relevant product and service markets for wholesale broadband and infrastructure access services, analysing these markets for effective competition and applying market remedies that will improve competition and investment in high-speed broadband infrastructure

	markets with a view to determining whether significant market power (SMP) exists on them.	
Directive 2002/20/EC (Authorisation Directive) as amended by Directive 2009/140/EC	Implementing a regulation providing for general authorisations and restricting the need for individual licences to specific, duly justified cases.	Replacement of the current licensing regime with general authorisations and simple notification procedures
Directive 2002/19/EC (Access Directive) as amended by Directive 2009/140/EC	Based on the market analysis carried out in accordance with Directive 2002/21/EC the National regulator in the field of electronic communications shall impose on operators found to have significant market power (SMP) on the relevant markets, appropriate regulatory obligations with regard to: - access to, and use of, specific network facilities - price controls on access and interconnection charges, including obligations for cost orientation - transparency, non-discrimination and accounting separation Wholesale broadband safeguards for Next Generation Access	Defining these measures for the priority markets of wholesale broadband and infrastructure access. Implement the specific requirements of COMMISSION RECOMMENDATION of 11.9.2013 on consistent non-discrimination obligations and costing methodologies to promote competition and enhance the broadband investment environment
Directive 2002/22/EC (Universal Services Directive) as amended by Directive 2009/136/EC	Regulation on Universal Service obligations (USO), including the establishment of mechanisms for costing and financing	Implementation of full number portability and the European emergency number Implement the specific

	Number portability The single European emergency number 112 is not yet implemented	requirements from the Universal Service Directive relating to broadband quality
Decision 676/2002/EC on a regulatory framework for radio spectrum policy	Policy and regulations ensuring the harmonised availability and efficient use of spectrum, taking account of the market needs and the optimal use of scarce resources	Adoption of policy for use of "digital dividend" to promote universal high-speed broadband availability

Note: The above table refers only to the topics of the EU/ Ukraine Association agreement. In addition, there are a number of other priority areas for cooperation recommended that relate specifically to the additional EU Baseline requirements defined in this study, in particular for Leadership, policy, strategy and resources, investment and infrastructure.

Ukraine – additional gaps and recommendations

Additional topics of the EU baseline	Major gaps	Main recommended actions (priority areas for cooperation)
Leadership, policy, strategy and resources, investment and infrastructure	Broadband infrastructure funding and state aid rules Universal broadband targets	Implement state aid rules for broadband investment in line with EU Formulate "Digital Agenda" targets for universal high-speed broadband access
Directive 2002/21/EC (Framework Directive) as amended by Directive 2009/140/EC	Rights of way Definitions of broadband and infrastructure markets	Implement simple, efficient, transparent procedures, applied without discrimination or delay Implement COMMISSION RECOMMENDATION of 9.10.2014 on relevant product and service markets within the electronic communications sector
Directive 2002/19/EC (Access Directive) as	Wholesale broadband safeguards for Next	Implement the specific requirements of

amended by Directive 2009/140/EC	Generation Access	COMMISSION RECOMMENDATION of 11.9.2013 on consistent non-discrimination obligations and costing methodologies to promote competition and enhance the broadband investment environment

(For other Partner countries)

Armenia

Main achievements according to the EU baseline	Major gaps	Main recommended actions (priority areas for cooperation)
Some aspects of Directive 2002/21/EC (Framework Directive) as amended by Directive 2009/140/EC	Strengthening the independence and administrative capacity of the national regulator in the field of electronic communications Rights of way Definitions of broadband and infrastructure markets	Alignment with EU legal and regulatory framework Implement simple, efficient, transparent procedures, applied without discrimination or delay Implement COMMISSION RECOMMENDATION of 9.10.2014 on relevant product and service markets within the electronic communications sector
Some aspects of Directive 2002/20/EC (Authorisation Directive) as amended by Directive 2009/140/EC	Implementing a regulation providing for general authorisations and restricting the need for individual licences to specific, duly justified cases	Replacement of the current licensing regime with general authorisations and simple notification procedures
Some aspects of Directive 2002/19/EC (Access Directive) as amended by Directive 2009/140/EC	Wholesale broadband safeguards for Next Generation Access	Defining full access, transparency and pricing obligations measures for the priority markets of wholesale broadband and infrastructure access.

		Implement the specific requirements of COMMISSION RECOMMENDATION of 11.9.2013 on consistent non-discrimination obligations and costing methodologies to promote competition and enhance the broadband investment environment
Some aspects of Directive 2002/22/EC (Universal Services Directive) as amended by Directive 2009/136/EC	Only mobile number portability so far implemented The single European emergency number 112 is not yet implemented	Implementation of full number portability and the European emergency number Implement the specific requirements from the Universal Service Directive relating to broadband quality
Decision 676/2002/EC on a regulatory framework for radio spectrum policy	Policy and regulations ensuring the harmonised availability and efficient use of spectrum, taking account of the market needs and the optimal use of scarce resources	Adoption of policy for use of "digital dividend" to promote universal high-speed broadband availability
Leadership, policy, strategy and resources, investment and infrastructure	Broadband infrastructure funding and state aid rules Universal broadband targets	Implement state aid rules for broadband investment in line with EU Formulate "Digital Agenda" targets for universal high-speed broadband access

Azerbaijan

Main achievements according to the EU baseline	Major gaps	Main recommended actions (priority areas for cooperation)
Some aspects of Directive 2002/21/EC (Framework Directive) as amended by Directive 2009/140/EC	Strengthening the independence and administrative capacity of the national regulator in the field	Alignment with EU legal and regulatory framework

	of electronic communications Establishing public consultation procedures for new regulatory measures, –Establishing effective mechanisms for appeal against the decisions of the national regulator in the field of electronic communications, –Defining the relevant product and service markets in the electronic communications sector that are susceptible to ex ante regulation and analyse those markets with a view to determining whether significant market power (SMP) exists on them.	Implement COMMISSION RECOMMENDATION of 9.10.2014 on relevant product and service markets within the electronic communications sector
Some aspects of Directive 2002/20/EC (Authorisation Directive) as amended by Directive 2009/140/EC	Implementing a regulation providing for general authorisations and restricting the need for individual licences to specific, duly justified cases	Replacement of the current licensing regime with general authorisations and simple notification procedures
Some aspects of Directive 2002/19/EC (Access Directive) as amended by Directive 2009/140/EC	Based on the market analysis carried out in accordance with Directive 2002/21/EC the National regulator in the field of electronic communications shall impose on operators found to have significant market power (SMP) on the relevant markets, appropriate regulatory obligations with regard to: - access to, and use of, specific network facilities - price controls on access and interconnection	Defining these measures for the priority markets of wholesale broadband and infrastructure access. Implement the specific requirements of COMMISSION RECOMMENDATION of 11.9.2013 on consistent non-discrimination obligations and costing methodologies to promote competition and enhance the broadband investment environment

	charges, including obligations for cost orientation - transparency, non-discrimination and accounting separation Wholesale broadband safeguards for Next Generation Access	
Some aspects of Directive 2002/22/EC (Universal Services Directive) as amended by Directive 2009/136/EC	Only mobile number portability so far implemented The single European emergency number 112 is not fully implemented	Implementation of full number portability and the European emergency number Implement the specific requirements from the Universal Service Directive relating to broadband quality
Decision 676/2002/EC on a regulatory framework for radio spectrum policy	Policy and regulations ensuring the harmonised availability and efficient use of spectrum, taking account of the market needs and the optimal use of scarce resources	Adoption of policy for use of "digital dividend" to promote universal high-speed broadband availability
Leadership, policy, strategy and resources, investment and infrastructure	Separation of policy and regulatory functions for the sector Broadband infrastructure funding and state aid rules Universal broadband targets	Implement state aid rules for broadband investment in line with EU Formulate "Digital Agenda" targets for universal high-speed broadband access

Belarus

Main achievements according to the EU baseline	Major gaps	Main recommended actions (priority areas for cooperation)
Some aspects of Directive	Strengthening the	Alignment with EU legal and

2002/21/EC (Framework Directive) as amended by Directive 2009/140/EC	independence and administrative capacity of the national regulator in the field of electronic communications Rights of way Definitions of broadband and infrastructure markets	regulatory framework Implement simple, efficient, transparent procedures, applied without discrimination or delay Implement COMMISSION RECOMMENDATION of 9.10.2014 on relevant product and service markets within the electronic communications sector
Some aspects of Directive 2002/20/EC (Authorisation Directive) as amended by Directive 2009/140/EC	Implementing a regulation providing for general authorisations and restricting the need for individual licences to specific, duly justified cases	Replacement of the current licensing regime with general authorisations and simple notification procedures
Some aspects of Directive 2002/19/EC (Access Directive) as amended by Directive 2009/140/EC	Based on the market analysis carried out in accordance with Directive 2002/21/EC the National regulator in the field of electronic communications shall impose on operators found to have significant market power (SMP) on the relevant markets, appropriate regulatory obligations with regard to: - access to, and use of, specific network facilities - price controls on access and interconnection charges, including obligations for cost orientation - transparency, non-discrimination and accounting	Defining these measures for the priority markets of wholesale broadband and infrastructure access. Implement the specific requirements of COMMISSION RECOMMENDATION of 11.9.2013 on consistent non-discrimination obligations and costing methodologies to promote competition and enhance the broadband investment environment

	separation Wholesale broadband safeguards for Next Generation Access	
Some aspects of Directive 2002/22/EC (Universal Services Directive) as amended by Directive 2009/136/EC	Only mobile number portability so far implemented The single European emergency number 112 is not yet implemented	Implementation of full number portability and the European emergency number Implement the specific requirements from the Universal Service Directive relating to broadband quality
Decision 676/2002/EC on a regulatory framework for radio spectrum policy	Policy and regulations ensuring the harmonised availability and efficient use of spectrum, taking account of the market needs and the optimal use of scarce resources	Adoption of policy for use of “digital dividend” to promote universal high-speed broadband availability
Leadership, policy, strategy and resources, investment and infrastructure	Separation of policy and regulatory functions for the sector Broadband infrastructure funding and state aid rules Universal broadband targets	Implement state aid rules for broadband investment in line with EU Formulate “Digital Agenda” targets for universal high-speed broadband access

4 DETAILED STATE OF PLAY AND GAP ANALYSIS OF THE PARTNER COUNTRIES

Network, Information Security and Cybersecurity

Armenia

Leadership, policies, legal frameworks

The area is regulated by two main legal documents: the Concept on the Formation of Electronic Society 2010-2012 (2010) and the Convention on the Cybercrimes of the Council of Europe (signed in 2001, ratified in 2006, entered into force in 2007).[26] In addition, there are references to this area in such legal acts as IT Security Concept (2009), the Concept on the Development of Internet Society (2010), the Criminal Code, the Law on Personal Data and the draft Law on the Protection of the Personal Data (is developed according to EU standards). The latter specifically addresses the issue of guaranteeing the confidentiality of traffic data and public electronic communications services; it also defines criminal offences and sanctions in the area of attacks against information systems and computer data (in addition to the definitions given in the Civil and Criminal Codes). The new draft law on the Protection of Personal Data contains provisions requiring trust and other service providers to take adequate technical and organizational measures to minimize the impact of security incidents and in the case of the security breach they should notify the supervisory body.

Most of the initiatives undertaken so far relate to the Cybercrime Convention. Joining the Convention has prompted positive changes to the Civil Code to fully comply with the requirements of the Convention. All the legal requirements expressed by the Convention are included in the national legislation but the enforcement of the regulations is weak.

The IT Security Concept defines IT security but does not cover adequately the broader scope of NIS/cyber-security issues, some of which have been addressed by individual citizens, experts and non-government organizations by, for example, discussing new ways and formats of public-private partnerships, a possibility of establishing national CERT.

While the overall assessment of the NIS sector can be assessed as relatively strong, it is also obvious that, until now, the state's attention has been primarily focused on the conventional (physical) forms of security. Information and cyber-security is yet to be recognized as an equally critical national priority. Consequently, the actual practice (e.g. implementation of related initiatives, building resilient infrastructures, providing services, allocating resources) constitutes only a fraction of the EU baseline. The lack of clear strategy makes Armenia vulnerable against possible security threats with little resources (technical, human, financial) available to counter such threats. Current policies do not envisage or require assessing the vulnerability levels of critical information infrastructures. The private sector's infrastructure (except banking)[27] seems especially vulnerable. These are serious drawbacks. Cooperation with the EU is considered an important policy objective. That may help lower the existing barriers.

Strategy, implementation, resources, infrastructures

[26] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

[27] All banks operating in Armenia are mandated to undergo ISO 2007 IT Security Certification until the end of 2015.

Armenia does not have a stand-alone strategy in the field of NIS (cyber-security is covered partly by the CoE's Convention on Cybercrime). Strategic priorities in this area are not clearly defined and/or formulated which is evidenced by the absence of an official national/government CERT. To alleviate this problem, the government has initiated the creation of the local Internet Governance Forum to serve as a multi-stakeholder cooperation model. The Internet Governance Forum developed and submitted in March 2015 to the government a list of priority issues; among them a study on best international experience, setting up and operating CERTs and (b) developing infrastructure for addressing and preventing cyber-crimes. At the moment, the budgetary allocations are not sufficient to address the growing security-related challenges properly, with the significant effort coming from individuals and civil society working on a voluntary basis.

The government's current approach distinguishes between security of networks and infrastructures, on the one hand, and information content, on the other. The first domain is supervised by the National Security Service, while the second one is under the Centre on Public Relations and Information adjacent to the President Office. Technically, the government websites and internal networks are protected adequately.

Preparatory work has started in the area of cyber-attack simulation but it is not done consistently. Some elements of alert/hotlines have been introduced in the state sector only. No strategy exists to educate the public through awareness campaigns. The cyber-security products and standards are used in the state and banking sectors. Telecom operators are obliged to adequately meet a set of requirements that came with the license; however, these are mainly technical ones. There is no requirement of the minimal security level to be met. Legally, the competent national regulator is not obliged to inform the public when the disclosure of security breaches is in the public interest. No conceptual approach or a specific policy exists in these areas.

Armenia fares well in terms of Internet openness and freedoms ranking high in international comparisons. [28] As per the Cybercrime Convention personal insults, defamation and similar communications in the social media are not considered criminal offences. The new draft Law on Personal data Protection intends to guarantee the confidentiality and privacy on the publicly available electronic communications networks and services.

Institutions, services

Armenia does not have an official/government CERT unit, and there is no law/regulation and funds to having it. De facto, the Internet Society NGO provides some CERT services in a private manner (certified as a 'Trusted Introducer').

The National Security Service is responsible for the security of Government websites. The single firewall giving access to Government websites is operated and installed in the National Security Service (NSS). Other state websites, such as those of National Parliament, President Office, and Local State Authorities are not under NSS supervisory.

A separate function in this area is implemented by the Ministry of Defence regarding the defence sector alone. Activities are strictly confidential and are not available to public information. The banking sector stands out in terms of security both on policy and implementation levels. The Central Bank of

[28] 28th in Freedom of the Net, 7th in Obstacles to Access, 9th in Limits on Content, 12th in Violation of User Rights.

Armenia (CBA) is in charge of regulating this area. According to CBA regulations all banks operating in Armenia are mandated to undergo ISO 2007 IT Security Certification until the end of 2015.

List of institutions:

- Police force – level of involvement in the issue and cooperation with the EU is Medium; focal point for cooperation activities
- National Security Service (NSS) – involvement in the issue and cooperation with the EU is Low; responsible for the security of the government websites
- National Commission on Security – involvement in the issue and cooperation with the EU is Low; developed the Concept on IT Security
- Internet Society (ISOC) – involvement in the issue and cooperation with the EU is High; Non-governmental CERT
- Internet Governance Forum – level of involvement in the issue and cooperation with the EU is high; responsible for public consultations and discussions
- Ministry of Transport and Communication – level of involvement in the issue and cooperation with the EU is medium

Azerbaijan

Leadership, policies, legal frameworks

There is strong political will at the highest level to recognize the importance of NIS as a national priority issue. It is evidenced by the President's Decrees on the National Security Concept of the Republic of Azerbaijan (approved by Presidential Order #2198 of 23.05.2007) and the National Strategy for development of information society in the Republic of Azerbaijan for 2014-2020 (#708 of 26 September 2012). The former established two key organizations: (a) Special Communication and Information Security State Agency under Special State Protection Service of the Republic of Azerbaijan (CERT.GOV.AZ) and (b) Cyber Security Centre under the Ministry of Communication and High Technologies (CERT.AZ). In addition, there is a Computer Security Incident Group of Azerbaijan National Academy of Sciences – AzScienceCERT. The Decree has a clear objective to provide protection, stability and continuity of information processes, protection of information resources of government agencies, to prevent and analyse threats in the field of NIS.

There are many benefits seen by the authorities in Azerbaijan as a result of a possible cooperation with the EU ranging from the improved efficiency in the work of public bodies and advanced technology to safer and open internet and greater trust in digital communications.

However, the establishment of these important institutions has not been accompanied by the creation of the fully enabling legal and regulatory environment to increase the effectiveness and impacts of the national CERT unit. To do so, a thorough review of the international experience is needed, especially from Europe so as to create a pool of knowledgeable local experts who are not readily available in the country. For example, there are no legal provisions concerning the minimum requirements in the field of network, information and cyber security. Likewise, there is no legal clarity on how to handle security breaches on public communications networks and instruct providers of public electronic communications services in case of such breaches, except that law enforcement agencies have the right to obtain information from network and service provide for investigation purposes. As a rule, CERT.GOV.AZ and Cyber Security Centre (CERT.AZ), as well as AzScienceCert do inform the public

about security breaches via social media, TV and relevant websites and provide technical support to eliminate the effects of such breaches.

As far as the legislation on confidentiality of data and privacy protection is concerned, there are some provisions in (a) Law on Information, Informatisation and Protection of Information, (b) Law on access to information, (c) Law on State Secret. However, the legislation is fragmented and contains significant gaps to be eliminated.

Up to now, Azerbaijan has adopted 14 national standards that are identical to the existing international standards in the sphere of information.

There are minimum rules established that define criminal offences and sanctions in the area of attacks against information systems and computer data. These laws include

- Criminal code of the Republic of Azerbaijan
- Information, informatisation and protection of information
- The law of the Republic of Azerbaijan on Personal Data
- Decree of the President of the Republic of Azerbaijan about Improving activity on information security

Organizations dealing with information security in Azerbaijan pursue a policy of cooperation in (a) developing and funding a network of Cybercrime Centres of Excellence to facilitate training and capacity building including through mutual support, (b) creating a cooperation mechanism with counterparts to share early warnings on risks and incidents through a secure infrastructure and organizing regular peer reviews, (c) regularly publishing on a dedicated website (www.cert.az. www.cert.gov.az, www.sciencecert.az) unclassified information about early warnings on incidents and risks and on coordinated responses. International cooperation includes the international unions of Computer Emergency Response Teams (FIRST, Trusted Introducer, Anti-Phishing Working Group, the Organization of the Islamic Cooperation CERT), CERT Coordination Centre, CERT teams of different countries (such as Georgia, Bulgaria, Iran, Japan, Russia, Ukraine, Latvia, Slovakia, Kazakhstan and others), local and foreign cyber security organizations, software and hardware production companies which operate in the field of cyber security.

Azerbaijan's cyber-security policies draw on a principle of an open, safe and secure cyberspace prioritizing the protection of fundamental rights and personal data, freedom of expression and speech. However, there is no special policy on capacity building in the field of NIS to address these and other issues more effectively. The local CERT.GOV.AZ and Cyber Security Centre (CERT.AZ) undertake capacity building activities on an ad hoc basis in the form of trainings, workshops and discussions for strengthening staff capacities, establishment of laboratories for virus analysis and penetration tests.

Strategy, implementation, resources, infrastructures

The available legislation (especially the National Security Concept of the Republic of Azerbaijan) and the National Strategy for development of information society in the Republic of Azerbaijan for 2014-2020 has yet to be translated into a series of regulatory acts and strategies (programmes) to enforce the legislation more vigorously. A list of sectors with the critically important information infrastructures (prepared by the Cyber Security Centre of the Ministry of Communication and High Technologies) awaits official approval.

At the moment, the country does not have a specific national strategy on Network and information security/Cyber-security. The related activities that are being implemented fall under the National

Strategy for development of information society in the Republic of Azerbaijan for 2014-2020. These help enlighten the general public and private organizations about cyber security to form security culture, develop skills and competencies, create technical and methodical means, provide support for strengthening of cyber security, and enhance potential for R&D in this field.

Other activities being implemented address the development of the industrial and technological resources for cyber-security, reduction of the cybercrime level, elaboration of a cyber-defence policy, providing support to the existing CERTs, simulations of cyber-attack. However, the latter are not carried out regularly.

In terms of cyber-security products and standards, the ongoing activities have covered training activities to strengthen staff capacities in getting familiar with international information security standards to (a) prepare the proposals for introducing new national standards and creating new rules on their basis; (b) analyze of software and hardware products that widely used by users in terms of security; (c) collect and analyze information coming from users and software developers regarding other countries' experience in cyber-attacks, illegal intrusions, spread of malicious codes in the information systems and networks, computer equipment and software; (d) develop guidelines and recommendations about software and hardware; (e) give advice on selecting software and hardware tools for better security; (f) cooperate with vendors when defects and shortages are found in software and hardware devices.

Institutions, services

Following the accession to the Convention on Cybercrime, the Ministry of National Security of the Republic of Azerbaijan was appointed as coordinating body which is available on a 24/7 regime, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form in relation to criminal offence. In 2012, the President's Decree #708 established (a) Special Communication and Information Security State Agency under Special State Protection Service of the Republic of Azerbaijan and (b) Cyber Security Centre under the Ministry of Communication and High Technologies. In addition, there is a Computer Security Incident Group of Azerbaijan National Academy of Sciences – AzScienceCERT.

CERT.AZ (Cyber Security Centre) functions under Ministry of Communications and High Technologies. CERT.AZ is a state coordinating body and engages in coordinating the action of information infrastructure subjects, reporting about existing and potential risks at national level, educating public, private and other institutions in the field of cyber security and providing methodological assistance to them. CERT.AZ has its hotline (1654) and special email address for reporting security incidents. CERT.AZ cooperates with many international organizations and communities including FIRST - Forum of Incident Response and Security Teams, CERT® Coordination Centre (CERT/CC), Anti-Phishing Working Group (APWG), Trusted Introducer (TI). CERT.AZ has bilateral cooperation agreements with CERT teams from such countries as Russia, Georgia, Iran, Latvia, Slovakia, Kazakhstan, Ukraine and other countries.

CERT.GOV.AZ functions under Special Communication and Information Security State Agency of the Special State Protection Service of the Republic of Azerbaijan. Main duties of the Team are the development of recommendations for application of the most effective software-hardware tools ensuring the prevention of unauthorized interventions in the information systems for official users based on study and generalization of the international practice on ensuring computer security. CERT.GOV.AZ also provides advisory services and urgent technical aid to individual users timely informing them about threats to computer security. Support to authorities in investigation of the

computer incidents, advice in selecting software and hardware tools on ensuring computer security constitute an important part of the CETR's scope of work. There is "Report an incident" section on its website.

Belarus

Leadership, policies, legal/regulatory frameworks

There is a strong political will to minimize the negative impact of security threats/incidents on publicly available electronic communications networks and services, especially concerning the state information systems. It has resulted in passing the following key laws that regulate the area of NIS:

- Decree of the President of the Republic of Belarus of November 8, 2011 "On some issues of the Information Society Development in the Republic of Belarus"
- Decree of the President of the Republic of Belarus of September 1, 2010 "On licensing of certain activities"
- Law of the Republic of Belarus of November 10, 2008 № 455-Z" On information, informatisation and protection of information" (with special attention given to the secure exchange of electronic documents)
- Law of the Republic of Belarus of December 28, 2009 № 113-Z "On electronic document and digital signature"

The Concept on National Security (approved by the Decree of the President N 575 of 9 November 2010 and amended on 24 January 2014) gives a definition of the term 'information security' as a state of protection of the balanced interests of the individual, society and the state from external and internal threats in the information sphere. In addition, the Operational and Analytical Centre (OAC) under the President of the Republic of Belarus, as a single regulator in the area of technical and cryptographic information, issued a number of regulations (under the Order of 14 October 2012, № 79 "On some issues of functioning of the state system for management of open key digital signature verification in the Republic of Belarus"):

- Concept of the Development of the State system for management of open key digital signature verification of the Republic of Belarus
- Regulation on the State system for management of open key digital signature verification of the Republic of Belarus
- Regulations of the Inter-Ministerial Advisory Council on the development of the State system for management of open key digital signature verification of the Republic of Belarus

However, Belarus has not passed as yet a Law on personal data protection that would explicitly determine the requirements to protect personal data, although there is a plan to do so taking into account technological development and international experience. There is a strong economic incentive to pass such a law since the growing volume of the digital market and services require stronger security which cannot be ensured without the law guaranteeing the protection of personal data and privacy. The lack of confidence in the protection of personal data may hinder the uptake electronic services. According to the current legislation, personal data are regarded as the information of limited distribution and are protected at a high security level. Yet, in practice, not all organizations running information systems that may contain personal data are able to invest sufficiently to guarantee strong protection of data at their disposal. The liability for non-compliance with security requirements is rather light under the administrative punishment. There is no requirement that in the

case of the security breach trust and other service providers[29] notify the supervisory body within 24 hours after having become aware of the breach.

The National programme of accelerated development of services in the field of information and communication technologies (ICT) for 2011-2015 contains a sub-programme on Security of information and communication technologies and digital trust which includes as one of its activities the development of requirements and standards for security policies to be applied in public information systems.

Belarus has its own technologically advanced solutions for cryptographic protection of information that are on par with the world leading examples and intend to keep using such solutions, also from the national security perspective (it is argued that as many countries use local solutions across the EU as well). At the same time, for electronic document exchange internationally, the Law on Electronic Document and Electronic Digital Signature (of 28 December 2009 N 113-3) requires to use international treaties[30] and thus align with internationally recognized standards. Therefore the country can enter into bilateral agreements with other countries so as to mutually recognize local security solutions. Belarus has already signed the international agreement within Eurasian Economic Union that regulates security issues within the EEU.

The Operation and Analytical Centre (OAC) under the President of the Republic of Belarus is open for collaboration with the respective regulators in the EU countries to discuss and elaborate common solutions in this field. At the moment the level of cooperation with the regulators in the Commonwealth of Independent States (CIS) – including within the Customs Union and EEU – on technical regulation of NIS/Cyber-security is high. There is work underway to further harmonize the national system of accreditation with international standards and internationally recognized practices in order to ensure the mutual recognition of accreditation activities. For example, the Eurasian Economic Commission approved (the decision of № 154 of September 1, 2014) a Concept of using services and legally binding electronic documents in interstate information interactions. The Concept stipulates that the provision of cross-border exchange of legally binding electronic documents in an integrated system is implemented based on the trusted third party services. Such a system is under development. Another EEU's Decision (№180 of 30 September 2014) determines the order of keeping and exchanging electronic documents and data among the members of Customs Union for foreign trade. Alternative solutions that are not harmful to the national security and beneficial for business development could be considered taking into account the interests of all parties using the principles of the Trusted Third Party (T3P) system for mutual recognition of digital signatures across Eurasian Economic Union[31] and with the EU countries.

There are no stand-alone legal documents stating the importance of keeping the internet free and open in order to protect fundamental rights of individuals and democracy. The main emphasis has been placed to view the Internet as a tool for economic development, eGovernment services and as a channel of information delivery. The Law on Mass Media (N 427-3, of 17 July 2008) guarantees, among other freedoms, the freedom of opinion and expression including via the Internet, respect for human rights, diversity of opinion, while the Law On electronic communication (19 July 2005, No.45-

[29] There are two accredited trust service provides in Belarus.

[30] Articles 3, 5, 30.

[31] There have already been developed the Concept, Strategy and other legal regulations that could be used as a background material for extending the T3P system to electronic interaction with EU.

3) guarantees the secrecy of telephone communications and other messages transferred via electronic communications networks. If the information on security breaches is not classified, it is published on the website of the OAC. By now, there have no critical for society breaches of security; in most cases the revealed breaches are resolved in cooperation with Internet providers, mobile operators and banks that place the information on their websites. The users of electronic communications services are entitled to go court in case his/her rights have been violated and seek the compensation of the damage done in accordance with Regulations on the technical protection of information in information systems designed for processing of information, which distribution is not classified as state secrets approved by the Order of Operations and Analytical Centre under the President of the Republic of Belarus of 30.08.2013 № 62 (update 16.01.2015 № 3).

Strategy, implementation, resources, infrastructures

There is no explicit national strategy for Network and information security/Cyber-security The National programme of accelerated development of services in the field of information and communication technologies (ICT) for 2011-2015 contains the sub-programme on Security of information and communication technologies and digital trust which includes the enhancement of staff competencies in the field of information protection and security. In addition, the Operational and Analytical Centre (OAC) under the President of the Republic of Belarus (of 9 June 2011, № 48) issued an executive order "On Approval of the order of attesting of managers responsible for ensuring the protection of state secrets, and other employees of government agencies and other organizations working with state secrets, as for application of technological measures protecting state secrets" to ensure that heads and staff of departments for technical protection of information and other units active in the technical protection of state secrets, as well as officials of the organizations that perform these functions, undergo mandatory attestation.

While there are no systematic simulation of cyber-attacks and no national alert platforms, the OAC undertakes risk management exercises, monitors and studies the issue of cyber-attacks and exchanges information with its counterparts in other countries, interacts with antivirus companies. CERT.BY has opened hotlines for reporting on harmful content. However, the activities of CERT.BY are not sufficiently known in the country. Raising public awareness in the field of NIS is done mainly via professional training courses and IT education for students, and also through social advertising.

While the Operational and Analytical Centre (OAC) possesses all the necessary competencies to perform its functions, there is a shortage of qualified personnel outside the capital city due to the wages gap between the state sector and ICT industry.

Most of security-related standards applied in Belarus are based on respective ISO standards. All information security tools – whether local and not – should be certified by the OAC. Special security requirements are imposed in relation to critically important objects information.

Criminal offences and sanctions in the area of attacks against information systems and computer data are defined in the Criminal Code of Belarus (e.g. Chapter 31- Crimes against information security).

There is no specific legislation for the critical information infrastructure (although some regulation is being developed). The Concept on National Security (2010) highlights the importance of the development and introduction of modern methods and means of information protection in the information systems used in the vital for the country infrastructures. The status of the critically important objects of informatisation (CIOI) is assigned on the basis of sectoral criteria, taking into account the level of damage to the national interests in the political, economic, social, informational, ecological and other spheres. There is a definition of what the critically important objects of

informatisation are. There is no obligation on the part of telecom services providers, owners of information systems with limited distribution of information or the owners of the critically important objects of infrastructure to report to the authorities about all incidents which severely endanger their networks. However, it is a good practice to do so.

Institutions, services

Operational and Analytical Centre (OAC) under the President of Belarus is a national regulator that develops principles and implements activities related to NIS, in cooperation with the Ministry for Internal Affairs in the elaboration of draft laws. It is the most competent body in the country in the technical aspects of cyber-security. Among other functions, OAC develops draft regulations, including technical regulations, and receives (approves) such acts on technical and cryptographic protection of information; is involved in the development of draft regulations concerning informatisation; it is also a single regulator in the area of technical and cryptographic information in Belarus. As a national regulator OAC is empowered to coordinate and instruct the operators of public communications networks or providers of public electronic communications services in case of security breach. This is prescribed by the Decree of the President of Belarus of 16 April 2013 г. № 196 "On some measures of information protection improvement". OAC provides not only advice and consultation on critically important infrastructures but also assists other state organizations and private companies.[32]

The National Computer Emergency Response Team (CERT.BY) of Belarus deals with cyber-security incidents and is open to both state and private legal and physical entities. It serves as one of mechanisms (operating organization) for enabling the national cyber-security. CERT.BY collects, stores and processes statistics on malware dissemination and network attacks in Belarus, as well as on incidents response in the information systems of the state and other bodies. The types of threats and incidents that the CERT.BY is responsible for include:

- information access blocking;
- malware dissemination;
- unauthorized access, modification, theft of information;
- network attack.

To reduce the risks and minimize the number of required responses, CERT provides preventative and educational services for their clients, develops recommendations to address vulnerabilities in software and equipment used, as well as informs the users about exploits and viruses during the periods of their dissemination. The work schedule is determined based on the needs of particular sector (national, state academic, domestic, etc.). Since September 2013, CERT.BY is part of the international community of Incident Response and Security teams «FIRST». Collaboration with the EU is less active.

Georgia

Leadership, policies, legal frameworks

The government of Georgia demonstrates strong political will and commitment to minimize the negative impact of security threats/incidents on publicly available electronic communications networks

[32] E.g. responding to the requests from mobile operators during the mass fraud attacks that have happened in March 2015.

and services by passing necessary laws, taking adequate executive decisions and effectively implementing them in practice. The list of key laws includes:

- Convention on Cybercrime (signed in 2008, ratified in 2012, entered into force in 2012)
- National cyber security strategy 2012-2015. Work on a New cyber security strategy has begun, coordinated by the Council for State Security and Crisis Management
- Law on "Information Security"
- Criminal Code contains cybercrime provisions
- Various regulations have been adopted by relevant state entities in the field of Network and Information Security/ cyber Security

The secondary regulations include the following decrees by the Data Exchange Agency of Ministry of Justice:

- Decree of the Chairman of Data Exchange Agency about Computer incident response group
- Decree of the Chairman of Data Exchange Agency on procedures, technical standards, format and submission routes of data/information to unified state registry
- Decree of the Chairman of Data Exchange Agency on Minimal Information Security requirements
- Decree of the Chairman of Data Exchange Agency on Network sensor configuration rules
- Decree of the Chairman of Data Exchange Agency on management rules of information assets
- Decree of the Chairman of Data Exchange Agency on rules of Information Security Audits
- Decree of the Chairman of Data Exchange Agency on Rules of Authorization of Authorized persons and organizations and authorization fees
- Decree of the Chairman of Data Exchange Agency on minimal standards for information security managers of Critical Information Systems
- Code of Criminal Procedure of Georgia (procedural requirements of the Cybercrime Convention);
- Law on Operative and Detective Activities (procedural requirements of the Cybercrime Convention related to interception);
- Law on Electronic Communications (traffic data regulations);
- Law on Personal Data Protection (data security with respect to processing of personal data);
- Memorandum of Understanding between the Law Enforcement Agencies and Internet Service Providers based on the principles of cooperation in the field of cybercrime.

International cooperation is an important principle of the national policy in NIS/Cyber-security. Since March 2011, Ministry of Internal Affairs (MIA) is actively involved in the Council of Europe's new project for the Eastern Partnership countries "Cooperation against Cybercrime". The main objective of the present project is to strengthen the capacities of criminal justice authorities of Georgia for more effective cooperation against cybercrime. Joining the Cybercrime Convention has had a strong positive effect on enhancing international cooperation with police forces. The Cybercrime Division of

the Criminal Police Department was created in December 2012 as a specialized cybercrime investigation unit which hosts a 24/7 national contact point for cybercrime investigations, as required by the Convention on Cybercrime. The Cybercrime Division is backed up by the expert capacities of the Operative-Technical Department of the MIA in terms of digital forensics. Operative-Technical Department also serves as police CSIRT (CERT) and cooperates with the Ministry of Justice Data Exchange Agency's CERT.GOV.GE for various cyber security operations (botnet takedowns, website defacements, handling of incidents, etc.).

The bilateral project between Georgia and Estonia was implemented in 2012 to increase the capacities of the Georgian MIA operative units for combating cybercrime and the seizure of digital evidences. The MIA is also actively cooperates with US Federal Bureau of Investigation in handling cybercrime cases. Data Exchange Agency (DEA) of the Ministry of Justice cooperates with international partners in e-governance (the EU TWINNING initiative). DEA is also a member of IMPACT (the Cyber security executing arm of the ITU) and of The Trusted Introducer (the trusted backbone of the Security and Incident Response Team community in Europe). DEA has tried to start discussing cooperation with ENISA (in training), but the latter was not forthcoming at the time. Georgian CERT has become a member of FIRST – Forum of Incident Response and Security Teams (following an audit conducted by Austrian and Polish partners). It extensively cooperates with many other CERTs.

The law "Information Security" entered into force from July 1st, 2012. Its aim is to introduce the requirements of ISO/IEC 27001 international standard for critical information system subjects and to create legal grounds for operations of national CERT (CERT.GOV.GE). The Law stipulates a number of obligations for critical information system subjects, such as a duty to adopt information security policies compliant with ISO 27000 minimum requirements, appointment of information security officers and cyber security specialists, as well as a duty to perform information asset inventory assessment, in order to categorize these assets in terms of their criticality/confidentiality. The Law also confers the right upon critical information subjects to request information security audit, undergo penetration testing, and/or install and manage a network sensor for the detection of cyber incidents. The Law lists extensively competences of CERT.GOV.GE as a national CERT and its interaction and exchange of data with owners of critical information systems.

The law is also an acknowledgement of the increasing use of ICT by state institutions and private sector and the high role of security in such use. Apart from introducing the concept of "critical information systems", it refers to and regulates state and private entities of critical information systems and nonstop functioning of systems of significant importance for the country's security. To define these entities, the following criteria are used: volume and scale of expected results if information system is compromised, economic damage, importance of the service, number of customers, etc.

The Convention on Cybercrime specifies crimes committed in cyberspace that result in criminal responsibility. In Georgia, the Criminal Code (XXXV Chapter) lists illegal actions in cyberspace that lead to criminal responsibility: Illegal Interception of Computer System (Art. 284), Misuse of Computer Data or Computer System (Art. 285), Computer System or Data Interference (Art. 286). In addition, Georgian Criminal Code envisages criminal responsibility for Ensuring Availability of Child Pornography in any form (including online) (CCG Art. 255-2), Infringing of Copyright or Related Rights (Art. 189) and Cyber Terrorism (Art. 3241). In addition, there are extensive and complex provisions of the procedural nature in the Code of Criminal Procedure of Georgia (which contains a special Chapter XVI on Investigative Actions in relation to Computer Data) and the Law on Operative and Detective Activities (interception of electronic communication identifying data, Art. 7). These provisions have been discussed internally in Georgia and also reviewed by the Council of Europe Cybercrime

Committee through various cycles of assessments to confirm the compliance with the Cybercrime Convention.

In May 2013, Georgian President approved a Cyber Security Strategy for 2013-2015 that is the main document to define key trends in NIS/Cyber-security. Strategy has an action plan that provides future actions and responsible state bodies for their implementation.

The amendments to the Law on "Information Security" (December 2013) set up Cyber Security Bureau at the Ministry of Defence. The following additional regulations were adopted by the Ministry:

- Decree of the Minister of Defence of Georgia of February 6, 2014 on "Approval of Statute of LEPL Cyber Security Bureau"
- Decree of the Minister of Defence of Georgia on Minimal Information Security requirements
- Decree of the Minister of Defence of Georgia about Computer incident response group
- Decree of the Minister of Defence of Georgia on management rules of information assets
- Decree of the Minister of Defence of Georgia on Network sensor configuration rules

All secondary legal acts have been adapted are being enforced.

The internet is free and open in Georgia. It is not censored. Fundamental rights and freedom of expression are upheld in cyber space. The law on Personal Data Protection establishes general principles of personal data processing. More specific protection of privacy in electronic communications is set by the Law on Electronic Communications of Georgia by stating that "Information on users of electronic communications networks as well as information transmitted by users by means of electronic communications networks are confidential and shall be protected by the legislation of Georgia. Every person/entity working in the field of electronic communications shall protect confidentiality of information noted in paragraph 1 of this article. Persons employed in the electronic communications sectors as well as other persons shall be answerable for violating privacy of information, according to the legislation of Georgia" (Art. 8, par. 1 and 2).

Strategy, implementation, resources, infrastructures

The first National Cyber Security Strategy 2012-2015[33] is under completion and will be replaced by a new one. It defines priorities and objectives, such as:

- Strengthening national competent authorities:
  - Further development of the Computer Emergency Response Team (CERT.GOV.GE)
  - Establishment of the 24/7 high-tech crime (cybercrime) international contact point as required by the Cybercrime Convention
  - Designation of the expert support team/unit in cybercrime cases
  - Establishment of the format and modalities for public-private cooperation
- Raising the public awareness and increase relevant professional capacity
- Promoting research and analysis

[33] *http://www.dea.gov.ge/uploads/National%20Cyber%20Security%20Strategy%20of%20Georgia_ENG.pdf*

- Developing new legislative and regulatory framework
- Facilitating institutional coordination for ensuring cyber security
- Engaging in active international cooperation

The strategy places special emphasis on raising public awareness on cyber security issues. Data Exchange Agency and the Ministry of Internal Affairs together with the Ministry of Defence are active in dissemination activities and educative campaigns via social media, TV advertisements, lectures for teachers, leaflets, print calendars, etc. In addition, a 24/7 hotline for cybercrime is open for the public at Ministry of Internal Affairs. CERT.GOV.GE also operated hotline- incidents reporting mechanisms.

The national Cyber Security Strategy welcomes active cooperation with service providers and ISPs, for example, in the form of discussion forum. Clear criteria for critical information infrastructure are defined as well.

In June 2013, Ministry of Internal Affairs of Georgia elaborated a Draft Strategy on Combating Organized Crime that contains special chapter on combating cybercrime. This strategy has its action plan that provides future actions and responsible state bodies for their implementation.

Ministry of Internal Affairs of Georgia has taken important steps in the sphere of seizing digital evidences. More precisely, MIA elaborated Standard Operational Procedures on Handling the Digital Evidences. These Procedures specify types of software programs and technical rules that are used while searching and seizing digital evidences. Currently, this document is in the process of interagency discussion.

Ministry of Internal Affairs builds capacities of its units responsible for combating cybercrime including via training modules covering cybercrime case studies, search and seizure of electronic evidence, legal aspects of cybercrime and types of cyber-attacks.

Georgian government allocates sufficient resources to ensure the adequate functioning of key institutions and critical information infrastructures. Relevant institutions are funded by the state budget, in addition to other available funds and internal resources.

Penetration tests and cyber-attack simulations are performed by the Data Exchange Agency and CERT. Such simulations have been undertaken with active participation of the Cyber Security Forum, representatives of critical infrastructure systems as well as, representatives of financial institutions, banks and ISPs cyber security attack simulations had been performed.

The management and coordination of security incident with ISPs and providers of public electronic communication service providers is governed by the Law on Information Security of Georgia. It states that “identification of cyber incident shall be immediately reported to CERT and, where necessary, urgent measures undertaken in order to preserve and protect information about the incident” (Art. 10, par. 3). Communications providers operating critical information system appoint a cyber security specialist in order to coordinate incident reporting and response with national CERT. Such a specialist is available also beyond working hours and is responsible to for coordination with the Data Exchange Agency in case of ongoing or potential threat of cyber attack on critical information system subject including for handling the consequences of the attack (Art. 9, par. 3 of the same Law). The CERT.GOV.GE is empowered to coordinate the cases of “extraordinary threat to defence capability or economic security of the country, normal functioning of state institutions and society” and “is authorized to conduct temporary coordination of cyber security specialists in order to prevent, repeal or handle consequences of such attack” (Art. 9, par. 4 of the same Law). Moreover, all major ISPs have concluded a “Memorandum of Understanding between the Law Enforcement Agencies and

Internet Service Providers based on the principles of cooperation in the field of cybercrime" in January 2010, under the supervision of the Council of Europe Project on Cybercrime as a best practice model by Council of Europe Committee on Cybercrime. This document requires timely information exchange and cooperation between the ISP and the Ministry of Internal Affairs in cases of detection of cybercrime.

The Law on Information Security of Georgia provides that the national CERT is responsible for raising awareness on information security, including information on current threats and vulnerabilities in critical information systems, unless public availability of such information is an information security threat in itself", and for informing the general public about alerts and potential threats" (Art. 8, par. 3 (h) and (i)). The law specifically requires disclosing the information about existing vulnerabilities and threats to the public when the lack of such disclosure becomes an information security threat in itself. To this end, the CERT.GOV.GE lists information about ongoing and resolved cyber security incidents, as well as potential threats and alerts on its website (cert.gov.ge), as well as on a dedicated Facebook page. Regular presentations of the most common computer incidents and ways of handling them are made at the Cyber Security Forum, which met for the fourth time in March 2015, as well as at Georgian IT Innovations Conference which has been running annually since 2009.

Critical Information Infrastructure criteria are clearly defined in the Law on Information Security of Georgia (Article 3). There is a list of 38 public entities that are identified as critical. In future private service providers will be included as well. A specific list of critical information system subjects and their categorization as to criticality is defined by the Decree of the Government of Georgia; the draft thereof shall be presented by the Ministry of Justice Georgia with agreement of Ministries of Defence and Internal Affairs of Georgia.

The Law on Information Security contains provisions describing a reporting procedure for security breaches or threats in relation to critical information systems (their providers shall report immediately in case of such breaches and threats). The amendments to the Law on information Security to be adopted in 2015 will include special security requirements for Trust Service providers as well. Moreover, the Law on Electronic Communications of Georgia contains a newly adopted Article 8^3 that provides for retention of traffic data through installation of lawful interception systems, collecting such data in real-time, and storing these data for purposes of criminal investigations or operative-detective activity for a period of 2 years. The Law on Information Security gives national CERT the right to "configure and manage network sensor necessary for identification and study of computer incidents in subject's network" (Art. 10, par. 2) to identify the points of attack or security breach. CERT.GOV.GE currently monitors seven critical information systems.

The Law on Protection of Personal Data is adequately enforced, with the Office of Personal Data Protection Inspector having an effective enforcement mechanism in the form of mandatory audits and checks, appeal mechanisms. The real-time collection of traffic data[34] that might affect the protection of personal data and privacy is governed by the Code of Criminal Procedure of Georgia that refers to Article 20 of the Cybercrime Convention stating that in the case of a committed crime though a computer system the law enforcement authorities need a court ruling to collect real-time traffic data but the term of such collection should not exceed the time necessary for collecting evidence in criminal case.

Institutions, services

[34] The term "traffic data" is based on the definition of the Convention on Cybercrime (transposed into the Code of Criminal Procedure of Georgia).

- Ministry of Internal Affairs: since 2012, hosts and operates a Special Cybercrime Unit under the Central Criminal Police Department. The Unit is responsible for detection, suppression and prevention of illegal activities committed in cyberspace. A special sub-unit for Computer-Digital Forensics was created within system of MIA Forensics to carry out the functions of digital evidences.
- Ministry of Defence: since 2013, hosts and operates a Cyber Security Bureau to provide stability and security of the Ministry's ICT systems.
- Ministry of Justice: Data Exchange Agency (DEA) started its operations in 2010. The agency operates under the status of LEPL (Legal Entity of Public Law) and is governed by the Ministry of Justice of Georgia. DEA's activities are divided into several directions especially in supporting e-governance development and data exchange infrastructures, setting ICT standards for public sector entities and elaborating information security policies.
- Council for State Security and Crisis Management: an advisory board for Prime Minister under his direct supervision. It makes political decisions in respect to Cyber security as well.
- CERT.GOV.GE provides advisory and training services to public and private organizations and companies. Apart from issuing alerts/warnings and incident handling, the CERT team also performs security audits and assessments, educational trainings and workshops, offers intrusion detection services. The training courses are both based on cases elaborated by ENISA and also include the CERT's own training content and local practices. Such courses are free for critical infrastructure entities. CERT cooperates with CERT-EU.

Moldova

Leadership, policies, legal frameworks

Pillar IV 'Secured and Protected Digital Environment' of the National Strategy for Information Society Development 'Digital Moldova 2020' (Government Decision no.857 of 31.10.2013) identifies information security as a one of the priorities. It aims at

- Improving the cyber security level of the national critical infrastructure (public authorities/institutions, electronic communications networks, aqueducts, energy networks, transport networks).
- Increasing cyber security skills.
- Understanding cyber security risks and responding to them adequately.
- Promoting and developing international cooperation in cyber security.

Special attention is paid to cyber-security threats, such as:

- Cyber-attacks against the infrastructure that maintain public functions or services of the information society which disruption/damage could be a threat to national security.
- Unauthorized access to cyber infrastructure.
- Unauthorized modification, deletion or damage of information data or illegal access restriction to these data.
- Cyber espionage causing a loss of property, harassment and blackmail of individuals and legal entities, in the public and private sectors.

The Ministry of Information Technology and Communications (MITC) has initiated a project to amend the Law on Electronic Communication by adding a new chapter on security and integrity of networks and services of electronic communications. This chapter will regulate obligations of the provider of networks and services in the public domain of electronic communications to ensure security and integrity of the electronic network, as well as will empower the regulatory body to evaluate security measures. MITC has developed a Program on cyber-security to support the implementation of 'Digital Moldova 2020'.

The Law on Informatisation and state information resources (no.467 of 21.11.2003) includes specific provisions governing responsibilities in relation to information security.

Strategy, implementation, resources, infrastructures

At present, there is no stand-alone strategy on cyber and information security. The National Strategy 'Digital Moldova 2020' (Pillar IV) spells out main security-related priorities supported by the Action Plan (including resources allocation). Chapter 4 of the Action Plan "Creation of conditions for increasing security level and trust in digital space" stipulates the adoption of the legal framework, elaboration of policy documents, defining of the national critical infrastructure to protect form cyber attacks, creation of the CERT on the national level. The Chapter 9 Action Plan is devoted to cyber security. A list of key actions includes the following:

- Develop an action plan on cyber security of the Republic of Moldova.
- Define national critical infrastructure that is to be protected from cyber attacks
- Establish and operationalise a national cyber security system
- Supplement and harmonize the national legislation in the area. Establish and enforce minimum security requirements for national critical infrastructure, but also maintaining its operability
- Encourage mutual exchange of information between public and private sector concerning threats, weaknesses, risks, cyber incidents and attacks
- Train and inform public institutions employees on cyber security and cyber risks reduction matters
- Establish and apply appropriate training requirements for persons operating in cyber security environment and wide spreading of professional certifications in the area.
- Enclose some cyber security elements in training and professional development programs of private and public sector managers.
- Draw up User's Guide on minimum cyber security insurance with the provisions to institutionalize individual responsibility for cyber security
- Develop procedures for accessing information and the audit checking the compliance of these procedures.
- Strengthen CERT-GOV-MD team (creating structure / national level CERT team).
- Develop and improve the Plan for M-cloud protective and security measures.
- Guarantee personal data protection.
- Undertake national awareness campaigns regarding digital space risks and protection skills.

- Include in the public media programs promoting and training people to use electronic services.
- Sign international cooperation agreements for improving the response capacity in the case of major cyber attacks.
- Participate in international programs targeting cyber security area.
- Promote national cyber security interests in international cooperation formats where Moldova is a part of.

Implementing these comprehensive actions should ensure a significant progress in enhancing NIS/Cyber-security in Moldova.

While the creation of CERT-GOV-MD in 2010 was an important milestone to enhance cyber-security, there are no legally binding provisions for reporting security-related information to it. On the other hand, CERT-GOV-MD does not have defined responsibilities or sufficient capacity to meet the new challenges at the national level. Still it is a unique point of access for users of automated information systems of national importance. The Action Plan of the National Strategy 'Digital Moldova 2020' assigns an important role to CERT-GOV-MD in implementing the Plan.

Cyber-attack simulations have not been implemented in a systematic way. The establishment of the national alert platforms, hotlines for reporting on harmful content also needs to be implemented with more vigour. Same applies to the introduction of security standards/solutions, undertaking risk management exercises, establishing voluntary certification schemes. The principles of privacy by design, by default and accountability still need to be acknowledged and applied.

Article 20 of the Law 133 (2011) on personal data and the Government Decision no.1123 of 14.12.2010 regulate the privacy issues. The National Centre for Personal Data Protection Centre has the power to issue instructions for controllers in cases of data breach. The Government Plan for Harmonization of the Legislation for 2015 plans that the EU ePrivacy Directive and other relevant legal acts to be transposed in the national legal framework. Other actions in this regard are planned in the Action Plan for implementation of the association agreement between Moldova and the EU. Although the Law no. 241 On electronic communications obliges stakeholders to ensure confidentiality and security of data, the challenge of obliging providers of publicly available electronic communications services to guarantee the confidentiality of the related traffic data and services and informing the public when the disclosure of security breaches is in the public interest needs special attention and resolution.

The process of preparations of technical security-related Terms of reference (ToR) does not involve consultations with specialists in the area of privacy and the above-mentioned principles are not taken into account from the moment of solution design both in the public and private sectors

Chapter 11 of the Criminal Code and the Law no. 20 (2009) "On Prevention and combating cybercrime" contains references to the definition of criminal offences and sanctions in the area of attacks against information systems and computer data.

There is no regulation requiring in the case of security breach to notify the supervisory body within 24 hours after having become aware of the breach. It is planned that the implementation of the National Strategy Digital 'Moldova 2020'" critical information infrastructures will be defined.

The level of public awareness about cyber security is not adequate as yet.

<u>Institutions, services</u>

- Ministry of Information Technology and Communication.

- State Enterprise Centre for Special Telecommunications.
- Cyber security Department of the Ministry of Interior.
- National Centre for personal data protection of Moldova.
- e-Government Centre.
- Institute for Information Society Development.
- Computer Emergency Response Teams (CERT).

Government CERT provides a range of IT/advisory services. It is the unique point of access for the users of automated information systems of national importance. Its services and capacities will be enhanced with the implementation of the Action Plan of the National Strategy 'Digital Moldova 2020'.

Ukraine

Leadership, policies, legal frameworks

Ukraine's new leadership places a lot of emphasis for cyber security. There has been significant progress demonstrated in 2014 in the wholesale revision of the existing legal and regulatory framework governing information security issues. The National Security and Defence Council of Ukraine under the President of Ukraine, Cabinet of Ministers, Security Services of Ukraine, the President Administration and other state bodies have been active in reforming the cyber-security agenda in cooperation with the OSCE and major national stakeholders.

At present, there is a mix of some two dozens of new and old laws that regulate NIS, which complicates the legal and regulatory background and requires streamlining. The main new legal acts include:

- Order of National Security and Defence Council of Ukraine, signed by President № 449/2014 as of 28.04.2015 – includes provision for development and creation of the national wide cyber security system http://www.rnbo.gov.ua/documents/347.html.
- Action plan of the protection of information resources 2014-2016 signed by Cabinet of Ministers as of 05.11.2014 №1135-p – includes both legislative provisions and implementation arrangements (modernization of CERT-UA, international cooperation etc) http://www.kmu.gov.ua/kmu/control/uk/cardnpd.

Proposed new laws:

- Strategy on Cyber-security.
- Law on the Main Principles of Enforcing Ukraine's Cyber security – sets out legal and organizational principles of the national policy of protecting vital interests of the person and citizen, society and state in cyberspace and the main principles and areas of enforcing Ukraine's cyber security.

There are also older laws, such as

- President's Decree № 389/2012 on 08.06.2012 "On the creation of the Cyber security strategy of Ukraine".
- President Order of technical means of data protection (including crypto) dated 27.09.1999 № 1229/99.

- Decree of President of Ukraine № 514/2009 from July, 8 in 2009 On the Doctrine of information safety of Ukraine.

The law “On the bases of national safety of Ukraine” determines basic threats to national interests and national safety of Ukraine from the information security standpoint addressing freedom of speech and access of citizens to information; computer related crimes; disclosure of information owned by the state; handling of confidential information.

International cooperation in NIS is an important policy issue. The country actively cooperates with

- EU
- ITU
- FIRST (Forum for Incident Response and Security Teams - first.org) – CERT-UA (since 2007)
- IMPACT (International Multilateral Partnership against Cyber Threats) – CERT-UA (since 2012)
- NISA (nisassociation.org)
- OSCE workgroups
- NATO
- US Department of State

Strategy, implementation, resources, infrastructures

Since 2012, special attention has been given to the creation of a National Cyber security strategy approved by President’s Decree № 389/2012 on 08.06.2012 “On the creation of the Cyber security strategy of Ukraine”. However, no resources were allocated at that time. The new President Decree № 449/2014 dated 28.04.2014 asked to create the Strategy and the Law on Cyber-security of Ukraine.

Since 2014, the draft strategy and the draft law are being elaborated within the working group under the State Agency for e-Government coordinating its efforts with State Service for Special Communication and Information Protection of Ukraine (DSSZZI), the National Commission for the State Regulation of Communications and Informatisation (which is the National Regulator – NKRZI) and the National Defence and Security Council (RNBO).

An important step forward has become an Action plan on the protection of information resources 2014-2016 signed by Cabinet of Ministers (as of 05.11.2014, №1135-p). It includes important provisions to modernize CERT-UA and expand the scope of its international cooperation. The Action Plan welcomes bilateral and multilateral international agreements and defines the state functions and responsibilities of the CERT. There is no special budget for cyber-security.

Ukraine does not have limitations in using the Internet or censorship for ordinary users; there are some provisions for state institutions to ensure secure exchange of information and documents. The issue is being further discussed under the leadership of CERT-UA.

While the CERT-UA labs are capable to handle regular real-live cyber-attacks (only SOS and reaction approach at the moment implemented), it does not have sufficient capacities to engage in attack simulations. There are no alert platforms and hotlines for feedback from citizens. The web site of CERT-UA regularly updates information regarding cyber-attacks and possible precautions (www.cert.gov.ua). Periodically, CERT-UA cooperates with industry to ensure synergetic effects; e.g.

in 2014, following large-scale mobile virus attacks, CERT-UA cooperated with mobile operators for faster virus tracking through IMEI, fast recovery and quicker information provision to subscribers.

In terms of promoting cyber-security products, adopting security standards/solutions, DSSZZI historically owns and develops its own stream of cyber-security products and standards (a Soviet legacy). These standards are mandatory for compliance by any Governmental authorities, state enterprises or business entities that supply products for government use (databases, web-sites, workflow systems etc). Any newly developed or amended/upgraded information system requires a renewed certification/validation. The IT products arriving from other markets are required to pass additional certification/validation in Ukraine. In 2014, based on the clauses regarding standardization in the EU-Ukraine Association agreement, a process was launched to start mutual acceptance of digital certificates. Already the first 60 standards were accepted by the Ministry of Economics (effective January 2016).

Legally or otherwise, there are no binding minimum requirements in the field of Network and information security.

The Ukraine legislation doesn't contain provisions regulating the management of security breaches by way of empowering the competent national regulator to coordinate and instruct the operators of public communications networks or providers of public electronic communications services in case of security breach. However, some legal provisions are being developed by NKRZI to meet the requirements set to National Regulator in the EU-Ukraine Association Agreement context. According to the current legislation, in particular the Law on Information #2658-XII of 02.10.92 (the last update was made in July 2012 (http://zakon4.rada.gov.ua/laws/show/2657-12 providers have responsibility to make information disclosure. This topic is being further discussed within the overview of the current draft laws on the National Regulator and e-Commerce.

Ensuring confidentiality of traffic data and services by the providers of publicly available electronic communications services is regulated by the Law on Information #2658-XII dated 02.10.92 (the last update in July 2012 (http://zakon4.rada.gov.ua/laws/show/2657-12) and the Law on Personal Data protection #2297-VI dated 01.06.2010 (http://zakon4.rada.gov.ua/laws/show/2297-17). However, more changes are planned to be introduced.

The Ministry of Justice, in cooperation with the working group under the e-Government Agency, is currently working on new conditions for trust services and providers of such services. It is not clear whether trust and other service providers would be obliged taking adequate technical and organizational measures to minimize the impact of security incidents and in the case of the security breach notify the supervisory body within 24 hours after having become aware of the breach. At the moment, reporting is managed by DSSZZI as part of its annual control reports. There is a reference to a 24 hour reporting period contained in the DSSZZI Administration Decree №143 dated 24.07.2007

An issue of the definition and management of critical information infrastructures to prevent disruptions in the supply of critically important products is considered within the current draft of the Strategy on Cyber-security and within the activities on the Action Plan on Resources protection 2014-2016 signed by Cabinet of Ministers (05.11.2014, №1135-p, article 4). With reference to information assets, the DSSZZI order of 02.12.2014, № 660, defined the procedure to evaluate the security and protection level of state information assets (effective 28.01.2015). The Action Plan on Resources Protection 2014-2016 foresees giving a definition of the critical infrastructure objects, requirements and procedure to suggest and manage the list of such objects (responsible – DSSZZI, by the end of 2015. The plan also includes an analysis of the current state of the protection of critical infrastructure (responsible – DSSZZI, 2015-2016). The private sector infrastructures is regulated by the Law on

Information №2658-XII dated 02.10.92 (the last update was in July 2012, http://zakon4.rada.gov.ua/laws/show/2657-12). However, the conditions will be revised within the current draft of the Strategy on Cyber-security.

Institutions, services

- The State Service for Special Communication and Information Protection of Ukraine (DSSZZI) – high involvement; responsible for the Cyber security strategy and related legislation; a central executive body with a special status, with the main task of implementing the state policy on protection of state information resources within data networks, maintenance of the national system of confidential communication, cryptographic and technical protection of informationhttp://www.dsszzi.gov.ua/dstszi/control/en/index.
- National Security and Defence Council of Ukraine under the President of Ukraine (RNBO) – high involvement; defines priorities for national security and defence policy; coordinates and supervises activities of executive authorities in the area of national security and defence http://www.rnbo.gov.ua/en/.
- Computer Emergency Response Team of Ukraine (CERT-UA) – high involvement; established in 2007, accredited by FIRST; supports government authorities and the market players in cyber- security, cooperates with DSSZZI on formulating the national strategy for NIS/Cyber security http://cert.gov.ua/.
- National Commission for the State Regulation of Communications and Informatisation (NKRZI) – medium involvement; national regulator; regulates security of the market www.nkrzi.gov.ua.
- State Agency on e-Government – high involvement; central body responsible for state policy in the field of electronic information, e-governance, development of the information society; leads cross-functional working group on Cyber-security issues http://dknii.gov.ua/.
- Security Service of Ukraine (SSU) – high involvement; state law-enforcement agency http://www.ssu.gov.ua/sbu/control/en/index.
- Ministry of Defence of Ukraine – high involvement; hosts its own CERT http://www.mil.gov.ua/en.
- Ministry of Information – newly formed Ministry responsible for content protection only, not information/IT security.
- National Bank of Ukraine – sets IT requirements for the protection of information in the banking sector.

The government CERT-UA provides full support to government bodies and key players in the field of information and cyber-security. It closely cooperates with DSSZZI on formulating a national strategy on NIS and is present on social networks. There also are other sectoral emergency teams, e.g. Ministry of Internal Affairs, providing cyber-security services to the Ministry and hosting a 24/7 contact point.

Electronic identification and Trust Services

Armenia

Institutions

Ministry of Economy is the main government body responsible for policies in electronic infrastructure and services in Armenia's http://www.mineconomy.am. It is supported by e-Governance Infrastructure Implementation Unit ("EKENG") CJSC http://www.ekeng.am. It drafts the policy for the authorization procedures. Other public bodies that are relevant to the development of the digital market in general and eID/eTS in particular include the Government Staff www.gov.am and the Ministry of Justice http://www.moj.am/.

Legal and regulatory framework

There are two main laws regulating an area of eID/eTS: RA Law on Identity Cards and RA Law on Electronic Documents and Electronic Signature. The Ministry of Economy defines licensing regime and institutions. The 116-Ն Government Decree (adopted in 2008) defines the licensing procedures. Other relevant legal and regulatory acts include the Conception for Migration System of the Republic of Armenia and for Introduction of the System of Electronic Passports and Identification Cards with Biometric Parameters in the Republic of Armenia. Public procurement is regulated by Law on Procurement and by the Government decree on E-Procurement, and the Government Decree 160N.

The main challenge is the disconnect between the availability of the adequate technical infrastructure able to provide eID and trust services and the lack of relevant regulation and legislative basis that would allow to enable such services. There have been some initiatives undertaken to improve the work of the licensing institution[35] but more work is needed. Complying with the requirements of the EU baseline in the licensing regime and the adequate capabilities of the licensing institution would require significant financial investment. At the moment, there is no sufficient knowledge is available on how to comply with the EU standards.

The existing Law on Personal Data provides sufficient legal basis to enable citizens track the use of their personal data by different government agencies on the web portal www.ecitizen.am (via the AAC tool applied by the EKENG while processing personal data). Currently, the Parliament deliberates a new draft law on the Protection of Personal Data according by EU standards and requirements. It is expected that the law will be adopted by the end of 2015.

Infrastructure and interoperability

Armenia does have a functioning shared infrastructure for digital services, and is building at the moment a dedicated system of e-government interoperability (an Estonian model may be realized within the World Bank support programme). The Government Decree on interoperability model is expected to be issued by July 2015 to enable interoperability solutions in practice.

[35] Under the EU Guillotine programme.

While Armenia's digital infrastructure is compliant with high international standards, it does not allow the mutual recognition of electronic trust services provided by other countries. The main problem is in the lack of the relevant legislative basis, as no laws exist to regulate such recognition and no bilateral or multilateral agreements have been concluded with other countries to mutually recognize electronic identification and trust services.

eServices

The number of e-government services for citizens have been expanding (www.ecitizen.am), however it is still limited compared to the EU baseline, and are provided at lower maturity levels – one way information provision and downloadable forms (1st and 2nd stages of online sophistication). Such services include Income Taxes, Car Declaration, Police declaration. E-Services for businesses are better advanced. The majority of the 12 EU basics e-services (except Statistical data and Environment permits) are provided in Armenia online at the 4th stage of service maturity online (regulated by the Government Decree Ա5, adopted on February 5, 2015). However, no monitoring or benchmark is carried out.

eProcurement

In contrast, services for businesses are much better advanced, especially in the field of e-procurement which is fully automated at pre and post award levels. Post award stages are mainly administered by e-commerce tools. However, e-signature tools are not used for e-procurement using instead a name-password login format. However, the technical infrastructure allows using e-signatures. The area is regulated by the Law on Procurement and by the Government decree on E-Procurement, and the Government Decree 160N. During 2015, some 2,500 tenders announced by state agencies were administered online. All the tenders are mandatory to be submitted online. The local self-governance units will be mandated to submit their tenders online as of April 2015.

Personal data protection

While sufficiently well regulated (and with a new law meeting international standards upcoming), the protection of personal data and online privacy poses the highest risk. There is a challenge of awareness, as citizens are not competent to assess potential risks while their personal data are processed electronically. This will increase the trust of citizens to digital services, which is lacking at the moment.

Azerbaijan

Leadership and strategy

The government's strategy is concentrated on developing secure digital society without international boundaries that will stimulate both economic and social development by creating an e-Society in Azerbaijan with many fully automated and secure services for citizens and businesses.The government realizes the importance of the digital infrastructure by allocating budgetary resources and attracting qualified specialists, developing state programmes and implementing relevant actions plans. Yet stronger political will needs to be demonstrated to expand international cooperation and coordination between national and foreign experts in order to adopt relevant legislation for proper functioning of eID and eTS in line with international standards; new opportunities should be created for training and exchange programmes.

Institutions

Over the past several years Azerbaijan has been visibly advancing the use of ICTs in various fields of governance strongly supported at the highest political level. Ministry of Communications and High Technologies (MCHT) of the Republic of Azerbaijan serves as the main government body responsible for the overall coordination of ICT-related activities in general and for the development of respective national policies and programmes in electronic identification and trust services. It operates the national e-government portal, provides e-signature, and hosts the state register of information resources and systems.

MCHT is supported by the Ministry of Labour and Social Protection of Population which manages electronic registration of forms and documents for assigning the unemployment status and benefits and registers employment contracts.

Ministry of Taxes performs a number of important functions: supports online registration of individual entrepreneurs and legal business entities, supports online submission of a simplified tax declaration form (e-Declaration), supports online acceptance of tax invoices (E-tax invoice); it also runs a state register of VAT payers and participates in the registration of employment contracts jointly with the Ministry of Labour and Social Protection of Population and provides certificates for e-signatures issued by the ASAN Certificate Services Center.

Ministry of Interior Affairs runs the State register of resident identity of citizens that enables searching citizens' personal data according to Personal Identification Number (IAMAS). , State register of resident identity of citizens

Ministry of Justice serves as the registration authority for civil status acts. It also maintains the register of legal entities, non-profit and educational institutions, as well as hosts the state register on Personal Identification Number (IAMAS) of citizens including foreigners and on the stateless persons.

State Procurement Agency is responsible for supporting e-procurement and e-tenders.

State Customs Committee has implemented electronic declaration of customs services including customs examination, declaration of goods, online e-customs payments. Monitors applications and inquiries submitted to the Committee.

Legal/regulatory framework

The following legal and regularity acts are relevant to the area of electronic identification and trust services in Azerbaijan.

- Law of the Republic of Azerbaijan on "E-signature and e-document"
- Presidential Decree on "Implementation of e-signatures," in accordance with the Law of the Republic of Azerbaijan on "E-signature and e-document."
- Law of the Republic of Azerbaijan on "Individual data"
- Law of the Republic of Azerbaijan on "Information, informatisation and information exchange"
- Law of the Republic of Azerbaijan on "Obtaining of information"
- Law of the Republic of Azerbaijan on "Information Freedom"
- Law of the Republic of Azerbaijan on "Telecommunication"
- Law of the Republic of Azerbaijan on "E-trade" (E-commerce)
- Law of the Republic of Azerbaijan on "Reconnaissance and counterintelligence activity"

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (28.01.1981)
- Convention on "Cybercrime" (23.11.2001)
- National Strategy on Information-Communication Technologies for the Development of the Republic of Azerbaijan (2003-2012) was implemented in the framework of the “E-Azerbaijan” Programme. New strategic documents for the National Infrastructure for e-Document Circulation and e-Government Data Centre is currently under preparation.
- National Strategy for the development of information society in Azerbaijan for 2014-2020 (part of the ongoing State Programme on the Development of ICT).

eID tools

Electronic signature is obtainable via smart cards and mobile SIM cards. Both the Ministry of Communication and High Technologies (MCHT) and Ministry of Taxes issue their own electronic identification tools. MCHT provides eID services mostly to citizens and government officials, while the Ministry of Taxes targets the business sector. Electronic signature in Azerbaijan is not compulsory and therefore is not widely spread at the moment. eID cards (featuring the owner’s photo, personal data and a chip) are also used for offline identification (in addition to digital signature). While the eID card does not contain biometric data and fingerprints, medical information, and is not used as a means of online payments, it serves as a personal identity card, electronic identification and an e-signature tool at the same time.

Use of eSignature

In Azerbaijan, smart-card based electronic identification means e-signature. A Decree of the President of the Republic of Azerbaijan on “Implementation of e-signatures,” in accordance with the Law of the Republic of Azerbaijan on “E-signature and e-document”, entrusts the Certificate Services Centre of the Ministry of Communication and High Technologies (MCHT) with the authority to issue e-signatures (officially launched in September 2011). eSignature is issued to the three categories of users: (1) members of the general public, (2) legal and natural persons engaged in entrepreneurship, and (3) public servants. There is a service fee that is equivalent to 15, 30 and 60 Euros respectively.

As of 1 September 2014, the Ministry has issued some 23 thousand of e-signature certificates demonstrating the monthly growth rate of nearly 1,200 users. More than 17 thousand of these e-signatures have been issued to public servants, 1,500 – to legal entities and about 6,000 – to the general public. The introduction of online registration of employment contracts by the Ministry of Labor and Social Protection of Population has increased the use of eSignature. However, the smart card-based electronic identification is not widely used to access e-government services on the government e-service portal which had 1.5 million users in 2013-2014.

The Ministry of Taxes issued almost 50 thousand of mobile signatures (an ASAN eSignature). A SIM-card based e-identification – or mobile eSignature or ASAN (Easy) eSignature issued by the Certification Service of the Ministry of Taxes – was introduced in Azerbaijan by an Estonian company. Mobile ASAN eSignature enables users to register for e-services and issue e-signatures on documents. To enable this feature, a chip (SIM card) needs to be inserted into a mobile device. The card’s chip includes a cryptographic key, which makes it impossible to make alter the signed document. To obtain a card with a chip, users first need to approach a local mobile operator AZERCELL Telecom or ASAN Services Centers. ASAN eSignature service is available for 15 Euros to the general population, public servants and physical and legal persons who engage in

entrepreneurship activities. Each transaction using ASAN signature is charged extra 0.02 Euros. Between July 2013 and August 2014, some 55 thousand ASAN eSignatures were sold and 3.5 million transactions were conducted. e-Government portal services can be accessed using mobile eID as well by, first, downloading an application from the Apple Store.

Interoperability

Azerbaijan does not have a law on state information systems and data bases. The exchange of electronic data between public agencies is regulated by the Cabinet of Ministers' decree and inter-agency bilateral agreements. The lack of legal provisions regulating the exchange of personal, business and real estate data when rendering e-services leads among public entities is seen as a drawback. To address this challenge, the ASAN Service (State Agency for Public Service and Social Innovations under the President of the Republic of Azerbaijan) and the MCHT are developing a draft law regulating information resources and their exchange. The challenge is to be in line with the international standards, as well as to ensure better coordination between agencies and organizations. More efforts are required to raise awareness about ICT standards and interoperability across all government levels and units.

eProcurement

Online public procurement is not widely spread in Azerbaijan. It is mostly informational at the moment. Pre-award, ward and post-award stages have not been automated. As a result, there is a lot of untapped potential for the uptake of eID/eTS with the growth of electronic trade and procurement. At the moment, e-procurement is limited to the provision of information services (State Procurement Agency www.tender.gov.az). Public procurement should be made more transparent with the use of electronic means. The objective is to fully automate public procurement and overcome the unwillingness of some agencies to procure the goods in online regime.

eServices

According to 2014 statistics, 11.5% of the population of Azerbaijan used e-government services with a sufficiently high degree of user satisfaction. Those e-services that are currently offered by various state organizations through the single portal (www.e-gov.az) ensure adequate level of security and privacy for citizens who access such services. E-government is also accessible from mobile devices. While over 413 services are published on e-government portal, these are mostly one-way informational services. Some of the EU 20 basic e-services for citizens and businesses that are available electronically are at the 1st, 2nd and 3rd levels of online maturity, some are not available at all. All EU basic e-services for citizens are accessible electronically (except customs e-declarations, with most of them being at the 3rd, 4th and 5th level of service sophistication. Stronger leadership is required to advance transactional e-services which will require secure electronic identification. Special effort need to be made for cross-border accessibility of such services. At the moment e-services are not recognized as trusted internationally. All services are monitored and benchmarked centrally, from the portal.

Standards

There are government documents describing the minimal level of requirements needed for security devices. Also, the audit procedures are being revised as well in this field to improve the quality, interoperability and compliance of ICT infrastructures with higher standards.

Belarus

Institutions

The main government bodies involved in electronic identification and trust services include:

- Ministry for Communication and Informatisation
- Operative and Analytical Center (OAC) under the President of the Republic of Belarus
- National Center for Electronic Services of the Operative and Analytical Center under the President of the Republic of Belarus

OAC is the main government body responsible for electronic communications and information protection. Its functions include

- Operator of the interagency information systems, the root certification center and subordinate certification centers of the State system for management of public-key digital signature (GosSUOK),
- Provider of public electronic services to organizations and individuals
- Design and development on the contractual terms of information systems and resources for the provision of electronic services
- Participation in the formation and development of the state system of providing electronic services to organizations and individuals
- Provider of electronic services to public bodies, other organizations and individuals for a fee and free of charge
- Provide the establishment, operation and development of interdepartmental information cooperation between state bodies and organizations

Legal/regulatory framework

- Law № 455-З of 10 November 2008 on Information, informatisation and information protection.
- Presidential Decree of November 8, 2011 № 515 "On some issues of the Information Society in the Republic of Belarus"
- The concept of the State system for digital signature verification public-key management of the Republic of Belarus (GosSUOK)
- Regulations on the GosSUOK
- Regulation on the Interagency Advisory Council on the development of the GoSSUOK
- Law of the Republic of Belarus of December 28, 2009 № 113-Z "On Electronic Document and Digital Signature"
- Presidential Decree of 30 December 2010 № 708 “On conducting electronic auctions”
- Presidential Decree dated November 17, 2008 № 618 “On public procurement in the Republic of Belarus”
- National Programme of accelerated development of services in the field of information and communication technologies (ICT) for 2011-2015, sub-programme “e-government”
- Decision No. 180 of 30 September 2014 on the Procedure for Keeping and Application of Register of Structures of Electronic Documents and Information Used by Realization of

Information Interaction within the Integrated Information System of Foreign and Mutual Trade of the Customs Union

e-Signature

There is sufficient legal certainty in field of electronic identification in general and PKI/eSignature in particular.[36] However, legally, electronic trust services provided by other countries may not be recognized in Belarus (except few cases governed by international agreements). Also, there is a lack of legal basis for eID cards, although the plan to introduce a national eID card is discussed. Any natural or legal person in the Republic of Belarus may have a private key digital signature suitable for the signing of documents in various government information systems. Registration of a new subscriber and issuance of certificate for digital signature costs make about 30 Euro for one year or 45 Euro for 2 years. The level of digital signature use by legal entities is high reaching, as of December 2014, 173,166 organizations and 266,990 small entrepreneurs. All legal entities that pay VAT have to do it electronically. Certification service-providers operate in a competitive environment.

Citizens rarely use digital signature due to the lack of electronic services that would justify such a use. For example, eID is not integrated into the Unified Payment System when paying for communal services, which undermines security of electronic transactions and potentially gets access to the payment history of other persons.

eProcurement

As of 1 January 2914, three countries of the Eurasian Economic Union – Belarus, Kazakhstan and Russian Federation – can participate in public procurement using their e-signatures issued by the accredited institutions and based on the special cryptographic arrangements. Such a special regime is does not cover other countries. However, it is discussed to expand the interoperability of digital signature internationally by using electronic trust services of third parties.

The country's legal and regulatory frameworks governing the use of electronic signature and electronic identification schemes contain regulations that guarantee only a partial (not full and unrestricted) access to some stages (not the entire process) of public procurement online. Electronic trading platforms provide the accredited persons access to be able to upload the information and free access to the official website visitors to view uploaded information.

For certain categories of goods (works, services), regulated by law, public procurement procedures do not require posting information online (closed competition) or include only the use of downloadable forms (open competition, single-source procurement, which represents the initial stages of service sophistication online). Only in the case of trading and electronic auctions it is possible to enter into contracts electronically. A degree of automation by procurement stages is at least 50%, which includes publication of an announcement on purchases and electronic registration, while the post-award stage (after the winner selection) is not automated for functioning online; it can be carried out with the help of ICT using other online-instruments.

Over 65% of public procurement is realized online through electronic trading platforms (, makes up more than 65% (about 35% is non-competitive public procurement, the information about which is not subject to online placement). The draft of the new edition of the Law "On public procurement of goods (works, services)" envisages that starting on January 1, 2016 all public procurement procedures will be conducted in electronic format only including issuing award contracts.

[36] http://nces.by/wp-content/uploads/2014/10/zakon113.pdf

Personal data protection

There is no single direct law on personal data, regulating the rights and liabilities of the parties in corresponding relations. No legal basis exists for access control services to enable citizens tracing the use of their personal data by the government.

e-Government and Interoperability

An executive decision by the OAC[37] determines the requirements for interdepartmental and inter-system electronic compatibility (interoperability). In particular, it ensures compatibility of all newly developed state information systems used by the government agencies for interdepartmental services. E-government services offered in the country to citizens and businesses are provided through the National Automated Information System (NAIS) which is still being at an early development stage. Therefore, the provision of e-government services on it does not require user authentication and authorization. The development level of information systems in agencies does not allow for full compatibility of the NAIS with a full range of government services provided by other agencies in electronic form. In future, the NAIS will serve as a safe platform, compatible with other systems, built on the principles of distributed architecture that takes into account the existing branch specification and infrastructure in order to completely integrate electronic services, provided by other establishments.

At the moment, the NAIS consists of:

- basic software and hardware
- departmental software and hardware complexes implementing technological interaction with the basic software and hardware complex for the integration of information resources into the NAIS
- basic and other government information resources integrated into the NAIS
- single portal of e-services for citizens and organizations (Internet portal)
- portal for government agencies and organizations (Intranet portal)

The existing legislation and practice don't allow carrying out secure electronic identification in a mobile environment.

Services

Citizens of Belarus have access to at least 12 high-impact e-government services defined as basic services by the legislation of Belarus. However, these are not the services defined as basic e-services in the EU. The level of their online sophistication is yet low, with most of them being one-way information services; this is usually an opportunity to download at the official websites forms to fill out. Only one service is a full-fledged transactional service (filing a tax return when possessing a digital signature). Such services offered by different organizations are rather fragmented and, with a few exceptions, are not available through National Automated Information System (NAIS).

Electronic services are monitored and assessed through user satisfaction surveys.

The services, referred to the basic one in the EU terminology are provided at the low development level (they are limited to opportunity to download at the official websites the forms to fill out).

[37] No. 33 dated 27 May 2013

Services for businesses are better advanced with 7 important electronic state services provided online. Yet the level of the electronic maturity of such services is still low since they are designed to primarily provide information from data bases and registers. It is not always possible to access all the e-services through a single government portal of electronic services.

Georgia

Legal/regulatory framework

There is sufficient legal basis and certainty in the provision of electronic services, such as eID and trust services. Electronic services are governed mainly by the Law on Electronic signature and Electronic Document, but also by regulations issued by the Ministry of Justice (Georgia Data Exchange Agency), Government, National Bank. The regulations also include a Government's Decree on "Technical Norms of Digital Signature certificate and issuing authority of digital signature".

Amendments are being introduced to the law on Electronic signature and electronic document. It redefines electronic signature, trust services and other regulations and brings the law in compliance with Directive 1999/93/EC and Regulation 910/2014. Qualified trust services definition, respective rights and obligations, as well as, qualification criteria are also included in new amendments. Data Exchange Agency will be authorised supervision and authorisation body (National Authorisation Authority). A principle of the mutual recognition of third countries' providers of trust services is planned to be legislated if the qualified trust service providers are accredited with National Authorisation Authority or on the basis of mutual recognition of countries based on respective international agreements. However, it is not clear what is should be a preferable modality of mutual recognition, i.e. is it to be done on a bilateral basis by concluding country-specific agreements or through the EU-wide multilateral agreement?

The laws on (1) Electronic Signature and Electronic Document and (2) Personal Data Protection provide clear provisions and sufficient ground for the protection of personal data and online privacy. The Data Exchange Agency and Office of Personal Data Protection Inspector oversee the adequate enforcement implementation of these laws. All services at my.gov.ge have been verified by the Personal Data Protection Inspector's office. There are also mandatory audits (both in public and private sectors) to ensure compliance with the laws.

eProcurement

State Procurement Agency and Data Exchange Agency are key players in the field of public procurement services. Georgia is a national eProcurement system as part of the broader activities aimed at e-service provision. The use of eID or electronic signature is not in practice yet during online procurement. Yet it is planned in the future in line with the amendments to be introduced to the law on Electronic Signatures and Electronic Document.

Infrastructure and Interoperability

National e-governance strategy includes sectoral specifications and aims at establishing interoperable environment for e-service. Data Exchange Agency is entitled with major responsibility of developing and implementing interoperability. It defines data standards and principles of interoperability of information systems. Its aim is to reach the compatibility of information standards of Georgia with international standards. At the moment, Georgia does not have a full-fledged interoperability framework also containing clear ICT standards and specifications. The development of such a framework is planned for the near future. An interoperability framework has to ensure that principles of interaction are implemented at all levels in line with the principles of the European Interoperability

Framework that addresses legal, organisational, semantic and technical interoperability. Business sector will be part of the interoperability framework as well.

The Georgian Government Gateway (G3) is a data exchange infrastructure between different (public) organisations and bodies which ensures guaranteed message delivery and is based on a number of modules that include mail and secure message/communication time stamped logs. G3 also comprises RoR (Register of Registries – a unified state register) which was enacted in June 2011. It requires that all state bodies provide information on content of registers' services in their organisations within the common software solution – a RoR Portal http://ror.dea.gov.ge/. Through this portal, government bodies can provide primary registration of their registries and services as well as registration of notifications on significant changes in them, their expansion, combining, cancelling, destroying, archiving and transferring. Currently 85 registry entities are registered on the portal which in turn is home for 344 registries and 315 services. Further implementation of "Registry of Registries" project will be based on the analysis undertaken by EU-funded project "Public Administration Improvement".

Institutions

Ministry of Justice, Government's Data Exchange Agency are the key players in Georgia in the field of eID/eTS.

Strategy and resources

There is a clear e-governance strategy that includes the assessment of existing gaps, including in legal framework and developing tools for addressing these gaps. Planned amendments include list of actions to be implemented by various authorities in Georgia to adequately implement law and relative regulations. Planned actions are already reflected in the state budget or international donor funded projects (e.g. with Austria).

Services

The government has been promoting introduction of various e-services for over eight years. Functions are divided between Ministry of Justice, Ministry of Finance and Ministry of Internal Affairs with most services available for the public use. Other e-services are available at Ministry of Agriculture, Ministry of Economic Development and Ministry of Education.

Provision of high quality and interactive online services for citizens and businesses constitute a main challenge for Georgia. This is where the main gap with the EU is recorded. To date, the prevailing emphasis has been on digital services for passport and eID card issuance, residential registration, life-cycle event services (marriage, divorce, birth adoption, change of name, death, power of attorney etc) on my.gov.ge portal. Its services (can also be obtained outside Georgia) require the use of an eID card, card-reader and the Pin code received together with the eID card (or being registered at a Public Service Hall to get username and password). It is estimated that the available 12 high impact services are provided at the 3rd to 5th levels of online maturity.

While government institutions provide various e-services, the monitoring of their take-up and user satisfaction is not adequate. The successful cases include the declaration of property tax (almost fully implemented online); however, the change of residential address is hardly used online.

Georgia has implemented some e-services for businesses, e.g. the mandatory use of the Revenue Services' Digital Declarations through www.rs.ge (which is integrated with companies' and government ICT systems), e-Procurement/ e-Auction (which are part of the Public Finance Management System), e-NRMS (Electronic Natural Resource Management System service (which has been developed by the Ministry of Finance). There are e-services implemented for spatial,

geological, and environmental and pollution related issues that are offered by the Ministry of Environment Protection and Natural Resources on www.meteo.gov.ge. Most services for businesses are available at the 3rd, 4th and 5th levels of online sophistication. However, the overall level of e-services use for businesses (demand and take-up) remains relatively low.

eProcurement

All Public procurement in Georgia is undertaken via eProcurement system electronically at pre-award and award stages.[38] There is 100% take-up rate. However, eIDs tools are not as yet integrated into electronic procurement, with the registration is implemented through web page, which is administered by the State Procurement Agency. Pre-award and award stages are fully automated and managed by the State Procurement Agency, while the post-award stages are within mandate of the procuring state entities. Therefore, the level of automation at this stage varies.

Leadership

The Georgian government demonstrates strong political will and leadership to advance electronic identification and trust services. There is sufficient operational capacity to do it in an adequate manner. The government has empowered the Data Exchange Agency) with inter-agency coordination and regulatory functions. The Agency's is sufficient to timely propose laws/adopt regulations needed for the effective functioning of electronic identification and trust services. It's effectively enforced the passed laws/adopted regulations by elaborating relevant policies and strategies/action plans.

Moldova

Legal/regulatory framework

The law on Electronic signature and Electronic Document no. 91 of 29.05.2014[39] is fully aligned with the Directive no. 1999/93 / EC on a Community framework for electronic signatures, published in the Official Journal of the European Communities no. L 13 of 19 January 2000. It is key to Moldova's integration into the EU Digital Market. It sets the main requirements to validity of digital signature and certification services and establishes types of electronic signatures, principles of their use, and legal effects of the use of electronic signatures and requirements that will be imposed to service certification.

Other relevant legal and regulatory documents include

- The Government Decision no.710 on the Strategic Program for Governance Technological Modernisation (e-Transformation)40
- Government Decision no.122 of 18.02.2014 on Program on Public Service Reform for 2014-201641
- Government Decision no.656 of 5.09.2012 on approving the Interoperability Framework Program42

[38] http://procurement.gov.ge/getattachment/ELibrary/AnalyticalStudiesReports/spa_report_2013.pdf.aspx

[39] http://lex.justice.md/viewdoc.php?action=view&view=doc&id=353612&lang=2

[40] http://egov.md/images/normative/Strategic_Program_for_Governance%20_Technological_Modernization_ENG.pdf

[41] http://lex.justice.md/viewdoc.php?action=view&view=doc&id=351705&lang=2 (RU)

- Government Decision no.404 of 02.06.2014 of Implementation of the Interoperability Platform 43
- Government Decision no.405 of 02.06.2014 on electronic governmental integrated digital signature service (M-Sign)
- Government Decision no.1090 of 31.12.2013 on electronic service on control and authentication of access (M-PASS)

The Interoperability Program, approved by Government Decision no.656 of 5.9.2012, is a planning document. The best practices and recommendations have been taken into consideration in the process of elaboration. It describes the current situation in the area, defines the scope, objective, the necessary actions and measures for all implementation phases and responsibilities for all actors involved in implementation of efficient exchange of data, including the necessary at the organizational, semantic and technical levels."

There are no plans to amend the legal framework in the area of eID/TS. However, the Government plans to amend the legislation to extend the availability of e-signature from 1 year to 5 years on the bases of international experience in order to motivate citizens to use electronic services as well as to enable a catalyst for creating digital market in the country in general and the development and adoption of electronic services, in particular.

Services

Government Decision no.710 of 20.09.2011 stipulates that by 2020, all public services that can be digitized will be delivered to citizens and business electronically, alongside traditional methods. Ministries and other public authorities have prepared plans to digitize public services within their mandate. Government Decision no.122 on adoption of the Program on reforming the public service also contributes to the expansion of e-services. In addition, M-PASS has a secure and flexible mechanism for authentication and control of access of users in information system, including e-services. An Order of the Fiscal Service no.1223 of 26.08.2014 approves the mode of using of electronic fiscal services. At the moment, only 5 out of 12 online basic public services for citizens and 6 out of 8 for businesses are fully automated and provided on the internet. It is possible to submit VAT declaration online (e-Declaration). While online registration of businesses does not exist yet, a project is underway to produce a relevant e-service with a 4th level of online sophistication. E-reporting for statistical data contains only 4 forms for submission online (out of approximately 200 forms). About of 40% of customs declarations (for exports) have been submitted electronically through an e-customs service as 4th stage of online maturity. The Platform of registers (government common service) allows handle the issuance of permissions at the 3rd stage of service maturity.

Since September 2012, such services as obtaining criminal records, licensing (connected to the mobile signature), electronic reporting (connected to mobile signature), normative documents in construction (www.ednc.gov.md) and others are provided online with the use of eID tools. The digitization of the civil status service archive (SIGEDI) is under implementation is implemented in 9 ministries. Recently the State Fiscal Service and Center for Electronic Governance through the medium of SE "Fiscservinform" optimized the process of submitting statements concerning the income tax for physical persons, connecting it to the mobile signature. More e-services should be are

[42] http://egov.md/images/normative/Moldova_Interoperability_Framework_Program.pdf

[43] http://lex.justice.md/viewdoc.php?action=view&view=doc&id=353238&lang=2

planned for launch within the framework of the projects managed by the Center for Electronic Governance. The portal Servicii.gov.md contains an electronic catalogue of public services provided by the authorities to citizens and the businesses. Out of 425 services presented on the portal, 100 are e-services open for access with a varied degree of service maturity. In future, under the Open Government Action Plan and the Government Technological Modernisation Strategy citizens will be able to over 500 e-services.

Interoperability and infrastructure

The Interoperability Program, approved by Government Decision no.656 of 5.9.2012 (supplemented later by the Government Decision no.404 of Implementation of the Interoperability Platform) is based best European practices and recommendations. It describes the current situation in the area, defines the scope, objective, the necessary actions and measures for all implementation phases and responsibilities for all actors involved in implementation of efficient exchange of data, including the necessary at the organizational, semantic and technical levels. M-Cloud h hosts the Platform of Registers and permissions (through Government Decision no.717 of 29.08.2014). This Platform offers public authorities from the Republic of Moldova an infrastructure on which they can create electronic services for enterprises that responsible for issuance of permissive acts at the 3rd stage of service maturity. It is planned to adopt the regulatory framework for the implementation of the interoperability platform (M-Connect) for 2015-2020.

All standards and technical specifications that are used in Moldova are in full conformity with the EU Framework in Interoperability.

eProcurement

At present, the State Register for Public Procurment permits publishing information ranging from invitation to tenders to the identification of winners and publication of the contract. It is also possible to register the number of procedure, CPV code, time of procedure, date of opening the tender, contracted authority, status of the procedure, and name of the object of procurement. Approximately 25% (2,700) of the “open tender” procurement were implemented online in 2014 through State Register for Public Procurment.

However, at present, it does not permit online submission and evaluation of offers. Reengineering of business processes is planned for ensuring possibility to submit online and align this service with EU standards on public procurement. In 2015, the mode for online electronic auctions is expected to be developed. It is planned to integrate it with new electronic services such as e-Invoice. While e-Ordering and e-Payment services are not part of the responsibilities of the Public Procurement Agency (PPA), once available online, they will be integrated into the State Register for Public Procurment.

eID/eSignature

Law no. 91 of 27.6.2014 on Electronic Signature and Electronic Document establishes mandatory accreditation procedure of public key certification service providers for qualified advanced electronic signatures. Expiry dates of public key certificates of users have been extended to 1 year. Competences for the Intelligence and Security Service are established as well.

The State Enterprise “Registru” issues electronic identity document since May 2014. Until this moment, 88 electronic identification documents were issued. Citizens can access a number of electronic services with eID, including “access to personal data”. Other services include:

- Revocation of the public key certificate for advanced qualified signature for the electronic identity card
- Suspension of the public key certificate for qualified advanced signature for the electronic identity card
- Restoration of the public key certificate for the advanced qualified signature after suspension within the limits of validity for the electronic identity card
- Revocation of public key certificate for authentication and identification for the electronic identity card
- Suspension of public key certificate for authentication and identification on request for the electronic identity card
- Restoration of the public key certificate for authentication and identification after suspension within validity term for the electronic identity card

Ukraine

Services and e-Signature

The only at present eID tool is digital signature which is used both for online services (like taxation or customs) and for requests/inquiries. At the moment, the use of eSignature is possible within Ukraine only (two trust services are provided within Ukraine – an issuance of qualified certificates for electronic signatures and for electronic seals, and qualified time-stamping.

The cross-border aspects of electronic identification are addressed in new law drafts on interoperability and trust services. Other alternative personal identification instruments are not available due to the lacking legislation. Certain progress is being made in advancing a population register to take full benefit from the automation of personal unique identification number (Law "On the single demographic register"# 5492-17 from 1 January 2013 that came into force from 1 January 2015) in order to issue new biometric passports.

Most of the e-services for citizens are provided as one-way information provision or downloadable forms; however, some services provided via regional pilots demonstrate higher degree of online sophistication. The following e-services are not yet provided electronically: personal document (passport and driver's license), car registration (new, used, and imported), declaration to the police (to report on incidents), and change of residential address. Tax and customs related services are fully automated (sts.gov.ua).

Services for businesses are better advanced, with social contributions (for employees), corporate tax (declaration, notification), VAT (declaration, notification), submission of statistical data being fully automated. Other e-services are provided electronically either partially, or regionally, or being under development.

Infrastructure and interoperability

The country increasingly relies on the European experience in building its electronic infrastructure in general and in relation to eID and trust services. For example, the Estonian x-Road interoperability solution is being applied as a prototype coupled with the Moldovan model (which also is based in the x-Road model). Based on the pilot results, a decision will be made which model to keep. A new draft law has been prepared to regulate the electronic interaction between agencies which is an important

step towards full interoperability. A White Book on the concept of Electronic Identification has been prepared as well.

New government agenda

The new government has strongly committed to align with European legal framework and practices including in eID/eTS. The country's leadership understand the importance of the digital market technologies and provides necessary support. A major recent breakthrough in aligning with best European practices has been the elaboration of a draft Law on Trust services and its public discussion.[44] Changes have been proposed in 2014 to the law on open government data, there use and re-use.

There is also a Cabinet of Ministers' Programme regarding eID and digital signature (Coalition Action Plan of 05.01.2015, Sustainable development "Ukraine 2020" Action Plan).

Institutions

The country does not have one government agency in charge of e-government in general and eID/eTS in particular. There are at least three different ministries that deal with e-government: Ministry of Justice of Ukraine addresses legal aspects of eID and trust services, Ministry of Economics – digital and e-services, as well as e-Procurement coordination, while a newly created (in 2014) State Agency for Electronic Governance within the Ministry for Regional Development, Building and Housing of Ukraine is charged with policy implementation (the Ministry also provides legislation support).

Other key institutions include: Cabinet of Ministers of Ukraine – strategy and legal framework, coordination of interagency workgroup, the National Commission for the State Regulation of communications and informatisation (telecom regulator), State Service for Special Communications and Informational Security (technical frameworks, accreditation, regulation, licensing in information security area).

Legal/regulatory framework

- Law on Digital Signature was passed on 15th of January 2009 N 852-15 - defines legal status of digital signature and regulates relations arising from digital signature using; determines subjects participating in the process of digital signature; defines requirements for PKI certificates.
- Law on electronic documents and electronic document workflow 22.05.2003 № 851-IV amended in 2005 and 2014 N 2599-IV of 31 May 2005 – creating, sending, transmitting, receiving, storing, processing, use and disposal of electronic documents; determines the electronic document information; determines the legal status of electronic document and it's copy.
- Law on the Concept of National Informational Development Program #75/98-BP – national informational development strategy, goals and expected results
- Law "On the single demographic register"# 5492-17 of 1 January 2013.

[44] Support was provided in the context of a bilateral Ukraine-Estonia project, http://etransformation.org.ua/2014/07/16/117/

- Law on Information Security and telecommunication systems of 5th of July 1994 N 81/94-BP – regulates the relations between subjects in the area of information security in telecommunication systems; determines information processing and security conditions; determines the mandate of public authorities

- Resolution of Cabinet of Ministers of Ukraine "Procedure of certification authority accreditation" of 13th of July 2004 N 930 – defines the order and rules of applying to the certification authorities and their accreditation process; defines technical and human resource requirements; defines requirements regarding information security and conditions of services provision

- Resolution of Cabinet of Ministers of Ukraine "On approval of the central certification authority" of 28th of October 2004 N 1451 – defines powers and duties of central certification authority

- Resolution of Cabinet of Ministers of Ukraine "On approval of usage of digital signatures by different types of organizations" of 28th of October 2004 N 1452 - defines requirements for applications of digital signature for different types of statement authorities, enterprises and public organizations

- Resolution of Cabinet of Ministers of Ukraine "On approval of the State Agency for Electronic Governance" from 1st of October 2014 N 492 - defines powers and duties of the State Agency for Electronic Governance

- Resolution of Cabinet of Ministers of Ukraine "On approval of the action plan for implementation of the Partnership and Open government initiative in 2014 – 2015 years" from 26th of October 2014 N 1176-p – preparation and submission to the Cabinet of Ministers of key law drafts to ensure that the national legal framework is in line with EU legislation; development of a Roadmap for the development of electronic democracy; preparation and submission to the Cabinet of Ministers of Ukraine of measures regarding the online publication procedures of government's open data

- Cabinet of Ministers Programme regarding eID and digital signature (Coalition Action Plan of 05.01.2015, Sustainable development "Ukraine 2020" Action Plan with decree #213 of 04.03.2001)

- Digital Signature law of 15th of January 2009 N 852-15 – defines legal status of digital signature and regulates relations arising from digital signature using; determines subjects participating in the process of digital signature; defines requirements for PKI certificates

- Law "On the single demographic register"# 5492-17 from 1 January 2013

There is sufficient legal and organizational clarity regarding the implementation of the planned activities in eID/eTS. All three governance branches – the Parliament, Cabinet of Ministers and individual ministries – coordinate their activities alongside the defined riles and responsibilities. It is expected that at the end of 2015 most of the strategic decisions in the field of electronic identification and trust services will be taken so as to deal with relevant applications and technologies in 2016.

<u>Institutions</u>

- Cabinet of Ministers of Ukraine – strategy and legal framework, coordination of interagency workgroup

- Ministry of Justice of Ukraine - legal aspects of eID and trust services

- Ministry of Economics – digital and e-services, e-Procurement coordination

- State Agency for Electronic Governance – policy implementation
- Ministry for Regional Development, Building and Housing of Ukraine – legislation support as the Ministry above the State Agency for Electronic Governance
- State Service for Special Communications and Informational Security – technical frameworks, accreditation, regulation, licensing in information security area
- National Commission for the State Regulation of communications and informatisation – telecom regulator

Infrastructure and interoperability

The country relies on the European experience in building its electronic infrastructure in general and in relation to eID and trust services. For example, the Estonian x-Road interoperability solution is being applied as a prototype coupled with the Moldovan model (which also is based in the x-Road model). Based on the pilot results, a decision will be made which model to keep. A new draft law has been prepared to regulate the electronic interaction between agencies which is an important step towards full interoperability. A White Book on the concept of Electronic Identification has been prepared as well.

Services and e-Signature

The only at present eID tool is digital signature. It is used both for online services, for example, in tax administration and customs, and for requests/inquiries. Except customs services, the use of eSignature is possible within Ukraine only. The available trust services include issuing qualified certificates for electronic signatures, electronic seals and qualified time-stamps.

Except taxation and customs related services that are fully automated (sts.gov.ua), most of e-services for citizens are provided as one-way information provision or via downloadable forms. There are no as yet online services for obtaining personal document (passport and driver's license), registering cars, sending declarations to the police (to report on incidents), changing of residential address. Services for businesses are better advanced, with social contributions (for employees), corporate tax (declaration, notification), VAT (declaration, notification), submission of statistical data being fully digitised. Other e-services are provided electronically either partially, or regionally, or being under development. Some regions have started providing on a pilot basis local e-services of a higher degree of online sophistication.

The cross-border aspect of electronic identification is addressed in new law drafts on interoperability and trust services. Certain progress is being made in advancing a population register to take full benefit from the automation of personal unique identification number (Law "On the single demographic register"# 5492-17 from 1 January 2013 that came into force from 1 January 2015) in order to issue new biometric passports. Other alternative personal identification instruments are not available due to the lacking legislation.

In practice, there is a possibility to use one of two types of cross-border transactions protected with secure eID technologies. One is Ukraine Customs services operating in cooperation with IRU (The International Road Transport Union) in the form of a two-way exchange of TIR related books and data. This information is protected with e-signature using the RSA standard (not yet official in Ukraine). The other type is used by Ukraine Railroads (a state enterprise under the Ministry of Transport) for exchanging transportation data, including fiscal information about transported goods, with relevant railway counterparts in Russia and Belarus. The security of such cross-border exchanges is ensured by the electronic signature that first decrypts a foreign encryption standard and then, in addition,

applies a local eID standard. Yet this cross-border practice not always fully reliable. Other cross-border practised exchanges and transactions on the state level are not cryptographically protected.

Standards

There are 60 locally developed ICT standards, partially harmonized with e-signature and crypto standards that have been accepted by the Ministry of Economics Order in December 2014 (effective from January 2016). There is a need to harmonize over 100 standards to align with the EU requirements.

Personal data protection and confidence

The available law on data protection is not accompanied by working mechanisms of its application in practice, with no responsibilities assigned (the data protection responsibility has recently been transferred to a newly formed state body – Ombudsman's commission following the abolishment of the Personal Data Protection State Service). Specific actions /plans are yet to be announced. Public awareness programmes for informing citizens on their rights, for there is a lot of evidence of the existing distrust on the part of citizens due to the fear of data and privacy breaches.

eProcurement

There are six e-Procurement platforms available for procurement below the threshed of 40 thousand USD, with no need for eID. There is a draft law State Procurement and new appointments made by the government in April 2015. The new legislative framework should oblige state bodies to run procurement/tenders only electronically which is not the case at the moment. Only the pre-award stage of public procurement has been automated. The volume of online procurement is not known. The NGO-supported web resource prozorro.org tracks the transparency of public procurement.

eCustoms

Detailed description of the impact of the EEU membership on the HDM with the EU

The Eurasian Economic Union (EEU) has a significant impact on eCustoms development in all Partner countries due to historical economic linkages between these countries. At present, the EEU plays the role of the driving force of innovation and progress in the development of paperless trade, risk management approaches, uniform user management and interconnection of national information systems.

The most important aspects of the role and the benefits of the Eurasian Economic Union's membership on the HDM with the EU are presented in the following sections.

Risk Management Framework

Within the framework of the Customs Union, work has being done on constant basis to unify national systems of risk management based on gained national experience in the issues of risk assessment and management. The information exchange between customs authorities is carried out in accordance with the international contacts of member-states of the Customs union. The process of the organization of risk management process and application of risk management system by the customs authorities are described in the Draft Customs Code of the EEU, which is to come in force by mid-2016.

The harmonisation of certain aspects of the EU risk management framework with the provisions of the EEU Customs Code would facilitate the creation of a more secure environment for the EaP on its external borders with the countries of the EEC. Dissemination of risk information such as information regarding the protection measures relating to avian influenza in Thailand, will allow better protect the citizens of the EaP and the EEU from external safety risks.

Authorised Economic Operator status

There is an opportunity to harmonise the usage of the AEO status between the EaP and the EEC to the mutual benefit of both parties. In the EEU, the authorized economic operator is entitled to special simplifications in the customs territory of the Union with due consideration of the provisions of the Code[45]. The notion of a "person with a status of "Faithful participant of foreign economic activity"– authorized economic operator" is determined in the Customs Code of the Customs Union.

The criterion of granting a business unit the status of the authorized economic subject differs from that of the EU and vary within the territory of the Customs Union– these criterion are very alike in Belarus and Russia, but still they are different. They are not mutually recognized in Russia and Kazakhstan. Preliminary work is being carried out to ensure mutual recognition of this status. Nowadays within the framework of the CU only status of customs carrier is mutually recognized which allows importing goods and placing them unsecured under the procedure of transit.

In addition, the draft of Customs Union Code stipulates that according to the international documents of the Union with third party specific simplifications stipulated by this Code can be provided on mutual base to the authorized economic operators of non-states of the Union. This present an opportunity to harmonise the usage of the AEO stats between the EaP and the EEC.

[45] Decision of the Commission of the Customs Union dated 09 December 2011 No. 872 "On determination of criterion to the persons implementing activities to produce and (or) export goods to which export customs duties are not applied, making claims to obtain status of the authorized economic operator "– came in force 01 January 2012.

Paperless environment

The unified structure and format of the documents applied within the framework of the Customs Union, is governed by the Commission of the Customs Union -for instance, the structure of soft copy of transit declaration and goods declaration. The SCC set the structure of statistic declaration, soft copy of notification. Today, the structure and format of electronic certificate is being approved.

Within the framework of the Customs Union, a single system and a single database of issued licenses has been created. The system includes the Ministry of Trade, Ministry of Health, Ministry of Internal Affairs, and Republican Unitary Enterprise on telecommunications oversight "BelGIE" at the Ministry of Communications, Ministry of Natural Resources.

Electronic interfaces to conduct all customs-related business

At present the information exchange between the EU and Belarus and Belarus and the Customs Union from each other – these are completely different streams of information. The CU operates its own model of information exchange. Customs services of the CU exchange large sets of information about the three main processes: transit, temporary admission and confirmation of actual export. The full information about the document is sent within the Customs Union there is an exchange of electronic information, not electronic documents, i.e., there is no certification of documents with electronic signature.

Interoperating systems of export/import/transit

During last years, in the customs authorities there were introduced a number of subsystems and complexes of software, combined into an integral automated subsystem "Transit of Customs Union."

The draft of the Customs Code of the EEU provides for an introduction of the Unified Electronic Document Management System with single submission of information to the field of EEU customs by 2021. The system will allow the interested parties to receive in real time a range of services concerning export, import and transit operations in the course of interaction with public authorities and authorized organizations of member states.

In view of the existing problems of integration of national information systems of customs and other government regulatory bodies, in the specification requirements "Integrated information system of foreign and mutual trade of the Customs Union (IISFMT) " by the Commission Decision of the Customs Union No. 771of 16 August 2011, there is stipulated that IISFMT should be used for the effective process control of customs operations and customs control of the member states of the Customs Union, as well as for data integration of information systems at the international level.

Uniform user management & electronic signatures

For electronic document flow within the EEU, a system is in development based on the mechanism of a trusted third party, which will ensure mutual recognition of electronic signature certificates issued in EEU countries.

On the level of the Customs Union neither legislation nor technical equipment is developed enough to use EDS between the customs authorities of the Customs Union. Only now, in the framework of the Customs Union the introduction of a cross-country acceptance of electronic signature is being discussed, as each state has its own requirements for the formation of EDS.

Summary electronic declaration

Within the Customs Union, an e-declaration is lodged to the customs service of the country where the goods are imported. Information from the e-declaration is used for control purposes in terms of non-

tariff regulation (prohibitions and restrictions on the transport of goods) and risk analysis. The use of the preliminary electronic information system with the application of various communication means is regulated by the relevant resolutions and orders of the SCC. Within the framework of the Customs Union, the Agreement on the Representation and Exchange of Preliminary Information about Goods and Vehicles Crossing the Customs Border of the Customs Union has been signed.

National single window

At present, each country of the Union is developing its own national single window system. In Belarus, such system is represented by the Nationwide automated information system NAIS, which is operated by the National Electronic Services Centre. As for now, the NAIS does not render services in the sphere of customs issues. There are plans to create the Single Window system (the decision of the Eurasian Commission on general principles for establishment of the Single Window system within the Customs Union). A unified electronic documents flow system with a single data submission is planned to be introduced into the customs sphere of the EEU before 2021[46].

Anti-Counterfeiting and Anti-Piracy System

For now, the Single Customs Register of Intellectual Property Units of the Member States of the Customs Union does not contain any registered intellectual property units. The register is developed in accordance with the Agreement on the Single Customs Register of Intellectual Property Units of the Member States of the Customs Union.

[46] According to the statement by Vladimir Goshin, member of the Board (Minister) for Customs Cooperation of the Eurasian Economic Commission

Armenia

National background information

The Ministry of Finance, which has recently combined the national tax and customs authorities, is responsible for the sector of external trade. Armenia has been implementing harmonization towards the EU regulations in the area of eCustoms. Significant achievements have been recorded in ensuring paperless environment for customs clearance, access to national single window, single databases of operators of foreign trade, etc. However, the interoperability with other internal state systems and especially with international counterparts is quite limited. Armenia's integration to Eurasian Economic Union is a new era for the eCustoms area. The Ministry of Finance is already working on policies to harmonize Armenia's regulations to the EEU standards.

State of play

Indicator 1: Legal framework

1.1 – Common Risk Management Framework

Armenia's national risk management system is developed based on the WTO requirements. According to the recent program/study conducted by Twinning Armenia's regulations in this area are in accordance to EU regulations almost 100%. In relation to the integration of Eurasian Economic Union, the legal framework of the latter applies that the currently deployed risk management systems in the member states are not subject to change. The Eurasian countries will continue using their national risk management systems. The priority areas in the risk management system are defined by each of the countries.

The exchange of risk information is currently done based on requests through the Ministry of Foreign Affairs or Ministry of Finance. The risk analysis uses automated data processing techniques but is not fully automated.

There is no single interface or platform available with other countries. As of now if there is any information to be shared regarding the risk management area, the ministry of foreign affairs does this.

The system cannot be fully automated is continuously upgraded. Next technical upgrade of the risk management system is expected at the end of 2015.

1.2 - Authorised Economic Operator status

The Law defines the requirements, procedures and benefits of the authorized economic operators. The requirements for AEOs are not as strict as that of the European Union. Despite the amended version of the regulations, there are no registered AEOs in Armenia. The lack of motivation for local enterprises to become AEOs can be reasoned by several factors:

- The benefits of joining AEO schemes are limited;
- The number of economic agents with significant foreign trade volumes is very low.

1.3 - Paperless environment for customs and trade

The electronic customs system is in place, however the exchange of data with other countries is not implemented.

Indicator 2: Infrastructure

2.1 - Electronic interfaces to conduct all customs-related business

Economic agents in Armenia can declare their goods at any cross border point within the country independently of the exact point of exit of the product. However, the examination (if needed) is done only in one centre – in Yerevan.

However, the country's single access point is not connected to other countries access points. There is no single information infrastructure in place. The existence of a single platform will require integration of corresponding legislations and regulations in one place which is a significant effort and requires considerable time. By 2017 Armenia will have elaborate legislative framework agreed with the EEU requirements in place.

2.2 – Interoperating systems for import, export and transit

The system is almost 100% electronic. The interfaces for the export, import and transit areas are different but they operate in the same environment and can exchange information among each other.

The systems are fully interoperable among the country's systems but are not connected to other countries' systems.

2.3 - Integrated tariff information system

The binding tariff system is in place. All information sources refer to the Law on Customs for the reference about the binding classification. Currently the Ministry of Finance works with the Eurasian Union on harmonizing 18 components in this area.

2.4 - Single Point for Entry or Exit of Data (SPEED) portal

The country's transit system is not connected to SPEED system. Currently there are no plans under discussion targeting this area.

2.5 - Uniform user management & digital signatures

The e-signature system is in place in Armenia. The interoperability is valid within the country however, there is no mutual recognition with other countries.

Indicator 3: Services

3.1 - Registered Exporters System

As soon as a company is registered in the state registry, the data about the company is automatically entered into the database of the Ministry of Finance. It does not matter if it is an exporter or not. When the company begins to export, its activities are recorded in the same database. The regulatory framework does not allow registering the data of the local companies in the European REX database. There are no efforts undertaken in registering local exporters in European REX.

3.2 - Economic Operators Registration and Identification system

A system of registered economic operators with unique Registration and Identification (EORI) numbers is not in place in Armenia. Consequently, there is no connection to EC EORI system. The introduction of such system is not discussed in Armenia as of now.

3.3 - Exchange of data about Authorised Economic Operators

Economic operators are registered in different registries, including state registry, tax payers' registry and customs registry. The AEO area is regulated by the Law, however there are not yet registered AEO in Armenia. No mutual recognition of AEOs is possible now in Armenia.

3.4 - Summary electronic declaration

An electronic summary declaration containing the required pre-arrival or pre-departure information will be ready by the end of 2015. Currently the information is exchanged via the Ministry of Finance. Ministry of Foreign Affairs provides the information without any limitation in the countries.

3.5 - National Single Window System

According to corresponding order by the President of the Republic of Armenia, the single window principle is implemented in various areas, such as pharmaceuticals, food safety, etc. In a number of areas the introduction of Single Window is underway according to the planned timeline (Government Decree 2015-2017).

3.6 - Anti-Counterfeiting and Anti-Piracy System

Armenia is part of intellectual property agreements (IPM). No other exchange of information is taking place.

Gap analysis

Indicator 1: Legal framework

1.1 – Common Risk Management Framework

Armenia has clearly defined national risk management framework in customs controls for goods brought into or out of the country. The framework is fully harmonised with the EU common criteria and priority control areas.

The risk analysis uses automated data processing techniques but is not fully automated. Risk Information Form currently cannot be exchanged electronically with customs offices of the EU countries or any other countries.

1.2 - Authorised Economic Operator status

The customs authorities of the country apply common criteria and harmonised requirements for granting the status of authorised economic operators (with some simplifications comparing to the EU criteria), allow the use of simplifications by authorised economic operators and recognise the status of AEOs registered in the EU member states or other countries.

There are no registered AEOs in the country yet due to the lack of interest and evident benefits by Armenian enterprises. National system of identification and registration for economic operators does not interoperate with the Authorised Economic Operators EU system.

1.3 - Paperless environment for customs and trade

National legal provisions are defined for secure, integrated, interoperable and accessible electronic customs systems for the exchange of data contained in customs declarations, documents accompanying customs declarations, certificates and the exchange of other relevant information.

The electronic customs system does not currently allow the exchange of data between the customs authorities of Armenia and customs authorities of any other country, economic operators, other administrations or official agencies involved in the international movement of goods.

Indicator 2: Infrastructure

2.1 - Electronic interfaces to conduct all customs-related business

Information systems of the country does not have a service of single access point enabling economic operators to use one single interface to lodge electronic customs declarations to the customs systems

of other countries (the EU member state or others). This work within the Eurasian Economic Union has been planned to start by development of a required legal framework.

2.2 – Interoperating systems for import, export and transit

The country systems for import and export interoperate with the system for transit and can enable the seamless flow of data. There is no service that can currently ensure transfer of data between the national customs systems to/from customs system of the EU member states.

2.3 - Integrated tariff information system

The country has implemented a national centralised binding tariff information system that allows getting tariff classification for goods. The system is interconnected with other tariff related IT systems to facilitate re-use of data and functionality of one system to another.

2.4 - Single Point for Entry or Exit of Data (SPEED) portal

The country's computerised transit, export, import or economic operators systems are not connected to the SPEED portal and allow data exchange for electronic customs systems between the country and the EU.

Single Portal for Entry and Exit of Data (SPEED) has the key objective to facilitate trade of the EU with third countries and/or exchanges with non-Customs systems. To support this initiative, a generic technical solution has been developed which permits each partner (e.g. third country) to connect to a system developed centrally by DG TAXUD.

2.5 - Uniform user management & digital signatures

A system based on mutual recognition of solutions for electronic signatures is operational in the country and enables the national economic operators to send information to other administrations than customs, and to enable these administrations to verify the authenticity of the author, of the sender and of the information.

The national electronic signature framework is not interoperable with e-signature frameworks of other countries (the EU member states or the Eurasian Economic Union).

Indicator 3: Services

3.1 - Registered Exporters System

Armenia has a national database of legal entities that also include data on their export activities. This cannot be considered as a proper Registered Exporters System.

There is no possibility for automated verification of the exporters' registration number from the declarations in the national Customs declaration system. The country does not cooperate with the EU in order to register national exporters into the EU REX central database managed by the European Commission.

3.2 - Economic Operators Registration and Identification system

Registration and Identification numbering system is not operational in the country. The national systems containing profiles of traders are not interconnected with the EORI central database managed by the European Commission.

3.3 - Exchange of data about Authorised Economic Operators

The country does not have a dedicated information system for registration and Identification of economic operators. Armenia has not concluded an agreement of mutual recognition of the country's

registers of economic operators and the Authorised Economic Operators in the EU. There is not system-to-system interface allowing the economic operators' data received from the country to be disseminated to the EU member states and the validation of the county' AEO status in the EU transaction systems.

3.4 - Summary electronic declaration

By the end of 2015, it will be possible to lodge an electronic summary declaration containing the required pre-arrival or pre-departure information before any goods are brought into or out of the territory of the country. All information will be provided to the customs and other authorities in electronic format. Existing country's infrastructure allows such information to be shared electronically with third countries where an international agreement so provides.

3.5 - National Single Window System

The national single window and one-stop shop in the area of external trade (different degree of readiness for different applications) is in place and allows submission of all required information and documents in electronic format (application for certificates, customs declaration, required documents, permits). Administrations or agencies will be able to deliver certificates required for import or export authorisation in electronic format.

3.6 - Anti-Counterfeiting and Anti-Piracy System

There is no electronic service in place providing traders with the possibility to submit a claim asking the intervention of Customs in order to take measures against goods infringing certain intellectual property rights. There is no exchange of electronic information with the EU centralised Anti-Counterfeiting and Anti-Piracy System information system, which is accessible by all Member States.

Azerbaijan

National background information

Organisations involved

State Customs Committee of Azerbaijan is the central executive body responsible for formation, execution and regulation of state policy on Customs in Azerbaijan.

Relevant legislation

- Customs Code of the Republic of Azerbaijan
- Resolution of the Cabinet of Ministers of the Republic of Azerbaijan on the "Approval of the Rules for rendering of electronic services by central executive bodies on specific spheres" and on the "Approval of the list of e-services' types", dated 24.11.2011, #191

ICT platforms and services

According to Cabinet of Ministers' Resolution dated 24.112011, on approval of "Rules for rendering of e-services on specific spheres by central executive bodies" and on approval of "List of e-services' types" a number of e-services to be rendered by State Customs Committee were incorporated into E-Governmnet portal.

Currently the following 14 e-services are rendered by State Customs Committee:

- e - Customs Declaration / Goods
- e - Pre-arrival Information

- e - Customs Declaration / Passengers
- e - Monitoring
- e - Imports / Exports
- e - Customs Examination
- Goods Nomenclature
- Application for permission to establish duty-free shop
- Submission of application and documents to get, terminate or annihilate the license for operating as customs broker and customs carrier
- Submission of application and documents to get, terminate or annihilate the license for establishing customs warehouses and warehouses of temporary storage
- Online monitoring of application and inquiries submitted to the State Customs Committee
- e - CPPIN
- e - Customs Payments
- Calculation of customs payments for import of light vehicles

State of play

Indicator 1: Legal framework

1.1 – Common Risk Management Framework

Risk management system operates as a module of the Unified Automated Management System (UAMS). It was created and developed based on recommendations of the World Customs Organization (WTO Risk Management Compendium) and other international tools.

1.2 - Authorised Economic Operator status

The legislative base of the Institute of the Authorized Economic Operator (AEO) is fully formed in the country. Chapter 5 of the Customs Code of the Republic of Azerbaijan and Decree # 230 of the Cabinet of Ministers, 27 August 2013 set forth rules on how to get a status of AEO by legal entities, including requirements on AEO's operations. These legal acts provide simplified procedures in line with the best international practices. Implementation of the project on AEO is at a stage of development and currently there is no registered AEO in the country.

1.3 - Paperless environment for customs and trade

Data exchange contained in customs declarations, corresponding documents, certificates and exchange of other relevant information can be carried out within the framework of international treaties.

Indicator 2: Infrastructure

2.1 - Electronic interfaces to conduct all customs-related business

UACS is in a position to provide one-stop access for electronic customs declarations and data exchange.

2.2 – Interoperating systems for import, export and transit

Import, export and transit subsystems are interoperating and completely integrated under the Unified Automated Management System of the Customs Service of the Republic of Azerbaijan. Nevertheless, at the moment the Customs Service of the Republic of Azerbaijan does not carry out any electronic data exchange on import, export or transit with EU.

2.3 - Integrated tariff information system

There is a unified system on tariff classification of goods within the UACS. The system is fully integrated into other components of the UACS.

2.4 - Single Point for Entry or Exit of Data (SPEED) portal

The computerized transit system of the State Customs Committee (SCC) of Azerbaijan is one of the components of the UACS. The system can be accessed based on the Single Sign-On concept. An electronic data exchange with EU countries is not being carried out.

2.5 - Uniform user management & digital signatures

The legislative base for operating electronic signature is fully formed and operation. Economic operators have all legal and technical possibilities for using an electronic signature for the purpose of transferring information to the customs and other administrative bodies.

Indicator 3: Services

3.1 - Registered Exporters System

The registration of foreign economic activity participants is carried out through the Taxpayer identification number in the UAMS system, which enables to automatically verify registration numbers from declaration. There is no registration being carried out of national exporters in the central database Registered Reporters System (REX).

3.2 - Economic Operators Registration and Identification system

The State Customs Committee of the AR does not use EORI system.

3.3 - Exchange of data about Authorised Economic Operators

There is an information system for identifying economic operators in the country, however no data exchange with EU is being carried out.

3.4 - Summary electronic declaration

The Customs legislation of the Republic of Azerbaijan allows filing of summary e-declarations, specifically stipulated in the Articles 113-116 of Customs Code. Current infrastructure of SCC of the Republic of Azerbaijan can transfer such information to third countries in an electronic version. This is possible if there is an international legal mechanism in place.

3.5 - National Single Window System

To modify customs service and provide more favourable conditions for businesses and international trade “Single Window” (One-Stop-Shop) system was introduced in accordance with Presidential Decree dated 11.11.2008. The authority of the regulatory state body on state borders was given to the State Customs Committee of the Republic of Azerbaijan. It allows integration of different control mechanisms on the border, including eliminating bureaucracy and burdensome trade procedures. It was achieved by transferring of some functions of the Ministries of Health, Transport, Agriculture and Veterinary Service to the State Customs Committee. This project also was beneficial for improving Azerbaijan’s rating in World Bank “Doing Business” report and helped to make significant steps for creating National Single Window System.

3.6 - Anti-Counterfeiting and Anti-Piracy System

There is no Anti-Counterfeiting and Anti-Piracy System in the country. There is only a service for online monitoring of applications and inquiries submitted to the State Customs Committee.

Gap analysis

Indicator 1: Legal framework

1.1 – Common Risk Management Framework

A clearly defined national risk management framework in customs controls for goods brought into or out of the country is in place and automated. It is harmonised with the WTO international criteria which also cover the EU common criteria and priority control areas. Risk Information Form cannot be exchanged electronically with customs offices of the EU countries.

1.2 - Authorised Economic Operator status

The customs authorities of the country apply common criteria and harmonised requirements for granting the status of authorised economic operators, allow the use of simplifications by authorised economic operators and recognise the status of AEOs registered in the EU member states or other countries. However, currently there are no registered AEOs in the country.

1.3 - Paperless environment for customs and trade

National legal provisions are defined for secure, integrated, interoperable and accessible electronic customs systems for the exchange of data contained in customs declarations, documents accompanying customs declarations, certificates and the exchange of other relevant information.

Indicator 2: Infrastructure

2.1 - Electronic interfaces to conduct all customs-related business

Information systems of the country have a service of single access point enabling economic operators to use one single interface to lodge electronic customs declarations. However, there is no current possibility of submission to the customs systems of other countries (the EU member state or others).

2.2 – Interoperating systems for import, export and transit

The country systems for import and export do not interoperate with the system for transit and enable the seamless flow of data. There are no developed services that can ensure transfer of data between the national customs systems to/from customs system of the EU member states.

2.3 - Integrated tariff information system

The country has implemented a national centralised binding tariff information system that allows getting tariff classification for goods. The system is interconnected with other tariff related components to facilitate re-use of data and functionality of one system to another.

2.4 - Single Point for Entry or Exit of Data (SPEED) portal

The country's computerised transit system is not connected to SPEED portal. There is no data exchange between electronic customs systems of Azerbaijan and the EU countries.

2.5 - Uniform user management & digital signatures

A common solution for electronic signatures is operational in Azerbaijan and enables the national economic operators to send information to other administrations than customs, and to enable these administrations to verify the authenticity of the author, of the sender and of the information. No interoperability framework for mutual recognition of electronic signatures with other countries has been established.

Indicator 3: Services

3.1 - Registered Exporters System

The country has established a UACS system that allows an automated verification of the exporters' registration number from the declarations in the national Customs declaration system. The country does not currently cooperate with the EU in order to register national exporters into the EU REX central database managed by the European Commission.

3.2 - Economic Operators Registration and Identification system

Azerbaijan does not use a system of economic operators' registration and identification numbers assigned to economic operators. There is no common reference numbering system in the country to organise relations of economic operators with customs authorities throughout the country and for the exchange of information between the customs authorities and other authorities.

3.3 - Exchange of data about Authorised Economic Operators

Azerbaijan has a registration and identification information system of economic operators. It has not concluded any agreement of mutual recognition of the country's register of economic operators and the Authorised Economic Operators in the EU. There is not system-to-system interface that could allow the economic operators' data received from the country to be disseminated to the EU member states and the validation of the county' AEO status in the EU transaction systems.

3.4 - Summary electronic declaration

An electronic summary declaration containing the required pre-arrival or pre-departure information is lodged before any goods are brought into or out of the territory of Azerbaijan. All information can be provided to the customs and other authorities in electronic format. Existing country's infrastructure allows such information to be shared electronically with third countries where an international agreement so provides.

3.5 - National Single Window System

The national single window and one-stop shop is in place and allows submission of all required information and documents in electronic format.

3.6 - Anti-Counterfeiting and Anti-Piracy System

A basic electronic service is in place providing traders with the possibility to submit a claim to the State Customs Service about goods infringing certain intellectual property rights. There is no national Anti-Fraud Information System.

Belarus

Relevant legislation

- The Customs Code of the Customs Union (Attachment to the Contract on the Customs Code of the Customs Union dated 27 November 2009)
- Common customs tariff of the Customs Union of the Republic of Belarus, the Republic of Kazakhstan and the Russian Federation, approved by the Decision of the Council of the Eurasian Economic Commission dated 16 July 2012 No. 54
- The Law of the Republic of Belarus dated 10 January 2014 No.129-З "On customs regulation in the Republic of Belarus "
- The Resolution of the Council of Ministers of the Republic of Belarus dated 27 May 2014 No. 509 "On measures of realization of the Law of the Republic of Belarus "On customs regulation

in the Republic of Belarus ”

The list of the international contracts serving as a contract and legal base for the Customs Union includes inter alia:

- Protocol on the exchange of information in electronic form between taxing authorities of the states-members of the Customs Union on the paid amounts of indirect taxes dated 11 December 2009
- Agreement on application of information technologies for electronic documents exchange in foreign and mutual trade in the uniform customs territory of the Customs Union dated 21 September 2010
- Agreement on creation, function and development of the integrated information system of foreign and mutual trade of the Customs Union dated 21 September 2010

Organisations involved in the HDM process

State Customs Committee of the Republic of Belarus

In the structure of the State Customs Committee of the Republic of Belarus the issue of the implementation of information technologies in customs procedure is entrusted to the Administration for the Development of Customs Infrastructure and Administration for Information Technologies, Customs Statistics and Analysis. Information systems are applied in the activity of the Administration for the Organization of Customs Control; Administration for Counter-Contraband Operations and Infringement of Administrative Customs Offences; Administration for Tariff Regulation and Customs Payments, Management of Risk Analysis and Operational Control.

Beltamozhservis

The Republican Unitary Enterprise “Beltamozhservis”, founded by the State Customs Committee of the Republic of Belarus. The enterprise is the largest operator in the logistics services market of Belarus. Logistic activity carried out by the enterprise in the territory of the Republic of Belarus is based on creation of institutional logistic system with application of recent IT-technologies, status of 3PL-provider, developed infrastructure in all the regions of the country.

Scientific and Practical Republican Unitary Enterprise “The Inter-branch Scientific and Practical Centre for Identification Systems and E-business Operations” of the National Academy of Sciences of Belarus

The Identification centre was created in 2006 as the organization specializing in the sector of automatic identification and electronic business operations.

Decision making process

Within the country SCC acts as a leading body developing and implementing state policy in the eCustoms sector. When elaborating the customs IT projects to be carried out within the framework of the National Programme for Accelerated Development of ICT for the years 2011-2015, the SCC interacted with other state bodies: the Ministry of Economy, the Ministry of Communications and Informatisation.

The Order of the Chairman of the State Customs Committee of the Republic of Belarus dated 21 November 2012 No. 493-ОД stipulates creation of expert-advisory group on IT technologies including the representatives of various organizations participating in customs affairs, including representatives of business, scientific, and infrastructure sectors.

The international interaction of customs authorities of the Russian Federation, the Republic of Belarus

and the Republic of Kazakhstan is realized within the framework of common bodies: the Council of Customs Services Heads of CIS member-states, the Council of Customs Services Heads under Integration Committee of the EurAsEC, panel of the Union State Customs Committee.

National plans

Currently running is the Sub-programme “eCustoms” of the National programme of accelerated development of services in the field of information and communication technologies (ICT) for 2011-2015

The Concept of creation of the Single Portal for Foreign Trade has been approved; the body in charge of its implementation is the Ministry of Foreign Affairs (MFA)

The strategy of development of information society in the Republic of Belarus for the period up to 2022

International agreements

Memorandum of Understanding between the Secretariat of the Customs Union Commission and UN Conference on trade and development (United Nations confederation on Trade and Development)

Memorandum of Understanding between the Secretariat of the Customs Union Commission and the United Nations Economic Commission for Europe

Agreement on creation, functioning and development of the integrated information system of foreign and domestic mutual trade of the Customs Union - 2010

State of play

Indicator 1: Legal framework

1.1 Common Risk Management Framework

The State Customs Committee of the Republic of Belarus has formed legal and methodological framework of risk analysis and management system (RAMS), the corresponding organization structure has been created, the Concept of risk analysis and management system for years 2010-2015 and up to 2020 in prospect was elaborated and approved.

When performing customs check the customs authorities of the Republic of Belarus apply principle of selectivity and use the forms of customs check to the extent that is necessary to ensure compliance with customs legislation, i.e. when performing customs check risk analysis and management system is applied. In Belarusian system of risk management general principles of management applicable both for the Customs Union, and for the EU are laid down. It is governed by the supranational and national legislation.

Belarusian system of risk management obtains data from National Automated Information System of Electronic Declaration (NAISED)[47], whereto the concerned parties send data, for instance, data from customs declaration forms related to the goods. In risk management system such notions as risk indicator and risk profile can be singled out. Solution on application of the corresponding measures is made automatically on the basis of the processing of the indicators.

Within the framework of the Customs Union, work is being done on constant basis to unify national systems of risk management based on gained national experience in the issues of risk assessment

[47] http://gtk.gov.by/ru/eldeclaration_new/informacija_o_NASED

and management. It has been estimated that the customs authorities interexchange information on the measures applied to minimize risks, as well as the information enhancing efficiency of customs control under the procedure established by the international contract of member-states of the Customs Union.

The information exchange between customs authorities is carried out in accordance with the international contacts of member-states of the Customs union, including also with use of information system and IT. In the Draft Customs Code of the EEC , that is to come in force by mid-2016 the process of the organization of risk management process and application of risk management system by the customs authorities is also described.

Existing system has not been harmonized with the principles of the EU. Priority areas of control in Belarus were outlined, but these are different from that applicable in the EU due to the specific structure of economic system and peculiarities of legislation in the Customs Union countries.

Within the framework of the project “Assistance in creation of electronic system of preliminary information exchange between the customs authorities of Belarus and Ukraine (PRINEKS)”, financed by the European Union in the end of 2015 new risk management system will be implemented, which will enhance security of the countries in relation of the illegally moved goods.

1.2 - Authorised Economic Operator status

The Decree of the President of the Republic of Belarus No. 319 dated 18 July 2011 “On some issues of customs regulation, on the implementation of activities in the field of customs and the authorized economic operator” includes Provision on the procedure of issue of certificate on entering the Register of Authorized Economic Operators and its withdrawal. It also includes Provision on implementation of activities in the field of customs, governing the procedure for shaping registers of the persons implementing activities in the field of customs.

The status of authorized economic operator is assigned to the concerned person by the State Customs Committee by granting certificate. For all the authorized economic operators (AEO) still in Belarus similar simplifications are applied. A tendency towards implementation of categorizing of business units exists and depending on such category various methods of customs control will be applied.

There is the Register of Authorized Economic Operators containing information on number of business units to which the customs trust and that allows certain simplifications in standard procedures. There is no Register of Economic Operators with EORI numbers in Belarus, to identify economic operators taxpayer identification number (TIN) is used which is assigned to every business unit.

The business unit registration system of Unified State Register of Legal Entities and Individual Entrepreneurs is maintained by the Ministry of Justice. In Belarus there is “AIS Vzaimodeistvie” information system is used by several state bodies, within the framework of which all the procedures related to the support of business units –registration, interaction with social welfare fund, taxing authorities, and liquidation hereof – are carried out. SCC has access to this system as well as to the data base of the Ministry for Taxes and Levies. The Register of Authorized Economic Operators is located on the site of SCC in the form of a table in WORD document, it contains the list of 334 authorized economic operators as of 03 February 2015. (valid till 03 March 2015) with the number of the AEO certificate.

Decision of the Commission of the Customs Union dated 09 December 2011 No. 872 “On determination of criterion to the persons implementing activities to produce and (or) export goods to

which export customs duties are not applied, making claims to obtain status of the authorized economic operator "– came in force 01 January 2012. The authorized economic operator is entitled to special simplifications in the customs territory of the Union with due consideration of the provisions of the Code. The notion of a "person with a status of "Faithful participant of foreign economic activity"– authorized economic operator" is determined in the Customs Code of the Customs Union.

The criterion of granting a business unit the status of the authorized economic subject differs from that of the EU and vary within the territory of the Customs Union– these criterion are very alike in Belarus and Russia, but still they are different. They are not mutually recognized in Russia and Kazakhstan. Preliminary work is being carried out to ensure mutual recognition of this status. Nowadays within the framework of the CU only status of customs carrier is mutually recognized which allows importing goods and placing them unsecured under the procedure of transit.

In addition, the draft of Customs Union Code stipulates that according to the international documents of the Union with third party specific simplifications stipulated by this Code can be provided on mutual base to the authorized economic operators of non-states of the Union.

1.3 - Paperless environment for customs and trade

There is the elaborated regulatory basis for the issues of e-declaration, structure of electronic copies of documents, as well as requirements set to the foreign information systems (see questions 1 and 5 of the topic eID).

Interaction between state bodies according to the principle "system to system" on the whole is not quite developed in Belarus. SCC and taxing authorities exchange information, but they do not cooperate. According to the specific regulation the SCC provides to the taxing authorities the corresponding information, for instance, once per two weeks. On the whole, the SCC electronically cooperates with about 40 state organizations. But with each department such cooperation is yet implemented separately, as each of them has their own departmental information systems, and requirements to the composition and format of the document may vary. There is no single format of data exchange between state bodies established. To solve this problem SAIS is being built in Belarus, and through this system the state will make cooperation between state organizations obligatory. This system is built on web-services with standard format of data transfer in XML.

There is no specific requirement to the certain customs systems in Belarus. There are regulatory acts governing flow of e-documents within information systems, including also state bodies, on the whole. There are requirements to the rules of forming Electronic Digital Signature. There is a resolution setting technological regulation of EDS flow. There are several regulatory acts adopted by the OAC binding for all the state bodies governing issues of creation of necessary systems for protection of state information systems, on the procedure of certification thereof and commissioning of the system. In case all the requirements are fulfilled, the system is considered as protected and can be used also for customs purposes.

The unified structure and format of the documents applied within the framework of the Customs Union, is governed by the Commission of the Customs Union, for instance, the structure of soft copy of transit declaration and goods declaration. The SCC set the structure of statistic declaration, soft copy of notification. Today, the structure and format of electronic certificate is being approved. I.e. the set of the necessary regulatory acts for the purposes of organization of interaction of the concerned parties with the customs has not been elaborated yet.

Within the framework of the Customs Union a single system and a single database of issued licenses is created. The system includes the Ministry of Trade, Ministry of Health, Ministry of Internal Affairs,

and Republican Unitary Enterprise on telecommunications oversight "BelGIE" at the Ministry of Communications, Ministry of Natural Resources.

The State Customs Committee has started to implement the principle of “integrated border management” (based on the organization of information exchange among the checkpoint control services and the participants of foreign trade through the development and implementation of Automated system for controls in the road checkpoint.

There is no common regulatory act governing the interaction procedure with the EU. A set of the international contracts has been signed by the Government of the Republic of Belarus and the governments of the corresponding EU countries on interaction in customs issues that gives legal platform for interaction between customs administrations. The SCC discusses issues and establishes the corresponding technology and technical regulations with each country that Belarus signed such agreement with. For each country today absolutely different format and composition, and method of information exchange can be applied.

Indicator 2: Infrastructure

2.1 - Electronic interfaces to conduct all customs-related business

The Republic of Belarus uses National Automated Information System of Electronic Declaration (NAISED) – a system that provides information support and automation of customs operations carried out by customs officials and concerned parties (declarants) using written and electronic documentsi. It also provides informational interaction of customs authorities of the Republic of Belarus with concerned parties and customs of other countries.

Submission of an electronic customs declaration and supporting documents to the NAISED requires using a special software and hardware that enable interaction with information systems of customs authorities of the Republic of Belarus for the exchanging of electronic documents and obtaining public verification key certificates for digital signatures. In Belarus, there are several commercial companies that write and distribute software designed for information exchange with the customs authorities of Belarus.

Services for electronic declaration are available to participants of foreign economic activity throughout the country.

Currently there is a control system, which is based on information interaction of Belarusian and Russian customs which allowed to exclude control and customs clearance on the inside Belarusian-Russian border. Unified Automated Information System of the Union State Customs Committee (UAIS) is developed as part of the common customs area formation.

At present the information exchange between the EU and Belarus and Belarus and the Customs Union from each other – these are completely different streams of information. The CU operates its own model of information exchange. Customs services of the CU exchange large sets of information about the three main processes: transit, temporary admission and confirmation of actual export. The full information about the document is sent within the Customs Union there is an exchange of electronic information, not electronic documents, i.e., there is no certification of documents with electronic signature.

2.2 – Interoperating systems for import, export and transit

The customs authorities of the Republic of Belarus use near 40 various information systems. Most of these systems are integrated into a Single automated information system of the Customs authorities. There are national systems for import, export and transit (they contain data from customs declarations

and accompanying documents, certificates and other relevant information). They are secure, integrated, interoperable and accessible by customs bodies in Belarus. They interoperate with the system for transit and enable the seamless flow of data.

During last years, in the customs authorities there were introduced a number of subsystems and complexes of software, combined into an integral automated subsystem "Transit of Customs Union."

The draft of the Customs Code of the EEU provides for an introduction of the Unified Electronic Document Management System with single submission of information to the field of EEU customs by 2021. The system will allow the interested parties to receive in real time a range of services concerning export, import and transit operations in the course of interaction with public authorities and authorized organizations of member states.

In view of the existing problems of integration of national information systems of customs and other government regulatory bodies, in the specification requirements "Integrated information system of foreign and mutual trade of the Customs Union (IISFMT) " by the Commission Decision of the Customs Union No. 771of 16 August 2011, there is stipulated that IISFMT should be used for the effective process control of customs operations and customs control of the member states of the Customs Union, as well as for data integration of information systems at the international level.

2.3 - Integrated tariff information system

Belarus has implemented a national not centralised tariff information system. Integrated tariff environment enables the reuse of data across the connection of systems of export and import to the National System for Customs declarations and to the National control system (within the customs information systems, the tariff system is integrated separately)

For the tariff classification the economic operator must determine the commodity code. In Belarus there is no automated system for economic operators that allows receiving the tariff classification of goods. In Belarus, the economic operator is responsible for the commodity code identification – he should correctly identify it in the customs declaration. For this purpose, the declarant may use the Uniform tariff FEACC codes classifier which operates in three countries of the Customs Union.

Customs services have the FEACC codes classifier integrated into existing departmental systems, but concerned parties have no access to this system.

FEACC codes classification is supported in software products developed for the declarants in Belarus by commercial firms. These information systems support the same tariff classifier, as in the system of customs services, and it is updated by software developer. Depending on the commodity code there is a method of calculation of customs duties, each code has a rate of customs duty and VAT, and it is possible to calculate customs duties. But it is difficult to provide the correct tariff classification using these systems, because the commodity description is rather general, and there are some features cannot be integrated into the system.

In case of wrong code identification the economic operator will have to pay the debts incurred in connection with the wrong code identification and calculation of tariffs. In Belarus the customs authorities render such paid service as providing a preliminary decision on the FEACC code of goods on the basis of the documents submitted.

The Decision of the Eurasian Economic Commission No.54 of July, 16 2012 approved the Foreign Economic Activity Commodity Classification of the Customs Union (hereinafter – FEACC CU) and the related Uniform customs tariff of the Customs Union Unified Customs Tariff of the Customs Union.

Tariff information system does not interact with the general system of preferences and export goods

to the EU.

2.4 - Single Point for Entry or Exit of Data (SPEED) portal

The country's computerised transit and other systems are not connected to EU SPEED portal.

2.5 - Uniform user management & digital signatures

In Belarus, electronic digital signature (EDS) is used by the declarants when submitting electronic documents into the National Automated Information System of Electronic Declaration (NAISED). Certification centres for users of public key infrastructures of customs authorities of the Republic of Belarus are available in customs offices of all regions of the country. Economic operators are able to send information to other administrations than customs to verify the authenticity of the author, of the sender and of the information (not via NASED but individually to these authorities)

Belarus introduced in 2014 a State Public Keys Management System (SPKMS) in order to solve the problem of interagency electronic documents. The Root Certification Authority and National Certification Authority were put into operation. Previously each state agency had its own certification authority, including the customs authorities. Now the country and the customs authorities also begin to use SPKMS, and it will allow the transmission of documents not only to the customs but also to other public authorities.

EDS are not applied for the information exchange between customs authorities within the country because other means for information security protection in the system are used, the system is not available to external users.

There is still no opportunity for economic operators to send information to administrations of foreign countries, such as EU member states or the countries of the Eurasian Economic Union.

For electronic document flow within the EEU, a system is in development based on the mechanism of a trusted third party, which will ensure mutual recognition of electronic signature certificates issued in EEU countries.

In the opinion of respondents, on the level of the Customs Union neither legislation nor technical equipment is developed enough to use EDS between the customs authorities of the Customs Union. Only now, in the framework of the Customs Union the introduction of a cross-country acceptance of electronic signature is being discussed, as each state has its own requirements for the formation of EDS. The only way that allows checking the signature of another country - using a trusted third party.

Sending of the information to the EU countries with the use of electronic signature is not possible until the introduction of an appropriate mechanism for the trusted third party.

Indicator 3: Services

3.1 - Registered Exporters System

There is no separate comprehensive register of registered exporters in the country.

Decree of the President of the Republic of Belarus No. 319 of 18 July 2011"On some issues of customs regulation, on the implementation of activities in the field of customs and the authorized economic operator" includes Provisions on the operation in the field of customs, which regulates the formation of the register of persons operating in the field customs. As of 03 February 2015, the register of authorized economic operators contains 334 authorized economic operators with the number of the AEO certificate.

Also, there is a portal for export information support (operator - National Centre for Marketing and

Price Study of the Ministry of Foreign Affairs of the Republic of Belarus), containing a database of Belarusian enterprises-exporters, a database of exported goods and services, a database of commodity distribution network objects. The information in these databases is placed directly by enterprises on a voluntary basis. These databases are not linked to the information systems of customs authorities, not connected with the UAIS, do not allow carrying out any administrative procedures or the exchange of electronic documents, and functioning as general information retrieval system.

3.2 - Economic Operators Registration and Identification system

An electronic system for storing and exchanging Economic Operators Registration and Identification (EORI) numbers is not yet operational in the country.

A unique number (not EORI) is assigned to each economic operator (a payer account number). It serves as a common reference in relations of economic operators with customs authorities throughout the country and for the exchange of information between the customs authorities and other authorities.

Non-residents (Russia, Kazakhstan, Poland, Lithuania, and others.) do not get additional numbers (numbers are used, taken for the identification of business entities in these countries, including EORI).

3.3 - Exchange of data about Authorised Economic Operators

Belarus maintains a separate register of authorised economic operators, which contains data on the number of business entities, whom the customs trust and give certain simplifications. Criteria for granting this status to operators do not meet the criteria applied in other countries in the EU or the EEU. There are no agreements on mutual recognition of authorized economic operators either with the EU or the EEU. In principle, there is no system-to-system interface either with the EEU or the EU.

Based on the profiles of economic operators registered in the national system, the country’s authorities can attribute different trust level status to different economic operators. Now, the gradation "normal" and "authorized" is used. The more detailed gradation is planned under the Customs Code of the Customs Union.

3.4 - Summary electronic declaration

The Belarusian legislation has two different terms: pre-declaration and preliminary information.

The preliminary declaration, which is filed electronically, is used mainly for export and contains a minimum set of data for risk assessment, thereafter complete information is submitted. The customs declaration is always submitted as an electronic document, or it is accompanied by a mandatory electronic copy, which is necessary for processing and verification.

An electronic summary declaration containing the required pre-arrival or pre-departure information is lodged before any goods are brought into or out of the territory of the country (preliminary declaration). All information is provided to the customs and other authorities in electronic format.

Data set and format for the summary declaration are defined by the national legislation and the regulatory framework, and contain the particulars necessary for risk analysis and the proper application of customs controls, primarily for security and safety purposes.

Within the Customs Union, an e-declaration is lodged to the customs service of the country where the goods are imported. Information from the e-declaration is used for control purposes in terms of non-tariff regulation (prohibitions and restrictions on the transport of goods) and risk analysis.

The use of the preliminary electronic information system with the application of various communication means is regulated by the relevant resolutions and orders of the SCC.

Within the framework of the Customs Union, the Agreement on the Representation and Exchange of Preliminary Information about Goods and Vehicles Crossing the Customs Border of the Customs Union has been signed.

Existing country's infrastructure allows such information to be shared electronically with third countries where an international agreement so provides (now only within the Customs Union, and not in the form of interaction "system to a system" but in form of individual data exchange)

Submission of preliminary information is carried out electronically by means of interaction of the information system of the customs authorities of the Member States of the Customs Union and information systems of concerned parties or via web-portals of the Member States of the Customs Union.

3.5 - National Single Window System

The country has a unified system for filing e-declarations, but it is available only to the customs services; economic entities submit documents into the system electronically via the automated workstations (AWS) of a number of complementary software products developed by different developers.

For the time being, there is no system, which is able to provide all the necessary information and documents in electronic format (application for certificates, customs declarations, required documents, permits, etc.).

At present, each country of the Union is developing its own national single window system. In Belarus, such system is represented by the Nationwide automated information system NAIS, which is operated by the National Electronic Services Centre. As for now, the NAIS does not render services in the sphere of customs issues.

There are plans to create the Single Window system (the decision of the Eurasian Commission on general principles for establishment of the Single Window system within the Customs Union). A unified electronic documents flow system with a single data submission is planned to be introduced into the customs sphere of the EEU before 2021[48].

So far, it is impossible to submit a customs declaration to another country.

3.6 - Anti-Counterfeiting and Anti-Piracy System

It is possible to submit a request via email asking the intervention of Customs in order to take measures against goods infringing certain intellectual property rights. but there is no website where this could be done.

As a preventive measure, the customs authorities may render fee-based services upon the importer's / exporter's request to monitor compliance with their intellectual property rights when goods are crossing the borders. The customs body enters the request into a specific register and monitors it. If any economic entity tries to import counterfeit goods, the Customs will reveal this fact and prevent importation. However, this register is not shared with the EU.

Each national body has a register of intellectual property items, which is maintained on a central basis (in Belarus it is represented by the National Centre of Intellectual Property). To protect their intellectual property rights post factum, the exporter or importer must lodge an application and notify

[48] According to the statement by Vladimir Goshin, member of the Board (Minister) for Customs Cooperation of the Eurasian Economic Commission

of infringement on their rights (the Law of the Republic of Belarus dated 18 July 2011 “On Application of Citizens and Legal Bodies” allows for lodging an e-application with indication of all identification details).

There is no national unified anti-fraud information system.

In 2005, the Committee for Standardization of the Republic of Belarus (Gosstandart) established a system of measures to combat penetration of counterfeit goods into the domestic market of the country. In particular, an automated system for gathering information on such goods was created, and its characteristics and identification features for expert examination were defined. Control over authenticity of goods was organized on the trade markets of the republic. This system is not available for general public.

For a long time, Belarus has successfully applied the system for labelling of goods with control identification marks. In the near future, there will be transition to a new quality of this system, i.e. to labelling of goods with control (identification) marks containing RFID tags, and entry of data on produced and imported goods into the interdepartmental distributed information system known as “Data Bank of Electronic Goods Certificates”.

Interaction with the system of electronic certificates of goods via barcodes is also not included into current plans.

For now, the Single Customs Register of Intellectual Property Units of the Member States of the Customs Union does not contain any registered intellectual property units. The register is developed in accordance with the Agreement on the Single Customs Register of Intellectual Property Units of the Member States of the Customs Union.

Georgia

National background information

Georgia has developed and implemented an entire public finance management information structure, which is shared between different government entities.

The Public Finance Management System (PFMS) consists of a number of subsystems, each of it with a specific purpose. Sub-systems include:

- e-Budget – for budget planning and reporting to the Ministry of Finance;
- e-Treasury – for recording and managing public spending;
- e-DMS – electronic Debt Management System for international debt management and internal loan management;
- e-HRMS – electronic Human Resource Management System;
- RS.GE – Revenue Service;
- e-Procurement – a central unified platform for tendering and procuring goods, services and works for procuring entities as set by the Public Procurement Law (PPL) (including central and local government bodies);
- e-Auction.ge – a central platform where government bodies sell goods to private and civic sector actors.

Relevant legislation

eCustoms relevant national legislation is Tax Code of Georgia, Law on Revenue Service of Georgia

and Statute of Revenue Service, as well as, Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and Georgia, of the other part.

Best practices and Standards

Risk Management:

The management of customs operational risks is automated. Both the eCustoms (ASYCUDA World) and “Oracle” systems support the automation of risk management procedures. All tariff risks (import and export operations) are fully supported by the eCustoms system, while the “Oracle” system provides support for management of non-tariff risks related primarily to border-crossing and transit operations. The risk management issues are regulated by the Customs Risk Management Division of the Department for Administration of the Revenue Service.

Both systems are capable of managing the relevant risk profiles. Risk profiles are built on a wide spectrum of data stored in and collected from different sources (eCustoms, “Oracle” system, as well as external information systems and databases). The prevailing portion of data (operational inputs), is collected, exchanged and processed in real time. Some of the information, primarily information concerning the management of risk profiles (risk group lists, analysis of suspicious transit routes, enforcement cases etc.), is collected, traced, and analyzed manually.

In addition to managing risk profiles, customs maintain a database of qualified traders (a so-called “Golden List”). Companies included in the list are granted allowed to process consignments through simplified procedures. The “Golden List” (alternative programme for the Authorized Economic Operators programme) is a part of the eCustoms system and is mainly used for processing import operations.

Tariff Risks:

Import and export operation risk management are organized through a built-in eCustoms module. The data accumulated in different customs declarations, including advance import declaration (if available), serves as a basis for processing risk assessments.

Based on the Order No. 290 of the Minister of Finance of Georgia, the Revenue Service carries out customs control on goods through the application of the ASYCUDA system (upgraded eCustoms), which is based on a risk management system. In particular, during customs control, declarations are routed through different channels based on selectivity criteria and random selection:

Green Channel: goods go without examination and are immediately released;

Blue Channel: goods are examined a later stage after already being released;

Yellow Channel: a documentation check is performed but the goods themselves are not physically examined;

Red Channel: goods are physically examined and go through a documentation check.

The eCustoms risk management module allows for the maintenance of different special risk profiles, which are created based on trader information of those who have been previously suspected of violating or have already violated customs legislation pertaining to specific goods, routes, etc.

A selective examination approach is used for all traders (all declarations) regardless of their status. Selective examination algorithms, which are directly connected to risk profiles, are incorporated in the eCustoms risk management module. This selective approach lessens the possibility of arbitrary and unjustified discrimination against specific traders. In particular, the criteria for risk analysis are

determined inter alia HS codes, the nature and description of the goods, the country of origin, the country from which the goods were shipped, the value of the goods, the compliance record of traders and the type of means of transport.

The eCustoms risk management module is flexible enough to create corresponding risk profiles. All cases of physical examinations, as well as corresponding results, are stored in the eCustoms database.

Non-Tariff and Transit Risks:

The management of non-tariff and transit risks is organized through an in-house developed module, which operates as a part of the "Oracle" system. In addition to internal information (risk profiles, historical data), the risk management module consumes information obtained from the "PIRS" system, which is operated by the Patrol Police, as well as data processed in the eCustoms system. Information registered in the Internal Transit Document (T1 Form) serves as a basis for processing risk profiles. Risks connected to TIR operations are not incorporated in the risk management module and verification of TIR Carnets is handled through information provided by the CUTEWISE interface.

Risks related to persons and means of transport crossing the borders are processed in the PIRS system. Once the personal/means of transport information is registered, the system processes information and notifies the customs system ("Oracle" system) about the results of the assessment. Once the border crossing status is confirmed by the PIRS system, the in-route transit document can be registered in the system (eCustoms). Registration of the document triggers the risk assessment procedure, which is fully automated in the "Oracle" module. Selective examination algorithms are incorporated in the "Oracle" risk management module. These algorithms are directly connected to the risk profiles. Using the algorithms and profiles, the module automatically selects objects for physical examination.

This procedure is applicable for all consignments entering Georgian territory (transit, import, temporal storage).

Exchange of Electronic Data between Georgia and Republic of Turkey

As mentioned above, the exchange of electronic data with Turkey has been initiated under the Agreement between the Government of Georgia and the Government of Republic of Turkey on the Joint Use of Land Crossing Points of "Sarpi - Sarp", "Kartsakhi – Cildir/Aktas" and "Akhaltsikhe – Posof/Turkgozu" in 2010. The agreement is based on the Agreement between the Government of Georgia and the Government of Republic of Turkey on Cooperation and Mutual Assistance in the Field of Customs Affairs, signed on January 13, 1994 and Memorandum of Understanding between the Government of Georgia and the Government of Republic of Turkey on the Joint Use of the Customs Crossing Points, signed on June 11, 2010.

The Agreement is accompanied by the Protocol on Details for Electronic Data Exchange Regarding the International Passengers, Vehicles and Goods, and the technical provisional document "Data Exchange System", which defines the technical specifications for data exchange procedures. The exchange of electronic information was launched in test mode in 2013 and has been put in a production mode since April 2014. 2014.

Data is exchanged through a secure VPN channel. A digital signature generated via the cryptosystem utilizing private and public key pairs is utilized according to technical protocols. However, the use of digital signatures for authentication purposes is currently (temporarily) being substituted with built-in VPN authentication mechanisms.

Communication is carried out in real time. Data is submitted via SOAP Web Services. The “push” (“Accept Message”) method is used to submit information, and the “Acceptance of Message” confirms receipt of the message.

The data set includes consignor/exporter information, references to the original document (e.g. the export declaration) as assigned by the sender’s system, consignee information, country of dispatch/export (which is mandatory for TIR operations), country of destination, identity and nationality of transporter, means of transport, mode of transport on the border, a description of the good(s) that includes up to six-digit HS codes and two-digit HS codes for transit, the number and kind of packages, other marks and numbers, gross mass, TIR Carnet number, and seal number (if applicable). Additionally, detailed information about the driver and the means of transport are included in the message.

XML 1.0 schema is used as a standard and information is encoded in UTF-8. No other standards (e.g. the WCO data model) are used for structuring XML messages. The structure of the message is fully customized for the purposes of the project.

Agreed classifiers are used for customs offices, countries and territories, codes of goods, measurement units, and means of transport, currencies and customs regimes. A transliteration method is used for the exchange of non-coded information, which is provided in different national languages.

On the Georgian side, information exchange is supported by the “Oracle” system, which communicates with the eCustoms system through exporting and importing flat files. The mechanism for publishing and consuming of services is expected to be reviewed and updated based on the capabilities of the new version of the eCustoms system.

Exchange of Electronic Data between Georgia and Republic of Ukraine

As mentioned above, the channel for exchanging electronic data between the customs authorities of Georgia and Ukraine has been established and is stable. Data is exchanged under the Protocol between the Revenue Service of the Ministry of Finance on Georgia and the State Customs Service of Ukraine (SCSU) on Organizing the Exchange of Preliminary Information on Goods and Vehicles Transiting across the State Borders of Georgia and Ukraine. The agreement was signed under the umbrella of the GUAM Trade and Transport Facilitation Project.

The agreement is accompanied by the Technical Specifications for Organizing the Exchange of Preliminary Information on Goods and Vehicles Transiting across the State Borders of GUAM member states document, which fully defines the technical details of data exchange.

The transport subsystem is built on the IBM WebSphere MQ Series for Windows v 6.0. A secure VPN connection is used to support communication between the systems.

Like with Turkey, the “push” method (sending the “Information” message) is used. Receipt of information must be confirmed via a confirmation message, assuming that either a positive (Information has been received) or negative (“Information” has not been received) notification returns.

The message assumes that the exchange of detailed sets of information is compatible with the WCO data set. The data set covers information, usually available in customs declarations of goods, including restricted commercial information (the factual value of the contract). The completeness of information depends on the nature of the sources document. Agreed classifiers are used for customs offices, countries and territories, codes of goods, measurement units, and means of transport, currencies and customs regimes.

No particular XML standard (e.g. the WCO data model) is used for structuring XML messages. The structure of the message is customized according to the needs/purpose of a project.

Like with Turkey, Georgia uses the “Oracle” system for information exchange. The “Oracle” system communicates with eCustoms through exporting and importing flat files.

Unlike information exchange with Turkey, information exchanged with Ukraine is not used for operational purposes. Instead, it is mainly used to compare original information as well as for risk management purposes. Therefore, there are no plans to move the orchestration of data exchange to the eCustoms system. Additionally, only a restricted portion of the functionalities defined in the technical specifications document has been implemented. Plans to improve existing practices are being considered.

The “XML-Signature Syntax and Processing. W3C Recommendations”[49] syntax is being used as a prototype for the authentication system. Enveloping authentication tags are utilized. The technical specification does not suppose the existence and use of detached signatures.

ICT platforms

eCustoms

Customs has been operating ASYCUDA World since 2007. Initially launched in pilot mode, ASYCUDA World fully replaced ASYCUDA++ in 2010. Currently, customs is in the process of upgrading of the system to the most recent release. The new system, named eCustoms is currently in operational mode.

eCustoms is a scalable and fully internet client-server n-tier, 100% web-based system with built-in security features. The Oracle®11g is utilized as a RDBMS (relational database management system). eCustoms is an open system with flexible data exchange capabilities. The system fully supports the exchange of both EDIFACT and XML messages. Database access (processing data) is organized through built-in Java classes. The data model and data sets of eCustoms are fully compatible with the WCO data model and data sets.

eCustoms provides a web-based user interface for both internal staff and external users (authorized economic operators). User authentication utilizes user groups, user names and passwords. Asymmetrical encryption (several levels and types of encryption algorithms are available) and built-in security features (PKI), electronic signatures, etc. are available to ensure a high level of security.

“Oracle” System

The “Oracle” system is a fully in-house developed web-based system, built on the Oracle®10g platform. The system, serving needs of both customs and tax authorities, represents a set of different modules communicating with each other through direct access to a single consolidated database.

The “Oracle” system has two-tier client-server architecture. The business logic of the system is realized on the level of database procedures. The client end of the system is built on the Oracle® Form 10g component. The Oracle® Database 10g built-in authentication mechanisms are utilized for authorization of both internal and external users of the system.

The “Oracle” system is fully open and is flexible enough to support the exchange of electronic

information. The system provides the backend execution of all currently available data exchange services, utilization of external data sources, as well as provision of electronic services, dedicated for both business customers and external authorities. Additionally, the “Oracle” system provides a restricted web-based user interface for authorized external users (authorized economic operators).

Organisations involved

Revenue Service, a legal entity of public law of the Ministry of Finance of Georgia, executes state control on the whole territory of Georgia with areas of responsibility (relevant to area) is responsible for tax administration, as well as, Customs administration. Three departments at the Revenue Service key to implementation of eCustoms systems with respective responsibility areas: Customs Department, information technology Centre and Department of International Relations.

International agreements

Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and Georgia, of the other part, Title IV Trade and Trade related matters and annex XIII;

Agreement between the Government of Georgia and the Government of Republic of Turkey on Cooperation and Mutual Assistance in the Field of Customs Affairs, signed on January 13, 1994 and Memorandum of Understanding between the Government of Georgia and the Government of Republic of Turkey on the Joint Use of the Customs Crossing Points, signed on June 11, 2010.

Protocol between the Revenue Service of the Ministry of Finance on Georgia and the State Customs Service of Ukraine (SCSU) on Organizing the Exchange of Preliminary Information on Goods and Vehicles Transiting across the State Borders of Georgia and Ukraine.

State of play

Indicator 1: Legal framework

1.1 – Common Risk Management Framework

National Risk Management System has been established and is automated since 2007. The risk management issues are regulated by the Customs Risk Management Division of the Department for Administration of the Revenue Service. Risk management criteria are created base on common risk assessment criteria elaborated by the respective division.

The formal study or comparison of risk criteria established in Georgia with the Common Risk Management Framework establish in EU has not been performed. There was no need at this stage of association and cooperation. In case such requirement is in place the comparison will be implemented in due time.

Customs controls, other than spot-checks are based on the risk analysis using data processing techniques. Elaborate risk management systems are implemented.

The management of customs operational risks is automated. Both the eCustoms (ASYCUDA World) and “Oracle” systems support the automation of risk management procedures. All tariff risks (import and export operations) are fully supported by the eCustoms system, while the “Oracle” system provides support for management of non-tariff risks related primarily to border-crossing and transit operations. The risk management issues are regulated by the Customs Risk Management Division of the Department for Administration of the Revenue Service.

Both systems are capable of managing the relevant risk profiles. Risk profiles are built on a wide

spectrum of data stored in and collected from different sources (eCustoms, “Oracle” system, as well as external information systems and databases). The prevailing portion of data (operational inputs), is collected, exchanged and processed in real time. Some of the information, primarily information concerning the management of risk profiles (risk group lists, analysis of suspicious transit routes, enforcement cases etc.), is collected, traced, and analyzed manually.

In addition to managing risk profiles, customs maintain a database of qualified traders (a so-called “Golden List”). Companies included in the list are granted allowed to process consignments through simplified procedures. The “Golden List” (alternative programme for the Authorized Economic Operators programme) is a part of the eCustoms system and is mainly used for processing import operations.

1.2 - Authorised Economic Operator status

Pursuant to the Tax Code of Georgia, any person (legal/natural) can register as the taxpayer and carry out the customs operation (import, export, transit, customs warehouse etc.). The Revenue Service has one single database for all taxpayers.

AEO status implementation is part of the strategy, as part of the Association Agreement between the European Union and Georgia’s implementation plan (annex XXIII) it is envisaged within 4 years from the signature of this agreement.

1.3 - Paperless environment for customs and trade

Implementation of Paperless environment has already launched. The automation of customs operations in Georgia is organized through two independent and fragmentally integrated information systems: eCustoms (built on ASYCUDA World) and “Oracle”. While the eCustoms system is dedicated entirely to support customs operations, the “Oracle” system represents a unified integrated platform that processes all revenue collection-related data and operations. Both the eCustoms and “Oracle” systems are web-based applications, providing interfaces for external users using secure communication channels. The systems are integrated through direct links between databases.

Further steps are planned though Trade Facilitation System Project, launched in 2012 (the pilot will be launched summer 2015). Trade Facilitation System (TFS) is the system aiming at harmonization of the electronic flow of information among key participants in the logistics, shipping, and transport industries, both public and private.

Data exchange is provided between different agencies within country. In addition, Currently, Georgian customs exchanges electronic information with the customs authorities of two countries: the Republic of Turkey and Ukraine. In both cases, the exchange of electronic information is determined by bilateral agreements between the countries and all legal and technical issues of electronic information exchange are regulated by technical amendments to the agreements.

The Agreement between the Government of Georgia and the Government of Republic of Turkey on the Joint Use of Land Crossing Points of “Sarpi - Sarp”, “Kartsakhi – Cildir/Aktas” and “Akhaltsikhe – Posof/Turkgozu” in 2010. The agreement is based on the Agreement between the Government of Georgia and the Government of Republic of Turkey on Cooperation and Mutual Assistance in the Field of Customs Affairs, signed on January 13, 1994 and Memorandum of Understanding between the Government of Georgia and the Government of Republic of Turkey on the Joint Use of the Customs Crossing Points, signed on June 11, 2010.

Within framework of GUAM Trade and Transport Facilitation Project the agreement - Protocol between the Revenue Service of the Ministry of Finance on Georgia and the State Customs Service

of Ukraine (SCSU) on Organizing the Exchange of Preliminary Information on Goods and Vehicles Transiting across the State Borders of Georgia and Ukraine was signed.

Indicator 2: Infrastructure

2.1 - Electronic interfaces to conduct all customs-related business

Single access point with other countries has not been implemented. As said above data exchange agreements had been signed and are operational with Turkey and Ukraine.

In case, respective strategy is adopted and/or international agreements signed, single access point with other countries will be implemented.

2.2 – Interoperating systems for import, export and transit

Georgia systems for import and export interoperate with the system for transit and enable the seamless flow of data, but it is not integrated with EU Systems, such as AIS, AES or NCTS.

No relevant obligations are place in current Association Agreement, apart general Common Transit and SAD Convention of 20 May 1987 on the Simplification of Formalities in Trade in Goods Convention of 20 May 1987 on a common transit procedure.

The approximation with the provisions of the above mentioned Conventions, including through a possible accession to these Conventions by Georgia, shall be carried out within four years following the entry into force of the Association Agreement (30.08.2014).

2.3 - Integrated tariff information system

National Goods Nomenclature for External-Economic Activities has been adopted in 2002, the last update has been adopted on July 11, 2012.

Nomenclature is publicly available and is used for estimation of tariffs for goods for import and export purposes. Nomenclature is based on International Convention on the Harmonized Commodity Description and Coding System (with annex), as amended by the Protocol of Amendment of 24 June 1986. Concluded at Brussels on 14 June 1983.

Nomenclature is integrated for active and real time re-uses by National Declaration Processing Systems., but is not integrated with national surveillance systems

2.4 - Single Point for Entry or Exit of Data (SPEED) portal

Integration or connection is not part of the Association Agreement agenda. Georgia’s automated eCustoms system is not connected to SPEED portal.

2.5 - Uniform user management & digital signatures

Georgia has introduced eSignatures with Law on electronic Signatures and electronic documents in 2008. Electronic signatures are not used in customs operations and therefore are not exchanged with other countries, including EU.

Indicator 3: Services

3.1 - Registered Exporters System

According to the Tax Code of Georgia, any person (legal/natural) can register as the taxpayer and carry out the customs operation (import, export, transit, customs warehouse etc.). The Revenue Service has one single database for all taxpayers.

Georgia has not established and harmonised Registered Exporter System for preferential trade

arrangements with EU countries.

3.2 - Economic Operators Registration and Identification system

Economic Operators Registration and Identification (EORI) numbers are not operational in country

3.3 - Exchange of data about Authorised Economic Operators

According to Tax Code of Georgia, any person (legal/natural) can register as the taxpayer and carry out the customs operation (import, export, transit, customs warehouse etc.). The Revenue Service has one single database for all taxpayers.

The database, as well as, information contained is not harmonised with EU universal AEO system.

3.4 - Summary electronic declaration

Summary electronic declarations are used in Georgia, while relevant authorities (Revenue service) undertake information exchange with the republic of Turkey as per agreement of joint use of Land Crossing Points. Information is filed and provided in electronically and is equal to Entry Summary Declaration.

3.5 - National Single Window System

Single window for submission of all required information is provided within country. Single window is managed by Revenue Service, Ministry of Finance of Georgia. No other harmonisation requirements are applicable at this point.

3.6 - Anti-Counterfeiting and Anti-Piracy System

Under the framework of the Association Agreement, Regulation (EU) No 608/2013 of the European Parliament and of the Council of 12 June 2013 concerning customs enforcement of intellectual property rights and repealing Council Regulation (EC) No 1383/2003 shall be implemented. The approximation with the provisions of the above mentioned Regulation, with the exception of Article 26, shall be carried out within three years following the entry into force of this Agreement. The obligation on approximation to Regulation No 608/2013 in itself does not create any obligation on Georgia to apply measures where a right in intellectual property is not protected under its substantive IP laws and regulations.

Therefore, national information system on IPR has not yet been created and no information exchange has been undertaken with internationally or with EU centralised Anti-Counterfeiting and Anti-Piracy System. IPR oriented National Anti-Fraud system has not been implemented.

Detailed action plan will be elaborated in line with obligations described above, within joint inter agency action plan for implementation of the Association Agreement

Gap analysis

Indicator 1: Legal framework

1.1 – Common Risk Management Framework

A clearly defined national risk management framework in customs controls for goods brought into or out of the country is harmonised with the EU common criteria and priority control areas. Risk Information Forms are currently not exchanged electronically with customs offices of the EU countries.

The formal study or comparison of risk criteria established in Georgia with the Common Risk Management Framework establish in EU has not been performed. There was no need at this stage of association and cooperation.

1.2 - Authorised Economic Operator status

The customs authorities of the country does not currently apply common criteria and harmonised requirements for granting the status of authorised economic operators, allow the use of simplifications by authorised economic operators. Recognition of the status of AEOs registered in the EU member states or other countries has not been yet implemented.

1.3 - Paperless environment for customs and trade

Indicator 2: Infrastructure

2.1 - Electronic interfaces to conduct all customs-related business

Information systems of the country does not have a service of single access point enabling economic operators to use one single interface to lodge electronic customs declarations to the customs systems of other countries. However, data exchange agreements had been signed and are operational with Turkey and Ukraine.

2.2 – Interoperating systems for import, export and transit

The country systems for import and export interoperate with the system for transit and enable the seamless flow of data. The service does not currently ensure transfer of data between the national customs systems to/from customs system of the EU member states.

2.3 - Integrated tariff information system

The country has implemented a national centralised binding tariff information system that allows getting tariff classification for goods. The system is integrated for active and real time re-use by National Declaration Processing Systems, but is not interconnected with other tariff related IT systems to facilitate re-use of data and functionality of one system to another.

2.4 - Single Point for Entry or Exit of Data (SPEED) portal

Georgia's computerised transit system and other such as export, import systems are not connected to SPEED portal and do not allow data exchange for electronic customs systems between the country and the EU. However, the current level of development of automated eCustoms information system already allows data exchange with two countries.

2.5 - Uniform user management & digital signatures

A common solution for electronic signatures (or a system based on mutual recognition of existing solutions) is not operational in the country. As electronic signature is not used in eCustoms system, national economic operators are not using this mechanism for sending information to the customs administration.

Indicator 3: Services

3.1 - Registered Exporters System

The Revenue Service has established a unified database of taxpayers combined with exporters' registration data. The database (equivalent of registered exporters system) should allow an automated verification of the exporters' registration number from the declarations in the national eCustoms declaration system. Georgia currently does not cooperate with the EU on registration of national exporters into the EU REX central database managed by the European Commission.

3.2 - Economic Operators Registration and Identification system

Georgia has not implemented a system for registration and identification of economic operators based

on an equivalent of EORI number that serves as a reference in relations of economic operators with customs authorities throughout the country and for the exchange of information between the customs authorities and other authorities. There are no interconnections with the EORI central database managed by the European Commission.

3.3 - Exchange of data about Authorised Economic Operators

Georgia has a registration and identification information system of economic operators. It has not concluded any agreement of mutual recognition of the country's register of economic operators and the Authorised Economic Operators in the EU. System-to-system interface allowing the economic operators' data received from the country to be disseminated to the EU member states and the validation of the county' AEO status in the EU transaction systems has not been implemented.

3.4 - Summary electronic declaration

Through established information exchange with the republic of Turkey, an electronic summary declaration containing the required pre-arrival or pre-departure information could be lodged before any goods are brought into or out of the territory of the country. All information is provided to the customs and other authorities in electronic format. Existing country's infrastructure allows such information to be shared electronically with third countries where an international agreement so provides.

3.5 - National Single Window System

The national single window and one-stop shop is in place and allows submission of all required information and documents in electronic format (application for certificates, customs declaration, required documents, and permits).

It has not been confirmed that the administrations or agencies deliver certificates (permits) required for import or export authorisation in electronic format.

3.6 - Anti-Counterfeiting and Anti-Piracy System

In Georgia there is no electronic service in place that provide traders with the possibility to submit a claim asking the intervention of Customs in order to take measures against goods infringing certain intellectual property rights. The national Anti-Fraud Information System has not been yet created.

Moldova

Relevant legislation

- Government Decision no.404 of 2.6.2014 on piloting the Interoperability Platform.[50] It establishes the owner of the Platform and responsibilities of the key actors involved in this process.
- Government adopted the Decision no.122 of 18.02.2014 on the public services reform program for 2014-2016.[51]
- The creation and administration of the Public Services portal is regulated by the Government Decision no.330 of 28.15.2012 on creation and administration of the unique public services

[50] http://lex.justice.md/viewdoc.php?action=view&view=doc&id=353238&lang=2

[51] http://lex.justice.md/viewdoc.php?action=view&view=doc&id=351705&lang=2

portal.[52]

- The Government adopted the Decision no.329 of 28.15.2012 on electronic governmental service on electronic payment.[53]
- Government adopted the Decision no.280 of 24.4.2013 on certain actions for implementation of Governmental Service of e-Payment (M-Pay)[54]
- Government has approved the Decision.1090 of 31.12.2013 on governmental service on authentication and access control (M-Pass).[55]
- Government has implemented the Governmental Technological Platform (M-Cloud). It adopted the Decision no.128 of 20.2.2014[56]
- Government Decision no.405 of 2.6.14 adopted the governmental e-service of digital signature (M-Sign)[57]
- Government Adopted the Decision no.708 of 28.8.2014 Governmental e-service M-Log[58]
- Government Decision no.709 of 20.09.2011 could also be consulted as it establishes a number of projects to be implemented and actors responsible for their implementation.[59]
- Decision of the Government is no.717 of 29.8.2014 on governmental platform of registers and permissive acts[60]

National plans

The Government Decision nr.710 of 20th September 2011 the Strategic Program for Governance Technological Modernisation (E-Transformation)61

General objective: By 2020, the government will become more transparent, and responsive, and perform better due to intelligent investments in IT and their massive use in the public sector.

Specific objectives:

- Modernization of public services through digitization and business process reengineering. Citizens and businesses can easily access through a single government portal information and electronic services provided by the Central Public Authorities. These services will be accessible through various channels: Internet, mobile, kiosks, interactive terminals and others.
- Optimization of government operations through interoperability, IT asset consolidation, and data reuse. Citizens will benefit from a connected and efficient government. Public institutions will overcome departmental silos and will operate and interact through a shared technology

[52] http://lex.justice.md/viewdoc.php?action=view&view=doc&id=343406&lang=2

[53] http://lex.justice.md/viewdoc.php?action=view&view=doc&id=343404&lang=2

[54] http://lex.justice.md/viewdoc.php?action=view&view=doc&id=347873&lang=2

[55] http://lex.justice.md/viewdoc.php?action=view&view=doc&id=351035&lang=2

[56] http://lex.justice.md/viewdoc.php?action=view&view=doc&id=351760&lang=2

[57] http://lex.justice.md/viewdoc.php?action=view&view=doc&id=353239&lang=2

[58] http://lex.justice.md/viewdoc.php?action=view&view=doc&id=354589&lang=2

[59] http://lex.justice.md/viewdoc.php?action=view&view=doc&id=340300&lang=2

[60] http://lex.justice.md/viewdoc.php?action=view&view=doc&id=354598&lang=2

[61]http://egov.md/images/normative/Strategic_Program_for_Governance%20_Technological_Modernization_ENG.pdf

platform in order to offer high quality services. Citizens will be able to offer personal data to government only once, and public institutions will be able to reuse this data for the delivery of services."

In the past 3 years, the Government approved annual Action Plans to implement the above-mentioned Decision (I will double check with them if the 2015 was approved because the legal search engine does not find it. I admit that it was not because Moldova has received the credit for 4 years. If necessary, I will get official information about extension).

Government Decision no.656 of 05.09.2012 on approving the Interoperability Framework Program[62]

Overall objective: Implement the Interoperability Framework with the aim to increase the Government performance due to an efficient data exchange within the public sector, as well as between the public and private sector.

Specific objectives are as follows:

- Insuring IT systems interoperability in the public sector through implementation and efficient operation of a common interoperability platform;
- Insuring efficient and secure data exchange and reuse by connecting the state-owned information resources and services to the common interoperability platform; III. insuring a favourable framework for public services optimization through reusing information resources and services;
- Insuring a favourable framework for an open government through automatic mechanisms for collection and publishing of open government data."

Please also consider the sub-chapter 4.8 Interoperability Framework Implementation

International agreements

Association Agreement[63] between Moldova-EU – in particular, chapters of Title V.

Government Decision no.808 of 7.10.2014 to adopt the Plan of Actions to implement the Association Agreement Moldova-EU for 2014-2016 – there are a few relevant actions, including p.84 what concerns implementation of the title V chapter 5 (*customs administration and facilitation of commerce*)[64] etc.

Government Activity Program[65] - relevant paragraphs are: chapter IV A p.16; IV D; IV B; IV M; VII C

State of play

Indicator 1: Legal framework

1.1 – Common Risk Management Framework

The Moldovan legal framework in this area is in accordance with the EU legal framework. More than

[62] http://egov.md/images/normative/Moldova_Interoperability_Framework_Program.pdf

[63] Law on ratification of the Association Agreement http://lex.justice.md/viewdoc.php?action=view&view=doc&id=353829&lang=2 the English version of the Agreement is here: http://eeas.europa.eu/moldova/pdf/eu-md_aa-dcfta_en.pdf

[64] http://lex.justice.md/viewdoc.php?action=view&view=doc&id=354939&lang=2

[65] http://gov.md/ru/advanced-page-type/programul-de-activitate-guvernului

53.3% of exports of the RM are oriented towards the EU market.

Moldovan Customs risk management system is based on the automated selectivity system in ASYCUDA World. The Customs Service is willing to exchange customs data with the EU for the scope of the risk management. Currently, Moldova is negotiating with the EU Commission the implementation of the pilot project on the pre-arrival of exchange of customs data. The pilot project is planned to be launched in 2015 at the boarding crossing point with Romania Leuşeni Albiţa.

The Customs Service has consulted the EU Legal Framework, in particular, the Community Risk Management Framework laid down in the Regulation (EC) 648/2005 while developing its national Risk Management System. In this process, Moldova benefits from expertise offered by EU experts, including EUBAM, EUHLPAM, and BRITE USAID.

Government Decision no.1144 of 03.11.2005 on approving the concept of risk management in the Customs Service. Describes the functionality of the risk management system on the national level. Principle of selective customs control based on risk management provided in Article 192 of the Customs Code.

1.2 - Authorised Economic Operator status

Customs Code, section 27 indice 1 and 28 indice 1, Government Decision no.647 of 7.8.2014 to apply the provisions of the Customs Code, section 27 index 1 and 28 index1.The relevant EU legal framework is transposed to these legal provisions, including requirements for granting the statement of AEO and simplified declarations.

Until today, the Moldovan Customs Service has issued 59 certificates for AEO. The AEO Register is published on the web portal of the Customs Service (customs.gov.md).

1.3 - Paperless environment for customs and trade

As from March 2013, Moldovan customs implement electronic export declaration and the share of eExport submissions growth till 42% in January 2015. As from September 2014, electronic import declaration has been implemented too.

At present a number of projects are being implemented which will permit electronic exchange of information within the public sector. The Customs Service participates in this process.

The Government has adopted the Government Decision no.656/2012 on Interoperability framework[66] and is currently implementing the technical layer of interoperability (pilot project) in accordance with Government Decision no.404 of 2.06.2014.

Government Decision no. 561 of 18.05.2007 on integrated customs information system. Government Decision no.904 of 13.11.2013 on electronic customs clearance of goods. Customs Service Order no.346 of 24.12.2009 for technical norms on completing and use of customs declaration.

Indicator 2: Infrastructure

2.1 - Electronic interfaces to conduct all customs-related business

There is no single access point enabling economic operators to use one single interface to lodge electronic customs declarations to the customs systems of other countries.

2.2 – Interoperating systems for import, export and transit

[66] http://egov.md/images/normative/Moldova_Interoperability_Framework_Program.pdf

Not currently in place. However, a Twinning Project Fiche for Moldovan Customs for implementing NCTS has been drafted by the EU Commission and it is expected to be launched in 2015.

2.3 - Integrated tariff information system

Currently this procedure is paper based and it is not supported by an IT tool. No initiative for development of such a system has been initiated. Article 141 index 3 and 4 of the Customs Code, Order of the Customs Service no.80 of 28.02.2012 on implementing banding tariff information.

2.4 - Single Point for Entry or Exit of Data (SPEED) portal

Currently, Moldova is negotiating with the EU Commission the implementation of the pilot project on the pre-arrival of exchange of customs data. The pilot project is planned to be launched in 2015 at the boarding crossing point with Romania Leuşeni Albiţa. Draft terms of reference for the pilot project have been elaborated by the EU Commission.

2.5 - Uniform user management & digital signatures

e-signature used for customs operations is one issued for other operations too and can be accepted by other institutions. Financial mean are lacking to ensure the necessary developments in the customs information system by the UNCTAD developer of ASYCUDA World. The implementation is based on the developed legal framework: Law no 91 of 27.06.2014 on e-signature and electronic document, Government Decision no.904 of 13.11.2013 on procedure on eDeclaration of goods.

Indicator 3: Services

3.1 - Registered Exporters System

A draft concept on paper on automatic procedure has been prepared. There is no such system in place. No cooperation with the EU on this subject has been initiated.

3.2 - Economic Operators Registration and Identification system

There is a centralised system for registration of the economic operator in Asycuda World. There is no special registration and identification numbering for customs unique registration in place.

3.3 - Exchange of data about Authorised Economic Operators

There is no exchange of electronic data. Draft terms of reference for a pilot project on unilateral recognitions of the EU AEO at Leuşeni Albiţa Moldova-Romanian border crossing point have been prepared.

3.4 - Summary electronic declaration

The Moldovan Customs Service implements the pre-arrival exchange of data with Ukrainian customs in electronic format from 2008 with the support of the EUBAM. The exchange is done in separate System. This system has an interaction with Asycuda but is not integrated in it.

3.5 - National Single Window System

No national single window is in place. A Twinning Fiche has been drafted by the European Commission experts for supporting the Moldovan Customs in developing the single window approach.

3.6 - Anti-Counterfeiting and Anti-Piracy System

No service or system is in place.

Gap analysis

Indicator 1: Legal framework

1.1 – Common Risk Management Framework

Moldova has implemented a national risk management framework in customs controls for goods brought into or out of the country that is harmonised with the EU common criteria and priority control areas. Risk Information Forms cannot be currently exchanged electronically with customs offices of the EU countries.

1.2 - Authorised Economic Operator status

The customs authorities of Moldova apply common criteria and harmonised requirements for granting the status of authorised economic operators, allow the use of simplifications by authorised economic operators and recognise the status of AEOs registered in the EU member states or other countries. National system of identification and registration for economic operators does not interoperate with the Authorised Economic Operators EU system

1.3 - Paperless environment for customs and trade

National legal provisions are defined for secure, integrated, interoperable and accessible electronic customs systems for the exchange of data contained in customs declarations, documents accompanying customs declarations, certificates and the exchange of other relevant information. Appropriate system applications are in the process of implementation.

Indicator 2: Infrastructure

2.1 - Electronic interfaces to conduct all customs-related business

Information systems (customs declarations) of Moldova do not have a service of single access point enabling economic operators to use one single interface to lodge electronic customs declarations to the customs systems of other countries (the EU member state or others).

2.2 – Interoperating systems for import, export and transit

The country systems for import and export do not interoperate with the system for transit and do not enable the seamless flow of data. There is no service that ensures transfer of data between the national customs systems to/from customs system of the EU member states.

2.3 - Integrated tariff information system

The country has not yet started implementation of a national centralised binding tariff information system that allows getting tariff classification for goods.

2.4 - Single Point for Entry or Exit of Data (SPEED) portal

The country’s computerised transit system (or other such as export, import or economic operators systems) is not connected to SPEED portal and there is no data exchange for electronic customs systems between the country and the EU

2.5 - Uniform user management & digital signatures

A common solution for electronic signatures is operational in the country and enables the national economic operators to send information to other administrations than customs, and to enable these administrations to verify the authenticity of the author, of the sender and of the information. No mutual recognition frameworks of e-signatures with other countries have been implemented.

Indicator 3: Services

3.1 - Registered Exporters System

Moldova has not established a Registered Exporters System (or similar) that allows an automated verification of the exporters' registration number from the declarations in the national Customs declaration system. The country currently does not cooperate with the EU in order to register national exporters into the EU REX central database managed by the European Commission.

3.2 - Economic Operators Registration and Identification system

An electronic system for storing and exchanging Economic Operators Registration and Identification numbers is partially operational and based on Asycuda World. The national system is not interconnected with the EORI central database managed by the European Commission.

3.3 - Exchange of data about Authorised Economic Operators

Moldova has a registration and identification information system of authorised economic operators and is in process to conclude an agreement of mutual recognition of the country's register of economic operators and the Authorised Economic Operators in the EU within a pilot project. There is no yet a system-to-system interface that allows the economic operators' data received from the country to be disseminated to the EU member states and the validation of the county' AEO status in the EU transaction systems.

3.4 - Summary electronic declaration

An electronic summary declaration containing the required pre-arrival or pre-departure information can be lodged before any goods are brought into or out of the territory of the country. All information is provided to the customs (and other authorities) in electronic format. Existing country's infrastructure allows such information to be shared electronically with third countries where an international agreement so provides.

3.5 - National Single Window System

The national single window and one-stop shop is not yet implemented. There is no possibility to submit required information and documents in electronic format (application for certificates, customs declaration, required documents, and permits).

3.6 - Anti-Counterfeiting and Anti-Piracy System

In Moldova, there is no electronic service providing traders with the possibility to submit a claim asking the intervention of Customs in order to take measures against goods infringing certain intellectual property rights.

Ukraine

In Ukraine, the customs clearance is carried out using electronic customs declaration signed with digital signature. Other documents are processed in electronic format.

Since 2006, the process is carried out through the developed automated customs clearance system (ASMO) "Inspector-2006". Since 2010, Unified Automated Information System of the State Customs Service of Ukraine is in operation covering the integration aspects of customs procedures.

Relevant legislation

Ukrainian law for electronic documents and electronic document workflow from 31st of May, 2005 N 2599-IV

- Regulates the process of creating, sending, transmitting, receiving, storing, processing, use and disposal of electronic documents
- Determines the information contained in electronic document
- Determines the legal status of electronic document and it’s copy

Order from 04.11.10 № 1341 "On approval of the unified automated information system of the State Customs Service of Ukraine"

Law of Ukraine on the accession of Ukraine to the International Convention on the Simplification and Harmonization of Customs Procedures the amended in accordance with Annex I to the Protocol on Amendments to the International Convention on the Simplification and Harmonization of Customs Procedures from 15th of February 2011, N 3018-VI

- Authorised recording of communications and the related traffic data in the course of lawful business practice / confidentiality of the communication
- Allowance to process user traffic data by the provider of an electronic communication service

Order № 216 from 17.03.11 On approval of the electronic declaration

- Order declares an automatic entry in the Register of enterprises permitted to e-declaration

Order of the State Customs Service of Ukraine from 28.03.12 N 191 "On the Concept of integration backbone components and special technical means of customs control of the automated system of customs clearance Customs Service of Ukraine"

- Approves the concept integrating system components and special technical means of customs control of the automated system of customs clearance of the Customs Service of Ukraine

Letter of the State Customs Service of Ukraine from 11.02.2013 g. N 18 / 12-15-1135-EP "To avoid queues at the processing of electronic customs declarations"

Order from March 1, 2013 N 61 "On approval of formats specification electronic messages"

ICT platforms and services

- The automated system of customs clearance (ASCC) "Inspector-2006", which is designed for automated customs documents in the structural units of the customs authority involved in the process of customs clearance.
- Single Automated Customs Information System - multifunctional integrated automated system that provides information and support to maintenance to customs in Ukraine and set several interconnected information systems, including automated information system "Centre", automated customs clearance systems, information and telecommunication systems "Email"

and other systems

- Automated customs clearance system (ACCS) - subsystem, which is part of the Unified Customs automated information system and ensures the use of electronic documents and electronic copies of documents on paper by customs officials for customs procedures
- Automated information system “Centre” – system at central system level, which is a set of subsystems, and centralized information systems storage of customs clearance - electronic copies of customs declarations in hard copy and electronic customs declarations, other electronic records and electronic copies of documents on paper used in the implementation of customs control and clearance of goods and vehicles crossing the customs border of Ukraine, provides two-way exchange of customs and other information with automated customs clearance systems and other systems (subsystems) at local level

Organisations involved

The key state body, responsible for eCustoms is the Customs Service of Ukraine[67] - a part of the State Fiscal Services of Ukraine[68]. Before 2014, it used to be a Ministry of Revenue and Collections, in 2014 changed into a service, and transferred under coordination of Ministry of Finance.

National plans

Presidential Decree On measures to improve the efficiency of Customs Service of Ukraine from 30th of March, 2006 N 272/2006[69]

- Develop proposals to improve legislation of Ukraine on customs and its harmonization with EU legislation
- Increase the use of information technologies, automated control systems and modern equipment by the customs authorities
- For the State Customs Service to work together with the National Bank of Ukraine on issue of creating a domestic customs non-bank payment system

Order of the Cabinet of Ministers from 17 September 2008 g. N 1236-r “On adoption of Concept of the Functional Complex System "Electronic Customs"

- Provisions for the implementation in three phases during 2009-2013
- Document aims to strengthen the customs security of Ukraine, adoption of unified automated information system of the Customs Service and the New Computerised Transit System of EU NCTS

Paperless environment for customs and trade

Unified Automated Information System assures paperless environment and exchanges of data with many state bodies. 92 % of tax declarations are paperless; still it’s mostly one-sided exchange with all involved bodies. Data exchange from State bodies to Customs Service is limited and/or is provided by bodies with limited capacities: from State Standard Agency data on forms, from the National Bank of Ukraine on banks enquiries, since March 2015 from Ukrainian Transportation Inspection data on fines and other related data. There is some lack of involvement from all state bodies (no sufficient financing to develop information systems, collect and clear data). In some cases, there are strict security

[67] http://arc.customs.gov.ua

[68] http://sfs.gov.ua/en/

[69] http://search.ligazakon.ua/l_doc2.nsf/link1/U272_06.html

requirement. For example, Ukraine border services (ARKAN system), according to current decree of information protection, any data exchange with this service is not possible.

The process of implementation of paperless environment is ongoing and depends on State bodies' interest and available financing. There is currently a project in implementation for data exchange with the State Veterinary and Phytosanitary Service of Ukraine that will assure provision of outgoing flow of information to the Veterinary Service. There is another project under discussion about data exchange with the Ministry of Health (drugs and medicine import-export).

With the appropriate political will (political support or special decree) and required involvement of the State bodies, all invoices, transport declarations and tax declarations can be exchanged in electronic forms with the Ministry of Health (permits, medicine, drugs), Ministry of Defence of Ukraine (radio frequencies, weapons), Ministry of Social Policy of Ukraine (humanitarian assistance). More cooperation is suitable with foreign countries: with Moldova (exchange of customs declaration is currently assured, exchange of data on transport means is in process of implementation), Russia (recently launched exchange of data from declarations), Belarus (in process of implementation data exchange about crossing of border points by heavy trucks), Poland (discussing extension of the currently available single point of customs crossing with one-way data exchange on car information, date, weight, with/without load).

International agreements

There are no specific agreement, apart from agreements with some countries on specific topics (like with Belarus on heavy trucks border crossing)

Memberships at international/regional organizations: WCO, WTO, BSEC, GUAM, CIS

International Conventions signed by Ukraine in relation to the customs:

WCO Conventions:

- Convention establishing a Customs Co-operation Council
- Convention on the Harmonized Commodity Description and Coding System
- Convention on Temporary Admission (Istanbul Convention)
- International Convention on the simplification and harmonization of Customs procedures (Kyoto Convention) as amended
- International Convention on mutual administrative assistance for the prevention, investigation and repression of Customs offences (Nairobi Convention)
- Customs Convention on Containers

UNECE Transport Agreements and Conventions:

- Customs Convention on the International Transport of Goods under Cover of TIR Carnets (TIR Convention)
- International Convention on the Harmonization of Frontier Controls of Goods
- Agreement on the International Carriage of Perishable Foodstuffs and on the Special Equipment to be used for such Carriage (ATP)

State of play

Indicator 1: Legal framework

1.1 – Common Risk Management Framework

There's an internally developed risks management system (risk profiles are developed and confirmed by a special Commission – the data is internal and confidential). The framework is regulated by the Tax Code, and specifics orders in case of changes and for risks specification. For the exchange of related data, there is functionality of data exchange, but not exchange of risks profiles.

The local system is considered to be well developed and can be considered as a best practice benchmark:

- Risk is evaluated not only on widespread selected criteria, but also takes into consideration positive and negative history (this way, risks is lowered in case the positive history was maintained for several previous iterations)
- The risk evaluation based on fuzzy logic algorithms

1.2 - Authorised Economic Operator status

The Tax Code provides the required basis for authorized economic operators, but there's no implemented mechanism and no regulations for implementation.

1.3 - Paperless environment for customs and trade

Unified Automated Information System assures paperless environment and exchanges of data with many state bodies. 92 % of tax declarations are paperless; still it's mostly one-sided exchange with all involved bodies. Data exchange from State bodies to Customs Service is limited and/or is provided by bodies with limited capacities: from State Standard Agency data on forms, from the National Bank of Ukraine on banks enquiries, since March 2015 from Ukrainian Transportation Inspection data on fines and other related data.

There is some lack of involvement from all state bodies (no sufficient financing to develop information systems, collect and clear data). In some cases, there are strict security requirement. For example, Ukraine border services (ARKAN system), according to current decree of information protection, any data exchange with this service is not possible.

The process of implementation of paperless environment is ongoing and depends on State bodies' interest and available financing. There is currently a project in implementation for data exchange with the State Veterinary and Phytosanitary Service of Ukraine that will assure provision of outgoing flow of information to the Veterinary Service. There is another project under discussion about data exchange with the Ministry of Health (drugs and medicine import-export).

With the appropriate political will (political support or special decree) and required involvement of the State bodies, all invoices, transport declarations and tax declarations can be exchanged in electronic forms with the Ministry of Health (permits, medicine, drugs), Ministry of Defence of Ukraine (radio frequencies, weapons), Ministry of Social Policy of Ukraine (humanitarian assistance). More cooperation is suitable with foreign countries: with Moldova (exchange of customs declaration is currently assured, exchange of data on transport means is in process of implementation), Russia (recently launched exchange of data from declarations), Belarus (in process of implementation data exchange about crossing of border points by heavy trucks), Poland (discussing extension of the currently available single point of customs crossing with one-way data exchange on car information, date, weight, with/without load).

Since 2012, the cooperation with the EU has being discussed on technical possibilities and data transfers. There is also cooperation within GUAM, and a signed protocol of mutual interests with Turkey.

Indicator 2: Infrastructure

2.1 - Electronic interfaces to conduct all customs-related business

The service of single access points enables economic operators to use one single interface to lodge electronic customs declarations, notably for NCTS. There is insufficient cooperation with other countries and state bodies.

2.2 – Interoperating systems for import, export and transit

The customs information systems assure interoperating between import, export and transit components.

2.3 - Integrated tariff information system

The subject is regulated by Law of Ukraine on Customs Tariff. National Binding Tariff Information system is implemented and integrated with the single customs system.

2.4 - Single Point for Entry or Exit of Data (SPEED) portal

There is currently no solution based on single service bus for data exchange. Exchange of data is assured by online one-to-one systems exchange. Periodically, exchange of emails is practiced for about 50 customs declarations per day. State Agency for E-Governance in Ukraine currently develops a solution of single service bus.

2.5 - Uniform user management & digital signatures

Absence of country-wide electronic identification principles. They are defined in the draft of Law on electronic identification.

The digital signatures provided by State Fiscal Service is applicable in most of case inside of Ukraine. An alternative digital signature solution is used within banking system. For external exchanges, the Customs Services are using MSAT–RSA signatures because of the requirement for RSA certification/ESI compatibility.

Indicator 3: Services

3.1 - Registered Exporters System

The procedure on Registered Exporters is defined by the Ministry of Finance in its order from 07.10.2014 № 1013 in application since 23.12.2014.

The development of technical solutions is in progress. There is no cooperation with EU about registration into the EU REX central database.

3.2 - Economic Operators Registration and Identification system

A national system based on the principles of EORI numbering exists since 1996. There is no interconnection with the EC EORI.

The Tax Code of Ukraine (Section 1, part 2 – some amendments done in 2012, 2013) identifies the requirements for national Economic Operators.

3.3 - Exchange of data about Authorised Economic Operators

Centralised Economic Operators Registration and Identification information and communication system supporting the registration of the Authorised Economic Operators is not implemented in Ukraine.

3.4 - Summary electronic declaration

Summary declaration is not currently used. The submission of preliminary customs declaration is

implemented since 1998 (full electronic since 2011). It requires providing all information available prior to border crossing.

3.5 - National Single Window System

The single window application is available but due to lack of integration with other involved ministries, it cannot serve as a fully integrated single window. The technical readiness of related state bodies to connect to single Customs system is low. There is no of single bus solution that could resolve the potential obstacle (it is currently developed by State Agency for E-Governance in Ukraine).

3.6 - Anti-Counterfeiting and Anti-Piracy System

Anti-Fraud requests are submitted and managed based on paper applications, an electronic system is available only for internal use. The internal system is not exchange data with the EU information system.

The legislation need to be updated. There's a reference to Ukraine-EU Association Agreement Action Plan, approved by Cabinet of Ministers of Ukraine dated 17.09.2014 № 847-p – Action 116, in reference to Article 84, Amendment XV: legislation development in reference to EU Decree № 1383/2003 dated 22.07. 2003 on customs activities in reference to intellectual property rights (no deadlines, responsibility on Ministry of Finance, Customs Service, Ministry of Economics and State Services on Intellectual property.)

Gap analysis

Indicator 1: Legal framework

1.1 – Common Risk Management Framework

Ukraine has a clearly defined national risk management framework in customs controls for goods brought into or out of the country. It is not harmonised with the EU common criteria and priority control areas. Risk Information Form cannot be exchanged electronically with customs offices of the EU countries.

1.2 - Authorised Economic Operator status

The customs authorities of the country do not apply common criteria and harmonised requirements for granting the status of authorised economic operators due to absence of the regulations.

1.3 - Paperless environment for customs and trade

National legal provisions are defined for secure, integrated, interoperable and accessible electronic customs systems for the exchange of data contained in customs declarations, documents accompanying customs declarations, certificates and the exchange of other relevant information.

Indicator 2: Infrastructure

2.1 - Electronic interfaces to conduct all customs-related business

Customs information systems of Ukraine have a service of single access point enabling economic operators to use one single interface to lodge electronic customs declarations to the customs systems of other countries (the EU member state or others) only for the NCTS.

2.2 – Interoperating systems for import, export and transit

The country systems for import and export interoperate with the system for transit and enable the seamless flow of data. The service can partially ensures transfer of data between the national customs systems to/from customs system of the EU member states (NCTS and TIR).

2.3 - Integrated tariff information system

Ukraine has implemented a national centralised binding tariff information system that allows getting tariff classification for goods. The system is interconnected with single customs system to facilitate re-use of data and functionality of one system to another.

Interconnection with other tariff related IT systems has to be confirmed.

2.4 - Single Point for Entry or Exit of Data (SPEED) portal

The country's computerised transit systems (or other such as export, import or economic operators systems) are not connected to SPEED portal. There is some data exchange for electronic customs systems between the country and the EU by semi manual procedures.

2.5 - Uniform user management & digital signatures

There is no a common solution for electronic signatures. There is a partial system based on mutual recognition of existing solutions (digital certificates delivered by 2 authorities) operational in the country and enables the national economic operators to send information to the customs. National economic operators cannot submit information digitally signed to other countries (EU member states).

Indicator 3: Services

3.1 - Registered Exporters System

The country has not yet established a Registered Exporters System that allows an automated verification of the exporters' registration number from the declarations in the national Customs declaration system. The country does not cooperate with the EU in order to register national exporters into the EU REX central database managed by the European Commission.

3.2 - Economic Operators Registration and Identification system

An electronic system for storing and exchanging Economic Operators Registration and Identification (EORI) numbers is operational in the country. The national system is not interconnected with the EORI central database managed by the European Commission.

3.3 - Exchange of data about Authorised Economic Operators

The country does have a registration and Identification information system of economic operators (based on principle of AEO in the EU) and has not concluded an agreement of mutual recognition of the country's register of economic operators and the Authorised Economic Operators in the EU.

3.4 - Summary electronic declaration

Submission of an electronic summary declaration containing the required pre-arrival or pre-departure information is not currently lodged before any goods are brought into or out of the territory of Ukraine.

3.5 - National Single Window System

The national single window and one-stop shop is only partially in place (customs services). For most of involved state bodies, it does not allow submission of all required information and documents in electronic format (application for certificates, customs declaration, required documents, and permits).

3.6 - Anti-Counterfeiting and Anti-Piracy System

No electronic service is in place providing traders with the possibility to submit a claim asking the intervention of Customs in order to take measures against goods infringing certain intellectual property rights. The national Anti-Fraud Information System is not connected with the centralised EU

information system, which is accessible by all Member States.

eCommerce for SMEs

Armenia

State of play

At present, there are no dedicated legislation and regulations regarding eCommerce in Armenia.

Relevant legislation

The Ministry of Economy, together with the Ministry of Transport and Telecommunication and other stakeholders have developed and submitted to the Government and public discussion a package of legal documents, including changes in 4 existing laws and in the Civil Code. The amendments have been developed according to EU acquis. The discussions have been in place for over 2 years now. Until the package of the changes is adopted the sector cannot be considered as regulated. For this reason, the answers to the questionnaire are filled based on the assumption that the package of the proposed legal acts and amendments to the existing would be adopted. The component of ePayments is regulated and supervised by the Central Bank of Armenia.

The Ministry of Economy initiated the formation of the legal field for eCommerce sector. Certain provisions and regulations concerning eCommerce are proposed to be included in the following legal acts:

- Civil Code,
- Law on Trade and Services,
- Law on Consumer Rights,
- Law on Electronic Document and Electronic Signature,
- Law on Cash-Desk Operations.

ICT platforms

There are several ePayment platforms, such as national payment system www.arca.am or private payment system www.edram.am. The system for e-signatures and trust services is operated by the state agency EKENG. No other dedicated support platforms are available in Armenia.

Organisations involved

The main legislative and regulatory bodies in the area eCommerce are the Ministry of Economy and the Ministry of Transport and Telecommunication.

Decision making process

After draft legal acts and proposed amendments to the existing legislation are developed by the Ministry of Economy together with the Ministry of Transport and Telecommunication, they are submitted for public consultations. The final proposals are then presented to the Parliament. The executive agencies have the obligation to amend related regulatory acts during a defined period after the new legislation is in place.

National plans

The only ongoing discussion is over the above-mentioned draft legislation package.

There is a Concept on the Development of Electronic Society in Armenia for 2010-2012 and a Strategic Program on eGovernment 2014.

International agreements

No international agreements are in place or under discussion.

1. Internet security and privacy

1.1 Allowance to process user traffic data

The proposed Law on the Protection of the Personal Data defines the necessity of the consent of the individual to process or use his/her personal data. However, no reference is made to the processing requirements of traffic data for marketing needs.

1.2 Specific liability regime for intermediary service providers

The caching and hosting services are defined as telecom services in the Armenian regulation. Until 2005 these services could be referred to telematics services as defined by the Law on Licensing. After the amendments to this law the telematics services were excluded from the list of activities subject to licensing and are not defined in any way in any of the laws.

Asides from the gap in the definition of the services, there is also an uncertainty regarding the liability regimes of the service providers. For example, the court can convict a hosting service provider in disseminating pornography (which is a cyber-crime according to RA Criminal Code). The decisions are made case by case.

1.3 Obligation for providers to monitor transmitted or stored information

The providers of transmission services such as mobile operators do not have the right to monitor the content of the information transmitted through their networks and are not liable for this information as defined by the Law on Electronic Communication.

2. Consumer rights

2.1 Online trustmarks for retail websites

There are no established country-wide trustmark schemes that help to reassure consumers on the reliability of accredited online traders and service providers. Trusmarks of foreign providers are used by individual eCommerce websites for electronic identification and trust services for electronic transactions.

2.2 Minimum general information by information society service provider

By the proposed changes in the Law of Trade and Services (article 4.1) the eCommerce service provider is required to place information about the company legal name, status, address and contacts details, state registration and VAT numbers, licensing information.

2.3 Transparency of commercial communications information to be provided

The area is regulated by the Law on the Advertisement and the Law on the Television and Radio. However, no specific regulations are available for internet advertising and internet marketing.

There is no explicit obligation to ensure that online commercial communications such as promotional offers, discounts, premiums, promotional competitions or games, meet certain transparency requirements. Both the commercial communication and the natural or legal person responsible for it should be clearly identifiable, and any conditions (price, delivery cost, delays of delivery etc.) attached to the offers, discounts etc. must be easily accessible.

2.4 Requirements for distance contracts and off-premises contracts

By the proposed changes in different laws:

- the consumers must be in advance provided information about the product, its features and attributes and other aspects defined by the law (Civil Code article 511),
- the consumers must be warned about all the processes, procedures and their specifications to encounter during the eCommerce transaction (Law on Trade and Services, article 4.1)
- the consumers must be in advance provided information about the seller (Law on Trade and Services, article 4.1)
- the consumers must be in advance provided information about the payment options and procedures, delivery terms and return policy (Law on the Protection of Consumer Rights, article 24.1)

2.5 Consumer protection international cooperation mechanisms

The international consumer protection cooperation brings together the public authorities in different countries who are responsible for the enforcement of consumer protection laws. Cooperation is done in the frame of IPM and Armenia is part of.

2.6 Out-of-court dispute settlement

A working group of the Ministry of Justice has initiated the process, and has commenced the work on drafting proposed amendments to the laws. However, no official documents or drafts are presented to the public yet.

2.7 Online dispute resolution system for consumers for eCommerce transactions

Setting up of an online dispute resolution platform (an interactive website free of charge) facilitates and speeds up resolution of disputes related to eCommerce transactions. This tool can provide reassurance to both sides, service providers and consumers, and build trust in eCommerce transactions. Online dispute resolution system for consumers for eCommerce transactions is not yet deployed in Armenia.

2.8 Requirements for sending of unsolicited commercial communication

Unsolicited commercial communications (spam) sent by e-mail is considered as a fundamental way of commercial promotion of products and services, and is an important factor for the development of eCommerce.

The legal framework of Armenia is not specific on this matter. It does not explicitly prohibit nor allow the sending of unsolicited commercial communications by e-mail.

3. Competition

3.1 Free movement of eCommerce services

The proposed changes in the Law on Trade and Services (Article 4.1) defines that “eCommerce services can be provided by legal entities or individual entrepreneurs based on invoicing forms and documentation as defined by the tax regulations in Armenia”. No other restrictions or requirements are defined in the Law.

3.2 Authorisation to pursuit the activity of eCommerce service provider

The current legislation does not explicitly restrict the freedom to provide eCommerce services by a provider from another country. The package of proposed legal changes does not hold any requirements for authorisation to provide eCommerce services.

In the information service sector authorisation may be required only in telecom and TV services sectors, where the operator requires numbering or frequency.

4. ePayment

4.1 Fees for the use of means of eCommerce payment

Any rules on the fees for the use of certain means of payment (e.g. credit or debit cards, electronic valets) that can prohibit traders from charging consumers excessive fees in respect of the use of a given means of payment have not been identified in the current legislation. The domain of electronic payments is regulated by the regulations and decrees of the Central Banks of Armenia.

4.2 Equal treatment between paper and electronic invoices

The vast majority of invoicing in Armenia is processed through electronic platforms. The latter is favoured compared to the paper invoicing.

The proposed changes in the Law on Electronic Document and Electronic Signature define that the electronic document/invoice which does not hold electronic signature but can validate that it is submitted by the consumer can fully replace the paper invoices with handwritten signatures.

5. eLogistic

5.1 Equal validity of electronic and offline contracts

The regulations for eContracting are in place. The electronic contracts signed by electronic signatures have equal validity as the paper contracts. In addition, trade deals/contract concluded at distance can be considered valid even without electronic signature.

5.2 Conditions for the risk of loss of or damage to the goods

By the proposed changes in the Law on the Consumer Rights (article 23), the customers of distance trade (including eCommerce) will also have the right to give back or change the purchased good during 14 days of the purchase. The necessary preconditions for the change are defined in the Law.

5.3 Rights on delivery of goods

By the proposed changes in the Law on the Consumer Rights (article 24) the time of delivery of distant trade items is defined maximum 30 days, if the contract does not say otherwise.

Gap analysis

1. Internet security & privacy

1.1 Allowance to process user traffic data

The national legislation does not define any rules of processing of user traffic data by the provider of an electronic communication service for the purposes of marketing electronic communications services or for the provision of value added services.

1.2 Specific liability regime for intermediary service providers

The national legislation does not clearly define specific liability regimes for three categories of online service providers: transmission conduit operators, caching providers and hosting services providers.

1.3 Obligation for providers to monitor transmitted or stored information

Obligations of information transmission service providers to monitor information are regulated. However, the national legislation does not include requirements and conditions on providers of eCommerce and other information services caching and hosting, to monitor the information which they transmit or store in order to detect any illegal activity. Types of illegal on-line activities are not defined.

2. Consumer rights

2.1 Online trustmarks for retail websites

The country has not established country-wide trustmark scheme(s) for electronic identification and trust services for electronic transactions which assure the trustfulness of qualified eCommerce service providers.

2.2 Minimum general information to be provided by information society service provider

The amended Trade Law will impose the obligation on the information service provider to render easily, directly and permanently accessible to both recipients of services and the competent authorities the defined scope of information about the service provider.

2.3 Transparency of commercial communications information to be provided

The national legislation does not explicitly impose that advertisements on the Internet indicates natural or legal person responsible for commercial communication and any conditions attached to the offers.

2.4 Requirements for distance contracts and off-premises contracts

The current legislation and proposed amendments include the requirements for contracts with indication of minimum of legally defined pre-contractual information.

2.5 Consumer protection international cooperation mechanisms

The country has established international cooperation mechanisms between the national public authorities and the authorities of other countries who are responsible for enforcement of consumer protection laws, including for eCommerce.

2.6 Out-of-court dispute settlement

The national legislation does not currently allow the use of out-of-court schemes for dispute settlement regarding provision of eCommerce services, including by appropriate electronic means.

2.7 Online dispute resolution system for consumers for eCommerce transactions

The country does not have an online dispute resolution platform through which parties can initiate alternative dispute resolution in relation to disputes concerning online transactions.

2.8 Requirements for sending of unsolicited commercial communication

The national legislation does not clearly define the requirements applied to sending of unsolicited commercial communications by e-mail.

3. Competition

3.1 Free movement of eCommerce services

The national legislation does not restrict the freedom to provide eCommerce services compliant to the national laws by a lawful service provider established in another country.

3.2 Authorisation to pursuit the activity of eCommerce service provider

The country applies the principle excluding prior authorisation to pursuit the activity of eCommerce service provider.

4. ePayment

4.1 Fees for the use of means of eCommerce payment

The regulations and decrees of the Central Bank of Armenia define the requirements for eCommerce payments and define the rules on the fees for the use of means of electronic payment.

For example, private payment system iDram[70] applies the following conditions applied to legal persons: receiving online payments for products and/or services, sold by legal persons - 2.5-5% commission. It takes 2-5 days to connect to the system.

4.2 Equal treatment between paper and electronic invoices

The national legislation assures equal treatment between paper and electronic invoices (e-invoices). The framework of a common national data model of e-invoicing format has not been defined.

5. eLogistics

5.1 Equal validity of electronic and offline contracts

The national legislation establishes the equal validity of electronic contracting and contract concluded offline together with defining the specific requirements to electronic contract

5.2 Conditions for the risk of loss of or damage to the goods

The proposed amendments to the current legislation will define some conditions for the risk of damage to the goods purchased within eCommerce transaction and responsibilities of the parties involved.

However, these legal provisions should also define the conditions for the risk of loss of or damage to the goods and responsibilities of the trader, the consumer, a third party indicated by the consumer, or the carrier.

5.3 Rights on delivery of goods

The proposed amendments to the current legislation will define the requirements for time of delivery of goods purchased through eCommerce transaction.

[70] http://idram.am/index.php?lang=eng&level_id=462

Azerbaijan

Firms using their own Website - 32.5%

Firms Using Email to Communicate with Clients/suppliers - 64.8%[71]

Internet hosts: 46,856 (2012)

Internet users: 2.42 million (2009)[72]

State of play

Azerbaijan occupies one of the lowest positions in development of retail e-commerce among the CIS countries, which is clearly seen in the comparative analysis of the volume of e-commerce in Azerbaijan with Belarus, Kazakhstan, Ukraine and Russia.

According to the State Statistics Committee (SSC) of Azerbaijan, in 2013 the volume of retail e-commerce in Azerbaijan amounted to AZN 2.6 million. For comparison, in Belarus, with the same number of population (9.4 million people), and the level of internet penetration is 66%, last year the volume of e-commerce was $ 300 million, which is almost a hundred times more than in Azerbaijan. In Kazakhstan, the figure was $ 600 million, Ukraine - $ 2 billion, Russia - $ 15 billion.

But it is noteworthy that, according to official statistics, the level of Internet penetration in Azerbaijan is 70% and on this indicator, Azerbaijan is the absolute leader in the CIS. The SSC reports that during 2014, the volume of retail e-commerce turnover in Azerbaijan increased 2.4 times and amounted to AZN 6.4 million, compared to the same period of 2013. 91.2 percent of the consumer goods purchased by the population online were bought on trade networks of legal entities and 8.8 percent was purchased on trade networks of individuals. Non-food products accounted for 94.9 percent of e-commerce market turnover.

Relevant legislation

The main legislative act that defines the legal framework for the organization and implementation of electronic commerce in the Azerbaijan Republic, the rights and duties, and responsibilities of its members for violation of legislation on electronic commerce is Law of the Republic of Azerbaijan “On eCommerce”. The law regulates all spheres of e-trade excluding financial market, insurance and securities market. There are also some provisions in the Civil Code that regulate the e-commerce activities, such as General provisions on Agreements (Article 331.5 “Written agreements”), General provisions on obligation (Article 386.4 “Grounds for obligation”), Performance of obligations (Article 430.3 “Refusal of the obligations performance”). Appropriate responsibility for violation of e-commerce activities also considered in the Code on Administrative Offences.

ICT platforms

Currently there are about 15-20 e-commerce web sites operating in Azerbaijan. These web sites are for the sale and delivery of different goods: gifts, flowers, auto accessories, household appliances, jewellery, electronic devices, perfumes, clothes, foodstuffs, personal belongings, IT and other equipment, etc. However, there are some deficiencies on the work of these sites, such as scarcity of information on the products; no filtration options for the cost, product type, brand, etc., no information in some web sites on delivery terms. There is no constant updating information on the availability, pricing and new arrivals of goods. Underdeveloped is also infrastructure delivery, resulting in its high

[71] World Bank - Enterprise Surveys: AZERBAIJAN - 2013

[72] CIA World Factbook - https://www.cia.gov/library/publications/the-world-factbook/geos/aj.html

cost. Another problem is the return shipping. Most online stores items are not returnable.

Organisations involved

Even though general foreign economic and trade activities are regulated by the Ministry of Economy and Industry, it is not responsible however for e-commerce activities. The reason is that this activity sphere is quite new in Azerbaijan. Although the Law on E-commerce was signed in 2005 first e-commerce transaction was held in 2009.

National plans

There are some measures undertaken by the Government to stimulate the development of eCommerce in Azerbaijan.

Currently, there are no any government or national implementation plan aimed for development of eCommerce. However, in the State Program on Socio-economic development of regions for 2014-2018 years it is considered to carry out appropriate works on exploration and development of the opportunities for wide use of electronic trading in export.

Moreover, the Action Plan for the same State Program considers establishing “Electronic Trade” by creating information-marketing points.

As part of the Plan of Actions to implement the State Program on Reliable Provision of the Population with Foodstuffs in 2008-2015 enacted by the presidential decree dated August 25, 2008, the Ministry of Economic Development of Azerbaijan Republic was tasked to intensify efforts towards creating Electronic Commerce in Azerbaijan. With a view to achieving this task as well as facilitating private business, in particular producers of agricultural products, to have free access to the market, the ministry decided to launch e-Trade portal (www.b2b.az). The e-Trade portal created on a B2B (business to business) model is the first electronic trade portal in Azerbaijan (2010). The portal aims to support establishment of business relationships through distributing information on local business circles as well as their products and services to potential buyers as well as to provide free access to the markets.

In this stage, Azerbaijan is only just finishing the first phase of eCommerce implementation. Major pioneer merchants are connecting and offering at least some products and services online. In the next phases, an increase in the number of complex eCommerce solutions will likely be made available. These will include services such as online ticketing for airlines and trains (it is currently in place but with limited possibilities), online food ordering, and better online shops. Consumers will start demanding that a company offers its product or service online. In turn, merchants will expand their offerings and improve already existing services. In the fourth and final phase, e-Commerce will form a sizeable percentage of the country’s economy. Consumers will transact with each other and businesses do so as well.

International agreements

Azerbaijan has not signed any International Agreements in this sphere.

State of play

Azerbaijan occupies one of the lowest positions in development of retail e-commerce among the CIS countries, which is clearly seen in the comparative analysis of the volume of e-commerce in Azerbaijan with Belarus, Kazakhstan, Ukraine and Russia.

According to the State Statistics Committee (SSC) of Azerbaijan, in 2013 the volume of retail e-commerce in Azerbaijan amounted to AZN 2.6 million. For comparison, in Belarus, with the same

number of population (9.4 million people), and the level of internet penetration is 66%, last year the volume of e-commerce was $ 300 million, which is almost a hundred times more than in Azerbaijan. In Kazakhstan, the figure was $ 600 million, Ukraine - $ 2 billion, Russia - $ 15 billion.

But it is noteworthy that, according to official statistics, the level of Internet penetration in Azerbaijan is 70% and on this indicator, Azerbaijan is the absolute leader in the CIS. The SSC reports that during 2014, the volume of retail e-commerce turnover in Azerbaijan increased 2.4 times and amounted to AZN 6.4 million, compared to the same period of 2013. 91.2 percent of the consumer goods purchased by the population online were bought on trade networks of legal entities and 8.8 percent was purchased on trade networks of individuals. Non-food products accounted for 94.9 percent of e-commerce market turnover.

1. Internet security and privacy

1.1 Allowance to process user traffic data

The national legislation defines that for the purpose of marketing electronic communications services or for the provision of value added services, the provider of an electronic communications service may process user traffic data to the extent and for the duration necessary for such services or marketing. This is conditioned by the requirement that the subscriber or user to whom the data relate has given his/her consent.

1.2 Specific liability regime for intermediary service providers

There is no provision in the national legislation on the regimes for online service providers. The national legislation should be definitive about specific liability regimes for three categories of online service providers: transmission conduit operators, caching providers and hosting services providers.

1.3 Obligation for providers to monitor transmitted or stored information

The national legislation does not have any provisions about the requirements for information services providers on monitoring information transmitted to detect illegal activities. Cases when information service providers have obligations to inform the competent public authorities of alleged illegal activities are not defined. However, by the decision of court, the activities of e-commerce parties, as well as information services providers can be checked to detect illegal activities.

2. Consumer rights

2.1 Online trust marks for retail websites

Azerbaijan has not yet established its national eCommerce trust mark as an indication that the online shops displaying the national trustmark offer a high level of service. However, individual eCommerce service providers use international online trustmark services. This practice however is not widely used.

2.2 Minimum general information by information society service provider

The national legislation should impose the obligation on the information service provider to render easily, directly and permanently accessible to both recipients of services and the competent authorities the defined scope of information about the service provider.

The Law on eCommerce (Article 5.3-The requirements for eCommerce service provider) sets the requirement for the supplier to give the information on its registration details, contacts, registration number of register or other identification information, tax ID, etc.

This provision is fully compliant with the EU baseline.

2.3 Transparency of commercial communications information to be provided

The national legislation imposes that advertisements on the Internet indicates natural or legal person responsible for commercial communication and any conditions attached to the offers.

Article 6 of the Law on eCommerce (Commercial notification) defines the rules of transparency in the commercial communication for eCommerce. According to the Law, the seller using commercial notification to advertise the goods should meet the following terms: commercial character of notification must be clearly stated; Name and address of notification sender should be exactly shown; Additional conditions (privileges, awards and gifts, as well as terms for obtaining them must be stated and these proposals must be open to familiarization; Information on competitions and games should be clearly shown, terms of participation in them should be stated and these proposals must be open to familiarization.

2.4 Requirements for distance contracts and off-premises contracts

For distance (concluded online or by electronic means) or off-premises contract, the national legislation requires that the trader provides the consumer with a minimum of legally defined pre-contractual information and comprehensive explanation of contractual terms.

The Article 8 of the Law on eCommerce on (Requirements for concluding a contract) stipulates that Seller (supplier) must provide following information before the buyer (customer) orders: name, address of supplier; main information on features of goods (services, jobs); prices of goods (services, jobs) including taxes; cost and other terms of delivery if it is considered; terms of implementation of payment and order; chance to use the right of denial stated in this Law; validity of offer on signing contract or price; minimal term of permanent or temporal supply of goods (doing services, jobs) if required; way of singing the contract and its stages; registration of contract and assurance of access to that by seller.

2.5 Consumer protection international cooperation mechanisms

The consumers' right are protected by the State Service for Antimonopoly Policy and Consumer Rights Protection under the Ministry of Economy and Industry. However, the international cooperation with its foreign counterparts is not so developed. On the Ministry level, it is limited to general economic activities[73].The country has not yet established international cooperation mechanisms with the authorities of other countries who are responsible for enforcement of consumer protection laws, including for eCommerce.

2.6 Out-of-court dispute settlement

The Law on eCommerce stipulates that disputes between parties can be solved by out-of-court means, as well as by electronic means. However, appropriate platform for settlement of disputes using electronic means is not yet developed.

According to the national legislation, the parties can agree for the dispute to be settled by the Court of arbitration. The Law on international private law permits the application of international law in Azerbaijan. However, the mechanism for implementation of orders of foreign courts in Azerbaijan is not yet developed. Azerbaijan is also party to the New York Convention 1958, on the Recognition and Enforcement of Foreign Arbitral Awards.

2.7 Online dispute resolution system for consumers for eCommerce transactions

[73]www.economy.gov.az

Even though the national legislation provides provisions for dispute settlement, including eCommerce transactions, using electronic means, there is no platform developed for this. The ministry of Justice currently works on development of the platform for online claims.

2.8 Requirements for sending of unsolicited commercial communication

The Law on eCommerce (Article 6.3 – unsolicited commercial communication by e-mail) allows sending unsolicited commercial communications by email or mobile communication means, but few requirements for this are defined. The Law on eCommerce indicates that service providers have to respect the opt-out registers to which natural persons not wishing to receive such commercial communications can sign up. Also, the legislation stipulates that absence of answer to an unsolicited commercial communication does not mean acceptance of its commercial offer.

Additional amendments to local legislation to set the requirements for sending unsolicited commercial communications are planned to make by the Parliament.

3. Competition

3.1 Free movement of eCommerce services

According to the Law on eCommerce, there is no restriction for foreign registered service providers. The general rule is that in order to be engaged in entrepreneurial activities on the territory of Azerbaijan foreign registered company should be registered locally. The Law on eCommerce (Article 4 – General principles of electronic commerce) stipulates the principle of free movement of services, goods and financial resources.

3.2 Authorisation to pursuit the activity of eCommerce service provider

According to the Law on eCommerce, except for activities requiring special consent (license) according to legislation of the Republic of Azerbaijan, legal person from the date of registration and physical from the date of getting right to deal with business activity not creating legal person can start e-commerce activity. So, for general eCommerce activities there is no need for prior authorisation. However, eCommerce activities in the areas of financial, insurance and securities markets are regulated by relevant laws on the mentioned areas.

4. ePayment

4.1 Fees for the use of means of eCommerce payment

Currently traders practice payments by credit or debit cards on Internet and some payments for utility costs using smart phones. Customers pay some fees to service provider for utility costs payments. The current legislation does not include the rules on the fees for the use of certain means of payment. Draft Law on Payment Services in under consideration at the Parliament.

4.2 Equal treatment between paper and electronic invoices

The practice of eInvoicing is not widely spread in Azerbaijan even though there is no any limitation for this. There is no solid technical platform for eInvoicing. The national legislation does not explicitly assure equal treatment between paper and electronic invoices and does not define the framework of a common national data model of eInvoicing format.

5. eLogistic

5.1 Equal validity of electronic and offline contracts

The Law on eCommerce (Article 7 on Signing the contract and Article 8 on Requirements for signing the contract) stipulates that the contract between seller and buyer of eCommerce is signed in the form of eDocument. The information to be provided by the seller before signing the contract is also stipulated in the law. The rules applied for placing of orders are defined.

5.2 Conditions for the risk of loss of or damage to the goods

Even though there are some provisions in the law on eCommerce on the delivery of goods, there is no provision about the risk of loss of or damage to the goods purchased within eCommerce transaction or the responsibilities of the parties.

5.3 Rights on delivery of goods

The Law on eCommerce (Article 10 - Fulfilment of contract) sets the period of 30 days for implementation by the seller of the order, from the day of ordering by customer. If seller can't supply the goods order due to the impossibility of supply, the seller should inform the customer and return the sum paid by customer within 7 days.

Gap analysis

1. Internet security & privacy

1.1 Allowance to process user traffic data

In general, the Law of Azerbaijan on eCommerce is compliant with the EU best practice in the aspect of the rules of processing of user traffic data by the provider of an electronic communication service for the purposes of marketing electronic communications services or for the provision of value added services. However, the legislation is not explicit about possibility for users or subscribers to withdraw their consent for the processing of traffic data. Also, it is not indicated if the service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing.

If the traffic data is processed within the investigation the subscriber or user is not informed about that. The processing and monitoring of traffic data is held by law enforcement agencies.

1.2 Specific liability regime for intermediary service providers

The EU Directive and the appropriate legislation of the EU member states define the specific liability regime for three categories of essential services assuring the provision of eCommerce online services. In Azerbaijan, the conditions for mere conduit operators (transmission in a communication network), caching providers (temporary storage of information) and hosting services are not defined. This can create uncertainty for some service providers, especially foreign companies, to provide eCommerce services. The aspect is important for services of streamed video and audio, hosting of different types of user data and information, Cloud computing, SaaS.

1.3 Obligation for providers to monitor transmitted or stored information

The absence of a general obligation on providers of such services as transmission, caching and hosting, to monitor the information which they transmit or store, is fully compliant with the recommendations of the EU legislation; so is the absence of a general obligation to actively seek facts or circumstances indicating illegal activity. However, the legislation does not explicitly define obligations to communicate to the competent authorities, at their request, information enabling the identification of actors of illegal activities.

2. Consumer rights

2.1 Online trustmarks for retail websites

Without country-wide trustmark scheme(s) for electronic identification and trust services for electronic transactions, customers can not be assured in the trustfulness of qualified of eCommerce service providers. Most of the EU member states have established their national online trustmarks. Now the Commission is exploring the usefulness and benefits of the EU-wide trustmark schemes to reassure consumers on the reliability of accredited traders across borders. The aim is also to encourage the establishment of pan-EU price-comparison websites.

When shopping from the sellers that display a national trustmark, customers will benefit from the defined and internationally recognised quality standards such as: comprehensive and accurate product description and merchant information before placement of on-line order, safe and legally compliant service, notification of all costs and any limitations / conditions prior to checkout, charges that are complete and simple to understand – including any tax and delivery and surcharges, access information on order progress / history, delivery as specified at the time of order, purchases arriving in good condition, helpful support with damaged / failed / late / attempted deliveries, a clear returns process with any limitations / conditions notified prior to purchase, personal data and rights being properly protected and managed.

2.2 Minimum general information to be provided by information society service provider

Compliant with the requirements of the Directive 2000/31/EC on electronic commerce Article 5.

2.3 Transparency of commercial communications information to be provided

Compliant with the requirements of the Directive 2000/31/EC on electronic commerce Article 6.

2.4 Requirements for distance contracts and off-premises contracts.

Compliant with the requirements of the Directive 2011/83/EC on Consumer Rights.

2.5 Consumer protection international cooperation mechanisms.

As Azerbaijan has not established international cooperation mechanisms between the national public authorities and the authorities of other countries who are responsible for enforcement of consumer protection laws, including for eCommerce, its citizens are much less protected when they purchase products and services from foreign traders established abroad. If international cooperation is established and when consumer interests are harmed, the State Service for Antimonopoly Policy and Consumer Rights Protection can call on their counterpart in the country where the trader is located and ask for action to stop the infringement. Enforcement authorities can also alert each other to malpractices they have spotted which may spread to other countries.

2.6 Out-of-court dispute settlement

Compliant with the requirements of the Directive 2000/31/EC on electronic commerce Article 17.

2.7 Online dispute resolution system for consumers for eCommerce transactions

As the country has not yet set up an online dispute resolution platform, it cannot facilitate and speed up resolution of disputes related to eCommerce transactions. This tool would provide reassurance to both sides, service providers and consumers, and build trust in eCommerce transactions. Through this website, parties can initiate alternative dispute resolution procedure in relation to disputes concerning online transactions without going through traditional court legal procedures that are time and resources consuming.

2.8 Requirements for sending of unsolicited commercial communication

The national legislation explicitly defines few requirements applied to sending of unsolicited commercial communications ("spams") by e-mail. The EU best practice in this domain preserves the possibility for Member States to either prohibit or allow the sending of unsolicited commercial communications by e-mail. Compliant with the requirements of the Directive 2000/31/EC on electronic commerce Article 7.

3. Competition

3.1 Free movement of eCommerce services

The national legislation of Azerbaijan does not restrict the freedom to provide eCommerce services compliant to the national laws by a lawful service provider established in another country. In the EU, the Internal Market clause of the eCommerce Directive aims to ensure the free movement of information society services between the Member States. Each Member State must ensure that information society services provided by a service provider established on its territory comply with the national provisions applicable in the Member State in question which fall within the coordinated field. It may not, for reasons falling within the coordinated field, restrict the freedom to provide information society services from another Member State. In these terms, the legislation in Azerbaijan is partially compliant with the EU best practices (Directive 2000/31/EC on electronic commerce Article 3) because it does not explicitly define the conditions of provision services or sales of goods in the territory of Azerbaijan by a service provider established abroad.

3.2 Authorisation to pursuit the activity of eCommerce service provider

The country applies the principle excluding prior authorisation to pursuit the activity of eCommerce service provider. This principle is without prejudice to authorisation schemes of Azerbaijan which are not specifically and exclusively targeted at information society services, or which are covered by another pieces of legislation. This is fully compliant with the EC Directive on electronic commerce that defines the principle excluding prior authorisation to pursuit the activity of an information society service provider (Directive 2000/31/EC on electronic commerce Article 4).

4. ePayment

4.1 Fees for the use of means of eCommerce payment

The national legislation does not yet define the requirements for eCommerce payments and does not define the rules on the fees for the use of means of electronic payment. A comprehensive national legislation for eCommerce payments by credit or debit card, on Internet, on phone, using mobile and other electronic payments presents a substantial benefit for eCommerce development and market integration in this field at European level. In the EU, rules on the fees for the use of certain means of payment (e.g. credit or debit cards, electronic valets) prohibit traders from charging consumers, in respect of the use of a given means of payment, fees that exceed the cost borne by the trader for the use of such mean(Directive 2011/83/EC on Consumer Rights).

4.2 Equal treatment between paper and electronic invoices

The national legislation of Azerbaijan does not explicitly assure equal treatment between paper and electronic invoices. This does not comply with the situation in the EU where the EC has identified a set of actions to support the uptake of eInvoicing by ensuring legal certainty and promoting the development of interoperable eInvoicing solutions based on a common standard, paying particular attention to the needs of small and medium-sized enterprises. Directive 2010/45/EU on the common system of value added tax as regards the rules on invoicing sets out new VAT rules regarding

eInvoicing and removes obstacles to the uptake of eInvoicing by creating equal treatment between paper and eInvoices, while also ensuring that no additional requirements are imposed on paper invoices. Removing of obstacles to the uptake of eInvoicing by creating equal treatment between paper and eInvoices assures that eCommerce transactions can be concluded faster. eInvoicing also significantly reduces the cost of business procedures related to keeping, processing, storing and delivery/postal expenses of paper invoices.

5. eLogistics

5.1 Equal validity of electronic and offline contracts

The law on eCommerce defines the validity of electronic contract exclusively for eCommerce transactions. However, the national legislation of Azerbaijan does not establish the universal equal validity of electronic contracting and contract concluded offline. The EC Directive on electronic commerce (Directive 2000/31/EC on electronic commerce, Articles 9-11) defines the fundamental principles of equal validity of electronic contracting and contract concluded offline, and not only for eCommerce.

5.2 Conditions for the risk of loss of or damage to the goods

The national legislation does not defines the conditions for the risk of loss of or damage to the goods purchased within eCommerce transaction and responsibilities of the trader, the consumer, a third party indicated by the consumer, or the carrier. It also does not stipulate the remedies available to consumers for damaged or faulty goods, entitlement of consumers to replacement or repair of goods, a refund or discount where specific circumstances apply. The Directive 2011/83/EC on Consumer Rights defines that the delivery of goods within a minimum of 30 days from execution of sale contract, seller bears risk of loss/damage until goods are received by consumer; automatic right of refund within 7 days of non-delivery. It also standardise the remedies available to consumers for damaged or faulty goods. Consumers will be entitled to replacement or repair in the first instance and a refund or discount only where specific circumstances apply.

5.3 Rights on delivery of goods

The national legislation defines the requirements for time of delivery of goods purchased through eCommerce transaction which are fully compliant with the EU baseline (Directive 2011/83/EC on Consumer Rights).

Belarus

In 2014, there were about 3,000 on-line shops in Belarus that are responsible for 1.5% (or approx. USD 430mln) total retail turnover. Belarus' eCommerce is assumed to reach USD 500 million by the end of 2014.

About a million users in Belarus effect on-line purchases. 65% of Belarusian Internet users have ever affected online purchases. Average on-line purchase cost amounts to USD 290.

Approx. 60% of the customers paid for their orders in cash against delivery, not always demanding the receipt, despite of requirement to use cash registers by current laws. About 12% of the buyers used their bank cards on site, 8% paid by bank transfer, 7% paid by "client-bank" system, 4% used e-money, and only 3% paid by bank cards against delivery.

Relevant legislation

In general, laws and regulations governing rendering services in Internet, including protection of consumers' rights, are not sufficiently developed yet to cover all aspects of eCommerce. There is no common national legal framework related to this area and different laws and regulations define the legal basis.

The term "electronic commerce (eCommerce)" is not explicitly defined by the legislation of the Republic of Belarus. On-line shop activity is covered by "trading-by-sample outdoor" definition. Rules approved by Resolution No. 31 of the Council of Ministers of the Republic of Belarus of January 15, 2009 "On approval of procedures for retail goods trading-by-sample" (as revised by Resolutions till No.709 dated 22 July 2014) govern relations between the customer and the seller in trading-by-sample and rendering of related services.

Different types of trade (including online) are covered by regulations on protection of consumers' rights:

- Law No.90-Z of the Republic of Belarus dated January 9, 2002 "On protection of consumers' rights"
- Resolution No. 649 of the Council of Ministers of the Republic of Belarus of April 29, 2010 "On online shop registration in the Trade Register of the Republic of Belarus, on procedures used to control on-line shop activity, and on amendments to certain Resolutions of the Council of Ministers of the Republic of Belarus" governs procedure of obligatory registration of on-line shops.
- Resolution No.6 of Ministry of Communications and Informatisation of the Republic of Belarus dated February 18, 2015 "Regulations for generation and storage of data on content accessed by Internet users"

Operation of cloud services and operators of communication services is governed by electronic communications and radio-frequency spectrum regulations.

- Resolution No.6/8 of Operations and Analysis Centre at the President of the Republic of Belarus and of the Ministry of Communications and Informatisation of the Republic of Belarus dated February 19, 2015 "Regulations for limiting of access to content (or parts thereof) published in global Internet network"

Other commercial activities related to eCommerce are included into commercial regulations:

- Law No.225-Z of the Republic of Belarus dated May 10, 2007 "About advertising"

- Decree No.201 of the President of the Republic of Belarus dated April 10, 2008 “About electronic interactive games”
- Resolution No. 767 of the Council of Ministers of the Republic of Belarus of August 7, 2014 establishes procedures for rendering express delivery services.

Best practices

Trade Register

From March 1, 2015 service providers of online shops have to register through a Web interface for the inclusion into the Trade Register. The information contained in the Trade Register can be checked on the website of the Ministry of Trade in the category “Trade Register”, subcategory “Publication of Information”. The Trade Register allows the user to check whether the seller specified on the online shop has been registered as a legal body or an individual entrepreneur (it is possible to search by tax identification number or name of the business entity) and get his contact details.

Radio frequency identification (RFID)

The RFID technologies are getting widely adopted in countries-members of the Eurasian Economic Union (EEU) in order to control illegal and adulterated products.

A pilot project related to natural fur clothing and products marking with control (identification) marks featuring RFID labels shall be started in year 2015. All countries-members of the EEU (both legal entities and individuals) shall have access to contents of the integrated information system of the Eurasian Economic Commission.

ICT platforms

Bank of electronic passports of goods (ePASS)

Scientific and Engineering Republican Unitary Enterprise “Intersectoral Scientific and Practical Centre for Identification Systems and Electronic Business Transaction Systems” of the National Academy of Sciences of the Republic of Belarus established an interdepartmental distributed information system named “Bank of electronic passports of goods” (ePASS)[74].

ePASS is a centralized information resource containing description of products presented in the format which complies with the international standards of eCommerce. Descriptions of products are obtained from the primary sources – manufacturers and importers. These descriptions are further transmitted to supply chains participants for application in business process automation systems. In accordance with the Government decree №1116 of 22.08.2011, ePASS has status of republican information system for maintenance of basic data on products for automation of record keeping and inventory in the commodity distribution networks, as well as for carrying out eCommerce processes.

Any legal entities and individual persons can obtain information from ePASS system on the basis of agreement (particularly but not exclusively via automated ‘system-system’ synchronization).Without a contract, information can be obtained using a free application ePASS.MOBILe for mobile devices under Android and iOS.

Unified payment and information space (ERIP)

The unified payment and information space of the Republic of Belarus (ERIP) is based on the Automated Information System “Raschet”.

[74] http://epass.by/

Organisations involved

At present, several Ministries govern rendering services via Internet for products and/or services in their relative fields. The Ministry of Trade governs trade, catering, and domestic services, only. Certain services are governed by respective branch ministries: travel services – by Ministry of Sport and Tourism, communication services – by Ministry of Communications, other services – by Ministry of Economic Affairs. The Ministry of Trade performs coordination functions and, being a body dedicated to protection of consumers' rights, may give recommendations when implementation of interdepartmental regulation of rendering services in Internet is started.

Other organisations are responsible for implementation of legislation in the area of digital and information services. These are the Ministry of Communications and Informatisation of the Republic of Belarus with its Department for Informatisation, Operations and Analysis Centre under the President of the Republic, Scientific and Engineering Republican Unitary Enterprise "Interdisciplinary Scientific and Practical Centre for Identification Systems and Electronic Business" of the National Academy of Sciences of Belarus (issuance of an EDI-provider certificate), Belarusian Association of Automatic Identification GS1 Bel (assigns in Belarus the Global Location Number to accommodate the description of the goods in ePASS system).

Decision making process

The decision making process in the areas related to eCommerce mainly based on interaction of several government organisations with some involvement of association of private sector organisations.

The main governmental body responsible for designing, introduction and implementation of policies in the field of ICT, are the **Ministry for Communication and Informatisation of the Republic of Belarus** and the Department of Informatisation of the Ministry of Communications and Informatisation of the Republic of Belarus. However, both the development of the Strategy and the Programme is performed through gatherings of lead specialists in particular fields within the temporary Working Groups and Councils. Some members of Councils are invited to particular meetings when the relevant issues are discussed.

The Council on development of the information society of the President of the Republic of Belarus serves as an advisory body to make decisions on the determining of the state information policy and improving the mechanisms for its implementation.

The Ministry of Trade plays the main role in developing draft laws and decisions of the President of the Republic of Belarus and of the Council of Ministers of the Republic of Belarus related to trade, domestic services, protection of consumers' rights, advertising, public purchase of goods (works, services). It adopts and enforces laws and regulations, supervises compliance, develops and approves technical regulations and standardization in compliance with laws and regulations of the Republic of Belarus. The Ministry of Trade forms a scientific and technical council intended to comprehensively discuss operating and development issues of trade, catering, domestic services; to make proposals and recommendations.

Interdepartmental Advertising Council is authorized to formulate and provide state bodies, other concerned organizations and individuals with opinion on current issues of advertisement production and distribution. It participates in development of proposals on improvement of advertising laws and regulations.

The Advisory Council on Protection of Consumers' Rights in Countries Members of CIS is a sectoral cooperation body of the CIS intended to coordinate interaction between governmental bodies.

As of September 2014, there have been acting at least 54 public associations (societies) for consumer rights protection; additionally, the authorized employees of executive committees are available for free-of-charge protection of customers' rights and their representation in the court.

National plans

The main national plans in relation to eCommerce development are:

- Strategy of Development of the Information Society in the Republic of Belarus up to 2015 (Strategy for 2016-2022 undergoes discussions now)
- National Programme for accelerated development of services in the sphere of ICT 2011-2015 (Programme for 2016-2022 is developed now). The main goal of the National Programme is to create conditions for the accelerated development of services in the field of ICT to facilitate the development of the information society on the basis of innovation and to improve the quality and efficiency of information relations of the population, business and government, including the formation of the state system of e-services. The Programme contains 9 sub-programmes, including related to eCommerce: ICT security and digital trust, eHealth, Development of export-oriented IT industry.
- Advertising market development plan of the Republic of Belarus to year 2016[75]. It includes the provision to reinforce control over advertising, and, in particular, over content of on-line shop web-sites. and provision to guarantee electronic services related to advertising.

International agreements

Most active is the international collaboration within the Customs Union and the Eurasian Economic Union that has replaced the Customs Union on 1 January 2015. In relation to eCommerce, a number of agreements have been concluded in the areas of trade, technical regulations, customs collaboration, and competitiveness. The Department of Information Technology is a structural unit of the Eurasian Economic Commission. One of its roles is organization of work to create and develop the integration (supranational) segment of the Commission of the integrated information system of foreign and mutual trade (IISVVT) of the Customs Union and the Common Economic Space.

Besides, international collaboration agreements are concluded in a multilateral manner among the Customs Union and the international organisations:

- Memorandum of Understanding between the Secretariat of the Commission of the Customs Union and the United Nations Conference on Trade and Development (UNCTAD) signed on 7 April 2011
- Memorandum of Understanding between the Secretariat of the Commission of the Customs Union and the United Nations Economic Commission for Europe (UNECE) signed on 7 April 2011

State of play

1. Internet security and privacy

1.1 Allowance to process user traffic data

[75] Advertising market development plan of the Republic of Belarus to year 2016 approved by Minutes No.15 of the meeting of the Board of the Ministry of Trade of the Republic of Belarus dated July 25, 2014

In the area of eCommerce trade, the regulation of the Department of Commerce regulates that within 2 years from the date of sale of goods, information about the act of sale have to be kept by the seller. This also affects a person's interest because items are purchased at eCommerce shops after identification and often paid by electronic means. However, the legislation does not require obtaining consent of the customer to store information about buying, because this measure protects the consumer. 2 years is the warranty period after the sale of goods, and during this period the seller should guarantee the rights of consumers in the event of the need for examination of goods by the seller. This provision applies only to products sold by any means, including the Internet (not for services).

In relation to communication services, the Law No.45-З of the Republic of Belarus dated 19 July 2005 "About electric communication" Article 56 "Electronic communication operator's subscriber databases" [76], stipulates that electronic communication operator should create databases on subscribers and telecommunication services rendered thereto. The law indicates the type of data about the subscribers (legal entities and natural persons) that have to be stored by service providers. Electronic communication operators may use subscriber databases created by them for reference and information services, including preparation and distribution of reference and information publications in various manners.

In case of written refusal of the subscriber to consent for usage of his/her personal data for reference and information services, such data cannot be used and shall be excluded from reference and information publications.

1.2 Specific liability regime for intermediary service providers

Liability of Internet providers is not determined clearly enough for individual categories ("communication channel operators", "cashing (temporary data storage) providers", and "hosting service providers"). Liability of other types of the communication service providers is regulated by different legislations.

The basics of security regulations are given in the Law No.455-P of the Republic of Belarus dated November 10, 2008 "On information, informatisation and information security".

Resolution No.1055 of the Council of Ministers dated August 17, 2006 "On Approval of the procedures for rendering electronic communications services" in 2012 legally introduced the terms "cellular mobile electric communication operator", "donor operator", "recipient operator" (applicable to cellular mobile communication customer number(s) transfer) and their liabilities.

1.3 Obligation for providers to monitor transmitted or stored information

The Resolution No.1055[77] stipulates that electric communication operator has to ensure storage of personal data of data transmission and telematics services users ensuring comparison of user's network credentials with their personal data, and other data within one year after the date of rendering service.

[76] http://pravo.by/webnpa/text.asp?RN=H10500045

[77] Resolution No.1055 of the Council of Ministers of the Republic of Belarus dated August 17, 2006 "On Approval of the procedures for rendering electronic communications services"

Since January 1 2016, Internet providers have to generate and store relevant data on Internet resources visited by users, including data on individual users and sole proprietors for the duration of one year after the date of rendering the service[78].

Resolution No.6/8[79] defines the rights to the Operations and Analysis Centre at the President of the Republic of Belarus to govern the conditions of limitation and resumption of access to information resources in Internet network.

Since February 26, 2015 access to information resources is subject to limitation, if the resources contain data messages and/or materials directed at drug-trafficking or other data prohibited or of limited distribution according to the law and regulations of the Republic of Belarus and effective judgments.

Internet providers then have to limit access to information resources on the basis of limited access list created and kept by the State Inspection on Electric Communications of the Ministry of Communications and Informatisation of the Republic of Belarus on the basis of decisions made by the Ministry of Information.

2. Consumer rights

2.1 Online trustmarks for retail websites

Regulatory bodies have worked through the issue of introducing a voluntary certification for activities of the eCommerce that requires endowing one of the governmental bodies with such function. An alternative of creating an Association in the field of eCommerce has been suggested, and that could allow the business entities to draft a Code of Conduct for eCommerce and grant such online trustmarks. The Ministry of Trade would eagerly accept one of this as soon as it develops fair competition and keeps the consumers updated with information about the number of sellers.

The Ministry of Trade is greatly involved in cooperation with eCommerce service providers on good practices of trade. The providers sign agreements with the Ministry that go beyond the current requirements of the law. They voluntarily assume stricter responsibilities and help the regulatory bodies to fight unconscientious eCommerce operators by creating much stricter principles of domestic policy.

eCommerce service providers have obligation to register in the Trade Register of the Ministry of Trade. The information contained in the Trade Register can be checked on the website of the Ministry of Trade and allows the user to check whether the seller specified on the online shop has been registered as a legal body or an individual entrepreneur (it is possible to search by tax identification number (TIN) or name of the business entity) and get his contact details.

2.2 Minimum general information by information society service provider

In case of trade carried out without or outside of a retail facility (distance trade)[80], the trader is obliged to bring to consumer's knowledge (through catalogues, leaflets, advertisements, brochures or present

[78] Resolution No.6 of the Ministry of Communications and Informatization of the Republic of Belarus dated February 18, 2015

[79] Resolution No.6/8 of Operations and Analysis Center at the President of the Republic of Belarus and of Ministry of Communications and Informatization of the Republic of Belarus dated February 19, 2005 "On approval of Statement on procedure of limitation of access to information resources (parts thereof) in global Internet network"

in photographs or any other information sources) the following information: its name (brand name, or last and firs name in case of individual entrepreneur); the retail facility name, working hours. The trader is also obliged to bring to the consumer's knowledge by any other means acceptable in the retail services the information about the number of the special permit (license), its validity time, governmental body or organization that issued the special permission (license). If the trader is an individual entrepreneur, the information about the state registration of the individual entrepreneur and the name of the body making his state registration as an individual entrepreneur, place of residence are provided.

For eCommerce through an online store, this information as well as the date of online store registration in the Trade register of the Republic of Belarus is posted on the main page of the online store web site. Owners of the information resources providing the traders with services connected with the eCommerce trade through an online store (eCommerce platforms) support the customers in protection of their consumer right by providing information about the trader: name and location of the organization, last name, first name, patronymic name (if exists) of the individual entrepreneur, data about the state registration of the individual entrepreneur. They also pass claims of customers to the trader, in case of unjustified rejection by the trader to accept such claim, they record the actual instance of application.

2.3 Transparency of commercial communications information to be provided

According to the Law No. 225-381 "On advertisement", the advertisements containing the information about realization of goods connected with business activities of the advertiser, must include name of the advertiser, his tax identification number and also last name and initials if the advertiser is a natural person. In case the advertiser is a foreign or international legal entity (organization that is not a legal entity), foreign citizen, the advertisement should contain the name of the country or a geographical name where the advertiser holds temporary or permanent residence. Requirements of this clause do not apply to the advertisement distributed by means of cellular mobile telecommunication by the telecommunication providers and to the advertisement distributed through the Internet that contains a link where the mentioned above information is published.

The legislation also imposes a number of requirements about conditions attached to the offers advertised online, such as price (has to be only in Belarus rubbles), address of manufacturer or importer, delays for products delivery, payment conditions, and other.

Advertising producer and advertising distributor are obliged to demand and the advertiser is required to provide a number of documentary proofs, such as the state registration certificate of this legal entity, copy of the state registration certificate of individual entrepreneur, a license (if the advertisement contains the information about the activities subject to licensing), original of a permit (if the distribution of the advertisement requires a permission). The law states that such requirement does not apply to the advertisements distributed on the Internet and containing such information. This indirectly reflects the requirement that advertisements distributed on the Internet has to contain the information about the name and location of the advertiser, and the information about permission (approval) of such advertisement (date of approval and the name of the body approving) or a link to the website, where such information is published.

---

[80] Resolution No. 31 of the Council of Ministers of the Republic of Belarus of 15 January 2009 "On the Rules of selling goods in retail trade by sample"

[81] Law No. 225-3 of the Republic of Belarus of 10 May 2007 "On advertisement"

2.4 Requirements for distance contracts and off-premises contracts

For distance (concluded online or by electronic means) or off-premises contract, the national legislation requires that the trader provides the consumer with a comprehensive legally defined pre-contractual information (name of goods, reference to the regulatory documents certifying the quality of goods, price and the terms of payment for the goods, and others).

Information about the complaints and claims policy, information about after-sale service, and consideration period do not qualify by the law as required to be provided before the contract conclusion. However, such information is normally present on the online stores' websites.

If the consumer is not given a possibility to receive the necessary and accurate information about the goods at the moment of delivery, the consumer has a full right to cancel the purchase without compensating the trader's costs for delivery.

Information about the documents that confirm the purchase of the goods and are supposed to be given by the trader to the customer together with the goods, samples of such documents and their handling procedure are to be posted on the online store web-site.

2.5 Consumer protection international cooperation mechanisms

Consumer protection cooperation agreement is set up with the Eurasian Economic Union and CIS, but not the EU member states. Ministry of trade of the Republic of Belarus is a member of the CIS Consumer rights protection advisory council. A similar body has being created to affiliate to Eurasian economic commission. The Memorandum on cooperation between the CIS Consumer rights protection advisory council and the Interstate antimonopoly policy council has been signed. Agreement on the main lines of cooperation of the CIS member-states in the area of consumer rights protection has come into force.

Information exchange on the laws and financial literacy is in process within the CIS. Executive authorities can alert each other to malpractices that can affect the other countries even though it mostly covers big infringements. Public councils on consumer rights protection are a part of the international consumer system CI.

2.6 Out-of-court dispute settlement

National legislation clearly defines the mechanisms of dispute settlement in case of disagreement between a provider and a recipient of the services. In the area of eCommerce they are determined by the Resolution No. 31 "On the rules of trade by samples"[82] for a case when the trader receives a prepayment for the goods or the delivery of services. There is a graded system of dispute settlement with indication of the consumer rights for exaction of a fine at certain steps of such dispute settlement. Mechanisms of dispute resolution between consumers and electronic services providers are defined by the Resolution No. 1055 "On the rules of rendering electronic services"[83].

As Belarus develops a socially oriented state, government officials are asked to help the consumers in their rights protection. There is a system of authorized officials to protect the consumer rights, one in each executive committee and at the Ministry of Trade, who can be addressed instead of lawyers.

[82] Resolution No. 31 of the Council of Ministers of the Republic of Belarus of 15 January 2009 "On the rules of trade by samples"

[83] Resolution No. 1055 of the Council of Ministers of the Republic of Belarus of 17 August 2006 "On the rules of rendering electronic services"

Executive committees can also represent the consumers in court, moreover do it free of charge. Such kind of pre-court resolution allows the executive committees to act as intermediates in the settlement of disputes; legal action is a last resort when the dispute on moral and property damage appears.

For consumer rights protection local executive and regulatory bodies are to handle consumer applications according to the legislation on citizens' and legal entities' applications including the electronic applications, organize legislative interpretation and provide legal assistance on the consumer rights protection, send written notices to manufacturers (traders, suppliers, representatives, contractors, repair contractors) about the violation of consumer rights and start a legal action on consumer rights protection.

2.7 Online dispute resolution system for consumers for eCommerce transactions

According to Law No. 300-3 "On public and legal entities appeals"[84], citizens of the Republic of Belarus, legal entities of the Republic of Belarus, individual businessmen have a right to appeal to organizations by submitting electronic applications as well (art. 3). Art. 25 determines the handling of electronic applications. Electronic applications that have been received to the governmental bodies or other governmental organizations are to be handled according to the procedures determined for written applications with regard to the aspects of this article. The share of electronic applications in the amount of application received by the Ministry of trade was 55 % in 2014; 68% in the first quarter of 2015 (or 573 electronic applications with claims, requests for explanation of trade regulations including the online trade).

There is no separate online-platform for alternative disputes resolution. There is a category on the Ministry of Trade web site where useful for consumers information is posted weekly. This can be, for example, list of stores that have violations, including online stores. Analysis of this information helps the consumer to track the dangerous stores and goods.

Certain Internet mediums have a functionality to comment and discuss about certain goods and traders (grading system at Onliner.by). Their forums often serve for resolution of disputes between a customer and a trader, especially when the trader starts to ignore the customer's calls.

2.8 Requirements for sending of unsolicited commercial communication

The Law No. 225-3 "On advertisements" protects the right of consumer to unsubscribe from advertisement delivered by any means, but the technical realisation of un-subscription from the unsolicited commercial communications is left to advertiser. Thus, a clickable link or "opt-out button" may be included in email to notify the sender that the recipient wishes to receive no further emails, but is not an obligatory technical solution. In practice, the shops prefer SMS-notifications to email-advertisements.

In case the consent of a subscriber or an addressee for receiving of the advertisement is included into a contract for rendering of email services that is concluded with a subscriber or an addressee in written form, the subscriber or the addressee is to be informed that he has a right to demand cancellation of advertisement distribution. A corresponding clause should be included into the contract and confirmed by the subscriber's or addressee's signature.

Regulatory bodies are drafting an amendment to the Law on advertisements that will protect the mailboxes of the households from advertisements, and most likely, it will create a register of

[84] Law No. 300-3 of the Republic of Belarus of 18.07.2011 "On public and legal entities appeals"

consumers who have refused to receive advertisements. This option will probably be introduced in the future for the advertisements distributed through electronic communication.

An advertisement of an electronic interactive game taking place in the Republic of Belarus is to contain registration certificate number of the electronic interactive game, registration date of the electronic interactive game register, name of the body that has issued the corresponding certificate. There are some exceptions when advertisements are broadcasted, including by electronic communication providers, and the advertisements that are placed in the Internet. In this case, the advertisement is to contain a link to a web site where all the above listed data is posted.

3. Competition

3.1 Free movement of eCommerce services

With the exception of some sectors of activity, providers of eCommerce services from other countries are not restricted to provide their services in Belarus. Consumers in Belarus can purchase goods and services from foreign suppliers by making electronic payments. They are all covered by the national legislative regulation. If goods with overall value higher than 200 euro/month cross the border of Belarus, customers have to pay customs duties.

The national legislation put some restrictions on using foreign cloud service providers for governmental information systems, and for all legal entities and natural persons. These restrictions concern storage of personal information, mandatory bookkeeping and statistical reporting. Such information can only be stored on the servers located in the Republic of Belarus.

3.2 Authorisation to pursuit the activity of eCommerce service provider

In relation to possible eCommerce applications, Decree No. 450 of the President of the Republic of Belarus "On Licensing of Certain Activities" regulates that the following electronic communications services of general use are subject to licensing: data transmission services, IP-telephony services, IP-television services, broadcasting of sound programs.

Execution of works and services that make up activities in the sphere of technical and (or) cryptographic protection of information is subject to licensing , i.e. if such services are provided via the Internet, such activities are subject to licensing for some type of processed information[85].

To provide services of public keys distribution for verification of electronic digital signatures in the State Management System of Public Keys (GosSUOK), the organization may be accredited by the Operations and Analysis Centre under the President of the Republic of Belarus on the applicant's initiative.

To conduct electronic interactive games, their provider must register them in the State Register of Electronic Interactive Games.

From July 1, 2010[86], activities on the sale of goods or provision of services in the territory of the Republic of Belarus with the use of information networks, systems and resources that are connected to the Internet, are carried out by legal and natural persons, with the use of information networks, systems and resources of the national segment of the Internet network located on the territory of the Republic of Belarus have to be registered under the established procedure.

[85] Law No. 455-3 of the Republic of Belarus of 10 November 2008 "On Information, Informatization and Protection of Information"

[86] Decree No. 60 of the president of the Republic of Belarus of 1 February 2010

Certain goods are not allowed (including goods sold via online shops) for sale by sample outside of retail facilities.

If a business entity is going to trade, he is obliged to obtain registration with the Trade Register that contains information about retail and wholesale trade facilities, including online shops.

Resolution No. 649 “On Registration of Online Shops in the Trade Register of the Republic of Belarus, …” stipulates that from 1 July 2010 legal bodies and individual entrepreneurs perform their retail trade activities via online shops registered in the Trade Register of the Republic of Belarus. Information confirming the registration of an online shop in the Trade Register of the Republic of Belarus is submitted to a licensing authority. The application for registration of online shops is submitted in paper or electronic format with the use of electronic digital signatures. Registration in the Register is free of charge and is valid indefinitely until it is cancelled.

4. ePayment

4.1 Fees for the use of means of eCommerce payment

The payment procedure for electronic communications services is specified in Law “About Electric Communication”87. Settlements for electronic communications services are made on a cash and non-cash basis by means of advanced payments or immediately after the delivery of services. The procedure and form of payments for electronic communications services are defined by a contract for the provision of electronic communications services, unless otherwise provided by law. The law defines several options of remote payments. When selling goods by sample via the online shop, the seller is obliged to provide buyers with the ability to pay for the goods purchased via the online shop by means of remote transfer of funds as an alternative to cash payments.

According to the results of the opinion poll on the use of means for cashless retail payments, published by the National Bank of the Republic of Belarus, 97% of respondents use cashless retail payments for goods and services by means of bank cards, e-money, internet-banking and mobile banking technologies. Excessive charges imposed on the consumers for the use of these means of payment were not mentioned among obstacles impeding the increase in the share of cashless payments for goods and services. When the respondents were asked if they are aware of the fees (%) charged by the designated bank and (or) the cost of services for operations with the use of means for cashless retail payments, 54% of them answered “yes”, and 45% — “No, I am under informed”. This indirectly indicates that the cost of such services is not critically high for users compared with the convenience provided by these services. Legislative regulations of these charges and fees have not been found.

4.2 Equal treatment between paper and electronic invoices

Resolution No. 202 of 7 March 2014 defines the rules on creation of shipping and commercial invoices as electronic documents, as well as providing information about them[88]. Consignments and invoices as electronic documents (electronic invoices) are considered established if they are signed by a digital signature of participants (consignor, consignee) in the framework of the electronic data

[87] Law No. 45-3 of the Republic of Belarus of 19 July 2005 “About Electric Communication”

[88] Resolution No. 202 of the Council of Ministers of the Republic of Belarus of 7 March 2014 "On creation of shipping and commercial invoices as electronic documents, as well as providing information about them and making additions to the resolution of the Council of Ministers dated October 31, 2001 № 1585 and February 17, 2012 № 156 "

interchange process (EDI) in terms of shipping and commercial invoices, transmitted and received through the operator(s) of electronic document flow (EDI-provider).

Sending and receiving electronic invoices can only be implemented by EDI-providers, which are the residents of the Republic of Belarus, and have obtained the certificate of the electronic document flow operator (certificate of EDI-provider). Information about EDI-providers who have received in accordance with the legislation the certificate of the electronic document flow operator in the commodity-transport and consignment notes, is placed on the Internet in the Register of EDI-Providers on the official website of the State Enterprise "Centre of identification systems." As of March 2015, the register of EDI-providers contained only one organisation – the Ltd. “Contemporary trade technologies”.

The national legal framework and technical standards, promoting the development of compatible (interoperable) solutions in the field of e-invoicing based on a single standard is currently in the process of development. The legislation related to the GosSUOK does not pay special attention to the needs of small- and medium-sized enterprises.

5. eLogistic

5.1 Equal validity of electronic and offline contracts

The legal validity of electronic contracting does not impose additional requirements on electronic contracts concluded for eCommerce services. These requirements coincide with that imposed to paper contracts.

Contracts concluded by electronic means have the same validity as contracts concluded offline by traditional means. This applies to all stages and acts of the contractual process, such as the contractual offer, the negotiation and the conclusion of the contract by electronic means, except for signing. Electronic signature is the only eligible means to electronic document validity.

The national legislation requires that online traders provide the consumer with specific information prior to the order being placed. According to the legislation, it is not compulsory to present to customers information on steps to follow to conclude an electronic contract and the filing of the contract by the service provider.

The rules applied for placing of orders are not legally defined (i.e. there is no requirement that online contract should be concluded through an "order" placed by the consumer, followed by an electronic "acknowledgment" of the online trader without undue delay).

The online trader is not requested by legislation to provide the consumer with the technical means allowing him/her to identify and correct input errors prior to the placing of the order.

5.2 Conditions for the risk of loss of or damage to the goods

Law No. 90-3 “On Protection of the Rights of Consumers”[89] defines the conditions for losses incurred by the consumer that shall be reimbursed in full above the penalty established by the law or contract. Payment of the penalty and reimbursement of the damages do not discharge the seller from his obligations to the consumer in kind. In addition, the Law provides for reimbursement of the damage caused in the result of defects of the goods (works, services) and compensation for emotional damage.

[89] Law No. 90-3 of the Republic of Belarus of 9 January 2002 “On Protection of the Rights of Consumers”

The law stipulates deadlines when individual customer requirements should be met in case of the acquisition of goods of inadequate quality, and regulates the consumer right to exchange and return goods.

When electronic communications services are the subject of e-commerce, the Law No. 45-3 “About Electric Communication”[90] stipulates that in case of non-performance or improper performance of the obligations arising from the electronic communications contract, the electronic communications user has the right to submit a claim to the electronic communications service operator and (or) the electronic communications service provider.

5.3 Rights on delivery of goods

Terms for delivery of goods are not stipulated by law on a special basis but are rather defined by contract. However, the seller must inform the buyer of delivery terms by providing such information via the website.

The services provision period is regulated only by trade rules for domestic services, i.e. if domestic services are the subject of eCommerce, the terms for their delivery are established depending on the type of services. In case when it becomes apparent to the consumer that services will not be provided in time, he is entitled to terminate the agreement or specify an additional period. If this period is not complied with, the consumer is entitled to demand a penalty for the delay (for pre-paid goods only).

In case the seller violates the terms for transfer of pre-paid goods the Law No. 90-3 “On Protection of the Rights of Consumers” defines that the contract providing for the consumer’s obligation to pre-pay for the goods must contain a provision on the term of the transfer of goods to the consumer.

[90] Article 57 “Submission and examination of claims” of Law No. 45-3 of the Republic of Belarus of 19 July 2005 “About Electric Communication”

Gap analysis

1. Internet security & privacy

1.1 Allowance to process user traffic data

The national legislation does not explicitly define the rules of processing of user traffic data by the provider of an electronic communication service.

The types of allowed data to be stored by service providers do not include any kind of traffic data. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of an electronic communications service may need to process the data to the extent and for the duration necessary for such services or marketing.

1.2 Specific liability regime for intermediary service providers

There are no clearly defined specific liability regimes for three categories of essential communication services assuring the provision of eCommerce online services: transmission conduit operators, caching providers and hosting services providers. The national legislation is well defined about the rights, obligations, privacy and security rules for cellular communication service providers and telecommunication networks providers to government bodies.

In the EU, the Directive 2000/31/EC on electronic commerce Articles 12-15 introduced a specific liability regime for these three categories of services.

Mere conduit. Where an information society service consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States ensure that the service provider is not liable for the information transmitted, on condition that the provider does not initiate the transmission, does not select the receiver of the transmission; and, does not select or modify the information contained in the transmission.

Caching. Where an information society service consists of the transmission in a communication network of information provided by a recipient of the service, EU Member States ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on some conditions such as the provider does not modify the information and others.

Hosting. This information society service consists of the storage of information provided by a recipient of the service. Member States ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages is not aware of facts or circumstances from which the illegal activity or information is apparent; or the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

1.3 Obligation for providers to monitor transmitted or stored information

The national legislation does not explicitly include requirements and conditions on providers of eCommerce and other information services of transmission, caching and hosting, to monitor the information that they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity. The services providers have to give access to the information collected to the competent government bodies in order to detect any illegal activity. Types of illegal on-line activities are defined. The legislation establishes obligations for information society service providers to

communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

Information services providers have to ensure storage of personal data of data transmission and telematics services users ensuring comparison of user's network credentials with their personal data, and other data within one year after the date of rendering service.

The obligations for information society service providers to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service is not explicitly defined.

According to the Directive 2000/31/EC on electronic commerce Article 15, Member States shall not impose a general obligation on providers, when providing the services of transmission, caching and hosting, to monitor the information which they transmit or store, nor a general obligation to actively seek facts or circumstances indicating illegal activity.

So, the legislation of the Republic of Belarus is almost compliant with the EU best practices.

2. Consumer rights

2.1 Online trustmarks for retail websites

The country has not yet established a country-wide trustmark scheme(s) for electronic identification and trust services for electronic transactions which assure the trustfulness of qualified eCommerce service providers.

Most of the EU Member States have established their national online trustmarks. The European Commission is exploring the usefulness and benefits of the EU-wide trustmark schemes to reassure consumers on the reliability of accredited traders. The aim is to encourage the establishment of pan-EU price-comparison websites. Such certified sites will help consumers to make informed decisions when using online retail services.

In the EU member states there a laws on self-regulation that gives certain rights to the companies and associations. There is no such law in Belarus and the regulatory bodies are eager to draft and issue one, as extra means for consumer protection are needed due to the remoteness and the distance of eCommerce service providers.

2.2 Minimum general information to be provided by information society service provider

The national legislation imposes the obligation on the information service provider to render easily, directly and permanently accessible to both recipients of services and the competent authorities the defined scope of information about the service provider that is compliant with the EU best practices.

Moreover, Article 5 (Directive 2000/31/EC on electronic commerce) requires the online service provider to establish an effective direct communication channel with its customers. It imposes the obligation on the service provider to render "easily, directly and permanently accessible" to both recipients of services and the competent authorities "the details of the service provider, including its electronic e-mail address, which allow it to be contacted rapidly and communicated with in a direct and effective manner" (Directive 2000/31/EC on electronic commerce Article 5).

In this aspect, the legislation of Belarus does not impose such requirement. This information is important and may even be vital for customers claiming their rights.

2.3 Transparency of commercial communications information to be provided

The national legislation of Belarus imposes that advertisements on the Internet indicates natural or legal person responsible for commercial communication and any conditions attached to the offers. Both the commercial communication and the natural or legal person responsible for it should be clearly identifiable, and any conditions (price, delivery cost, delays of delivery, etc.) attached to the offers, discounts etc. must be easily accessible.

However, the legislation does not state the requirements for advertising originating from the operator of an online marketplace and displayed by a search operator. This type of advertising must always disclose both the identity of the online marketplace operator and the fact that the trademarked goods advertised are being sold through that online marketplace (Directive 2000/31/EC on electronic commerce Article 6).

2.4 Requirements for distance contracts and off-premises contracts

For distance (concluded online or by electronic means) or off-premises contract, the national legislation requires that the trader provides the consumer with a number of legally defined pre-contractual information. The categories of the required information fully comply with the requirements of the Directive 2011/83/EC on Consumer Rights.

However, the Directive also asks that before the consumer is bound by a distance or off- premises contract, the trader shall provide the consumer with the information required about obligation to pay. If a distance contract to be concluded by electronic means places the consumer under an obligation to pay, the trader shall make the consumer aware in a clear and prominent manner, and directly before the consumer places his order. The formal requirements for distance contract also include delivery restrictions applied and which means of payment are accepted.

It appears that these two conditions are not explicitly reflected in the legislation of Belarus.

2.5 Consumer protection international cooperation mechanisms

Consumer protection cooperation agreement is set up with the Eurasian Economic Union and CIS, but not the EU member states. Within the CIS, a national authority in a country where consumer interests are harmed can call on their counterpart in the country where the trader is located and ask for action to stop the infringement. Enforcement authorities can also alert each other to malpractices they have spotted which may spread to other countries. There are no information systems established for the exchange of information between competent authorities of different countries for consumer protection in eCommerce field.

2.6 Out-of-court dispute settlement

The national legislation of Belarus allows the use of out-of-court schemes for dispute settlement regarding provision of eCommerce services, including by appropriate electronic means, however, the only electronic means used for this purpose is the possibility to address electronically (by email or through website) the public agency and receive a response in electronic form. The country's legislation clearly defines the mechanisms of dispute resolution, in the event of disagreement between an information society service provider and the recipient of the service.

2.7 Online dispute resolution system for consumers for eCommerce transactions

There is no online dispute resolution platform through which parties can initiate alternative dispute resolution procedure in relation to disputes concerning online transactions. However, the national entities responsible for settling alternative disputes receive the complaint electronically (via email) and seek to resolve the dispute through existing legal alternative dispute resolution mechanisms.

In the EU, the current actions aim at exploring initiatives on consumer Alternative Dispute Resolution with a view to adopting directive on Alternative Dispute Resolution (ADR) and a regulation on Online Dispute Resolution. It proposes to establish an EU-wide Online Dispute Resolution system for cross-border eCommerce transactions by 2012 (Directive 2013/11/EU on alternative dispute resolution for consumer disputes). Through this website, parties can initiate ADR in relation to disputes concerning online transactions. National ADR entities will receive the complaint electronically and seek to resolve the dispute through ADR, using the ODR platform exclusively if they wish.

2.8 Requirements for sending of unsolicited commercial communication

The legal framework of Belarus allows the sending of unsolicited commercial communications by e-mail. It defines the requirements applied to information service providers and describes the rights of consumers. The requirements ensure that such communication is clearly and unambiguously identifiable, and that service providers respect the opt-out registration by which consumers (natural or legal persons) not wishing to receive such commercial communications can sign up.

3. Competition

3.1 Free movement of eCommerce services

In general, the country's legislation does not restrict the freedom to provide eCommerce services by a lawful service provider established in another country.

For cloud services provided to legal, natural entities and government organisations, the legislation imposes some requirements regarding place of storage of some type of data. So, in compliance with the Directive 2000/31/EC on electronic commerce Article 3, the national legislation of Belarus clearly defines the requirements for provision of eCommerce services on its territory for any service provider lawfully established in another country.

3.2 Authorisation to pursuit the activity of eCommerce service provider

The legal framework of Belarus ensures that the taking up and pursuit of the activity of an information society service provider, including eCommerce activities, is not a subject to prior authorisation. The country restricts starting of eCommerce activities by a condition of getting prior authorization in some particular sectors and for some products (medicine, arms, etc.).

However, legal bodies and individual entrepreneurs can perform their retail trade activities via online shops that have to be registered in the Trade Register of the Republic of Belarus. Information confirming the registration of an online shop in the Trade Register of the Republic of Belarus is submitted to a licensing authority.

In general, the legislation of Belarus is compliant with the Directive 2000/31/EC on electronic commerce Article 4 which defines the principle excluding prior authorisation to pursuit the activity of an information society service provider, excluding for activities covered by other legislations.

4. ePayment

4.1 Fees for the use of means of eCommerce payment

Some national legislation has been developed in regard of eCommerce payments by credit or debit card, on Internet, on phone, using mobile and other electronic payments. The explicit regulations on the fees for the use of certain means of payment (such as credit or debit cards, electronic valets) that prohibit traders from charging consumers excessive fees in respect of the use of a given means of payment could not have been found within this study.

The Directive 2011/83/EC on Consumer Rights defines the rules on the fees for the use of certain means of payment and prohibit traders from charging consumers, in respect of the use of a given means of payment, fees that exceed the cost borne by the trader for the use of such mean.

The legal framework of Belarus in the area of eCommerce payments is well defined. However, the rules on the fees for the use of means of payment are not explicitly stated.

4.2 Equal treatment between paper and electronic invoices

The national legislation assures equal treatment between paper and electronic invoices. It is possible to use eInvoicing by means of equal treatment of paper and electronic invoices only by signing electronic invoices with electronic digital signatures.

Technically, in Belarus, it is now only possible to use electronic bills signed by electronic digital signatures issued in Belarus. Neither EEU members (Russian, Kazakh) nor EU member states electronic bills are recognized.

There is no yet a single and clear national semantic data model and a common eInvoicing format facilitating semantic interoperability and ensuring technology neutrality to facilitate the uptake of eInvoicing for eCommerce transactions for SMEs.

5. eLogistics

5.1 Equal validity of electronic and offline contracts

The national legislation establishes the equal validity of electronic contracting and contract concluded offline. However, it does not defining the full scope of specific requirements to electronic contract.

The Directive 2000/31/EC on electronic commerce Articles 9-11 defines the fundamental principles of equal validity of electronic contracting and contract concluded offline. It also defines the requirements applied to an electronic contract: treatment of contracts, specific information to be provided, placing of orders. For the two last requirements, the legislation of Belarus does not comply with the Directive.

5.2 Conditions for the risk of loss of or damage to the goods

The national legislation defines the conditions for the risk of loss of or damage to the goods purchased. These legal provisions define the conditions for the risk of loss of or damage to the goods and responsibilities of the trader, the consumer, a third party indicated. It also stipulates the remedies available to consumers for damaged or faulty goods, entitlement of consumers to replacement or repair of goods, a refund or discount where specific circumstances apply. The above is compliant with the Directive 2011/83/EC on Consumer Rights.

However, the national legislation does not explicitly specify the conditions for the risk of loss of or damage to the goods purchased within eCommerce transaction and responsibilities of the parties involved. This is covered by the general consumer protection legal framework.

5.3 Rights on delivery of goods

The legislation does not define the time of delivery when the trader shall deliver the goods by transferring the physical possession or control of the goods to the consumer without undue delay, but not later than a defined maximum number of days from the conclusion of the contract (30 days in the EU according to the Directive 2011/83/EC on Consumer Rights). Time of delivery is not separately specified by legislation, but is defined by the contract terms.

The legislation does not clearly define the conditions when the trader fails to fulfil his obligations to deliver the goods at the time agreed, additional period of time and the right of the consumer to

terminate the contract and get reimbursement of all sums paid under the contract. It however stipulates a possibility to negotiate an additional period of time and the right of the consumer to terminate the contract and get reimbursement of all sums paid under the contract.

Georgia

Firms using their own Website - 49.4%

Firms using e-mail to communicate with clients/suppliers - 75.8%[91]

Internet hosts: 357,864 (2012)

Internet users: 1.3 million (2009)[92]

Relevant legislation

No National Legislation related particularly on E-commerce is in place.

Although initial provisions necessary for the development of E-commerce, such as E-signature, EID, are in place, the legislation is lacking major rules and regulation as per EU baseline, therefore harmonization obligation in the sphere of e-commerce is defined AA/DCFTA with implementation schedule of 3 years from 2016 (Chapter 6 Establishment, trade in services and electronic commerce).

Existing legislation in the field of intellectual property in Georgia is corresponding to European standards, which has been confirmed during the process of negotiations on Deep and Comprehensive Free Trade Area (DCFTA). The minor legislative amendments in the norms regulating execution in the field of intellectual property protection might be implemented. Accordingly, IPR regulations and standards seem to be well in place in Georgia. These regulations cover protection of both, digital as well as non-digital artefacts. Along the current activities of "Promote the strengthening of E-Governance in Georgia (E-Government Georgia)'s legal component, e-Commerce regulations are under construction.

Best practices

Electronic Auction

It was created the electronic auction system eauction.ge, by the initiative of Service Agency of Ministry of Finance[93], along with the Financial Analytical Service and from March of 2010 started realization of movable property seized to the state, by this form. Now public auctions and related problems are in the past. As a result of the simplified regime, the bureaucratic procedures have been reduced to a minimum.

Reforms turned out to be quite productive; the population quickly gets to grips with new and simple system. Since 2011 all state agencies and property management and property management portals has joined the agency's web page and the property will be managed through the Agency's web page. It has become universal portal, which united all kinds of property sale / privatization in one space. Web site has become very popular and highly rated in short time. After the state structures, individuals and legal persons had joined and started to movable and immovable property buy – sell through www.eauction.ge.

Nowadays, anyone can buy both, state and private-owned movable and immovable property in comfortable environment, without leaving home or office.

Virtual Zone

[91] World Bank - Enterprise Surveys: Georgia - 2013

[92] CIA World Factbook - https://www.cia.gov/library/publications/the-world-factbook/geos/ge.html

[93] http://seragency.gov.ge/en/content/about-us

The Status of the Virtual Zone is a license (permit) to carry out business activities in a Virtual Zone. Virtual Zone business is the activity of creation of IT systems in Georgia by a legal person.

Standards

In the component on interoperability, an analysis of existing standards for data exchange is performed and an eGeorgia interoperability framework is developed. Some standard specifications have been developed between the private and the public sector regarding G2B and B2G interactions.

Organisations involved

- The e-commerce is currently in the mandate of Ministry of Economic development and as noted below is part of the Association agreement
- Service Agency of Ministry of Finance
- Georgian National Communications Commission
- Georgia government administrations
- Office of the State Minister of Georgia on European and Euro-Atlantic Integration

National plans

Association Agreement between the European Union and Georgia / DCFTA

International agreements

Association Agreement between the European Union and Georgia / DCFTA

State of play description

1. Internet security and privacy

1.1 Allowance to process user traffic data

The Law on Protection of Personal Data prohibits retention of user specific personal data. Implementation of the law is monitored by the Personal Data Protection Inspector's office. The mandate of the office was extended and now covers both state and private sectors.

Decree of Georgian National Communications Commission of March 16, 2006 on protection of consumers' rights in the field of electronic communications obliges communication service providers to retain data for certain period for billing and interconnection purposes.

Processing of consumer data is allowed for billing and interconnection purposes, such data shall be possessed by an operator for the period defined by the Georgian National Communications Commission. Retention of any data beyond time and purpose limits, including metadata is prohibited.

Moreover, Personal Data protection Office has extended mandate to control and monitor actions of private companies and government agencies (for example ministry of Internal affairs, prosecutors office, etc) on access to personal information and communication means[94].

1.2 Specific liability regime for intermediary service providers

The current legal framework[95] does not define categories of online services and therefore any graded system of responsibilities. All telecom operators are subject to uniform regulation when concerned with information disclosure or protection of personal data.

[94] Statute on the Activities of and Procedure for Discharge of Powers by the Personal Data Protection Inspector

1.3 Obligation for providers to monitor transmitted or stored information

National Legislation does not specify any obligation of information service providers to monitor transmitted information. The only obligation set in the consumer's rights protection decree by GNCC puts an obligation to the providers of hosting and registrars on the provisioning of legal content i.e. the provider of such services shall monitor the content and take it down in case it violates the law incl. Copyrights[96]. This general regulation on hosting and web-service providers to monitor legality of the content placed has not been yet applied and is considered to be amended.

2. Consumer rights

2.1 Online trustmarks for retail websites

The country has not established any country-wide online Trust Mark.

2.2 Minimum general information by information society service provider

The obligation of electronic service providers to provide information to the national regulatory commission is set by the law on electronic communication and law of broadcasting. The obligation to provide information as well as procedures – timing and etc. is set by the National Communications Commission. Registry of Electronic service providers is available at web-site of Georgian National Communications Commission[97]. Registry contains contact information, type of authorisation and area of service provision. Apart from general registration info, the regulator is authorised to request any information upon its decision and operator has an obligation to provide (whether provided information is made public or confidential is based on the arguments of the provider and judgement of the regulator).

As for information service or e-commerce providers there is no specific regulation as such type of providers are not defined by the current legislation and regulations.

2.3 Transparency of commercial communications information to be provided

None of such regulations had been developed or imposed.

2.4 Requirements for distance contracts and off-premises contracts

Such regulations are not in place.

2.5 Consumer protection international cooperation mechanisms

No international cooperation in this field. The Association Agreement contains the set of eCommerce issues, including international cooperation issues, though no steps or actions were undertaken yet.

2.6 Out-of-court dispute settlement

There are no out-of court dispute mechanisms available for eCommerce services. There are no explicit legal provisions in the national legislation for out-of-court dispute mechanisms for traditional

---

[95] Law on Protection of Personal Data; Statute on the Activities of and Procedure for Discharge of Powers by the Personal Data Protection Inspector; Decree of Georgian National Communications Commission of March 16, 2006 on protection of consumers right in the field of electronic communications

[96] One of ISPs, namely Silknet, has appealed to GNCC to rule against competitors placing illegal content (movies and other media) on the sites hosted and registered by competitors

[97] www.gncc.ge

commerce services. The telecommunications regulatory commission has a dispute resolution function as well. Arbitration is also available for general matters.

2.7 Online dispute resolution system for consumers for eCommerce transactions

No system in place.

2.8 Requirements for sending of unsolicited commercial communication

Personal Data Protection law gives general definition that any provider – sender of commercial – marketing information message shall also provide means to unsubscribe from such notifications. Such regulation has only been implemented in case of SMS marketing services. The regulation shall further be extended to eCommerce area.

3. Competition

3.1 Free movement of eCommerce services

Provision of telecom service by companies not registered in Georgia, virtually or online is not prohibited or regulated. For the entities providing service on the territory of Georgia authorization is required, which is a mere registration. Regulations about eCommerce activities are not in place.

3.2 Authorisation to pursuit the activity of eCommerce service provider

There is no legislation on eCommerce services.

4. ePayment

4.1 Fees for the use of means of eCommerce payment

Since there is no legislation on e-commerce, there are no rules about limitation of fees.

4.2 Equal treatment between paper and electronic invoices

eInvoicing in common data format has been introduced by the Revenue Service of the ministry of Finance[98] in 2010. It has a common format and has equal treatment to paper invoices.

Georgia has developed and implemented an entire public finance management information structure, which is shared between different government entities. eInvoicing is active part of this system has been established from 2010 and is fully implemented both in public and private sectors. The Public Finance Management System (PFMS) consists of a number of subsystems, each of it with a specific purpose (including eProcurement – a central unified platform for tendering and procuring goods, services and works for procuring entities as set by the Public Procurement Law, including central and local government bodies);

5. eLogistic

5.1 Equal validity of electronic and offline contracts

The law on electronic signature and electronic document specifies the equal validity of electronic and offline contracts (planned amendments bring current law into full compliance with Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC).

[98] www.rs.ge

5.2 Conditions for the risk of loss of or damage to the goods

No specific regulations are in place for the loss or damage of the good purchased through eCommerce.

5.3 Rights on delivery of goods

No legislation on the requirement for the delivery of goods purchase through eCommerce is available.

Gap analysis

1. Internet security & privacy

1.1 Allowance to process user traffic data

Some regulations are in place regarding processing (billing and interconnection purposes) of user traffic and personal data. However, the national legislation does not explicitly define the rules of processing of user traffic data by providers of an electronic communication service for the purposes of marketing electronic communications services or for the provision of value added services.

1.2 Specific liability regime for intermediary service providers

The national legislation does not define specific liability regimes for three categories of online service providers: transmission conduit operators, caching providers and hosting services providers.

1.3 Obligation for providers to monitor transmitted or stored information

In general, the national legislation does not define the requirements on information services providers to monitor information transmitted in order to detect illegal activities and to inform the competent public authorities (except for hosting providers to monitor the IPR infringements).

2. Consumer rights

2.1 Online trustmarks for retail websites

The country has not established any country-wide trustmark scheme(s) for electronic identification and trust services for electronic transactions which assure the trustfulness of qualified eCommerce service providers.

2.2 Minimum general information to be provided by information society service provider

The national legislation related to advertisements on the Internet is not in place. There are no explicit requirements that advertisements on the Internet indicates natural or legal person responsible for commercial communication and any conditions attached to the offers.

2.3 Transparency of commercial communications information to be provided

The national legislation does not impose that advertisements on the Internet indicates natural or legal person responsible for commercial communication and any conditions attached to the offers.

2.4 Requirements for distance contracts and off-premises contracts.

For distance (concluded online or by electronic means) or off-premises contract, the national legislation does not require that the trader provides the consumer with a minimum of legally defined pre-contractual information and comprehensive explanation of contractual terms.

2.5 Consumer protection international cooperation mechanisms

The country has not established international cooperation mechanisms between the national public authorities and the authorities of other countries who are responsible for enforcement of consumer protection laws, including for eCommerce.

2.6 Out-of-court dispute settlement

The national legislation does not explicitly allow the use of out-of-court schemes for dispute settlement regarding provision of eCommerce services (except for telecommunications), including by appropriate electronic means. This area can be however covered by the general regulations on arbitration.

2.7 Online dispute resolution system for consumers for eCommerce transactions

Georgia does not have an online dispute resolution platform through which parties can initiate alternative dispute resolution in relation to disputes concerning online transactions.

2.8 Requirements for sending of unsolicited commercial communication

The law defines overall requirement, but the national regulations do not define the requirements applied to sending of unsolicited commercial communications by e-mail.

3. Competition

3.1 Free movement of eCommerce services

The national legislation does not explicitly restrict the freedom to provide eCommerce services compliant to the national laws by a lawful service provider established in another country. However, for the entities providing service on the territory of Georgia an authorization is required.

3.2 Authorisation to pursuit the activity of eCommerce service provider

There are no explicit requirements for a prior authorisation to pursuit the activity of eCommerce service provider.

4. ePayment

4.1 Fees for the use of means of eCommerce payment

The national legislation does not define the requirements for eCommerce payments and does not define the rules on the fees for the use of means of electronic payment.

4.2 Equal treatment between paper and electronic invoices

The national legislation assures equal treatment between paper and electronic invoices (eInvoices) and defines the framework of a common national data model of e-invoicing format.

5. eLogistics

5.1 Equal validity of electronic and offline contracts

The national legislation establishes the equal validity of electronic contracting and contract concluded offline. However, the specific requirements to electronic contract have to be verified.

5.2 Conditions for the risk of loss of or damage to the goods

The national legislation does not define the conditions for the risk of loss of or damage to the goods purchased within eCommerce transaction and responsibilities of the parties involved.

5.3 Rights on delivery of goods

The national legislation does not define the requirements for time of delivery of goods purchased through eCommerce transaction.

Moldova

Firms using their own Website - 58.7%

Firms Using Email to Communicate with Clients/suppliers - 65.8%99

Internet hosts: 711,564 (2012)

Internet users: 1.333 million (2009)[100]

Relevant legislation

The existing national legal framework related to eCommerce area:

- Law no.133 of 8 July 2011 on personal data protection
- Law no.1069 on informatics
- Law no.284 of 22.07.2004 on eCommerce
- Law no.241 of 15.11.2007 on electronic communications
- Law no.38 of 29.02.2008 on protection of trademarks
- Law no.114 of 29.02.2012 on payment services and electronic money
- Law no.105 of 13.03.2003 on consumer rights
- Law for approving the National Development Strategy of the Personal Data Protection domain for the years 2013-2018 and the Action Plan for its implementation

Nevertheless, these acts require revision, in particular in line with the EU legal framework mentioned in the Actions Plan on implementation of the Association Agreement between the European Union and Moldova.

ICT platforms

- Government Decision no.128 of 20.02.2014 on M-Cloud platform
- Government Decision no 280 of 24.4.2013 on M-Pay platform
- Pilot project on e-Invoice
- M-Sign (mobile signature)
- M-log service
- Authentication and control access (M-Pass)

National plans

It is planned to amend the Law no.284/2004 on e-Commerce in line with the EU legal framework in the area of e-commerce. The timeframe to elaborate the draft law is the end of 2015 when it should be presented to the Parliament.

In this context, on 12.03.2015, the Minister of Economy issued the Order no.32 to create working groups by sectors to amend the national legal framework. The national legal framework will be elaborated in line with the EU legislation. The task for this working group is to examine the national

[99] World Bank - Enterprise Surveys: AZERBAIJAN - 2013

[100] CIA World Factbook - https://www.cia.gov/library/publications/the-world-factbook/geos/aj.html

legal framework in the area of electronic commerce to elaborate the concept for amending the legal framework in the area of e-commerce and the relevant areas. The working group shall analyze the national legal and regulatory framework in line with provisions of the Title V of the Government Decision no.808 of 7.10.2014. Members of the working group “Services and Free Movement of Capital”, that will focus on e-Commerce related subjects, are: Ministry of Economy, State Chancellery, e-Government Centre, Ministry of Information Technology and Communication, National Regulatory Agency for Electronic Communication and Information Technology of Moldova, National Bank of Moldova, Ministry of Finance, National Agency for Intellectual Property, Consumer Protection Agency, National Centre for Personal Data Protection.

At present, the Ministry of Economy has elaborated the draft law on consumer rights to conclude contracts, which transposes the EU legal framework on consumer rights, namely Directive no.83/2011. Both the EU directive and this draft law include requirements regarding distance contracts and off-premises contracts. At present, this draft is being consulted and in April it will be examined by the Government.

On 26.02.2015, the Government adopted the Decision no.16 on Harmonisation of the National Legislation for 2015. According to this Decision, a number of relevant directives will be transposed in the national legislation.

The Ministry of Economy intends to elaborate a questionnaire to submit to the private sector and civil society to request their opinion on obstacles concerning the electronic transactions.

What concerns resources to implement the Digital Market Agenda, including areas discussed in the questionnaire, they are limited. Moreover, expertise in the relevant areas is limited. Thus, further assistance will be necessary for successful implementation of the eCommerce related projects.

Digital Moldova 2020 Strategy (although planned in the action plan for implementation of this security, no policy document on this matter has been drafted, yet)

Program on e-Transformation

According to the new Activity Program of the Government of the Republic of Moldova for 2015-2018, the Government aims to build a civic society and a nation based on the European social model, contributing to the development of information technology and electronic services by supporting the creation of scientific-technological parks.

Government Decision no.16 of 26.02.2015 on Harmonisation of the National Legislation for 2015. According to this Decision, a number of relevant directives will be transposed in the national legislation. (p. 44 mentions Directive 2002/58/CE)

International agreements

On 7 October 2014, the Government adopted the Decision no.808 on approval of the National Action Plan for implementation of the Association Agreement Republic of Moldova EU in 2014-2016. Title V of this Action Plan is entitled Commerce and Aspects related to Commerce.

Moldova will transpose objectives included in a number of acts, including Directive 2000/31/EC. in particular, it was planned for 2014 that the Ministry of Economy and the Ministry of Information technology and Communication will draft the law on distance contracts (including eCommerce) (page 216 and the paragraph is 102). It has not been elaborated, yet.

Moreover, the same act states that the Government will transpose objectives of the Directive 2002/58 on ePrivacy. The ePrivacy Directive is also mentioned in the Action Plan for Harmonization of the

National legislation for 2015 (p.44 mentions Directive 2002/58/CE) Additionally, it is mentioned that the secondary acts to implement the Law no.91 of 29.05.2014 on eSignature and eDocument will be adopted in 2015.

State of play description

1. Internet security and privacy

1.1 Allowance to process user traffic data

Currently, neither the Law No.241 of 15.11.2007 “On electronic communications” nor the Law No.284 of 22.07.2004 “On electronic commerce” regulate the processing of user traffic data by the provider of an electronic communication service for the purposes of marketing electronic communications services or for the provision of value added services.

The Action Plan for the implementation of the Association Agreement between the European Union and the Republic of Moldova stipulates that the provisions of the Directive 2002/58/EC will be implemented by June 16, 2017. This particularly concerns implementing the country’s current regulation to ensure protection of fundamental rights and freedoms, in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and ensuring the free movement of such data and of electronic communication equipment and services.

The National Development Strategy of the Personal Data Protection Domain for the years 2013-2018 and the Action Plan for its implementation adopted by Law no.229 of 10.10.2013 plans the amendment in 2014 of the normative framework and revision of the national legislation in the area of electronic communication for the implementation into the national legal system of the specific rules of the European acquis for the telecommunication sector referring to the processing of personal data and protection of confidentiality in the electronic communication sector.

1.2 Specific liability regime for intermediary service providers

The Law No.241 “On electronic communications” does not define specific liability regime for intermediary service providers for the information transmitted in a communication network of information provided by a recipient of the service.

The Association Agreement between the EU and the Republic of Moldova stipulates the approximation by 16 June 2017 of the Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce. In particular, the following provisions of that Directive shall apply: harmonising limitations to liability of service providers acting as intermediaries when providing mere conduit, caching or hosting, stipulating no general obligation to monitor.

1.3 Obligation for providers to monitor transmitted or stored information

Intermediary service provider in eCommerce is not required to monitor and verify the accuracy of the transmitted, received and stored electronic documents and e-mails, as well as their compliance with the law, unless otherwise provided by the contract entered into by him with the participants of eCommerce, or the law (Art 12, Law No.284 of 22.07.2004 “On electronic commerce”).

2. Consumer rights

2.1 Online trustmarks for retail websites

The laws of Moldova do not specify the creation of the country-wide trustmark schemes that help to reassure consumers on the reliability of accredited online traders and service providers. In this context, on Minister of Economy has formed a sector working groups created to implement the action

plan adopted by Government Decision no. 808. Currently, some eCommerce websites established on the territory of the Republic of Moldova use online seals and SSL protection provided by foreign providers. The Certification Authority (Special Telecommunications Centre, a Public Key Certification Authority) is delegated to issue SSL certificates from Unizeto and Symantec that are recognized by the most of the browsers and insure high level of security[101].

2.2 Minimum general information by information society service provider

eCommerce service providers are obliged to provide to other subjects of eCommerce interaction, as well as to state control bodies, appropriate access to reliable information about themselves in electronic form in the Moldovan language, and if necessary, in other languages (Law No.284 of 22.07.2004 "On electronic commerce", Art 11).

2.3 Transparency of commercial communications information to be provided

The Law N1227 "On advertisement" does not specify any requirements to the advertisement on the Internet. The Law No.284 of 22.07.2004 "On electronic commerce" Art 11(2) defines that outgoing advertisement from the eCommerce service provider about the proposed goods, works or services must be submitted in electronic form that allows reproducing the information without distortion, and making a fair presentation of the eCommerce service provider. Advertisement also has to offer clear information about goods, works or services, prices and tariffs and their conditions of sale, execution or provision.

2.4 Requirements for distance contracts and off-premises contracts

The Law No.284 of 22.07.2004 "On electronic commerce" Chapter IV defines the general requirements applied to distance (concluded online or by electronic means) contract and minimum of legally defined pre-contractual information. If a distance contract to be concluded by electronic means places the consumer under an obligation to pay, the law indicates that the trader shall be required to make the consumer aware in a clear and prominent manner, and directly before the consumer places his order.

In addition, the Action Plan to implement the Association Agreement between the EU and the Republic of Moldova stipulates the approximation by 16 June 2017 of the Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce. In particular, the following provisions of that Directive shall apply: enhancing development of e-commerce; removing barriers to the cross-border provision of information society services; providing legal security to providers of information society services.

2.5 Consumer protection international cooperation mechanisms

No evidence about international cooperation between Moldovan other countries in the area of consumer protection has been presented by the Ministry of Economy. The general cooperation framework with the EU, including trade, is set up in the Association Agreement between the European Union and the Republic of Moldova.

2.6 Out-of-court dispute settlement

The country's legislation does not define the mechanisms of dispute resolution, in the event of disagreement between an information society service provider and the recipient of the service (Law N241 "On electronic communication", law No.284 of 22.07.2004 "On electronic commerce"). The

[101] https://pki.cts.md/en/services/servers-certificates.html

legislation does not include prerequisites for the use of out-of-court schemes, available under national law, for dispute settlement, including by appropriate electronic means.

The Action Plan to implement the Association Agreement between the EU and the Republic of Moldova stipulates the approximation by 16 June 2017 of the Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce. In particular, the following provisions of that Directive shall apply: enhancing development of e-commerce, removing barriers to the cross-border provision of information society services.

2.7 Online dispute resolution system for consumers for eCommerce transactions

No online dispute resolution system for eCommerce transactions has been deployed.

2.8 Requirements for sending of unsolicited commercial communication

Sending commercial messages by e-mail (unsolicited commercial communication) is prohibited, except in cases where the recipient previously agreed to receive such communications (Law N284 “On electronic commerce” Art 17). Any person has the right to opt out of receiving commercial messages. The law defines the requirements applied to information service providers and describe the rights of consumers. This ensure that such communication is clearly and unambiguously identifiable, legal or natural person sending unsolicited commercial communication is clearly indicated, conditions of promotions and discounts are described, act.

3. Competition

3.1 Free movement of eCommerce services

The subjects of eCommerce can be physical and legal entities, including foreign ones, regardless of the type of ownership and organizational - legal form, as well as the state as a legal entity. Participation in e-commerce, unless otherwise provided by contract or by law, cannot serve as a basis for establishing additional requirements, procedures or restrictions on entrepreneurial activity (Law N284 “On electronic commerce” Art 7).

3.2 Authorisation to pursuit the activity of eCommerce service provider

eCommerce activities can be carried out by economic actors in accordance with the law the right to engage in entrepreneurial activity. The right to carry out eCommerce activities arises from the date of state registration of the legal entity or individual entrepreneur, except in cases provided by the Law on regulation of entrepreneurial activity by licensing. If the items for sale, works or services must obtain a license or permit, eCommerce can be carried out after obtaining a license or authorization to engage in the relevant activity (Law N284 “On electronic commerce” Art 9).

4. ePayment

4.1 Fees for the use of means of eCommerce payment

The national legislation does not define the requirements for eCommerce payments and the rules on the fees for the use of means of electronic payment. Nevertheless, the Action Plan for implementation of the Association Agreement between the EU and the Republic of Moldova stipulates the approximation by 16 June 2017 of the Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce. In particular, the following related provisions of that Directive shall apply: enhancing development of e-commerce; removing barriers to the cross-border provision of information society services.

4.2 Equal treatment between paper and electronic invoices

The national legal framework stipulates that the handwritten signature is equivalent with the electronic one. However, there is no mechanism in place to verify that the invoice was signed by authorized person. It is not mandatory for everyone to sign electronically. Considering that, the legal framework requires on certain occasions to apply the stamp, even if documents are signed electronically they have to be printed put and stamped. The mechanism in this and related areas need to be put in place. Infrastructure is required to be implemented. The secondary legal acts needs to be revised. The secondary acts (including the technical provisions) to implement the Law no.91 of 29.05.2014 on eSignature and eDocument will be elaborated and adopted in 2015. It is not clear who has the mandate to monitor and verify application of the electronic signature.

Launched on February 11, 2014, the eInvoice service[102] represents a software solution designed for the economic agents from Moldova in terms of bills and invoices' development and electronic circulation. For using the eInvoice service, the user must be in possession of a digital (mobile) signature issued by an accredited certification centre.

5. eLogistic

5.1 Equal validity of electronic and offline contracts

Electronic contract consists of an offer and an acceptance. Legal force of electronic contract is equivalent to a contract drawn up in writing and signed by the parties, including those certified by the seal of the parties. Electronic contract on the probative value equivalent to a written contract. The legislation explicitly describes the cases when a contract cannot be signed in electronic format. Also, the provisions indicates requirements which are compulsory to include in electronic contract activity (Law N284 "On electronic commerce" Art 20). Nevertheless, pursuant to the Government Decision no. 808 of 7.10.2014 on approval of the National Action Plan on Implementation of the Association Agreement between RM-EU for 2014-2016 provisions of this legislative act was planned to be revised.

5.2 Conditions for the risk of loss of or damage to the goods

The legislation does not define the conditions for the risk of loss of or damage to the goods and responsibilities of the trader, the consumer, a third party indicated by the consumer, or the carrier. It does not stipulate the remedies available to consumers for damaged or faulty goods, entitlement of consumers to replacement or repair of goods, a refund or discount where specific circumstances apply.

5.3 Rights on delivery of goods

The current legislation only stipulates that electronic contract must contain the following prerequisites: conditions of declining the transaction, the procedure and terms of performance (Law N284 "On electronic commerce" Art 20).

The legislation does not define the requirements on the time of delivery when the trader shall deliver the goods by transferring the physical possession or control of the goods to the consumer. The legislation does not define the conditions when the trader fails to fulfil his obligations to deliver the goods at the time agreed, additional period of time and the right of the consumer to terminate the contract and get reimbursement of all sums paid under the contract.

Gap analysis

[102] http://egov.md/index.php/en/for-business/e-invoice#.VRE4lTSsVQc

1. Internet security & privacy

1.1 Allowance to process user traffic data

The national legislation does not explicitly define the rules of processing of user traffic data by the provider of an electronic communication service for the purposes of marketing electronic communications services or for the provision of value added services.

For the purpose of marketing electronic communications services or for the provision of value added services, the legislation should allow the provider of an electronic communications service processing the data to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes of subscriber billing and, prior to obtaining consent, for the purposes of marketing electronic communications services or the provision of value added services (Directive 2002/58/EC on privacy and electronic communications Article 6).

1.2 Specific liability regime for intermediary service providers

The national legislation does not define the overall degree of liability of the eCommerce intermediary service providers for the information transmitted in a communication network of information provided by a recipient of the service. It does not explicitly define specific liability regimes for three categories of online service providers: transmission conduit operators, caching providers and hosting services providers. The Directive 2000/31/EC on electronic commerce Articles 12-15 introduced a specific liability regime for three categories of services.

1.3 Obligation for providers to monitor transmitted or stored information

The Law “On electronic commerce” does not impose general obligations on information services providers to monitor information transmitted in order to detect illegal activities and to inform the competent public authorities. This is in accordance with the Directive 2000/31/EC on electronic commerce Article 15 that requires that the states dot not impose a general obligation on providers, when providing the services of transmission, caching and hosting, to monitor the information which they transmit or store, or a general obligation to actively seek facts or circumstances indicating illegal activity.

2. Consumer rights

2.1 Online trustmarks for retail websites

The country has not established country-wide trustmark scheme(s) for electronic identification and trust services for electronic transactions which assure the trustfulness of qualified eCommerce service providers. The Association Agreement between the EU and the Republic of Moldova does not include any approximation requirements regarding the Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market –eIDAS. Article 23 eIDAS by 1 July 2015 implementing act to provide for specifications with regard to the form, and in particular the presentation, composition, size and design of the EU trust mark for qualified trust services.

2.2 Minimum general information to be provided by information society service provider

The national legislation imposes the obligation on the information service provider to render easily, directly and permanently accessible to both recipients of services and the competent authorities the

defined scope of information about the service provider. In addition to the basic requirements of the Directive 2000/31/EC on electronic commerce Article 5, the information should include the following information: number and dates of validity of available licences, organisation(s) which issued licences, conditions of delivery and its price.

2.3 Transparency of commercial communications information to be provided

The requirements emphasising the need for transparency when advertisements are displayed on the Internet are generally provisioned in the legislation. It obliges to ensure that online commercial communications meet certain transparency requirements. Both the commercial communication and the natural or legal person responsible for it must be clearly identifiable, and any conditions attached to the offers, discounts etc. must be easily accessible. However, the legislation is not explicit about the specific requirements to the different types of commercial communications on the Internet such as promotional offers, discounts, premiums, promotional competitions or games.

2.4 Requirements for distance contracts and off-premises contracts

For distance (concluded online or by electronic means) or off-premises contract, the national legislation requires that the trader provides the consumer with a minimum of legally defined pre-contractual information and comprehensive explanation of contractual terms. These requirements are compliant with the corresponding provisions of the Directive 2011/83/EC on Consumer Rights. However, the compliance of the requirements for delivery restrictions applied and which means of payment are accepted should be further evaluated.

2.5 Consumer protection international cooperation mechanisms

The country has not yet established any international cooperation mechanisms between the national public authorities and the authorities of other countries that are responsible for enforcement of consumer protection laws, including the legal framework on eCommerce.

2.6 Out-of-court dispute settlement

The national legislation does not explicitly allow the use of out-of-court schemes for dispute settlement regarding provision of eCommerce services. The Directive 2000/31/EC on electronic commerce Article 17 instructs that in the event of disagreement between an information society service provider and the recipient of the service, their legislation does not hamper the use of out-of-court schemes, available under national law, for dispute settlement, including appropriate electronic means.

2.7 Online dispute resolution system for consumers for eCommerce transactions

The country has not yet deployed an online dispute resolution platform through which parties can initiate alternative dispute resolution in relation to disputes concerning online transactions.

2.8 Requirements for sending of unsolicited commercial communication

The national legislation clearly defines the requirements applied to sending of unsolicited commercial communications by e-mail.

3. Competition

3.1 Free movement of eCommerce services

The country's legislation does not restrict the freedom to provide eCommerce services by a provider from another country. The country ensures that eCommerce services provided by a service provider established on its territory comply with the national provisions.

3.2 Authorisation to pursuit the activity of eCommerce service provider

The legal framework of the country ensure that the taking up and pursuit of the activity of an information society service provider, including eCommerce activities, may not be made subject to prior authorisation or any other requirement having equivalent effect. The legislation restricts starting of eCommerce activities by a condition of getting prior authorization in some particular sectors or for some products. This fully complies with the provisions of the Directive 2000/31/EC on electronic commerce Article 4.

4. ePayment

4.1 Fees for the use of means of eCommerce payment

The national legislation does not define the requirements for eCommerce payments and the rules on the fees for the use of means of electronic payment. Current practice on the fees for the use of certain means of payment does not prohibit traders from charging consumers excessive fees in respect of the use of a given means of payment.

The legal framework needs to be revised to encourage sellers to move online. For example, the commission for selling goods online is minimum 2% and it has to be paid by the seller. This is the reason why sellers prefer to sell goods offline where people can pay by cash. A common practice, where 0% commission for cash withdraw, is used by banks. According to statistics, per year per person, there are 2.6 transactions.

4.2 Equal treatment between paper and electronic invoices

The national legislation assures equal treatment between paper and electronic invoices (e-invoices). However in the practice, management of companies can sign electronically, but then they print out documents and submits them further to authorities on paper. Otherwise, they are not accepted by some of public administrations. People may see the electronic signature as additional cost whereas the handwritten one is free. Thus, the legal framework needs to be revised in order to enforce the application of the laws. There is no defined framework of a common national data model of eInvoicing format (to confirm).

5. eLogistics

5.1 Equal validity of electronic and offline contracts

The national legislation establishes the equal validity of electronic contracting and contract concluded offline together with defining the specific requirements to electronic contract.

The national legal framework regulates electronic signature. There are at least 3 centres in the country, which offer the electronic signature, so most of the persons have to use at least 3 different types of electronic signatures depending of the document what is signed. For example, banks have their own procedure in this regard. The legal framework requires application of timestamp and it needs to be revised. Currently, it is not possible to submit contracts concluded online to some authorities. For example, the fiscal inspectorate requires stamped and signed documents. Mechanisms to verify transactions also need to be revised, as it is not duly finalised.

5.2 Conditions for the risk of loss of or damage to the goods

The national legislation does not define the conditions for the risk of loss of or damage to the goods purchased within eCommerce transaction and responsibilities of the parties involved. Pursuant to the Directive 2011/83/EC on Consumer Rights, the recommendable conditions are as follow: the delivery of goods within a minimum of 30 days from execution of sale contract; seller bears risk of

loss/damage until goods are received by consumer; automatic right of refund within 7 days of non-delivery. The missing provisions also concern the standardisation of the remedies available to consumers for damaged or faulty goods. Consumers should be entitled to replacement or repair in the first instance and a refund or discount only where specific circumstances apply.

5.3 Rights on delivery of goods

The national legislation of Moldova does not define the requirements for time of delivery of goods purchased through eCommerce transaction. According to the Directive 2011/83/EC on Consumer Rights, the rules on delivery define the requirements for time of delivery. Unless the parties have agreed otherwise on the time of delivery, the trader shall deliver the goods by transferring the physical possession or control of the goods to the consumer without undue delay, but not later than a maximum number of days from the conclusion of the contract (30 days by the Directive). It also should clearly define the conditions when the trader fails to fulfil his obligations to deliver the goods at the time agreed, additional period of time and the right of the consumer to terminate the contract and get reimbursement of all sums paid under the contract (need to be confirmed).

Ukraine

Firms using their own Website - 55.3%

Firms Using Email to Communicate with Clients/suppliers - 87.9%[103]

Internet hosts: 2.173 million (2012)

Internet users: 7.77 million (2009)[104]

eCommerce is one of the top fastest growing economic sectors in the country. There are at least 7 - 8 thousand online stores. The annual turnover has increased by 45%.

It is difficult to exactly evaluate the amount of players involved in eCommerce activities. There are over 7 to 8 thousand online stores according to bigmir.net. Top 300 of them controls 80% of the market. Only platform prom.ua hosts eShops of 481 771 companies with the total catalogue of 21 950 835 products and services.

Relevant legislation

There's no specific legislation currently covering the area of eCommerce. The related legislation is:

- Draft law "On Electronic Commerce"[105]
- Law of Ukraine "On Personal Data Protection"[106]
- Law "On Telecommunications"
- Law "On advertising"
- Law "On Consumer Protection"[107]
- Government Resolution № 295 «On rules of providing telecom services"

Art. 702 of the Civil Code of Ukraine from 16.01.2003, Number 435-IV stipulates that the goods can be sold by descriptions, catalogue, via the Internet etc. and there should be a contract of sale to confirm transaction. The terms of selling goods are defined for trade at distance or outside of office premises (from 19.04.2007 p. № 103). Companies may sell goods by order using remote connection. It defines the range of goods sold by order and outside of trade or business premises The document also describes the procedure for termination of contract concluded on distance.

Order of the Ministry of Health of Ukraine "Licensing terms for economic activity of drug, wholesale and retail of medical products" from 31.10.2011 g. № 723. It specifies that the medicine is the only prohibited goods for online sales.

Standards

- National Standard of Ukraine ISO 4303: 2004 "Retail and Wholesale. Terms and definitions". Terms of retail of products are approved by the Ministry economy of Ukraine on 19.04.2007 p. № 104.

[103] World Bank - Enterprise Surveys: Ukraine - 2013

[104] CIA World Factbook - https://www.cia.gov/library/publications/the-world-factbook/geos/up.html

[105] http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=52409

[106] http://zakon4.rada.gov.ua/laws/show/2297-17

[107] http://zakon4.rada.gov.ua/laws/show/1023-12

- Terms of selling in retail of food products, approved by the Ministry of economy in Ukraine from 11.07.2003, № 185.
- The conditions of conducting trading activities and rules of trade of services in consumer market were approved by the Cabinet of Ministers of Ukraine on 15.06.2006 p. № 833.

Organisations involved

Ministry of Economic Development and Trade of Ukraine. The recently formed in April 2015 a department of Digital Economy currently develops an Actions Plan and priorities.

Verkhovna Rada Committee on Financial Policy and Banking, Subcommittee on Securities, Stock Market, Credit Rating Agencies and e-commerce[108]. The Committee is a body of the Verkhovna Rada of Ukraine and consists of the elected Deputies. They are responsible for drafting of proposals, preparation and preliminary consideration of issues, implementation of measures, and control functions in certain areas. Key functions in relation to HDM: 1) Drafting of regulations and other acts; 2) preliminary consideration and preparation of opinions and proposals for the regulations.

State Agency on e-government affairs of Ukraine[109]**.** Agency is a central body of executive power, supervised by the Cabinet of Ministers of Ukraine, and directed by the Vice Prime Minister of Ukraine. The Agency implements state policy in the field of information, e-governance, development and use of national electronic information resources, development of the information society. One of the main objectives is the development of e-business. The Agency cooperate with technology companies that assure the development and application of technologies, e-commerce tools, use of digital signature and information security, implementation of remote services in the banks, continued integration of the national payment system with international payment systems.

National plans

Preparation of Digital Agenda is responsibility of the Ministry of Economy. Draft has not yet been prepared.

International agreements

The Association Agreement between the European Union and Ukraine

State of play

1. Internet security and privacy

1.1 Allowance to process user traffic data

The Law of Ukraine “On Personal Data Protection” regulates legal relations related to the protection and processing of personal data and aims to protect fundamental rights and freedoms of citizens, including the right to privacy in connection with the processing of personal data.

According to the Law, subscriber gives his/her perpetual consent for processing of the personal data. This is confirmed by subscriber in the agreement (for registered subscribers - in documents issued at registration), as well consignment about transfer of information from a special database containing personal data to third parties in accordance with applicable law.

1.2 Specific liability regime for intermediary service providers

[108] http://komfinbank.rada.gov.ua/komfinbank/control/uk/publish/article?art_id=46799&cat_id=44832%27

[109] http://dknii.gov.ua/

The current national legislation does not provide the specific liability regime for transmission conduit operators, caching providers and hosting services providers.

The purpose of the Law of Ukraine “On Telecommunications” is to ensure the provision of universal telecommunication service of sufficient range, volume and quality, promoting market economy, effective functioning of an open and fair competitive market. The law defines the principles of consumer protection and controlling of the telecommunications market by the state.

Ukraine’s Parliament will consider in the second reading the draft law “On Electronic Commerce”. The draft law describes the basic principles of the market regulation, the rights and obligations of the online vendors and their customers, differentiates responsibilities of good’s sellers, service providers of intermediate character such as Internet access, hosting, and domain name registrars.

1.3 Obligation for providers to monitor transmitted or stored information

Security Service of Ukraine to have the right to monitor transmitted or stored information. All providers and operators are required to provide lawful interception and link up to the SSU’s systems.

2. Consumer rights

2.1 Online trustmarks for retail websites

Not implemented. Absence of mechanism of defining eligibility criteria. The national legislation does not regulate this.

2.2 Minimum general information by information society service provider

The Law “On advertising” regulates the requirements on minimum general information to be by indicated by information society service provider.

2.3 Transparency of commercial communications information to be provided

The Law “On advertising” doesn’t regulate aspects in reference to natural persons.

2.4 Requirements for distance contracts and off-premises contracts

The law of Ukraine “On Consumer Protection” regulates relations between consumers of goods and services, and manufacturers and sellers of goods, executors and service providers of different ownership, establishes the rights of consumers and providing the mechanism for their protection and the basis of state policy in the field of consumer protection.

The legislation is not explicit about requirements for distance (concluded online or by electronic means) or off-premises contract.

2.5 Consumer protection international cooperation mechanisms

Consumer protection aspects are covered by the EU-Ukraine Association agreement. The Action plan of consumer rights protection to meet the EU Decrees requirements has been developed by the Ministry of Economy (deadline – 2nd half 2016).

2.6 Out-of-court dispute settlement

Out-of-court dispute settlement is not explicitly regulated by the current legislation. However, some basic principles will be reflected in the draft of the Law on eCommerce.

2.7 Online dispute resolution system for consumers for eCommerce transactions

The Government Resolution № 295 «On rules providing telecom services” includes an obligation about dispute resolution (art.40) and obligations of the service providers in case of now quality of their

services to del through the court system.

An online application mechanism for submission of claims is available.

2.8 Requirements for sending of unsolicited commercial communication

The Government Resolution № 295 «On rules providing telecom services". There is an obligation not to spread spam.

3. Competition

3.1 Free movement of eCommerce services

Not explicitly covered by the legislation.

3.2 Authorisation to pursuit the activity of eCommerce service provider

As there is no specific legislation to regulate e-Commerce activities, all preliminary approvals are required in a similar way as it to any other commercial activities in some sectors.

4. ePayment

4.1 Fees for the use of means of eCommerce payment

The topic has not yet been addressed in the current legislation. Potentially it can be covered with the specific Action Plan for EU standard on financial services and payments (EU-Ukraine Association Agreement Action Plan, item 136 – deadline March 2015, responsible – Ministry of Finance with participants, including National Bank of Ukraine).

4.2 Equal treatment between paper and electronic invoices

There is no legislation basis at the moment, though some documents can be circulated in electronic form (Tax Vouchers).

5. eLogistic

5.1 Equal validity of electronic and offline contracts

No reference found in the legislation.

5.2 Conditions for the risk of loss of or damage to the goods

The law of Ukraine "On Consumer Protection" regulates relations between consumers of goods and services, and manufacturers and sellers of goods, executors and service providers of different ownership, establishes the rights of consumers and providing the mechanism for their protection and the basis of state policy in the field of consumer protection.

5.3 Rights on delivery of goods

The national legislation does not define the requirements for time of delivery of goods purchased through eCommerce transaction.

Gap analysis

1. Internet security & privacy

1.1 Allowance to process user traffic data

The national legislation defines the general principles of data protection, but it does not explicitly define the rules of processing of user traffic data by the provider of an electronic communication

service for the purposes of marketing electronic communications services or for the provision of value added services.

1.2 Specific liability regime for intermediary service providers

The national legislation does not clearly define specific liability regimes for three categories of online service providers: transmission conduit operators, caching providers and hosting services providers.

1.3 Obligation for providers to monitor transmitted or stored information

The national legislation defines the requirements on information services providers to monitor information transmitted in order to detect illegal activities and to inform the competent public authorities. This is compliant with the general provisions of the Directive 2000/31/EC on electronic commerce Article 15.

Member States shall not impose a general obligation on providers, when providing the services of transmission, caching and hosting, to monitor the information which they transmit or store, or a general obligation actively to seek facts or circumstances indicating illegal activity.

However, the Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements (Directive 2000/31/EC on electronic commerce Article 15).

2. Consumer rights

2.1 Online trustmarks for retail websites

The country has not established country-wide trustmark scheme(s) for electronic identification and trust services for electronic transactions which assure the trustfulness of qualified eCommerce service providers.

Without country-wide trustmark scheme(s) for electronic identification and trust services for electronic transactions, customers can not be assured in the trustfulness of qualified of eCommerce service providers. Most of the EU member states have established their national online trustmarks. Now the Commission is exploring the usefulness and benefits of the EU-wide trustmark schemes to reassure consumers on the reliability of accredited traders across borders. The aim is also to encourage the establishment of pan-EU price-comparison websites.

When shopping from the sellers that display a national trustmark, customers will benefit from the defined and internationally recognised quality standards such as: comprehensive and accurate product description and merchant information before placement of on-line order, safe and legally compliant service, notification of all costs and any limitations / conditions prior to checkout, charges that are complete and simple to understand – including any tax and delivery and surcharges, access information on order progress / history, delivery as specified at the time of order, purchases arriving in good condition, helpful support with damaged / failed / late / attempted deliveries, a clear returns process with any limitations / conditions notified prior to purchase, personal data and rights being properly protected and managed.

2.2 Minimum general information to be provided by information society service provider

Compliant with the requirements of the Directive 2000/31/EC on electronic commerce Article 5.

2.3 Transparency of commercial communications information to be provided

The national legislation does not imposes that advertisements on the Internet indicates natural (for legal persons there is a legal requirement) responsible for commercial communication and any conditions attached to the offers.

2.4 Requirements for distance contracts and off-premises contracts

The national legislation does not explicitly require that the trader provides the consumer with a minimum of legally defined pre-contractual information and comprehensive explanation of contractual terms in case of distance (concluded online or by electronic means) or off-premises contract. This should be further investigated.

2.5 Consumer protection international cooperation mechanisms

Ukraine has not yet established international cooperation mechanisms between the national public authorities and the authorities of other countries who are responsible for enforcement of consumer protection laws, including for eCommerce.

As Ukraine has not established international cooperation mechanisms between the national public authorities and the authorities of other countries who are responsible for enforcement of consumer protection laws, including for eCommerce, its citizens are much less protected when they purchase products and services from foreign traders established abroad.

2.6 Out-of-court dispute settlement

The national legislation currently does not define the use of out-of-court schemes for dispute settlement regarding provision of eCommerce services, including by appropriate electronic means.

2.7 Online dispute resolution system for consumers for eCommerce transactions

Ukraine has an online application service for dispute resolution through which parties can initiate dispute resolution in relation to disputes concerning online transactions.

2.8 Requirements for sending of unsolicited commercial communication

The national legislation prohibits sending of unsolicited commercial communications by e-mail.

The EU best practice in this domain preserves the possibility for Member States to either prohibit or allow the sending of unsolicited commercial communications by e-mail. Compliant with the requirements of the Directive 2000/31/EC on electronic commerce Article 7.

3. Competition

3.1 Free movement of eCommerce services

The national legislation does not explicitly restrict the freedom to provide eCommerce services compliant to the national laws by a lawful service provider established in another country.

3.2 Authorisation to pursuit the activity of eCommerce service provider

Ukraine’s legislation does not explicitly define the principle excluding prior authorisation to pursuit the activity of eCommerce service provider. The regulation of authorisations for eCommerce activities falls under the overall legal framework. These principles without prejudice to authorisation schemes of Ukraine which are not specifically and exclusively targeted at information society services, or which are covered by another legislation. This is partially compliant with the EC Directive on electronic commerce that defines the principle excluding prior authorisation to pursuit the activity of an information society service provider (Directive 2000/31/EC on electronic commerce Article 4).

4. ePayment

4.1 Fees for the use of means of eCommerce payment

The national legislation does not yet define the requirements for eCommerce payments and does not define the rules on the fees for the use of means of electronic payment. A comprehensive national legislation for eCommerce payments by credit or debit card, on Internet, on phone, using mobile and other electronic payments presents a substantial benefit for eCommerce development and market integration in this field at European level. In the EU, rules on the fees for the use of certain means of payment (e.g. credit or debit cards, electronic valets) prohibit traders from charging consumers, in respect of the use of a given means of payment, fees that exceed the cost borne by the trader for the use of such mean (Directive 2011/83/EC on Consumer Rights).

4.2 Equal treatment between paper and electronic invoices

The legislation of Ukraine does not explicitly assure equal treatment between paper and electronic invoices. This does not comply with the situation in the EU where the EC has identified a set of actions to support the uptake of eInvoicing by ensuring legal certainty and promoting the development of interoperable eInvoicing solutions based on a common standard, paying particular attention to the needs of small and medium-sized enterprises. Directive 2010/45/EU on the common system of value added tax as regards the rules on invoicing sets out new VAT rules regarding eInvoicing and removes obstacles to the uptake of eInvoicing by creating equal treatment between paper and eInvoices, while also ensuring that no additional requirements are imposed on paper invoices. Removing of obstacles to the uptake of eInvoicing by creating equal treatment between paper and eInvoices assures that eCommerce transactions can be concluded faster. eInvoicing also significantly reduces the cost of business procedures related to keeping, processing, storing and delivery/postal expenses of paper invoices.

5. eLogistics

5.1 Equal validity of electronic and offline contracts

The national legislation does not explicitly establish the equal validity of electronic contracting and contract concluded offline together with defining the specific requirements to electronic contracts. The EC Directive on electronic commerce (Directive 2000/31/EC on electronic commerce Articles 9-11) requires the fundamental principles of equal validity of electronic contracting and contract concluded offline, and not only for eCommerce.

5.2 Conditions for the risk of loss of or damage to the goods

The national legislation does not explicitly define the conditions for the risk of loss of or damage to the goods purchased within eCommerce transaction and responsibilities of the trader, the consumer, a third party indicated by the consumer, or the carrier. It also does not stipulate the remedies available to consumers for damaged or faulty goods, entitlement of consumers to replacement or repair of goods, a refund or discount where specific circumstances apply. However, the law of Ukraine “On Consumer Protection” regulates relations between consumers of goods and services, and manufacturers and sellers.

The Directive 2011/83/EC on Consumer Rights defines that the delivery of goods within a minimum of 30 days from execution of sale contract, seller bears risk of loss/damage until goods are received by consumer; automatic right of refund within 7 days of non-delivery. It also standardise the remedies available to consumers for damaged or faulty goods. Consumers will be entitled to replacement or repair in the first instance and a refund or discount only where specific circumstances apply.

5.3 Rights on delivery of goods

The national legislation does not define the requirements for time of delivery of goods purchased through eCommerce transaction.

The harmonisation would increase international opportunities for hosting service providers and Cloud computing services providers. Increase competition brings better and cheaper services to users.

Digital Skills

Azerbaijan

The Ministry of Education of the Republic of Azerbaijan is the central executive body responsible for formation, execution and regulation of state policy on education process, as well as for performing methodical guidance to education process in Azerbaijan. The Ministry is also responsible for the development of digital skills.

There are a number of web based e-education resources of the Ministry, such as education portal, e-textbook, curriculum portal, etc.

As for e-services rendered by the Ministry they are divided into Interactive and Informative services.

The Interactive Services include:

- e-application
- Submission of applications and documents for recruitment of teachers to secondary schools
- State Program for study of Azeri youth abroad in the years 2007-2015
- Provision of information on current academic achievements of pupils
- Submission of applications and documents for admission to initial vocational education institutions
- Online-check of recognition of foreign higher education qualifications and definition of their equivalence as well as nostrification requirements/procedures.

The Informative Services include:

- Contact with senior officials of the Ministry of Education
- Education institutions
- Admission procedure to education institutions
- Current achievements of pupils (System for parental control)
- Assessments of pupil achievement
- Rules for changing education institutions
- Deinstitutionalization and children protection
- Nostrification
- Ethical standards model

The main legislative act regulating education activities is the Law “On Education”. A number of measures are stipulated in the “State Strategy for the development of education in the Republic of Azerbaijan” (covers 2015-2023) approved by Presidential Decree. There are not any international agreements on e-skills.

Belarus

Since there were no surveys held, there are no statistics on the actual number of IT specialists working in the country. The actual number is made of the number of High-Tech Park employees, the other IT companies that cannot enter this park (i.e. the companies that develop the products for information security, because it is supplied with hardware, or if the large share of income comes from

other activities than IT (i.e. from advertisement), and IT staff working for other sectors of economy (banks, enterprises, state organisations etc), and freelancers (individual entrepreneurs).

The IT sector in Belarus is considered to be the largest IT cluster in the Central and Eastern Europe (CEEOA 2010). Due to the limited domestic demand especially from industrial enterprises, it is rather well integrated into the world market, delivering outsourcing services to major IT vendors of the world (like HP, IBM, Microsoft, Oracle, SAP, 1C), but also possessing a developed network of constant smaller foreign partners.

The estimated number of software developers, web designers, network administrators, and other technical personnel working in the IT sector of Belarus is over 25,000 (Mamonenko 2010) up to 50000. Today almost 14.5 thousand IT specialists work at the HTP. More than 70 % of the Park's employees are young people under 28 years old. Approximately 650 companies and organizations operate on the ICT market of Belarus. Currently 125 companies are registered as the residents of HTP.

Because there is only a small domestic market for IT products (it is mainly represented by state institutions, financial enterprises, banks, and corporate customers, with a rather little share of industrial enterprises), Belarusian companies mainly target at Western customers' orders. The niche on the world IT market of Belarusian companies can be described as an offshore IT service provider (software development, outsourcing) for clients who expect the involvement of highly skilled technology resources under low costs.

In 2015, Belarus possesses a very productive cluster of IT companies, mainly oriented on software engineering. The competencies in IT marketing or implementation of IT in industry are not that good, but software development is Belarusian core competence. Over 90% of IT solutions are developed on the outsourcing model (Belarusian companies service the needs of leading IT vendors, banks, industrial companies etc all over the world. While servicing the highly demanding foreign customers, Belarusian IT developers accumulate the most advanced knowledge existing in the world. These competencies and knowledge can be used for international cooperation with EU to develop the Digital Single Market.

The organisations that take functions of developing the IT education are the Scientific and Technical Association "Infopark" and the State Establishment **"**Administration of High-tech park**".**

Infopark organizes round tables with attraction of educational establishments, banks, industrial enterprises, Ministry of Education and IT companies, where the problems of IT educations are discussed, the demand of IT companies for staff and the gap are communicated to educational establishments, the barriers at legislative level are communicated to relevant policy-makers, and joint solutions are discussed among stakeholders. Thus, there are endeavours to describe the situation and to seek for mutual solutions.

The High-Tech park administration investigates the needs of IT companies for staff.

The work was done to determine which competencies are needed for ICT specialists. This work has led to that the list of IT duty positions was supplemented by several contemporary professions. In Belarus, the National Classifier of the Republic of Belarus 006-2009 OKRB "Professions of workers and office employees" is used; the person cannot be hired as a specialist if this specialty is not included to the Classifier. For a long time before that, IT specialists have been hired as engineers; testers have been hired as translators; IT managers were hired as economists, because there were no such professions as programmers and testers in the Classifier.

There are activities present to identify, qualify and decrease the gap between supply and demand for IT staff, but these activities are not performed at the state level and do not have a systemic nature. Very little research work to study the gap is done in relation to IT users and no research work to study the gap was done in relation to eLeadership.

Simultaneously, on practical level there are many educational courses, seminars, initiatives from IT companies to increase the IT competencies of IT staff and IT users, including corporate users (there even special dedicated committees on IT for banking sphere, IT for industry, IT for transport, logistics and trade etc working at Infopark and annual conferences uniting the stakeholders). An example of recent work on eLeadership is the Competence Centre launched by Infopark to raise the competences of IT managers and potential start-ups in cloud computing business models.

The main problem is the gap between the existing system of education of highly qualified personnel for the IT industry, and the needs of IT businesses. The basic building blocks that make up this problem are as follows:

1. Classic universities and traditional technical universities focus on training of generalists, they try to develop students' systems thinking and ability to deepen their own specialization, if necessary ("learning to learn"). Accordingly, the curriculum suggests little flexibility, and leaves the activity on the formation of "competitive advantage", "core competence" at the discretion of the student.
2. As a result, the competence of graduate students are not enough to immediately begin work in the company using the latest technologies, so IT companies are forced to re-train the students. Accordingly, IT companies expect the transformation of the education system towards greater compliance with the profile of labour demand. To resolve this problem, IT companies have initiated supplementing of the existing classifier of professions in the country with six new specializations and professions that are demanded by the market, with detailed descriptions of their functions and necessary competencies.
3. Presentation of the new classifier to universities has tackled the problems of lack of institutions of higher education professionals able to teach new disciplines, and the unwillingness of the teaching staff to expand the list of courses lectured at the expense of internal resources. The universities have made a proposal to that the companies that are residents of the High-Tech Park (that receive profits from employing highly qualified staff) either undertake financial costs for the preparation of new teachers of special courses, either provide lectures on special courses required by the internal staff of IT companies.
4. The problem of training of teachers to meet the current needs of the labour market has several components: a) the difference in the salaries of teachers and professionals employed in IT companies, resulting in an outflow from the high schools to the High-Tech Park of young staff who has acquired the skills in the areas of expertise necessary to market. At the same time, low salaries of teachers are typical for the entire system of education in Belarus now, and by now the Ministry of Education is not prepared to raise the salaries of all teachers of the country to the level of salaries in the private sector; b) to maintain high qualification in translation of the most current knowledge to students, the teacher should regularly, at least once a year, update their practical experience that requires lecturers to combine teaching and practice; at present, training is required of teachers at least once every five years; c) due to the gap in the age pyramid of university teachers in the 1990s, today, most university professors are focused on the generation of fundamental education that makes a certain conservatism and lack of enthusiasm in the development of new knowledge.

5. The representatives of IT companies and HTP respond to requests of universities, noting that: 1. their experts can not break away from the project to give lectures, because lecturing is a separate very time-consuming work, 2. they are not able to provide high wages to all employees of universities that teach any discipline, herewith any weighty wage gap is negatively perceived by teachers that are not connected to the process of the development of new courses and leads to a moral rejection of new specialists ; 3. The fact that IT companies ask for the introduction of new courses and qualifications, as opposed to the traditional sectors of the economy, does not mean that they want some benefits from the educational system. It only means the high rate of growth of the ICT industry, and the need of the higher education system to look for stakeholders from other sectors to better ensure compliance with their needs in a highly specialized workforce.
6. Currently, the main problem of the functioning of educational IT laboratories and introduction of new IT courses in the universities is the **lack of qualified teachers** due to high migration from the education sector in the IT business. Some IT companies started to delegate their internal staff as teachers to high schools, however, this did not become a standard practice because it is difficult to distract good professionals from the projects. The difference in the level of wages of IT staff sent from IT companies to universities and the wages of regular university lecturers, causes problems of integration of IT specialists in the community of university lecturers.

The most relevant policy is set in the sub programmes of the *National programme of accelerated development of services in the field of information and communication technologies (ICT) for 2011-2015:*

The customers: The Ministry of Labour and Social Protection

The Ministry of Labour and Social Security has completed the development of the corporate data network and e-mail system. The following databanks (as well as the automated information systems functioning on their basis) were created and registered:

- "Data Bank under the account and the movement of the unemployed citizens",
- "Nationwide bank of vacancies",
- "Register of the individual accounts of the individuals insured in the individual (personalized) accounting system of the state social insurance system"

Measures of the sub programme:

Scientific support:

1. Development and implementation of an automated information system for the Social Security Fund to provide electronic services in the field of occupational pension insurance and individual (personalized) accounting within the state social insurance system.

2. Development of the state information system of social protection, including the creation of an Internet portal of social protection;

3. Creation of a hotline on social protection and other areas of activity of Ministry of Labour and Social Protection;

4. Creation of an electronic employment service based on the integration and development of information resources and electronic services through an information portal;

5. Development of guidelines for the integration of different types of social security for the population on the basis of ICT in a single system to ensure uniform procedures for interaction of government policy holders, financial system and the population

6. Development of the departmental IT standards for the development and operation of information systems in the field of labour, employment and social protection.

Customers: Ministry of Education, Academy of Public Administration under the President of Belarus, Ministry of Emergency Situations, Institute of retraining and skills at the Ministry of Emergency Situations, HTP administration

Measures:

1. Establishment of a national system of electronic educational resources on the main branches of knowledge

2. Creation of a distributed national library of scientific and educational R & D

3. Development of e-learning tools for use in correctional and educational process of individuals with special needs

4. Development of a national system of information for certification of teachers

5. Establishment of information services for the interoperability of educational institutions, government and the public

6. Creation of the national virtual educational space based on IP-broadcasting and video conferencing

7. Develop and implement a series of measures to protect the information in the sectoral information systems of the Ministry of Education

8. Development of information system of electronic university enrolment

9. Modernization and development of educational resources and information systems

10. Support for the operation of educational laboratory for the development of information technologies in special education "Education without Borders"

11. Development of new educational standards, plans and training programs in the field of ICT

12. Development of a unified national educational environment for continuing education training in the field of management

13. Modernization of automated information system of electronic registration of state managers

14. Development of information support and distance learning system for ideological workers on the basis of competence-based approach

15. Development of software tools to automate the construction of the complex network of computer training programs and management decision-making

16. Development of remote training system for managers and specialists in the field of prevention and liquidation of emergency situations on the basis of distance learning

Administrative and technical measures

18. Improvement and updating of the structure, scope and content of training for IT specialties in accordance with the expressed needs of the IT industry and world trends in the development of IT education

19. Implementation of school improvement programs in computer science and information technology for the initial training of IT specialists

20. Elaborate on expanding the training of specialists in the field of IT by senior students of other specialties

21. Elaborate on increasing enrolment of students in the field of IT, including the state budget form of training

22. Develop changes to the educational standards in higher education with their inclusion in the Standard Skills Reference Book of employees from January 1, 2010 the new posts of specialists engaged in the development, implementation and maintenance of information systems and technologies.

In January 2015, the Minsk City Council has approved the **Program of Informatisation of the city of Minsk in 2014-2015**.

The main direction of information in the system of education of Minsk is the development of resources and services of information educational environment.

The corporate network of educational institutions in Minsk has united more than 700 institutions as of September 1, 2013. Since 2012, the speed of internet connection at educational establishments has doubled. At the beginning of the 2013/2014 academic year, 12 students accounted for 1 computer, which was higher than the national average index, and the number of teachers per 1 computer was 4,4 person. The Programme marks the necessity to provide each teaching staff with portable (tablet) PC, with account to the plans of transition to electronic journals and diaries in a short term.

The education system faces the task of upgrading the infrastructure facilities. The long-term goal of informatisation is to create conditions for improvement based on the model of development of electronic educational services. The most high-demand services include:

- for administration: electronic smart cards (automation of accounting of delays and omissions, working time tracking, automation of registration and use of computer time and the access time to the Internet);
- for teachers - e-library;
- for parents - an electronic purse (the system of cashless payment for meals in educational institutions using smart cards).

The issues of education informatisation are also covered in the following Programmes:

• scientific and technical program "Development of electronic educational resources for preschool, general secondary, special, higher and further education teaching staff (" E-learning resources ") for 2012 - 2014;
• Programme for the Development of pre-school education in the Republic of Belarus for 2009-2014;
• Programme for the Development of secondary education in the Republic of Belarus for 2007-2016;
• State program for the development of special education in the Republic of Belarus for 2012-2016;
• State program for the development of vocational education in 2011-2015;
• State program of development of secondary special education for 2011-2015;
• State program for the development of higher education for 2011-2015;

• State program of development of physical culture and sports in the Republic of Belarus for 2011 - 2015 years;
• National Programme of Demographic Security of Belarus for 2011-2015.

The new National strategy of Information Society Development in the Republic of Belarus until 2022 is under construction now.

The issues of Digital Skills in it are covered in the chapter “Development of human capital for information society”. It acknowledges that “the level of human capital is determined on the one hand, by the level of proficiency in information technology of citizens who use them in their professional activities and daily life; on the other hand, the development of the information society requires highly skilled professionals providing performance of research and development in the ICT sector and the safe operation of information systems”. This changes the architecture of the educational system, the content and the methods of knowledge mastering, as well as the nomenclature of professions needed to address the needs of economy.

However, a clear long-term explicit digital skills policy for developing digital literacy for employability, e-inclusion and lifelong acquisition of digital skills yet needs to be developed on the basis of the National Strategy of the Information Society Development.

The country has no policy-level approach aligned to the EU’s “Grand Coalition for Digital Jobs”.

However there is a developed practice of collaboration among IT companies, educational establishments and ministries to address the gap between supply and demand for IT staff of relevant competencies.

IT companies start integration into the educational process of IT staff at an early stage. They organize practice (internships) for students and professional development of teachers in enterprises; finance the training activities of universities; participate in the correction of the nomenclature of specialties and curriculum content.

Thus, IT company “SaM Solutions” has signed partnership agreements with the majority of higher education institutions in Belarus. Forms of their cooperation include sponsorship, organization of conferences, research, establishment of joint laboratories and classrooms, lectures by experts from SaM Solutions, training of the most talented and highly motivated students with the possibility of further employment.

Organizations representing the interests of IT companies (Scientific and Technical Association “Infopark” etc) are actively involved in the forming of a multi-component system of IT education.

An example of cooperation of representatives of universities and IT companies was the project of the Association "Infopark" to improve the educational standards of IT specialties and to introduce the new professions in National Classifier of the Republic of Belarus 006-2009 OKRB "Professions of workers and office employees".

Resources

By now, there is no specific line in the state budget for the national Digital skills programme.

In the National programme of accelerated development of services in the field of information and communication technologies (ICT) for 2011-2015, the budget of sub programme “e-Employment and Social Protection” was covered by the own financial resources of the Ministry for Labour and Social Protection of the Population (no indication of budget size available). The budget of sub programme

“Electronic education and human capital development” was covered by the own financial resources of the Ministry for Education and the High-Tech Park Administration (no indication of budget size available).

The budget of the Sectoral program of informatisation of education in 2014-2015 has made about 2219962 Euro for 2014 and 2015 for all stages of education.

IT companies now are the main source of investments into augmentation of IT education in terms of provision of financial and human resources for new educational programmes within state universities and other stages of education. They are also a major (almost single) investor in IT courses delivered as professional retraining.

As for human resources (IT staff) dynamics, the number of graduates from sixteen universities of Belarus enrolled in 30 different professions in the field of ICT is growing every year; in 2009 it exceeded 4,000. Three of the sixteen universities play a major role in provision of the country with qualified personnel in the field of IT. A leading position belongs to Belarusian State University of Informatics and Radioelectronics (BSUIR). In 2009, about 1,789 students received bachelor and master degrees in 30 engineering specialties in nine of its faculties. Belarusian State University is the second largest supplier of qualified personnel for ICT companies. Specialists are trained in three departments: the Department of Applied Mathematics and Computer Science, Mechanics and Mathematics and Physics Faculty. Among the other universities are Belarusian State Technological University and the State University of Grodno. More than 90% of qualified personnel of the ICT sector are graduates of universities that are located in Minsk.

A number of IT companies launch their own training courses and even establish their own educational centres: learning Centre at "BelHard Group"; educational Establishment "Private courses of advanced training "Belsoft"; learning Centre at “SoftLine” ; learning Centre at “IBA” ; training centre of “EPAM Systems”.

It was suggested by Infopark to supplement Presidential Decree dated September 22, 2005 № 12 "On the High-Tech Park" by the expansion of the activities of the High-Tech Park by training, retraining and advanced training of specialists in the field of information technologies. The suggestion is to **introduce taxation benefits comparable to benefits offered in the High-Tech Park, for those entities that provide the services of IT education**. This would make the training of IT specialists economically profitable. Now, IT training is not profitable for IT companies because the salaries of IT staff are much higher than the average salaries in the country, so that in order to attract good professionals from IT sector to share their knowledge, one has to pay them a much higher salary than the salary of an average university lecturer and even professor. IT companies invest into good IT courses in order to provide themselves with a good workforce.

In 2009, three new specializations were introduced at the Faculty of Radio Physics and Electronics at the Belarusian State University, following the expansion of the National Classifier on specialisations and qualification: "Satellite Information Systems and Technologies"; "Smart technologies to protect information systems"; "Modelling and analysis of information systems".

In 2014, High-Tech Park in collaboration with the professional communities of developers, testers and business analysts developed new **occupational standards** for *testers* and *software developers*. Soon a project standard for *business analysts* will be completed. In the future, professional standards for *specialists for maintenance* will be developed. These four areas were chosen because these professionals work in most companies of the High-Tech Park.

The project clearly defines the **number of qualification levels**. Together with representatives of educational sphere, the **requirements to knowledge and skills of employees** were identified.

Thus, IT companies have communicated their wishes to universities about the desired knowledge and skills of their graduates.

Top-rated practitioners of IT companies hold *open seminars and workshops* for students of high schools on topics that are not included in the standard learning process, but that are important for the IT industry (i.e. in a framework of International Forum IST.EDU '2010 "Vocational Education and Research in Information Systems and Technologies") (Infopark 2010).

The establishment by IT companies of **joint training labs** enables students' learning on software development on modern platforms (e.g., Java, Perl, PHP, C #, Lotus Notes, 1C, etc.), allows post-graduate students to learn modern standards of software development and get prepared for certification exams (for example, of *Sun*), and creates the basis for long-term sustainable growth of the quality of training of IT professionals through professional development of teachers and development of advanced training courses. Establishment of joint training labs is a multi-purpose tool: it can provide the possibility for joint scientific research, or serve as a platform for parallel development of complementing skills (like basic IT plus foreign language and knowledge of foreign market), or even become a space for incubating students' start-ups.

- *Joint Training and Research Laboratory for Students "Information Technologies" was established in 2002 as part of cooperation agreement between the Belarusian State University and the JV IBA "International Business Alliance" dated 14 May 1999, for integrating their scientific and technical potential. The active cooperation of the IBA-BSU laboratory with leading software vendors (Sun, IBM and Microsoft) serves as a bridge between university and large foreign corporations that are yet little available directly to classical universities.*
- *Educational research and innovation lab at the base of Belarusian National Technical University, together with the IT-company SaM Solutions and the German Academic Exchange Service DAAD was launched in 2009 with a purpose of training of personnel with not only knowledge of modern information technologies, but also of German language for process optimization services for German speaking clients. On March 2013, the new joint HTP lab was launched at the Minsk state linguistic university will host classes held by experts from the HTP as well as EPAM Systems.*
- *In 2010, the IT lab of the "System Technologies" company at the Belarus State University of Informatics and Radioelectronics became a business incubator. The audience of the new generation realizes the concept of an open space: a round table, mobile computers, wireless Internet, freedom of movement and communication. In the business incubator, there will always be the curator, ready to help students in dealing with non-standard tasks. It is planned to organize seminars and workshops, training programs, educational and business games using the case method, meetings with well-known entrepreneurs and businessmen (Infopark 2013).*

Companies do not only seek for the larger number of IT staff: understanding that their competitive advantage lays in the technical level of staff, they invest into *support of scientific research profile of field-oriented departments.*

- *In March 2013, the Innovative Developments Studio was opened in Yanka Kupala State University of Grodno at the Department of Mathematics and Computer Science in collaboration with EPAM Systems (HTP 2013).*

- *On May 21, 2013, on the initiative of EPAM Systems, six department branches of Belarusian State University (BSU) and Belarusian State University of Informatics and Radioelectronics (BSUIR) (Theoretical and Applied Mechanics, Web Technologies and Computer Modelling and Functional Analysis of the Faculty of Mathematics and Mechanics of BSU; Software for Information Technologies, Computer Science and Electronic Computing Machines of the Faculty of Computer Systems and Networks of BSUIR) have been opened in the territory of HTP. This was done in order to make the higher education closer to the IT industry, applying theoretical knowledge to practice, improving the skills of specialists and making it easier for graduates to adapt to new workplaces (HTP 2013).*

By 2013, in the capital city Minsk, 96.7% of the schools have had access to the Internet. At the same time, 11% of computer classes used in the educational process were equipped with computers that are more than 10 years old.

By 2014, all institutions of higher, secondary special and vocational education and training in Belarus have had access to the Internet and their own websites. Connection of institutions of general secondary education (schools) to the Internet was almost completed, more than 80% schools use broadband access technologies

In order to create a long-term foundation to saturate their growing demand for IT personnel, IT companies *encourage the interest in education and work in the field of IT of the pupils of primary schools and organize specialized IT competitions and Olympiads for them.*

- *In 2008, at the initiative of resident companies of HTP, in 16 schools of Belarus an experimental elective course developed by Cisco was introduced: "Fundamentals of Information Technologies: Software and Hardware for PC". In the classroom the pupils have learned to assemble computers, install different versions of operating systems, peripherals and multimedia devices, connect a computer to the LAN and the Internet, receive information about the architecture of local area networks, network protocols; in the regional school in Marjina Gorka a computer lab was opened, equipped with three residents of HTP (HTP 2013).*

In the **Program of Informatisation of the city of Minsk in 2014-2015** approved by the Minsk City Council, particular emphasis is placed on the project **"Smart School"** (permanent access to electronic educational resources and services, including educational institutions, at home, on the road through the training equipment, infrastructure, as well as using their own mobile devices to attract students and workers to the educational process). To implement the model of "Smart School" in Minsk, the equipment of educational institutions with computers and equipment to create a single information-educational environment of the education system has started.

The regions are not covered by this programme. More resources are needed to implement the Smart School concept in the remote regions of the country.

Georgia

Development of digital skills has not been allocated as task to any particular institution though certain measures and actions had been taken by various public institutions[110].

With absence of formal digital skills framework, the legal environment is limited to laws on general and higher education of Georgia. Major areas of current actions are schools and universities, though particular programs and projects had been launched for the development ICT professionals and digital skills in rural communities of Georgia respectively by Georgian Innovation Agency, Ministry of Economic Development and Ministry of Justice of Georgia. Ministry of Labour, Health and Social affairs also has a political mandate in VET and skills gap analysis, such gap analysis had been previously performed though of not particular focus on digital skills. . Through internal program that has taken place in 2014-2015 Georgia has already got 58 retrained trainers. The ToT program has finished in March 2015. As a result Georgia has 200 retrained trainers who have obligation to teach target groups different ICT skills.

Ministry of Education of Georgia has a dedicated Education Management Information System (EMIS) Agency encompassing several tools and initiatives:

- Itvet.ge: public college" IT academy" providing training in computer animation and graphics, computer engineering and computer networks and systems training.
- Eflow.emis.ge: e-doc flow and document flow;
- Buki.ge: educational web portal;
- eCatalogue.emis.ge: Catalogue of educational institutions;
- Testing.emis.ge: e-testing system;
- E-school.emis.ge: school management information system;

Apart from the initiatives mentioned above, actions and plans at different levels are:

1. Schools:
   1.1 Infrastructure:

   Recent years had seen important initiatives in development of relevant infrastructure in schools via at first launch of Georgian Governmental Network and connection of the schools to Ministry of Education's network and internet and equipment of schools and pupils with notebooks. In the last four years all first grade pupils and the teachers of the primary schools were equipped with a notebook. Every school in Georgia is connected with broadband via fibre optic (25%) and Wireless/MMW(75%) connections. Apart from equipping primary grade pupils and teachers with Notebooks, the ministry has also launched and succeeded to equip all classrooms in major cities with computers, further work on delivering connectivity to these classrooms is still ongoing[111].

---

[110] Digital skill, Education and eInclusion are part of Egeorgia 2014-2018 strategy - http://www.dea.gov.ge/uploads/eGeorgia%20Strategy.pdf

Development of digital skills is also mentioned in Georgian Education and Science System Development Strategy http://www.mes.gov.ge/uploads/strategia..pdf

[111] The current initiative of MES are: "To ensure basic computer equipment for teachers", more then 40000 computers (notebooks) in 2015."

1.2 Curriculum

In 2004/5 a new curriculum was established for general education which has shifted the teaching of ICT skills from an own subject to an integral part of each subject. The curriculum no longer teaches coding or software development/programming skills, but rather ICT user skills[112]. Special competitions "Olympiads for Informatics" were suspended as well. Efforts to improve ICT teaching in school had been launched, in particular, draft plan had been prepared and presented to State innovation committee members as well as the ministry for approval.

1.3 Skills:

Teacher training programs had also been launched, with additional credit acquisition motivation in case of participation (credits are needed for license renewal). Teachers are encouraged to learn ICT skills and English leading to higher salaries. About 50% of the 65.000 teachers attended the basic ICT skill training and 30% the advanced ICT training.

1.4 Targets: Some targets identified and shared

- 40% of the teachers passed the advanced ICT skills exam by 2018;
- 60 new applications and content in Georgian language by 2016;
- Web portal with electronic resources accessible for teachers and pupils by 2016;
- 90% of the students with basic ICT literacy and knowledge use e-Services of the government by 2018;
- E-Learning and blended learning system is set up in pilot projects for schools in rural areas by 2017.
-

2. Higher education:

2.1 Infrastructure:

- No actions had been taken to launch joint nationwide ICT infrastructure development programs at higher education level. Each Higher education institution deals with the matter with its own budget resources and according to its estimated requirements. Several educational institutions formed Georgian Research and Educational Networking Association (GRENA) that at earlier stage attracted investments and provided basic communication services- broadband connectivity to Academy of Sciences of Georgia, Tbilisi State University, State Technical University of Georgia, Tbilisi State Pedagogical University, Tbilisi State Medical University, State Agrarian University of Georgia and High Energy Physics Institute of Tbilisi State University.

2.2 Curriculum:

Five accredited universities offer IT studies in Georgia. Curricula do not comply with the needs of the businesses as needs are not identified and studies by industry or education institutions.

2.3 Skills:

[112] In general education system curricula usually don't cover coding and programing skills. In teacher standard and national curricula are relevant sections for ICT skills.

There is a definite lack of lecturers that respond to current challenges and trends in the industry. Due to the lack of connection between the private sector and education systems in ICT, higher education systems is not able to benefit from the achievements, skills and knowledge accumulated in private sector.

3. Particular Projects and initiatives :

3.1 Program 40,000 IT specialists by 2020"

During 2014-2015, Legal Entity of Public Law- Georgia's Innovation and Technology Agency (hereinafter GITA) has implemented project for trainers in ICT field. Under this project, 53 trainers have been already retrained on the following topics: Java, Android, iOS, web programming, IT project management and quality assurance. The training was leaded by experienced trainers from Ukrainian training centre "Skill up". Georgian side plans to continue cooperation with Skill-up in 2015 in order to increase number of retrained trainers by 120.

It should be also mentioned here that, the trainers retrained by the organization of GITA, have obligation to train target groups in different training centres. There Trainings will increase the number of ICT practitioners in Georgia.

3.2 Connectivity to Villages: Computer literacy project

In a pilot project more than 300 villages were equipped with ICT devices and infrastructure. A competition was initiated among the villages to foster ICT skills. Skilled members of the villages help their neighbours in using ICT and convey them basic skills. The project was initially launched at the initiative of Ministry of Justice, though it has transformed as a spin-off project has little awareness and reduced scale now. This program was example of PPP good practice.

Apart from this, Legal Entity of Public Law Georgia's Innovation and Technology Agency works on "Society Innovation Centres" project. On the basis of the libraries GITA plans to open "society innovative centres". 500 libraries had been identified throughout the country. In 2015, 5 centres will be opened that will be equipped with modern technologies (computers, 3D printers etc.) and internet. In small towns and villages the population will have the opportunity to access the infrastructure and internet. Currently is being identified those 5 location where society innovative centres will be opened in 2015. On the basis of the centres are planned activities that will support the population to raise their competiveness in innovation and manufacturing field. That will help them to find new jobs.

Different contests will be held on the basis of the centres that will support to create new ideas. There are also planned different trainings and other distant sessions that will develop local innovative ecosystem.

3.3 Millennium challenge corporation: STEM education

MCC and the Government of Georgia signed a $140 million dollar compact to improve the quality of education in the science, technology, engineering, and math (STEM) fields and increase the earning potential of Georgians through strategic investments from the start of a student's general education to graduation from technical training and advanced degree programs. The compact includes a focus on increasing women's participation. The partnership with San Diego State

University had been signed. The program, which involves three Georgian universities as local partners, will offer young men and women the opportunity to earn internationally accredited degrees in science, technology, engineering, and math, all right here in Georgia.

Ministry of Labour, Health and Social Affairs of Georgia is responsible for the development of labour market, and has implemented several reviews and studies in recent years for the compliance of vocational education with the skills requirements. The development and implementation of the labour market information system is in progress. The ministry frequently holds the meetings with Georgian largest employers. The research of the Labour market is in progress since February, raw data will be published in April.

Moldova

The Prime-minister, the Minister of Information Technology and Communications, the Minister of Education, the US Agency for International Development (USAID) and the Microsoft and IBM Corporations have signed on 24 September 2014 a Memorandum of Understanding “on the formation of the Information Technology Centre of Excellence”.

This Centre of Excellence in IT that will be created within the Technical University of Moldova aims to foster technological education and new businesses creation by energizing research and development activities in Moldova and helping educate the skills needed to IT sector, hereby enabling the sector to continue to grow.

Telecom Rules

Armenia

A detailed description of the legal and regulatory framework and its implementation is contained in the February 2015 report – “Benchmarking Electronic Communications Markets in EaP countries ENPI / 2012 / 307-572.”

The Law on Electronic communications was adopted in 2005. The 2003 EU regulatory framework was taken into account during the preparation of Law of Armenia "On electronic communications" and in other legislation. In certain aspects, it meets the criteria set out by the EU regulatory frameworks, although in many cases only partially. Such is the case of interconnection and access regime, tariff regulation, market analysis, consumer protection, spectrum management, interconnection disputes etc.

Azerbaijan

A detailed description of the legal and regulatory framework and its implementation is contained in the February 2015 report – “Benchmarking Electronic Communications Markets in EaP countries ENPI / 2012 / 307-572.”

The Electronic communication law was introduced in 2005. The 2003 EU regulatory framework was partly considered in the regulatory legislation. Under the current ongoing State Programme on alignment of Azerbaijani legislation with EU legislation, certain normative acts are being reconsidered

while taking into account the EU regulatory framework. The Ministry of Communication and High Technology (MCHT) is preparing draft amendments to the existing Law "On telecommunications" with the aim of aligning it with the 2009 EU regulatory framework. More specifically, the areas of market analysis, spectrum management, universal service, consumer protection and clear division of policy making and regulatory issues should be undergoing the alignment process. Laws with regards to other EU regulatory frameworks (such as on e-commerce, e-signature, data protection etc.) are already adopted and applied.

The "National Programme on legal approximation of the legislation of the Republic of Azerbaijan with the EU Acquis" includes telecommunications and one of the fields to be covered for legal approximation. This document was approved by the Decree of the President of the Republic of Azerbaijan in 2007. However, many of the provisions in the telecommunications area have not yet been aligned and no clear date has been set for completion of the legal approximation work.

Regulation of electronic communications markets continues to be carried out by a small department within the MCIT, which has overall responsibility for the sector. The focus of the regulation has been traditionally towards retail price maintenance, basic universal services and interconnection rules.

Belarus

A detailed description of the legal and regulatory framework and its implementation is contained in the February 2015 report – "Benchmarking Electronic Communications Markets in EaP countries ENPI / 2012 / 307-572."

The Ministry of Communication and Informatisation (MCI) is the body responsible for governmental regulation, the management and implementation of the unified state policy in the area of communication and information and the creation of conditions for the development of organisations of every type of ownership to operate in this area. The Operational and Analytical Centre under the President of the Republic of Belarus is the independent regulator in the area of ICT that determines the policy of ICT development.

In Belarus, the legal person or individual entrepreneur who wants to provide public telecommunication services, including internet services needs to obtain a special permit/licence.

Belarus has the highest achieved fixed telephony penetration in the 6 EaP countries at 47 per 100 population. It has a slightly lower mobile penetration than the average for EaP countries (117% compared with 128%). For broadband services, fixed broadband stands at 28.3 per 100 population and mobile broadband at 54 per 100. This gives the highest broadband penetration in the EaP countries, with a gap of only 9% points under the EU average.

There is a "National program of accelerated development of services in the field of information and communication technologies for the period 2011 – 2015". The development of ICT is intended to promote the development of an information society based on innovation and increased quality in the interaction of information between citizens, business and government. This is also supported by the creation of the state system of provisions of electronic services.

These levels of service penetration have only been achieved in part through private investment and the competitive market still has restrictions. The results have been achieved primarily through applying state policy and state investment in the sector.

Georgia

A detailed description of the legal and regulatory framework and its implementation is contained in the February 2015 report – “Benchmarking Electronic Communications Markets in EaP countries ENPI / 2012 / 307-572.”

A detailed description of the legal and regulatory framework and its implementation is contained in the February 2015 report – “Benchmarking Electronic Communications Markets in EaP countries ENPI / 2012 / 307-572.”

In Georgia, the Law on Electronic Communication was introduced in June 2005. The 2003 EU legal and regulatory framework was considered in the process of introducing the regulatory legislation and the law has been updated to take account many aspects of the 2009 EU framework. As a result, Georgia has implemented many of the features of the EU baseline already, including separation and independence of sector regulation, general authorisation, and an ex-ante approach to competitive markets with obligations for access on operators with significant market power.

The Georgian National Communications Commission (GNCC) is a converged regulator which manages the telecommunications, broadcasting and internet markets. This has advantages, particularly in its role in spectrum management, where there is an integrated and liberalised approach to market needs, including the use of the “digital dividend” spectrum.

The Ministry of Economy and Sustainable Development of Georgia is responsible for ICT policy in the country. Georgia made an obvious progress in the ICT development in recent years, which is the result of latest reforms aimed at liberalization and de-monopolization of ICT Sector and simplification of business starting procedures. The development of ICT sector is being continued in the compliance with the EU and the ITU principles.

Georgia has made progress in telecommunications markets, competitive environment and absence of majority administrative barriers on the Georgian market is promoted by the legislative environment. Recent years’ (in 2006) legislative amendments had simplified licensing procedures. According to the law of “Electronic Communications” new entrants on the market only have to authorize to start an operation. Licensing is needed only for acquiring radio frequencies.

The introduction of digital technologies and a “digital modernization” of Georgia is one of the highest priority. On this direction Georgian government by the initiative of MESD has launched new Georgian Governmental Network GGN project that has started in November of 2006 year, in which were evolved almost all Ministries and governmental entities. There was established network management centre, maintained installation and switching in the net of IP telephony and also its technical service. At the same time mentioned network offers the customer wide internet services.

The modern technologies based GGN stipulates the development of IP protocol-supported, integrated and protected VPN type of computer network all over the Georgia that enables the online interconnection of governmental bodies, exchange of any type of digital data between central and regional agencies, considerably decreasing the communication costs of state authorities, allowing the use of high-speed, as well as that of the ordinary internet access at affordable rates. The GGN was the first technical platform and the most prominent step towards implementation of electronic governance in Georgia.

Under the initiative of the Governmental commission, headed by the Prime Minister was implemented the schools’ computerization project “Deer Leap”. Under this project all schools in Georgia are equipped with computer classes interconnected to internet network. Utilization of this project helps to

establish e-learning systems throughout the Georgia, to develop the broadband systems and to raise ICT awareness.

The Law of “E-signature and e-Document” elaborated by the MESD and on 2008 was approved by Parliament of Georgia, after that in 2008 by MESD was elaborated and adopted the technical rules and Accreditation and Audit Rules for the Certification Service Providers “Elaboration of technical rules towards e-signature certificate and issuing e-signature”. By the initiative of the Ministry of Finance was elaborated the Law of free IT Zones which was approved by Parliament of Georgia and since 1st January 2011 becomes effective. Law aims at development of information technology and creating a favourable environment for those that are in the field of information technology and focused on creation of software products. According the Low information technology products created in virtual zone and oriented on export have not taxation on profits, tax value added, and export taxes.

By the MSED was elaborated new Numbering System in the country. The Government of Georgia has approved regulation of National Numbering System of Electronic Communications Networks of Georgia deployment, which was realized in 2011 and realization of it contribute to the introduction of modern technical specifications and technologies and new types of services, it gives us opportunity to simplify numbering resources acquiring procedures and further development of business activity and long-term competition in the field of telecommunications. Now Georgia practices European model National Numbering System.

In recent years 3G mobile networks are being expanded by mobile operators and cover at least 90% of the population.

Georgian Law on ”Electronic Communications“ was amended in order to implement liberalization of radio frequencies and support development of the new broadband mobile/wireless technologies in the country, amendments are in compliance with EU regulations and obligations of EU–Georgia Association Agreement on radio frequency management.

For the results of utilizations so called “Digital Dividend” GNCC has been sold the license to ensure implementation of fourth-generation (4G) broadband services. In accordance with 2014 amendments in the law on "Electronic Communications" based on technological and service neutrality principle, the Georgian Communication Commission has completed the modification and 15-year term extension process for the use of radio frequency spectrum licenses at (800/900/1800/2100) MHz harmonized ranges. Accordingly, mobile operators have started provision of 4G broadband services.

Under the MESD, with the technical assistance of the European Bank for Reconstruction and Development (EBRD) and the Government of Finland, in the framework of the long-term program "Georgia: Information and Communications Policy and Regulation Development", the project “Digital Switchover Policy and its Implementation in Georgia” was elaborated in 2012. Base on this project and by participation of GNCC and stakeholders, the “Digital Terrestrial TV Broadcasting Switchover Action Plan and Recommendations” was elaborated and adopted by the Government in 2014. According above plan has started the construction of digital terrestrial television network on whole territory of Georgia and distribution of individual digital TV receivers (Set-Top-Box) to socially vulnerable families and in 2015 will be completed the digital terrestrial TV broadcasting switchover in the country.

As a result of above mentioned actions, Georgia has achieved an important success in the field of Information and Telecommunication Technologies, particularly in Network Readiness Index Georgia has moved from 88 to 60th place, improved its rating by 28 positions in the past 2 years. Development rate is one of the highest in this regard.

By the coordination of MSED, among the 269 Harmonized Standards for the R&TTE under the Directive 1999/5/EC , Georgia joined 168

There is good competition in infrastructures and consumer choice in the main cities and towns, giving a fixed broadband penetration of 21.5 per 100 population in urban areas. The penetration of fixed broadband in rural areas is significantly lower at only 2.1 per 100 population. Mobile broadband penetration is relatively low for the EaP region,. There is some obligation for mobile operators to accelerate 4G coverage into rural areas,4G geographical boundaries will extended and cover whole country . Overall mobile broadband penetration is 31.1 per 100 population.

According to above mentioned actions, in World Bank's annual report Doing Business 2014, Georgia ranked 8th in the world for ease of starting and doing business. Regarding business in low-risk assessment of corruption (TRACE Matrix index) among 197 countries Georgia takes 11th place.

• In Georgia for the first time is carrying out works on creation high technology and innovations development centre (technology park), which will be completed this year

• Under the grant program of Georgia's Innovation and technology agency was opened one Fab Lab and by the end of the year will be opened more 5 Fab Labs

• 3 iLab for mobile applications was opened directly of visual effects and computer gaming, while more 7 Innovation Lab will be opened by the end of this year

A recent initiative of MESD has been to consult with the commercial operators to analyse the broadband investment gap and it is hoped that this will lead to a new policy that will accelerate broadband infrastructure investments, especially into rural areas.

Georgia has signed an Association Agreement with the EU committing to harmonisation of the legal and regulatory frameworks, with specific milestones to be achieved in the electronic communications sector over 3 and 5 years, notably;

- Provisions of Directive No 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) as amended by Directive No 2009/140/EC of the European Parliament and of the Council of 25 November 2009 shall be implemented within 3 years.
- Provisions of 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) as amended by Directive No 2009/140/EC of the European Parliament and of the Council of 25 November 2009 shall be implemented within 3 years.
- The provisions of Directive No 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) as amended by Directive No 2009/136/EC of the European Parliament and of the Council of 25 November 2009 shall be implemented within 5 years.
- The measures resulting from the operation of Decision No 676/2002/EC of the European Parliament and of the Council of March 7, 2002 on a regulatory framework for radio spectrum policy in the European Community shall be implemented within 3 years.

Moldova

A detailed description of the legal and regulatory framework and its implementation is contained in the February 2015 report – "Benchmarking Electronic Communications Markets in EaP countries ENPI / 2012 / 307-572."

In Moldova, the Electronic communication law was introduced in 2008. It is based on the 2003 EU legal and regulatory framework, As a result, Moldova has implemented many of the features of the EU baseline already, including separation and independence of sector regulation, general authorisation, and an ex-ante approach to competitive markets with obligations for access on operators with significant market power.

The National Regulatory Agency for Electronic Communications and Information Technology (ANRCETI) is a converged regulator which manages the electronic communications market including broadcasting and internet markets. This has advantages, particularly in its role in spectrum management, where there is an integrated and liberalised approach to market needs, including the use of the "digital dividend" spectrum.
Mobile services (for voice and 3G data) cover 99% of the population and 4G currently covers 40%. Fixed broadband now includes fibre-to-the-home and cable networks in most towns and copper ADSL throughout the country. Public payphones are generally available to consumers at affordable prices, with free access to emergency services.

Moldova has signed an Association Agreement with the EU, committing to harmonisation of the legal and regulatory frameworks, with specific milestones to be achieved in the electronic communications sector over 3 and 5 years, notably;

- Provisions of Directive No 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) as amended by Directive No 2009/140/EC of the European Parliament and of the Council of 25 November 2009 shall be implemented within 3 years.
- Provisions of 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) as amended by Directive No 2009/140/EC of the European Parliament and of the Council of 25 November 2009 shall be implemented within 3 years.
- The provisions of Directive No 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) as amended by Directive No 2009/136/EC of the European Parliament and of the Council of 25 November 2009 shall be implemented within 5 years.
- The measures resulting from the operation of Decision No 676/2002/EC of the European Parliament and of the Council of March 7, 2002 on a regulatory framework for radio spectrum policy in the European Community shall be implemented within 3 years.

Ukraine

A detailed description of the legal and regulatory framework and its implementation is contained in the February 2015 report – “Benchmarking Electronic Communications Markets in EaP countries ENPI / 2012 / 307-572.”

In Ukraine, Law “On Telecommunications” was introduced in 2003 and has been elaborated further since - up to 2014, 32 additional amendments were included. The 2003 EU regulatory framework is partially implemented in the national legislation and it is currently undergoing an additional adaptation process. All new regulatory legislation acts that are being elaborated are based on the 2003 and 2009 EU regulatory framework. Legislation concerning the areas covered by other EU regulatory platforms (such as e-commerce, electronic signature, data protection etc.) is under development in Ukraine.

Many of the provisions in the EU baseline have not been fully implemented for basic services and there are very few regulations from the EU baseline that yet apply to next generation networks and broadband services. These include universal service policy and implementation, open access to infrastructure, regulations to promote broadband competition and investment. Although a “Digital Agenda” target has been announced for universal high speed (>30Mbps) broadband, there is no state aid available to accelerate investments and no specific state-aid rules or investment regulations to ensure cost effectiveness in high-speed broadband infrastructure and the promotion of competition.

The levels of service penetration vary considerably from urban to rural areas. The overall national penetration of basic fixed lines is 23.7 per 100 population. Fixed broadband is not available in many rural locations and nationally the penetration is relatively low at 13.7 fixed broadband lines per 100 population. Although the penetration of basic mobile subscriptions is relatively high, at 142.4 per 100 population, mobile broadband subscriptions are only just beginning to grow after a very late introduction of 3G services in Ukraine. Percentage of households with broadband internet access equals 39.3%.Mobile broadband penetration currently stands at 6.7 per 100 population. Fixed and mobile number portability are planned, but no date has been set for their introduction.

Ukraine has signed an Association Agreement with the EU, committing to harmonisation of the legal and regulatory frameworks, with specific milestones to be achieved in the electronic communications sector.

In April, 2015 the Cabinet of Ministers of Ukraine approved the Plan for the implementation of some legislative acts of the EU in the sphere of telecommunications, developed by the Administration of the State Service of Special Communication and Information Protection of Ukraine and NCCIR (hereafter – the Plan). The document is established pursuant to obligations of Ukraine concerning telecommunications sector in the framework of the Association Agreement between Ukraine and EU.

According to the Plan implementation in the telecommunications sector will be implemented by improving public policy and regulation, as well as implementing effective changes to the legal framework according to European standards.

For each item it is planned that additional information be provided in tabular form for short-, medium- and long-term priorities (for legal and institutional levels) with identification of the responsible authority and co-authorities, required measures / activities, deadlines, financial aspects (state budget funds, outside funds, investment funds and other enabling financial resources), possible risks and impediments (options and alternate solutions), mandatory results and implementation procedures, incoming information, data and reports.

5 RELEVANT NATIONAL ORGANISATIONS AND INTERVIEWED PEOPLE

Information, network and cyber security

Armenia:, Head of Cyber Crime Department, Police; Information Security Expert/Consultant, member of ISOC and IGF; Deputy CEO of Internet Society NGO, CEO of Internet Governance Forum.

Organisation	Level of involvement (High, Medium or Low)						Description	Key functions in relation to Electronic Identification and Trust Services	Contact details
	EU cooperation	National policy	Strategy	Legislation	Executive	Regulatory body			
Organisation 1 (RA Police)			Medium		Medium			The RA Police is the focal point for the area.	
Organisation 2 (National Security Service)	Medium							The National Security Service is responsible for the security of the government websites through the firewall.	
Organisation 3 (National Commission on Security)		Low						The National Commission on Security has developed the Concept on IT Security and has not been doing much work in the area since then.	
Organisation 4 (Internet Society NGO)					Low			Non-governmental CERT	
Organisation 5 (Internet Governance Forum)			Low		Low			Public consultations and discussions	

Azerbaijan: Chief Security Consultant, Electronic Security Centre under the Ministry of Communications and High Technologies (CERT.AZ) ; Security Consultant, Electronic Security Centre under the Ministry of Communications and High Technologies (CERT.AZ) .

Organisation	Level of involvement (High, Medium or Low)						Description	Key functions in relation to Electronic Identification and Trust Services	Contact details
	EU cooperation	National policy	Strategy	Legislation	Executive	Regulatory body			
Organisation 1 Cyber Security Centre under the Ministry of Communication and Information Technologies	Medium	Medium	High	Medium	High	Medium	The Centre is a coordinating state authority, which provides coordination of the activity of the entities of information infrastructure, awareness about existing e-	The activities of the Centre: - coordinate the activity of information infrastructure entities in the area of cyber security - collect and	Drogal lane 702,Baku Tel.: (+99412) 493 20 57 E-mail: reports@cert.az E-mail: team@cert.az www.cert.az

							dangers (and which can be arisen) on a country level, education of population, private entities and other organizations in the field of cyber security and also provides methodical assistance.	analyze information from users, manufacturers of SW, HW and technical equipment, similar structures in foreign countries and other sources about cyber-attacks, - trespassing, malicious computer programs (electronic threats of danger) directed against security of information systems and networks, computer equipment and their SW, local and corporate information systems and resources; - to carry out notification of existing and potential cyber threats, to raise awareness of users on issues of cyber-security; - prepare instructions and recommendations about the programs, technical facilities to be used against users and provide methodological support to counter cyber threats; - implement preventive measures in collaboration with the national Internet operator and MCHT to repel cyber-attacks in the global Internet traffic; - cooperate with other relevant bodies operating	

								in the country to provide preparedness for the cyber security.	
Organisation 2 Computer Emergency Response Team (CERT) of Special Communication and Information Security State Agency under the Special State Protection Service of the Republic of Azerbaijan	Medium	Medium	High	Medium	Medium	Medium	Computer Emergency Response Team (CERT) is responsible organization for security of information systems and networks of state organizations.	- Timely accepts information about computer incidents and render assistance to information systems and Internet network's users in preventing computer incidents, avoiding such cases and their investigation; - Provides mutual information activity with users through the team's website, places on the website the list of the computer-systems-protecting software tools usage of which is recommended, and the inquiry information; - The team guarantees that any information that was become known to it in the work process for avoidance of the computer incidents will not be disclosed to a third party without consent of the user as incurred damage from that incident.	68, Lermontov str., Baku Tel: (+99412) 435-18-37 Fax: (+99412) 498-96-48 Email: secretary@dmx.gov.az www.dmx.gov.az www.cert.gov.az
Organisation 3 (enter name)	Low	Low	Low	Low	Low	Low	AzScienceCERT is an information security incidents responding group in Internet network (AzScienceNet) of Azerbaijan National Academy of Sciences (ANAS). The main aim of AzScienceCERT is maintaining the information	AzScienceCERT realizes the collection, storage and analysis of the statistical data related with network attacks and malware infections in ANAS Internet network. In order to achieve the planned tasks AzScienceCERT cooperates with the similar groups	9, B.Vahabzade str., Baku AZ1141, Azerbaijan Republic Phone (+994 12) 5104253 Fax (+994 12) 4396121 E-mail info@sciencecert.az www.sciencecert.az

							security risks in AzScienceNet at an accepted level. For this purpose AzScienceCERT helps ANAS organizations and AzScienceNet users in detecting, preventing and informing the actions that violate information security.	in Azerbaijan Republic, the state organizations of Azerbaijan Republic, the foreign groups which work on information security incident processing and the other groups working in information security field.	
Organisation 4 Ministry of National Security	N/A	Medium	Medium	Medium	Medium	Medium	Central executive body responsible for implementation of state policy in the sphere of national security	Conducts mutual activity with the state bodies and communication enterprises in the field of technical-organizational arrangements of operatively-search measures in communication networks; Takes comprehensive actions in the field of protection of informational technologies and programs that have an importance in view of national security;	14, Parliament Avenue, Baku AZ1006 Tel.: (99412) 493-76-22 Fax: (99412) 493-76-22 E-mail: cpr@mns.gov.az www.mns.gov.az
Ministry of Communication and High Technologies (MCHT)	High	High	High	High	High	High	Central executive body which formulates and implements state policy, secures the legal normative regulation in the areas of communications (telecommunication, post) and high technologies (information technologies, microelectronics, space, nano, bio and other innovative knowledge-based technologies) (hereinafter referred to as relevant area)	- to analyze the state of cyber security in the country constantly, coordinate the activities of information infrastructure entities in the field of cyber security, to provide information to the public, private and other institutions on current and potential electronic threats, render them technical and methodical assistance, with national internet	77, Zarifa Aliyeva str., Baku Tel.:(+99412) 498 58 38 Fax:(+99412) 498 79 12 E-mail: mincom@mincom.gov.az www.mincom.gov.az

									operators and relevant government agencies to take preventive measures to prevent global cyber-attacks in the common internet traffic incoming in the country; - to implement measures with relevant government agencies to ensure information security and data protection; - with relevant government agencies to carry out audit of the security of information systems and networks in order to detect and prevent electronic threats; - with relevant government agencies to take measures to establish special-purpose telecommunication networks of state authorities, provide technical support to such networks and ensure their security	

Belarus: Operations and Analysis Center under the President of the Republic of Belarus; Belarusian State University; CJSC “Avest”.

Organisation	Level of involvement (High, Medium or Low)						Description	Key functions in relation to Electronic Identification and Trust Services	Contact details
	EU cooperation	National policy	Strategy	Legislation	Executive	Regulatory body			
Operation and Analytical Centre under the President of the Republic	+	+	+	+	+	+	See background information	See background information	

of Belarus										

Georgia:

Moldova: Professor at the Technical University of Moldova, Scientific Researcher at the Information Society Development Institute; eGovernment Centre of Moldova; Ministry of Information Technology and Communication; National Centre for Personal Data Protection of Moldova.

Ukraine: – State Service for Special Communication and Information Protection of Ukraine (DSSZZI); DSSZZI Computer Emergency Response Team of Ukraine (CERT-UA, accredited FIRST); Ministry for Regional Development and Building of Ukraine, State Agency for e-Governance of Ukraine.

Organisation	Level of involvement (High, Medium or Low)						Description	Key functions in relation to Electronic Identification and Trust Services	Contact details
	EU cooperation	National policy	Strategy	Legislation	Executive	Regulatory body			
The State Service for Special Communication and Information Protection of Ukraine (DSSZZI)	H	H	H	H	H		A central executive body with special status, with main task of implementing the state policy on protection of state information resources within data networks, maintenance of the national system of confidential communication, cryptographic and technical protection of information.	Key responsible for the Cyber Security strategy and subsequent legislation	http://www.dsszzi.gov.ua/dstszi/control/en/index
National Security and Defence Council of Ukraine (RNBO)		H	H				It is the coordinating body in matters pertaining to national security and defense under the President of Ukraine. Coordinates and supervises the activities of executive authorities in the area of national security and defense.	Defines priorities in Ukraine Security and defence policy	http://www.rnbo.gov.ua/en/
Computer Emergency Response Team of Ukraine (CERT-UA)			H		H		Computer Emergency Response Team of Ukraine, accredited by FIRST, since 2007	Supports the governmental authorities and the market players in questions of Cyber security, cooperates with DSSZZI on formulating the national strategy for NIS/Cybersecurity	http://cert.gov.ua/
NKRZI				M		H	National regulator	In process of defining responsibilities to regulate the Security part of the market	www.nkrzi.gov.ua
State Agency on e-government affairs of Ukraine	H	H	H				Agency is a central body of executive power implements state policy in the field of electronic information, e-governance, and development of the information society.	Leads cross-functional working group on Cyber-security issues.	http://dknii.gov.ua/
Security Service of		H	H				is a state law-enforcement organ of special purpose that	Defines priorities in Ukraine Security and	http://www.ssu.gov.ua/sbu/control/en/index

Ukraine (SSU)							provides the state security of Ukraine	defence policy	
Ministry of Defence of Ukraine		H	H		L		Is a state organ ensuring defence and integrity of the national borders of Ukraine	Defines priorities in Ukraine Security and defence policy Owns unofficial CERT	http://www.mil.gov.ua/en/

Electronic identification and trust services

Armenia: Director, e-Government Infrastructure Implementation Unit ("EKENG"), Ministry of Economy

Organisation	Level of involvement (High, Medium or Low)						Description	Key functions in relation to Electronic Identification and Trust Services	G320
	EU cooperation	National policy	Strategy	Legislation	Executive	Regulatory body			
Organisation 1 (EKENG)					high			Implementation, setup of electronic infrastructure	Armenia, 0002, Yerevan, Saryan St., 12 Building Tel: +374-10-512882 http://www.ekeng.am
Organisation 2 (Ministry of Economy)	high	high	high	high		high		Policy making, international programs	Armenia, 0010, Yerevan, Mher Mkrtchyan St., 5 Building Tel: +374-10-597206 http://www.mineconomy.am
Organisation 3 (Staff of the Government)				medium				Policy making	Republic Square, Government House 1, 0010 Yerevan, Republic of Armenia Tel.: (+37410) 51-57-03 www.gov.am
Organisation 4 (Ministry of Justice)				medium				Legislative	RA Minister of Justice Halabyan 41a, Yerevan, Armenia Tel.: 00374 38-03-89 http://www.moj.am/

Azerbaijan: Head of Department, Data Processing Centre under the Ministry of Communications and High Technologies.

Organisation	Level of involvement (High, Medium or Low)						Description	Key functions in relation to Electronic Identification and Trust Services	Contact details
	EU cooperation	National policy	Strategy	Legislation	Executive	Regulatory body			
Ministry of Communications and High	high	high	high	high	high	high	Increases rationality of the activities of state	E-government portal operator, E-government	**Address:**AZ1010 Baku, DilaraAliyeva 185 **e-mail:**office@rabita.az

Technologies of the Republic of Azerbaijan							bodies by the broad application of modern technologies. Reduces budgetary expenses, improving speed and efficiency in rendering state services and spending. Creates the centralized operational level data storage space for state bodies and ensures its security. The main projects are • Integrated network infrastructure for state bodies • E-government portal • E-government sluice • State register of information resources and systems • National infrastructure for e-signature • Participates in registration of employment contracts in combined project with MLSPP.	3.0,electronic certificates provider for e-signature, State register of information resources and systems	**phone:** (+99412) 498-80-44
Ministry of Labour and Social Protection of Population	high	high	high	medium	high	high	Provides registration of forms and documents for assignment of unemployment status and benefits.	Electronic information system on registration of employment contracts	**Address:** AZ 1009, Baku, Salatin Asgarova str., 85 **e-mail:** **phone:**(+994 12) 596-50-33
Ministry of Taxes of the Republic of Azerbaijan	high	high	high	medium	high	high	Supports online registration of the individual and legal businesses. Supports online submission of a simplified tax declaration to the tax authority (E-Declaration).Supports online acceptance of tax invoices (E-tax invoice). Participates in registration of employment contracts in combined project	E-Declaration, e-tax invoices, state register of VAT payers, ASAN certificate services provider	**Address:**AZ1073, Baku, Landau str.,16 **e-mail:**info@taxes.gov.az **phone:**(+99412) 403-89-70

							with MLSPP. Provide certificates for e-signature by accredited (ASAN Certificate Services Center).		
Ministry of Interior Affairs of the Republic of Azerbaijan	high	high	high	medium	high	high	A search system of citizens personal data according to Personal Identification Number (IAMAS), State register of resident identity of citizens	State register of resident identity of citizens.	**Address:**AZ1005, Baku, Azerbaijan avenue, 7 **e-mail:**info@mia.gov.az **phone:**(+99412) 590-92-22
Ministry of Justice of the Republic of Azerbaijan	high	high	high	high	high	high	Registration authority and the provision of information on state registration of acts of civil status. Registration of legal entities, non-profit and educational institutions, as well as providing information on the registration status. State register on the personal identification number of citizens of the Republic of Azerbaijan, as well as foreigners and stateless persons.	State register of legislative acts, State register on the personal identification number of citizens of the Republic of Azerbaijan, as well as foreigners and stateless persons.	**Address:** AZ1073, Baku, Builders avenue 1 **e-mail:**contact@justice.gov.az **phone:**(+994 12) 537-05-54
State Procurement Agency of the Republic of Azerbaijan	low	medium	medium	medium	high	High	Provision an information about public procurement carried out in the republic. Support for E-procurement and e-tender.	E-Procurement, e-tender	**Address:** AZ 1000, Baku, U. Hajibeyov street 40, Government House, Entrance 4, 2nd floor **e-mail:** mail@tender.gov.az **phone**: (+994 12) 498-24-01
The State Customs Committee of the Republic of Azerbaijan	high	medium	medium	high	high	high	Provision e - Customs Declaration services for declaration of goods. Support of e - Customs Examination services. Support of online e - Customs Payments. Online monitoring of application and inquiries submitted to the State Customs Committee.	e-Custom Declaration	**Address:** AZ1073, Azerbaijan, Baku, Builders avenue, 2 **e-mail:** international@customs.gov.az **phone**:(+99412) 404-22-00

Belarus: Republican Unitary Enterprise “National Centre for e-services”; Operations and Analysis Center under the President of the Republic of Belarus; Scientific and Practical Republican Unitary Enterprise “The Inter-branch Scientific and Practical Center for Identification Systems and E-business Operations” of the National Academy of Sciences of Belarus (State Enterprise "Centre for Identification Systems"); CJSC “Avest”.

Organisation	Level of involvement (High, Medium or Low)						Contacts
	EU cooperation	National policy	Strategy	Legislation	Executive	Regulatory body	
Ministry for Communication and informatisation	+	+	+	+		+	
Operative and Analytical Center under the President of the Republic of Belarus		+	+	+			
National Center for Electronic Services				+	+	+	

eCommerce

National organisations involved in development of eCommerce for SMEs, harmonisation with the EU

Armenia

Organisation	Level of involvement (High, Medium or Low)						Description	Key functions in relation to HDM	Contact details
	EU cooperation	National policy	Strategy	Legislation	Executive	Regulatory body			
Organisation 1 (RA Ministry of Economy)	High	High	High	High	High			Policy making, international programs	Armenia, 0010, Yerevan, Mher Mkrtchyan St., 5 Building Tel: +374-10-597206 http://www.mineconomy.am
Organisation 2 (RA Ministry of Transport and Communication)		Medium						Policy making	Armenia, 0010, Yerevan, Nalbandyan St., 28 Building Tel: +374-10-590021 http://www.mtc.am
Organisation 3 (Union of IT Enterprises)		Medium						Consultations on the policy making	Armenia, Hakob Hakobyan 3, Yerevan Tel: +374-11-548884 www.uite.org

Azerbaijan

Organisation	Level of involvement (High, Medium or Low)						Description	Key functions in relation to HDM	Contact details
	EU cooperation	National policy	Strategy	Legislation	Executive	Regulatory body			
Organisation 1 Ministry of Economy and Industry	Low	Low	Low	Low	Low	Low	Central executive body that develops the economic policy of Azerbaijan, provides economic and social forecasts, designs and implements the state policy for the development of different areas of the economy, foreign economic and trade contacts, raising, allocating and promoting investments, internal trade, development of and state support for entrepreneurship, development and promotion of competition, including elimination of unfair competition, protecting consumer rights and regulating the structure and innovations in the national economy, as well as regulates and exercises official control over issues within its area of activities.	To guarantee the execution of the task on creation of "electron trade" in Azerbaijan, electronic trade portal had been created by the Ministry of Economy and Industry for the purpose of supporting of entrepreneurs, especially guarantying an independent access of agriculture producers to markets.	84, U.Hajibayov Street, Baku (The Government House) Phone: (+99412) 4938867 Fax: (+99412) 4925895 E-mail: office@economy.gov.az http://www.economy.gov.az/eng

Belarus

Ministry of Communications and Informatisation of the Republic of Belarus: Department for Informatisation and Department for external affairs

Ministry of Trade of the Republic of Belarus

State Enterprise "Centre for Identification Systems"

Ministry for Economy of Belarus

Phone queries:

National Centre for Marketing and Prices Conjuncture

Belarusian Universal Commodity Market

Organisation	Level of involvement (High, Medium or Low)	Description	Key functions in relation to HDM	Contact details

	EU cooperation	National policy	Strategy	Legislation	Executive	Regulatory body			
Ministry for trade	+	+	+	+	+	+	See background information	See background information	
Ministry for taxation	+	+	+	+	+	+	See background information	See background information	
Centre for identification systems			+		+	+	See background information	See background information	

Georgia

Organisation	Level of involvement (High, Medium or Low)						Description	Key functions in relation to HDM	Contact details
	EU cooperation	National policy	Strategy	Legislation	Executive	Regulatory body			
Organisation 1 **Data Exchange Agency, Ministry of Justice**	√	√	√	√	√		Data Exchange Agency (DEA) started its operation on January 4, 2010. The agency operates under the status of LEPL (Legal Entity of Public Law) and is governed by the Ministry of Justice of Georgia. DEA's overall activity is divided into several directions. Each of them bears equal importance and strives to support the following fields: E-governance development, creation and installation of unified Georgian Governmental Gateway (3G) and its monitoring, establishment of data exchange infrastructure. Setting ICT standards for public sector entities and elaborating information security policies are the agency's another important responsibility. Subsequently, the agency's core functions can be split into 3 directions: - E-governance; - Data Exchange Infrastructure; - Information Security.	Data exchange agency plays a pivotal role in e-governance issues, it is the major counterpart and shall be coordinated on technical standards, procedures and other issues related to eCommerce,	

Organisation 2 Ministry of Economic Development	√	√	√	√	√		The ministry of Economic Development is part of the government of Georgia and responsible for Foreign Trade, Export support, Investor Relations, ICT, Tourism, Transport, State Property Management, Construction, National Quality Infrastructure and other areas.	Ministry of Economic Development bears main responsibility for the development of Ecommerce issues in Georgia, including implementation plan of AA obligations in relation to eCommerce	

Moldova

(1) Director “QSystems” http://qsystemsglobal.com, andrey.aydov@qsystems.md

(2) Business Solutions Manager, natalia.bogus@qsystems.md

(3) Ministry of Economy

Ukraine

1. Head of Digital Economy Division at Ministry of Economics of Ukraine 2. Olga Bielkova, the Deputy of Verkhovna Rada and the author of the draft Law on eCommerce.

Organisation	**Level of involvement (High, Medium or Low)**						**Description**	**Key functions in relation to HDM**	**Contact details**
	EU cooperation	National policy	Strategy	Legislation	Executive	Regulatory body			
Verkhovna Rada Committee on Financial Policy and Banking, Subcommittee on			X	X			The Committee is a body of the Verkhovna Rada of Ukraine, which consists of the People's Deputies to implement in certain areas of drafting, preparation and preliminary consideration of issues implementation, control functions.	1) Drafting of bills and other acts; 2) preliminary consideration and preparation of opinions and proposals to the bill.	http://komfinbank.rada.gov.ua/komfinbank/control/uk/publish/article?art_id=46799&cat_id=44832%27 Direct contact available

Securities, Stock Market, Credit Rating Agencies and e-commerce									
State Agency on e-government affairs of Ukraine		X	X		X		Agency is a central body of executive power, directed by the Cabinet of Ministers of Ukraine by Vice Prime Minister of country - Minister of Regional Development, Construction, Housing and Utilities and implements state policy in the field of information, e-governance, development and use of national electronic information resources, development of the information society.	One of the main objectives is the development of e-business. The above issue is solved by the development and application of technology companies and e-commerce tools; use of digital signature and information security; implementation of remote services in the banking system; ensure the continued integration of the national payment system with international payment systems.	http://dknii.gov.ua/ Direct contact available
The National Bank of Ukraine						X	The National Bank is the central bank of Ukraine, a special central body of the state administration. The main function is to ensure stability of the monetary unit of Ukraine.	The National Bank regulates the activity of payment systems and settlement systems in Ukraine, creates and provides continuous, reliable and efficient operation and development of payment systems.	http://www.bank.gov.ua/control/en/publish/article?art_id=37384&cat_id=37375 Direct contact available
Ministry of Economic Development and Trade of Ukraine			X		X		Ministry of Economic Development and Trade of Ukraine is the central body of executive power, directed by the Cabinet of Ministers of Ukraine.	The main tasks: state policy of economic and social development and trade, state industrial policy, state foreign policy, state policy in the field of technical regulations, conformity assessment and standardization of state property management, business development, public-private partnerships, public procurement.	http://www.me.gov.ua/Documents/List?lang=uk-UA&tag=PravoviZasadiDiialnosti Direct contact available
Ministry of Finance				X	X	X	Ministry of Finance is a central executive authority governed and coordinated by the Cabinet of Ministers of Ukraine.	Forming and implementing the financial, budget, tax and customs policy of the State(except for the administration of taxes, customs duties and sales tax and customs policies), policy in the area of state financial control, treasury	http://www.minfin.gov.ua/ Direct contact available

								maintenance of budget funds, accounting, lottery issue and conducting, securities issue organization and control, accountable documents, extraction, production, utilization and storage of precious metals and jewels, organogenic and semiprecious jewels, and their turnover and accounting, in the area of avoiding and combating criminal money legalizing (laundering), or financing terrorism.	

eCustoms

National organisations involved in development of eCustoms and harmonisation with the EU

Armenia

Organisation	Level of involvement (High, Medium or Low)						Description	Key functions in relation to HDM	Contact details
	EU cooperation	National policy	Strategy	Legislation	Executive	Regulatory body			
Organisation 1 (Ministry of Finance)	high	High	high	high	high	high		Policy making, implementation	RA Minister of Finance 1 Melik-Adamyan, Yerevan Tel.: 060-700-304 http://www.minfin.am/
Organisation 2 (enter name)									
Organisation 3 (enter name)									
Organisation 4 (enter name)									

Azerbaijan

Organisation	Level of involvement (High, Medium or	Description	Key functions in	Contact details

	Low)							relation to HDM	
	EU cooperation	National policy	Strategy	Legislation	Executive	Regulatory body			
Organisation 1 (The State Customs Committee of the Republic of Azerbaijan)	Low	High	High	High	High	high	Central executive body responsible for formation, execution and regulation of state policy on Customs in Azerbaijan.	- e - Customs Declaration / Goods - e - Pre-arrival Information - e - Customs Declaration / Passengers - e - Monitoring - e - Imports / Exports - e - Customs Examination - Goods Nomenclature - Application for permission to establish duty-free shop - Submission of application and documents to get, terminate or annihilate the license for operating as customs broker and customs carrier - Submission of application and documents to get, terminate or annihilate the license for establishing customs warehouses and warehouses of temporary storage - Online monitoring of application and inquiries submitted to the State Customs Committee - e - CPPIN - e - Customs Payments - Calculation of customs payments for import of light vehicles	Tel: (99412) 404-22-00 Fax: (99412) 404-22-17 E-mail: international@customs.gov.az http://customs.gov.az/

Organisation 2 (enter name)									
Organisation 3 (enter name)									
Organisation 4 (enter name)									

Belarus

(1) State Customs Committee of the Republic of Belarus

(2) Scientific and Practical Republican Unitary Enterprise "The Inter-branch Scientific and Practical Centre for Identification Systems and E-business Operations" of the National Academy of Sciences of Belarus (=State Enterprise "Centre for Identification Systems")

Organisation	**Level of involvement (High, Medium or Low)**						**Description**	**Key functions in relation to HDM**	**Contact details**
	EU cooperation	National policy	Strategy	Legislation	Executive	Regulatory body			
State Customs Committee		+	+	+	+	+	See background	See background	

Georgia

Organisation	**Level of involvement (High, Medium or Low)**						**Description**	**Key functions in relation to HDM**	**Contact details**
	EU cooperation	National policy	Strategy	Legislation	Executive	Regulatory body			
Organisation 1 **Revenue Service/ Ministry of Finance of Georgia**	√	√	√	√	√		Revenue Service, a legal entity of public law of the Ministry of Finance of Georgia, executes state control on the whole territory of Georgia with areas of responsibility (relevant to area) include tax administration, as well as, trade activities import, export and transit administration;	Revenue Service is the main counterpart for HDM eCustoms implementation and harmonisation issues.	Head of International Relations Department suridia@rs.ge Head of information Technology Centre

Organisation 2 Data Exchange Agency, **Ministry of Justice**	√	√	√	√	√		Data Exchange Agency (DEA) started its operation on January 4, 2010. The agency operates under the status of LEPL (Legal Entity of Public Law) and is governed by the Ministry of Justice of Georgia. DEA's overall activity is divided into several directions. Each of them bears equal importance and strives to support the following fields: E-governance development, creation and installation of unified Georgian Governmental Gateway (3G) and its monitoring, establishment of data exchange infrastructure. Setting ICT standards for public sector entities and elaborating information security policies are the agency's another important responsibility.	Data Exchange Agency as coordinator of E-governance initiatives would be responsible for inter-agency coordination, technical standards and procedures of data exchange between the eCustoms system and other e systems and services deployed within government.	

Moldova

(1) Customs Service of the R. Moldova

(2) Chamber of Commerce and Industry of Moldova

Organisation	**Level of involvement (High, Medium or Low)**						**Description**	**Key functions in relation to HDM**	**Contact details**
	EU cooperation	National policy	Strategy	Legislation	Executive	Regulatory body			
Organisation 1 (Customs Service)	H	M	M	M	H	H	Ensuring implementation of the National Customs Policy and legislation. The Customs Service is subordinated to the Ministry of Finance and ensures customs policy and legislation implementation.		
Organisation 2 (e-Government Centre)	H	M	M	M	M	M			
Organisation 3 (State chancellery)	H	H	H	M	M	M			
Organisation 4 (State Enterprise)	M	M	M	M	H	M			

Ukraine

1. State Fiscal Services of Ukraine, Department for IT and E-Services Development and Taxpayers' Registration: A.Dzyubaty, O.Ivashkovych

2. Ministry for Regional Development and Building of Ukraine, State Agency for e-Governance of Ukraine - O. Ryzhenko

Organisation	Level of involvement (High, Medium or Low)						Description	Key functions in relation to HDM	Contact details
	EU cooperation	National policy	Strategy	Legislation	Executive	Regulatory body			
The State Customs Service of Ukraine	X			P	X		The State Customs Service of Ukraine (SCSU) is a specially authorized central body of executive power in the area of customs practice that was created in 1991 with the mission to direct, co-ordinate, and control the activities of customs authorities, specialized customs institutions and organizations in implementing the laws of Ukraine on customs practice.	- Technical realization, eCustoms operations and support (IT Department); - EU cooperation support (Foreign Department); - Methodology development (OrgMytcontrol).	http://arc.customs.gov.ua/dmsu/control/en/index
Ministry of Finance (MinFin),		X	X	X		X	Principal authority among central executive authorities forming and implementing the financial, budget, tax and customs policy of the State. Has recently formed Department on Tax and Customs	- National Policy and Strategy set-up, - Legislation and regulations; - Development of specific Action plan in reference to all Customs-related action steps for the EU-Ukraine Association	http://Minfin.gov.ua

							Policy.	Agreement	

Digital skills

Azerbaijan

Organisation	Level of involvement (High, Medium or Low)						Description	Key functions in relation to HDM	Contact details
	EU cooperation	National policy	Strategy	Legislation	Executive	Regulatory body			
Organisation 1 (Ministry of Education of the Azerbaijan Republic)	Medium	High	High	High	High	High	Central executive body responsible for formation, execution and regulation of state policy on education process, as well as for performing methodical guidance to education process in Azerbaijan.	Azerbaijan Educational Network, pilot project "E-school", "e-resurs.edu.az" portal, www.e-test.edu.az, www.video.edu.az, www.e-derslik.edu.az portals	49 Khatai Avenue, Baku, Azerbaijan Republic, AZ-1008 Phone: (+ 99412) 599-11-55, fax: (+ 99412) 496-34-83 www.edu.gov.az
Organisation 2 (Ministry of Labour and Social Protection of Population / State Employment Service)	Low	High	High	High	High	High	Central executive body contributing to high-levelled execution of social policy, improvement of welfare state of country's population	N/A	AZ 1009, Baku, Salatin Asgarova str., 85 Phone: (+994 12) 596 50 33 http://www.mlspp.gov.az

Belarus

Belarusian State University

Scientific and Technological Association "Infopark"

Itransition

Ministry for Economy of Belarus

Ukraine

1. Ministry of Economic Development and Trade of Ukraine, Digital Economy Division

2. IT Association NGO

Organisation	Level of involvement (High, Medium or Low)	Description	Key functions in	Contact details

	EU cooperation	National policy	Strategy	Legislation	Executive	Regulatory body		relation to HDM	
Ministry of Economic Development and Trade of Ukraine, Department of Digital Economy	H		H	H	H		Ministry of Economic Development and Trade of Ukraine is the central body of executive power, directed by the Cabinet of Ministers of Ukraine. The main tasks: state policy of economic, social and digital development and trade, state industrial policy, state foreign policy, state policy in the field of technical regulations, conformity assessment and standardizatio n of state property management, business development, public-private partnerships, public procurement.	Owner of the Digital Agenda, intended to centrally cover related topics	http://www.me.gov.ua/Documents/List?lang=uk-UA&tag=PravoviZasadiDiialnosti
State Agency on e-government affairs of Ukraine		H	H		H		Agency is a central body of executive power implements state policy in the field of electronic information, e-governance, and development of the information society.	One of the main objectives is the development of e-business, e-commerce, digital signature, information security, implementatio n of remote services in the banking system.	http://dknii.gov.ua/

Telecom rules

Armenia

Organisation	Level of involvement (High, Medium or Low)						Description	Key functions in relation to HDM	Contact details
	EU cooperation	National policy	Strategy	Legislation	Executive	Regulatory body			
Organisation 1 (PSRC)	high	medium	medium	high	high	high		Regulation	Armenia, 0002, Yerevan, Saryan St., 22 Building Tel: +374-10-584529 http://www.psrc.am
Organisation 2 (Ministry of Transport and Communication)	high	high	high	high				Policy making	Armenia, 0010, Yerevan, Nalbandyan St., 28 Building Tel: +374-10-590021 http://www.mtc.am
Organisation 3 (Ministry of Economy)	high	high	high	high	medium			Policy making, international programs	Minister Armenia, 0010, Yerevan, Mher Mkrtchyan St., 5 Building Tel: +374-10-597206 http://www.mineconomy.am
Organisation 4 (SCPEC)						medium		Protection of competition, ex-post	Armenia, 0010, Yerevan, Mher Mkrtchyan St., 5 Building, Tel: +374-10-543985 http://www.competition.am
Ministry of Foreign Affairs	high							International relations, programs	Edward Nalbandyan, Minister Armenia, 0010, Yerevan, Hanrapetutyan Sq., Government House 2 Tel: +374-60-620000 http://www.mfa.am
Staff of the Government	medium		medium	medium	medium			Policy making, implementation of special programs	Republic Square, Government House 1, 0010 Yerevan, Republic of Armenia Tel.: (+37410) 51-57-03 www.gov.am

Belarus

(1) Ministry of Communications and Informatisation of the Republic of Belarus

(2) State Inspection on Telecommunication of the Republic of Belarus at the Ministry Of Communications and Informatisation of Belarus

(3) Operations and Analysis Centre under the President of the Republic of Belarus:

Ukraine

1. ICT Committee of American Chamber of Commerce in Ukraine, Regulatory Division at life:) - one of the 3 mobile operators

2. Ministry of Economic Development and Trade of Ukraine, Digital Economy Division

3. State Service of Special Communications and Information Protection of Ukraine (DSSZZI)

4. National Commission for the State Regulation of Communications and Informatisation (NKRZI)

6 BIBLIOGRAPHY AND SOURCES

World Bank – Enterprise Surveys / Innovation and technology

Eurostat - ENP countries: information society statistics

ENISA 'Practical Guide on Development and Execution' for National Cyber Security Strategies (2012) http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

ENISA 'Good Practice Guide on National Cyber Security Strategies' http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper;

EaPeReg Benchmarking Report – Benchmarking Electronic Communications Markets in EaP countries, 2015.

7 QUESTIONNAIRES

7.1 NETWORK AND INFORMATION SECURITY AND CYBER-SECURITY

Study on the Harmonisation of the Digital Markets (HDM) in the Eastern Partnership (EaP) countries

[Senior Expert 1, version 19th March 2015]

QUESTIONNAIRE FOR NETWORK AND INFORMATION SECURITY AND CYBER-SECURITY

Introduction

Network and information security (NIS) and Cyber-security are key enablers for secure cross-border electronic transactions and central building blocks of the Digital Single Market. This document is a guide for filling out the Questionnaire for this HDM priority area. Annex 1 of the Terms of Reference for the Study describes this area as follows: "The forthcoming Regulation on "*NIS refers to the security of the Internet and the private networks and information systems underpinning the functioning of our societies and economies. The EU approaches NIS from an internal market/ economic and industrial angle both from a policy perspective and in terms of legislation. Cybersecurity is even wider and multi-dimensional issue where other perspectives come to play: home affairs/fight against cybercrime, defence, diplomacy and foreign relations*."

EU baseline for Network and information security (NIS) and Cyber-security

As stated in the paragraph 2.3 of the project Terms of Reference, the EU baseline consists of relevant EU legislation, EU practices, standards and ICT platforms as appropriate for each HDM area. NIS refers to the security of the Internet and the private networks and information systems underpinning the functioning of our societies and economies. The EU approaches NIS from an internal market/ economic and industrial angle both from a policy perspective and in terms of legislation. Cyber-security is even wider and multi-dimensional issue where other perspectives come to play: home affairs/fight against cybercrime, defence, diplomacy and foreign relations.

For Network and information security/cyber-security, this EU baseline has been defined in consultation with DG CONNECT and presented in the attached document to be used in conjunction with this questionnaire. The baseline for this questionnaire is governed largely by:

EU Legislation

- Articles 13a and 13b in page 55 of the Framework Directive contain security risk management and incident reporting requirements for electronic communications operators.
- Proposal for a DIRECTIVE concerning measures to ensure a high common level of network and information security across the Union **-** still under discussion with the EP and the Council.

EU Agency

- European Union Network and Information Security Agency (ENISA) - current mandate is set out in Regulation 526/2013

Most recent Policy Communications

- Cybersecurity strategy of the EU - Joint Communication JOIN(2013) 1
- Commission Communications on Critical Information Infrastructure Protection (CIIP): COM(2009) 149 and COM(2011) 163

The actual EU baseline prepared for this study is presented in Table 1.

Objective and gap assessment

The Questionnaire aims at determining the current state of play in the EaP countries assessed in relation to the relevant EU baseline expressed in the form of 18 key benchmarks selected for this study. Its specific objectives are as follows:

- to establish (for each EaP country) the results already achieved in relation to the EU baseline for Network and information security/Cyber-security;
- to capture opinions on the conditions required for the achievement of full harmonization of digital markets with the EU in respect to Network and information security/Cyber-security;
- to identify possible areas (technological, political, economic) for any expected benefits from harmonization;
- to identify and list the organizations involved in the field of Network and information security/Cyber-security.

Benchmarks and gap analysis

The questionnaire contains 22 benchmark statements (derived from the EU baseline) grouped around eight main benchmark indicators. These are:

Enablers:

- Leadership benchmark 1 – Political will and commitment
- Policy benchmark 1 – International cooperation
- Policy benchmark 2 – Open and free internet
- Policy benchmark 3 – Capacity building
- Strategy benchmark 1 – Availability of the national strategy
- Strategy benchmark 2 – National priorities and governing institutions

- Resources benchmark 1 – Adequacy of resource base
- Implementation benchmark 1 – Cyber-attack simulations
- Implementation benchmark 2 – Alert platforms, hotlines, public awareness
- Implementation benchmark 3 – Cyber-security products and standards

Results:

- Legal framework benchmark 1 – Regulatory and institutional environment
- Legal framework benchmark 2 – Minimal security levels
- Legal framework Benchmark 3 – Management of security breaches
- Legal framework benchmark 4 – Transparency and openness
- Legal framework benchmark 5 – Confidentiality of data and privacy protection
- Legal framework benchmark 6 – Attacks against information systems
- Legal framework benchmark 7 – Reporting on security incidents
- Infrastructure benchmark 1 – Understanding critical information infrastructure
- Infrastructure benchmark 2 – Identifying critical information infrastructure
- Infrastructure benchmark 3 – Private sector critical information infrastructures
- Services benchmark 1 – Services by Computer Emergency Response Team (CERT)
- Services benchmark 2 – Services to National Regulatory Authority (NRA)

The interviewees (respondents) should be asked by the National Experts to agree or disagree with the relevance of these benchmark statements to their countries. The level of relevance is measured on a five-point scoring scale, which comprises the following answering options: Strongly disagree; Disagree; Uncertain; Agree; Strongly agree. These answers should demonstrate the proximity of the national state of play to the EU Baseline on each specific benchmark.

By selecting one of the above answer options, respondents express their own opinion (judgment) based on the professional experience and available evidence. They should be prepared to explain the rationale behind the answer and support it with concrete facts and data. The respondents also should be asked to assess existing risks, challenges, obstacles, opportunities and possible benefits both in relation to the specific benchmark area and in general, as far as the implementation of the entire HDM initiative is concerned.

The proposed benchmark statements in the questionnaire allow for the assumption that the EaP countries are not yet on par with the EU baseline, i.e. there is a gap to be closed. At the same time, the EU baseline has been formulated in such a way that it is relevant and important for all EaP countries in its own right where the progress can realistically be made. In other words, alignment to the baseline is expected to have real national benefits (technological, political, and economic) regardless of the need to harmonize with the EU per se.

Each EU baseline benchmark is described in detail in the Benchmark notes field, which should enable you to understand the key elements of each question without having to read the vast volume of EU Directives, Commission recommendations etc. that are referred to in the baseline.

Structure of the Questionnaire

The questionnaire consists of two parts. Part 1 contains the EU baseline benchmarks that manifest the results already achieved in practice in terms of their relevance for making progress towards these benchmarks.

The format of the questionnaire is a series of statements relating to the Baseline, for example: ***"Your country has adopted and is implementing a national strategy for Network and information security/Cyber-security"*** (Strategy benchmark 1). The respondent is asked to strongly agree, agree, express uncertainty, disagree or strongly disagree with this statement viewed in the context of his/her country's circumstances. The notes that accompany each question describe what needs to be in place for "full applicability". Recording accurate and comprehensive evidence will be key for indentifying existing gaps with the EU baseline.

In additions to the questions associated with three results-based benchmark indicators (i.e. Legal frameworks, Infrastructure, and Services), the respondents should be asked to provide their views about key enablers – Leadership, Policy, Strategy, Resources, Implementation; that is, the task is to clarify the key factors behind the results and related activities, namely: what was the role of political will and leadership, availability of developed strategies and approved policies, allocation of resources (human, technical, financial), clarity of implementation procedures. Responses to such questions will be recorded in the Questionnaire's dedicated fields.

Part 2 collects factual information on the organizations involved in developing digital markets in the country as far as Network and information security/Cyber-security are concerned.

Questions of clarification

Any questions about the structure and requirements of this questionnaire should be referred to yuri.misnikov@gmail.com.

QUESTIONNAIRE FOR NETWORK AND INFORMATION SECURITY AND CYBER- SECURITY

Country name……

[Note: This questionnaire is intended to be completed by the National Experts in the HDM Study Team. It is not intended to be left with the officials in each country (e.g. in ministries and regulatory organizations) that are interviewed as part of the Study.]

Part 1: Country's results

Leadership benchmarks

Leadership benchmark 1 – Political will and commitment

Answer options	Score				
	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one score box only)					
Leadership benchmark 1	**The government of your country demonstrates strong political will and commitment to minimize the negative impact of security threats/incidents on publicly available electronic communications networks and services by passing necessary laws, taking adequate executive decisions and effectively implementing them in practice.**				
Benchmark notes	The benchmark seeks evidence to prove leaderships demonstrated by the government in advancing Network and information security (NIS)/ Cyber security. Adopting appropriate legal and regulatory frameworks, developing and implementing relevant policies and strategies, including the allocation of sufficient resources to enforce such policies and strategies, constitute the areas where such leadership and political will can be demonstrated and documented. One of such areas is the level of empowerment of national regulatory authorities so as these have sufficient powers and capabilities to govern Network and information security (NIS)/ Cyber-security in an effective and transparent manner; for example, to issue binding instructions to operators of public communications networks or providers of public electronic communications services including: - provide information needed to assess the security and/or integrity of their services and networks, including documented security policies; - submit to a security audit carried out by a qualified independent body or a competent national authority and make the results thereof available to the national regulatory authority. The cost of the audit shall be paid by the undertaking.				
Please record relevant evidence in support of the answer given by the respondent; includes reporting on key enablers when concrete results have been achieved	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Role of leadership for achieving the reported results* _____ _____				

	Availability of developed strategies and approved policies for achieving the reported results _____ *Allotted resources for achieving the reported results* _____ *Clarity of the implementation plan for achieving the reported results* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ _
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____

	Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Other remarks

_____

Policy benchmarks

Policy benchmark 1 – International cooperation

Answer options	Score				
	Strongly disagree	**Disagree**	**Uncertain**	**Agree**	**Strongly agree**
Enter your response (tick one score box only)					
Policy benchmark 1	**Cooperation with the European Union and/or other countries in the field of Network and information security (NIS)/Cyber-security is an important policy objective/priority of your country supported by relevant legal/regulatory provisions and the actual practices.**				
Benchmark notes	The objective of this benchmark is to check out whether international (or regional for that matter) cooperation has become an important issue of				

domestic policies in NIS)/Cyber-security area. For the European Union in general and Member States specifically, pan-European cooperation is indispensible for ensuring the required level of Network and information security (NIS)/Cyber-security. All major legal and regulatory documents, as well as more specialized policy recommendations – such as those of the European Network and Information Security Agency (ENISA) regarding capacity building of national/government Computer Emergency Response Teams (CERTs) – make cooperation between the EU Members States, on the one hand, and between the latter and the European governing institutions (the European Commission in the first place), on the other, a fundamental policy priority.

For example, the Digital Agenda for Europe (DAE) and Cyber Security Strategy aim at increasing the level of cooperation among EU Member States with regard to all NIS/Cyber-security related aspects.

The scope of such cooperation includes:

- developing and funding a network of national Cybercrime Centers of Excellence to facilitate training and capacity building including through mutual support;
- further supporting the EU-wide Computer Emergency Response Team (CERT-EU) responsible for the security of the IT systems of the EU institutions, agencies and bodies (established in 2012);
- creating a cooperation mechanism among Member States and the Commission to share early warnings on risks and incidents through a secure infrastructure and organizing regular peer reviews;
- regularly publishing on a dedicated website unclassified information about on-going early warnings on incidents and risks and on coordinated responses;
- organizing cyber-incidents simulations and the supporting to EU-wide cyber security preparedness;
- further empowering the European Union Agency for Network and Information Security (ENISA) to carry out its tasks in the field of electronic communications and thus contributing to the proper functioning of the internal market;
- increasing cooperation and transparency about security in ICT products;
- promoting a Single Market for cyber security products across equipment manufacturers, software developers, information society services providers to make security a priority;
- creating incentives to carry out appropriate risk management and adopt security standards and solutions, as well as establish voluntary EU-wide certification schemes building on existing schemes in the EU and internationally;
- promoting the adoption of coherent approaches among the Member States to avoid disparities causing locational disadvantages for businesses;
- collaborating and exchanging information with other regulatory bodies, and in particular personal data protection authorities.

Please record relevant evidence in support of the answer given by the respondent; includes reporting on key enablers when concrete results have been achieved	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence regarding additional (supplementary) questions, if relevant:* _____ *Role of leadership for achieving the reported results* _____ *Availability of developed strategies and approved policies for achieving the reported results* _____ *Allotted resources for achieving the reported results* _____ *Clarity of the implementation plan for achieving the reported results* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____

Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Other remarks

_____

Policy benchmark 2 – Open and free internet

Answer options	Score				
	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one score box only)					
Policy benchmark 2	**Keeping the internet free and open in order to protect fundamental rights of individuals, democracy and the rule of law in the cyberspace is an important policy objective/priority of your country.**				
Benchmark notes	This benchmark examines whether the national cyber-security policy is based on the assumption that fundamental rights, democracy and the rule of law need to be protected in cyberspace as well, just as in the physical world. The EU 'Cyber-security Strategy of the European Union: An Open, Safe and Secure Cyberspace' presumes that cyber-security can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values. Reciprocally, individuals' rights cannot be secured without safe networks and systems. The EU Cyber-security Strategy explicitly protects open internet, online freedom and opportunities. Freedom online requires safety and security. Therefore cyberspace should be protected from incidents, malicious activities and misuse. While private sector and civil society drive Internet innovations, governments should have a clear policy aimed at ensuring a free, safe and reliable cyberspace. These are the main principles for cyber-security in the EU: - Protecting fundamental rights, freedom of expression, personal data and privacy. - Access for all. - Democratic and efficient multi-stakeholder governance. - A shared responsibility to ensure security.				
Please record relevant evidence in support of the answer given by the respondent; includes reporting on key enablers when concrete results have been achieved	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence regarding additional (supplementary) questions, if relevant:* _____				

	Role of leadership for achieving the reported results _____ *Availability of developed strategies and approved policies for achieving the reported results* _____ *Allotted resources for achieving the reported results* _____ *Clarity of the implementation plan for achieving the reported results* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ _
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)*

and opportunities to achieve the EU baseline, as viewed by the respondent	Conditions: _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits: _____ Technological benefits: _____ Political benefits: _____ Other benefits: _____

Other remarks

_____

Policy benchmark 3 – Capacity building

Answer options	Score				
	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one score box only)					
Policy benchmark 3	Your country has a clear national policy/programme aimed at enhancing institutional, administrative, technical and human resource				

	capacities in the field of Network and information security (NIS)/Cyber-security.
Benchmark notes	The EU has a clear policy to build and constantly enhance capacities in NIS/Cyber-security by supporting a network of the national/government Computer Emergency Response Teams (CERTs) at the Member States level including an EU-wide Computer Emergency Response Team (CERT-EU). Such support includes, for example, the development of policy recommendations issued by the European Network and Information Security Agency (ENISA) to enhance capabilities of national CERTs to ensure that: - Critical information infrastructure (CII) becomes an integral part of a national social and economic policy agenda; - Best practices identified and templates developed to comply with data protection regulations to empower CERTs with more authority to require telecom service providers and ISPs to implement security measures and changes.
Please record relevant evidence in support of the answer given by the respondent; includes reporting on key enablers when concrete results have been achieved	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence regarding additional (supplementary) questions, if relevant:* _____ *Role of leadership for achieving the reported results* _____ *Availability of developed strategies and approved policies for achieving the reported results* _____ *Allotted resources for achieving the reported results* _____ *Clarity of the implementation plan for achieving the reported results*

	_____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____

this benchmark between the partner countries and with the EU, as viewed by the respondent	Technological benefits: _____ Political benefits: _____ Other benefits: _____

Other remarks

_____

Strategy benchmarks

Strategy benchmark 1 – Availability of the national strategy

Answer options	Score				
	Strongly disagree	**Disagree**	**Uncertain**	**Agree**	**Strongly agree**
Enter your response (tick one score box only)					
Strategy benchmark 1	**Your country has adopted and is implementing a national strategy for Network and information security/Cyber-security.**				
Benchmark notes	The benchmark examines the availability of the strategic vision and related officially approved national frameworks that exist in the field of Network and Information Security (NIS) and Cyber security. The EU has a number of relevant strategic frameworks such as the European Digital Agenda for Europe including Cyber security strategy.				
Please record relevant evidence in support of the answer given by the respondent; includes reporting on key enablers when concrete results have been	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence regarding additional (supplementary) questions, if*				

achieved	*relevant:* _____ *Role of leadership for achieving the reported results* _____ *Availability of developed strategies and approved policies for achieving the reported results* _____ *Allotted resources for achieving the reported results* _____ *Clarity of the implementation plan for achieving the reported results* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ _
Please record main obstacles obstructing achievement of the EU baseline, as	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____

viewed by the respondent	
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Other remarks

_____

Strategy benchmark 2 – National priorities and governing institutions

Answer options	Score				
	Strongly disagree	**Disagree**	**Uncertain**	**Agree**	**Strongly agree**

Enter your response (tick one score box only)					
Strategy benchmark 2	**Your country's national strategy for Network and information security/Cyber security includes a set of clearly defined objectives and related priority actions that include the designation of a national competent authority to deal with cyber security incidents.**				
Benchmark notes	This benchmark concerns the scope and breadth of the national strategic frameworks that exist in the field of Network and Information Security (NIS) and Cyber-security. For example, the European Digital Agenda for Europe defines EU's five strategic priorities in cyber-security (Achieving cyber resilience; Drastically reducing cybercrime; Developing cyber defense policy and capabilities related to the Common Security and Defense Policy (CSDP); Developing the industrial and technological resources for cyber-security; Establishing a coherent international cyberspace policy for the European Union and promoting core EU values) and contains 14 actions under Pillar III on Trust & Security, among which there are 4 specific actions that need to be implemented by Member States. The key among them is the establishment of government/national Computer Emergency Response Teams (CERTs).				
Please record relevant evidence in support of the answer given by the respondent; includes reporting on key enablers when concrete results have been achieved	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence regarding additional (supplementary) questions, if relevant:* _____ *Role of leadership for achieving the reported results* _____ *Availability of developed strategies and approved policies for achieving the reported results* _____ *Allotted resources for achieving the reported results*				

	_____ _____ *Clarity of the implementation plan for achieving the reported results* _____ _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ _
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)*

economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	Economic benefits: _____ Technological benefits: _____ Political benefits: _____ Other benefits: _____

Other remarks

_____

Resources benchmarks

Resources benchmark 1 – Adequacy of resource base

Answer options	Score				
	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one score box only)					
Resources benchmark 1	Your government allocates sufficient resources, especially financial, to ensure the adequate functioning of key institutions and critical infrastructures in the field of Network and information security (NIS)/Cyber-security.				
Benchmark notes	This benchmark investigates whether the government allocates sufficient financial, technical, organizational and human resources needed to ensure the adequate protection and upgrade of the country's critical information infrastructure and services. For example, in the EU, specific funding provisions exist to enable national/government Computer Emergency Response Team (CERTs) meet their responsibilities and create a network of national Cybercrime Centers of Excellence to facilitate training and capacity building. Through its recommendations, ENISA helps identify necessary				

	experts and policymakers. The EU governing bodies envisage budgetary support in the case of modernizing the existing national infrastructures (Proposal for a Directive of 7.2.2013).
Please record relevant evidence in support of the answer given by the respondent; includes reporting on key enablers when concrete results have been achieved	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence regarding additional (supplementary) questions, if relevant:* _____ *Role of leadership for achieving the reported results* _____ *Availability of developed strategies and approved policies for achieving the reported results* _____ *Allotted resources for achieving the reported results* _____ *Clarity of the implementation plan for achieving the reported results* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____

viewed by the respondent	Risks: _____ _
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits:

	_____

Other remarks

_____

Implementation benchmarks

Implementation benchmark 1 – Cyber-attack simulations

Answer options	Score				
	Strongly disagree	**Disagree**	**Uncertain**	**Agree**	**Strongly agree**
Enter your response (tick one score box only)					
Implementation benchmark 1	**Your government maintains a practice of carrying out regular cyber-attack simulations as part of the national implementation plan in the field of Network and information security (NIS)/Cyber-security.**				
Benchmark notes	This benchmark looks at the key aspects that are needed in order to put the national NIS/Cyber- security strategy and policies into practice effectively. Digital Agenda for Europe (DAE) and its Cyber Security Strategy includes Actions 39 according to which the EU Member States are to carry out cyber-attack simulations. Almost all Member States have carried out such simulations.				
Please record relevant evidence in support of the answer given by the respondent; includes reporting on key enablers when concrete results have been achieved	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence regarding additional (supplementary) questions, if relevant:* _____ *Role of leadership for achieving the reported results* _____ *Availability of developed strategies and approved policies for achieving the*				

	reported results _____ *Allotted resources for achieving the reported results* _____ *Clarity of the implementation plan for achieving the reported results* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions: _____

	Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Other remarks

_____

Implementation benchmark 2 – Alert platforms, hotlines, public awareness

Answer options	**Score**				
	Strongly disagree	**Disagree**	**Uncertain**	**Agree**	**Strongly agree**
Enter your response (tick one score box only)					
Implementation benchmark 2	**Your government implements a coherent range of activities aimed at setting up national alert platforms, organizing hotlines for reporting on harmful content and raising public awareness as part of the national implementation plan in the field of Network and information security (NIS)/Cyber-security.**				
Benchmark notes	This benchmark looks at key aspects that are needed in order to putting the national NIS/Cyber security into practice effectively. Digital Agenda for Europe (DAE) and its Cyber Security Strategy includes Actions 40 and 41				

	according to which the EU Member States are Member States to implement harmful content alert hotlines and Member Stat to set up national alert platforms. ENISA, for example, has been involved in raising awareness through publishing reports, organizing expert workshops and developing public-private partnerships. Europol, Eurojust and national data protection authorities have been active in raising awareness about cyber security in the context of the Safer Internet Programme (focused on the safety of children online, with best practices demonstrated by Latvia. Luxemburg, UK). Almost all Member States have fully implemented hotlines and organized awareness raising campaigns on online safety for children (best practices demonstrated by Latvia. Luxemburg, UK). Over 50% Many Member States have set up national alert platforms as one-stop-shop for the public who can play an active role in reporting illicit online activity and collecting statistics on alerts and thus track the development of cybercrime at national level (best practices demonstrated by Luxemburg, Belgium).
Please record relevant evidence in support of the answer given by the respondent; includes reporting on key enablers when concrete results have been achieved	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence regarding additional (supplementary) questions, if relevant:* _____ *Role of leadership for achieving the reported results* _____ *Availability of developed strategies and approved policies for achieving the reported results* _____ *Allotted resources for achieving the reported results* _____ *Clarity of the implementation plan for achieving the reported results*

	_____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____

this benchmark between the partner countries and with the EU, as viewed by the respondent	Technological _____	benefits:
	Political _____	benefits:
	Other _____	benefits:

Other remarks

_____

Implementation benchmark 3 – Cyber-security products and standards

Answer options	Score				
	Strongly disagree	**Disagree**	**Uncertain**	**Agree**	**Strongly agree**
Enter your response (tick one score box only)					
Implementation benchmark 3	**Your government has a practice of promoting cyber-security products, adopting security standards/solutions, undertaking risk management exercises, establishing voluntary certification schemes using experience of other countries.**				
Benchmark notes	This benchmark looks at the key issues that are needed in order to put the national NIS/Cyber-security strategy and policies into practice effectively. Digital Agenda for Europe (DAE) and its Cyber Security Strategy Digital Agenda for Europe (DAE) and Cyber Security Strategy aim at promoting a Single Market for cyber-security products across equipment manufacturers, software developers, information society services providers, creating incentives to carry out appropriate risk management and adopt security standards and solutions, as well as establish voluntary EU-wide certification schemes building on existing schemes in the EU and internationally to avoid disparities causing locational disadvantages for businesses.				
Please record relevant evidence in support of the answer given by the respondent;	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:*				

includes reporting on key enablers when concrete results have been achieved	_____ *Supporting evidence regarding additional (supplementary) questions, if relevant:* _____ *Role of leadership for achieving the reported results* _____ *Availability of developed strategies and approved policies for achieving the reported results* _____ *Allotted resources for achieving the reported results* _____ *Clarity of the implementation plan for achieving the reported results* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____
Please record	*(Filled in by NEs during/after conducting interview(s) with national*

main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Other remarks

_____

Legal framework benchmarks

Legal framework benchmark 1 – Regulatory and institutional environment

Answer options	Score				
	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one score box only)					
Legal framework benchmark 1	**Your country's legislation and other regulatory acts in the field of Network and information security (NIS)/Cyber-security contain provisions that require establishing a national/government Computer Emergency Response Team (CERT, or equivalent entity) and formulating national NIS/Cyber security strategies.**				
Benchmark notes	The benchmark investigates the completeness, effectiveness and adequacy of the national legal and regulatory frameworks to ensure the continuity of supply of services provided over public electronic communications networks. In the EU, the law requires taking appropriate technical and organizational measures to minimize the negative impact of security threats and incidents on publicly available electronic communications networks and services. Such measures, among other issues, include adopting national NIS/Cyber security strategies, establishing specialized national Computer Emergency Response Team (CERT), empowering the national competent regulatory authority, undertaking awareness raising campaigns on online safety, especially for children, simulating cyber attacks, implementing hotlines/one-stop-shops and early warning systems to ensure the security and integrity of the networks.				
Please record relevant evidence in support of the answer given by the respondent; includes reporting on key enablers when concrete results have been achieved	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence regarding additional (supplementary) questions, if relevant:* _____ _____ *Role of leadership for achieving the reported results* _____ _____ *Availability of developed strategies and approved policies for achieving the*				

	reported results _____ *Allotted resources for achieving the reported results* _____ *Clarity of the implementation plan for achieving the reported results* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions: _____

	Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Other remarks

_____

Legal framework benchmark 2 – Minimal security levels

Answer options	Score				
	Strongly disagree	**Disagree**	**Uncertain**	**Agree**	**Strongly agree**
Enter your response (tick one score box only)					
Legal framework benchmark 2	**Your country's legislation and other regulatory acts contain provisions that establish legally or otherwise binding minimum requirements in the field of Network and information security (NIS)/Cyber-security for public and private operators of electronic networks and service providers.**				
Benchmark notes	The objective of this benchmark is to understand whether there are minimum requirements in the area of Network and information security (NIS)/Cyber-security. For example, there is an intention in the EU to implement specific measures to ensure a high common level of network and information security				

	across the Union and establish legally binding common minimum requirements for NIS at national level (Proposal for a Directive of 7.2.2013).
Please record relevant evidence in support of the answer given by the respondent; includes reporting on key enablers when concrete results have been achieved	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence regarding additional (supplementary) questions, if relevant:* _____ *Role of leadership for achieving the reported results* _____ *Availability of developed strategies and approved policies for achieving the reported results* _____ *Allotted resources for achieving the reported results* _____ *Clarity of the implementation plan for achieving the reported results* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____

viewed by the respondent	Risks: _____ _
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits:

	_____

Other remarks

_____

Legal framework Benchmark 3 – Management of security breaches

Answer options	Score				
	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one score box only)					
Legal framework benchmark 3	**Your country's legislation and other regulatory acts in the area of Network and information security (NIS)/Cyber-security contain provisions that empower the competent national regulator to coordinate and instruct the operators of public communications networks or providers of public electronic communications services in case of security breach.**				
Benchmark notes	This benchmark investigates whether the competent national regulatory authority is sufficiently empowered to manage and coordinate security incidents among public and private entities, including the investigation of non-compliance and its consequences for the security and integrity of the networks. The EU-wide and national laws in Europe provide sufficient powers to the competent regulator to ensure compliance.				
Please record relevant evidence in support of the answer given by the respondent; includes reporting on key enablers when concrete results have been achieved	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence regarding additional (supplementary) questions, if relevant:* _____ *Role of leadership for achieving the reported results* _____				

	Availability of developed strategies and approved policies for achieving the reported results _____ *Allotted resources for achieving the reported results* _____ *Clarity of the implementation plan for achieving the reported results* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ _
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____

	Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Other remarks

_____

Legal framework benchmark 4 – Transparency and openness

Answer options	**Score**				
	Strongly disagree	**Disagree**	**Uncertain**	**Agree**	**Strongly agree**
Enter your response (tick one score box only)					
Legal framework benchmark 4	**Your country's legislation and other regulatory acts in the area of Network and information security (NIS)/Cyber-security contain provisions that require the competent national regulator to inform the public when the disclosure of security breaches is in the public interest.**				
Benchmark notes	This benchmark investigates whether the competent national regulatory authority is obliged to disclose security breaches of public importance. In the				

	EU, this is an important measure of government openness to keep the public informed – in line with legislation governing the provision of and access to Public Sector Information (PSI) – about significant security failures in electronic communication and services that affect citizens and businesses. It is also a means of exercising the public control over government performance to create and maintain an effective and transparent system of Network and Information Security (NIS).
Please record relevant evidence in support of the answer given by the respondent; includes reporting on key enablers when concrete results have been achieved	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence regarding additional (supplementary) questions, if relevant:* _____ *Role of leadership for achieving the reported results* _____ *Availability of developed strategies and approved policies for achieving the reported results* _____ *Allotted resources for achieving the reported results* _____ *Clarity of the implementation plan for achieving the reported results* _____
Please record main challenges and risks for	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)*

achieving this EU baseline and implementing HDM in general, as viewed by the respondent	Challenges: _____ Risks: _____ _
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____

	Other benefits: _____

Other remarks

_____

Legal framework benchmark 5 – Confidentiality of data and privacy protection

Answer options	Score				
	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one score box only)					
Legal framework benchmark 5	**Your country's legislation and other regulatory acts in the area of Network and information security (NIS)/Cyber-security contain provisions that require the providers of publicly available electronic communications services to guarantee the confidentiality of the related traffic data and services.**				
Benchmark notes	The objective of this benchmark is to analyze whether there are conditions for ensuring that the providers of public electronic communications services take appropriate technical and organizational measures to safeguard the security of its services, which includes the guaranteed confidentiality of the communications and related traffic data. This benchmark should be viewed in the context of the legal requirement to protect online privacy of citizens and their personal data during information processing.				
Please record relevant evidence in support of the answer given by the respondent; includes reporting on key enablers when concrete results have been achieved	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence regarding additional (supplementary) questions, if relevant:* _____				

	Role of leadership for achieving the reported results _____ *Availability of developed strategies and approved policies for achieving the reported results* _____ *Allotted resources for achieving the reported results* _____ *Clarity of the implementation plan for achieving the reported results* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ _
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)*

to achieve the EU baseline, as viewed by the respondent	Conditions: _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits: _____ Technological benefits: _____ Political benefits: _____ Other benefits: _____

Other remarks

_____

Legal framework benchmark 6 – Attacks against information systems

Answer options	Score				
	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one score box only)					

Legal framework benchmark 6	**Your country's legislation and other regulatory acts in the area of Network and information security (NIS)/Cyber-security contain provisions that establish minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems and computer data.**
Benchmark notes	This benchmark seeks to find out whether national laws and regulations clearly define illegal attacks against information systems that are considered (and punished) as criminal offences. The EU law treats any attempt to illegally interfere with (a) information systems (by way of inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible, intentionally and without right) and (b) computer data (by way of deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible, intentionally and without right) as a punishable criminal offence.
Please record relevant evidence in support of the answer given by the respondent; includes reporting on key enablers when concrete results have been achieved	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence regarding additional (supplementary) questions, if relevant:* _____ *Role of leadership for achieving the reported results* _____ *Availability of developed strategies and approved policies for achieving the reported results* _____ *Allotted resources for achieving the reported results* _____

	Clarity of the implementation plan for achieving the reported results _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____

harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	Technological benefits: _____ Political benefits: _____ Other benefits: _____

Legal framework benchmark 7 – Reporting on security incidents

Answer options	Score				
	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one score box only)					
Legal framework benchmark 7	Your country's legislation and other regulatory acts in the area of telecommunications and/or Network and information security (NIS)/Cyber-security contain provisions requiring that trust and other service providers take adequate technical and organizational measures to minimize the impact of security incidents and in the case of the security breach they notify the supervisory body within 24 hours after having become aware of the breach.				
Benchmark notes	The benchmark's aim is to describe whether there are any security and risk management policies requiring, as in the EU, trust service providers to ensure that they take appropriate technical and organizational measures to minimize the impact of security incidents; for example, by ensuring that such measures will guarantee the level of security at least at the same level as a potential degree of risk. There is also a policy requirement to inform the supervisory body (e.g. the competent national body for information security or the data protection authority) of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data such services may contain within 24 hours after having become aware of the breach; the affected natural or legal persons to whom the trusted services have been provided must be informed as well without undue delay. Moreover, the public should be informed if the disclosure of the breach of security or loss of integrity is in the public interest.				

Please record relevant evidence in support of the answer given by the respondent; includes reporting on key enablers when concrete results have been achieved	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence regarding additional (supplementary) questions, if relevant:* _____ *Role of leadership for achieving the reported results* _____ *Availability of developed strategies and approved policies for achieving the reported results* _____ *Allotted resources for achieving the reported results* _____ *Clarity of the implementation plan for achieving the reported results* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____

Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Infrastructure benchmarks

Infrastructure benchmark 1 – Understanding critical information infrastructure (CII)

Answer options	Score				
	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one score box only)					
Infrastructure benchmark 1	**Your country's national strategic framework in Network and information security (NIS)/Cyber security clearly emphasizes the importance of enhancing security and resilience of critical information infrastructures in order to prevent disruptions in the of the supply of critically important products in the vital for socio-economic development areas.**				
Benchmark notes	This benchmark's aim is to find out whether the notion of the Critical Information Infrastructure (CII) viewed from the perspective of cyber security and resilience has become a matter of strategic importance and part of the national policy planning in the field of Network and information security (NIS)/Cyber security. The European Commission's proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (part of a Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 7.2.2013) states that cooperation and exchange of information between Member States should be supported by a secure infrastructure. Over the past several years, the EU's key governing institutions (the European Commission, the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions) have made the issue of CII protection a key item of the European Cyber Security strategy. For example, in 2008, Directive 2008/114 (COM(2006) 786)) on European critical infrastructures and their protection helped identify and designate European critical infrastructures (ECIs), as well empower European Network and Information Security Agency (ENISA) to provide policy and advisory services to implement Article 13 of the EU telecom framework regarding security measures and incident reporting. In 2009, the Commission adopted a Communication on Critical Information Infrastructure protection (CIIP) (further to a similar Communication of 2006) focusing on the protection of Europe from cyber disruptions by enhancing security, which was followed up by a new				

	Communication on CIIP in 2011 ("Achievements and next steps: towards global cyber-security") to take stock of the results achieved since the adoption in 2009 of the CIIP action plan. The Digital Agenda for Europe (DAE) of 2010 emphasized the need for all stakeholders to join forces in a joint effort to ensure the security and resilience of ICT infrastructure, by focusing on prevention, preparedness and awareness, as well as to develop effective and coordinated security mechanisms. Further, in 2012, the European Parliament passed in 2012 a Resolution "Critical Information Infrastructure Protection: towards global cyber-security" with the aim to stimulate and support the development of a high level of preparedness, security and resilience capabilities both at national and European level. This approach was broadly endorsed by the Council in 2009. Most recently, the Commission's Proposal for a Directive of the European Parliament and of the Council (2013) defined measures to ensure a high common level of network and information security across the Union. At the same time, the European Network and Information Security Agency (ENISA) issued policy recommendations (Baseline Capabilities of National/Governmental CERTs) made cyber-security as a part of national policy.
Please record relevant evidence in support of the answer given by the respondent; includes reporting on key enablers when concrete results have been achieved	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence regarding additional (supplementary) questions, if relevant:* _____ _____ *Role of leadership for achieving the reported results* _____ _____ *Availability of developed strategies and approved policies for achieving the reported results* _____

	_____ *Allotted resources for achieving the reported results* _____ _____ *Clarity of the implementation plan for achieving the reported results* _____ _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ _
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____

Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Other remarks

_____

Infrastructure benchmark 2 – Identifying critical information infrastructure (CII)

Answer options	Score				
	Strongly disagree	**Disagree**	**Uncertain**	**Agree**	**Strongly agree**
Enter your response (tick one score box only)					
Infrastructure benchmark 2	**Using clear guidelines and criteria, your government has identified specific sectors whose information infrastructures are designated as critically important for the functioning of economy and society at large.**				
Benchmark notes	This benchmark investigates the availability of the officially designated Critical Information Infrastructures (CCI) identified on the basis of existing guidelines and criteria. The EU law requires that Member States identify potential European Critical Infrastructures (ECIs). Member States should make use of a series of developed criteria to identify these potential ECIs. Some criteria are cross-sectoral to take proper account of possible casualties and economic and public effects, while other focus on particular ECI sectors (e.g. at the moment energy and transport sectors and their subsectors are prioritized). Some ECIs span over more than one Member State and in this situations the latter should go through a cooperative designation process for potential ECIs located on their territory. This process involves discussions with other Member States, which could be significantly affected in case of the loss of service provided by an infrastructure. In order for an infrastructure to be formally designated as an ECI, the Member State on whose territory it is located must give its assent.				
Please record relevant evidence in support of the answer given by the respondent; includes reporting on key enablers when concrete results have been achieved	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence regarding additional (supplementary) questions, if relevant:*				

	_____ *Role of leadership for achieving the reported results* _____ *Availability of developed strategies and approved policies for achieving the reported results* _____ *Allotted resources for achieving the reported results* _____ *Clarity of the implementation plan for achieving the reported results* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____

Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____

	Political benefits: _____ Other benefits: _____

Infrastructure benchmark 3 – Private sector infrastructures

Answer options	Score				
	Strongly disagree	**Disagree**	**Uncertain**	**Agree**	**Strongly agree**
Enter your response (tick one score box only)					
Infrastructure benchmark 3	**Your country's national strategic framework in Network and information security (NIS)/Cyber-security ensures that the private sector operators adopt appropriate and proportionate measures to prevent disruptions in the supply of critically important products/services and report to the authorities about all incidents which severely endanger their networks.**				
Benchmark notes	This benchmark investigates whether the government efforts to enhance security and resilience of critical information infrastructures also extend to cover the private sector operators of such infrastructures (as it is the case in the EU), especially those that supply critically important products and services in such vital for the society and economy areas as financial services, transport, energy, health, app stores, e-commerce platforms, Internet payment, cloud computing, search engines, social networks take appropriate and proportionate measures to ensure network and information security. An important element of the enhanced security and resilience of critical information infrastructures is a requirement to report to the authorities about security breaches and incidents affecting their services and products.				
Please record relevant evidence in support of the answer given by the respondent; includes reporting on key enablers	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____				

when concrete results have been achieved	*Supporting evidence regarding additional (supplementary) questions, if relevant:* _____ *Role of leadership for achieving the reported results* _____ *Availability of developed strategies and approved policies for achieving the reported results* _____ *Allotted resources for achieving the reported results* _____ *Clarity of the implementation plan for achieving the reported results* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ _
Please record main obstacles obstructing	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)*

achievement of the EU baseline, as viewed by the respondent	Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Services benchmarks

Services benchmark 1 – Services by Computer Emergency Response Team (CERT)

Answer options	Score				
	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one score box only)					
Services benchmark 1	**Your country's Computer Emergency Response Team (CERT) or equivalent body provides a coherent range of IT/advisory services in the field of Network and information security (NIS)/Cyber-security to other government agencies and other organizations and companies.**				
Benchmark notes	The benchmark enquires whether the national agency responsible for Network and information security (NIS)/Cyber-security is sufficiently empowered to provide guidance and related IT/advisory services to other public bodies and private sector operators. In the EU, such services are provided at European and national levels. The EU-wide Computer Emergency Response Team (CERT-EU) provides security services for EU institutions, agencies, bodies including implementation of related projects and initiatives to ensure the coordinated approach to the application of such services (part of the European Cyber Security Strategy and Digital Agenda). At the Member State level, such functions are performed by the national/government Computer Emergency Response Team (CERTs) that are supported by CERT-EU and the European Network and Information Security Agency (ENISA) that provides policy advisory services to CERTs to improve their capabilities. National CERTs also provide a range of other services to the general public.				
Please record relevant evidence in support of the answer given by the respondent; includes reporting on key enablers when concrete results have been achieved	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence regarding additional (supplementary) questions, if relevant:* _____ *Role of leadership for achieving the reported results*				

	_____ _____ *Availability of developed strategies and approved policies for achieving the reported results* _____ _____ *Allotted resources for achieving the reported results* _____ ____ *Clarity of the implementation plan for achieving the reported results* _____ ____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ _
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____

respondent	Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Other remarks

_____

Other remarks

_____

Services benchmark 2 – Services to National Regulatory Authority (NRA)

Answer options	Score				
	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree

Enter your response (tick one score box only)					
Services benchmark 2	**Your country's National Regulatory Authority (NRA) receives competent guidance in order to evaluate the compliance of public telecommunications network and service providers with the existing legal requirements in the field Network and information security (NIS)/Cyber-security.**				
Benchmark notes	The benchmark examines the availability of IT security related services provided for National Regulatory Authorities (NRAs) about security measures they should take into account when evaluating the compliance of public communications network and service providers with the existing legal requirements, as well as when reporting on significant incidents. In the EU, such services are provided by ENISA (European Network and Information Security Agency) in the form technical guidelines to facilitate the implementation of security-related Article 13a 'Security and integrity' of EU Directive 2009/140/EC (Telecom Framework Directive).				
Please record relevant evidence in support of the answer given by the respondent; includes reporting on key enablers when concrete results have been achieved	(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer) Rationale: _____ Supporting evidence regarding additional (supplementary) questions, if relevant: _____ Role of leadership for achieving the reported results _____ Availability of developed strategies and approved policies for achieving the reported results _____ Allotted resources for achieving the reported results _____				

	Clarity of the implementation plan for achieving the reported results _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	(Filled in by NEs during/after conducting interview(s) with national stakeholders.) Challenges: _____ Risks: _____ _
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	(Filled in by NEs during/after conducting interview(s) with national stakeholders.) Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	(Filled in by NEs during/after conducting interview(s) with national stakeholders.) Conditions: _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark	(Filled in by NEs during/after conducting interview(s) with national stakeholders.) Economic benefits: _____

between the partner countries and with the EU, as viewed by the respondent	Technological benefits: _____ Political benefits: _____ Other benefits: _____	

7.2 ELECTRONIC IDENTIFICATION AND TRUST SERVICES

HDM QUESTIONNAIRE

Electronic Identification and Trust Services

Country name _____

Interviewer name _____

Respondents (interviewee) name and title _____

Place and date _____

[Note: This questionnaire is intended to be completed by the National Experts in the HDM Study Team. It is not intended to be left with the officials in each country (e.g. in ministries and regulatory organizations) that are interviewed as part of the Study. For questions and advice, please contact yuri.misnikov@gmail.com].

Introduction

This document is a guide for filling out the Questionnaire for the HDM priority area ***Electronic Identification and Trust Services***. Annex 1 of the Terms of Reference for the HDM Study describes this area as follows: "The forthcoming Regulation on "electronic identification and trust services for electronic transactions in the internal market" sets a comprehensive general legal and technical framework for electronic transactions by regulating the mutual recognition of notified electronic identification schemes and means, by provisioning electronic trust services (i.e. e-signature, e-seals, e-time stamp, e-registered delivery, and website authentication) as well as by ensuring the non-discrimination of electronic documents vis-à-vis their paper equivalent, thus ensuring the legal validity of electronic transactions." The main lessons learned and achievements so far are guided by (i) E-Signature Directive 1999/93/EC and Draft Regulation on "electronic identification and trust services for electronic transactions in the internal market" – EU Legislation; (ii) Mandate M460 given by the Commission to CEN and ETSI (to be revised and extended) – EU Standardisation initiatives/cross border tools; (iii) Large Scale Pilots (such as STORK, STORK 2.0, PEPPOL, SPOCS, e-SENS…) – EU Best practices.

Objective and gap assessment

The Questionnaire aims at determining the current state of play in the EaP countries assessed in relation to the relevant EU baseline expressed in the form of nine key benchmarks selected for this study. Each benchmark includes a statement that describes the EU baseline in a particular sector of Electronic Identification and Trust Services, namely: *(a) Legal frameworks* (and related regulations/ executive decisions), *(b) Infrastructure*, and *(c) Services*. The interviewees (respondents) are asked by the interviewers to agree or disagree with the relevance of these benchmark statements (derived from the EU experience) for their countries. The level of relevance is measured on a seven-point scoring

scale, which comprises the following answering options: (1) Not applicable; (2) Don't know; (3) Strongly disagree; (4) Disagree; (5) Uncertain; (6) Agree; (7) Strongly agree. These answers should demonstrate the proximity of the national state of play to that of the EU.

By selecting one of the above answer options, respondents present their own personal opinion (judgment) based on the professional experience and support their answers with evidence (which includes explaining the rationale behind the answer and relevant facts). The respondents will be asked to provide other information including the existing risks, challenges, obstacles, opportunities, benefits both in relation to the priority area and in general as far as the implementation of the entire HDM initiative is concerned.

Additionally, the interviewers in Armenia and Belarus will seek the respondents' views on the role and possible impact of the Eurasian Economic Union and the Eurasian Customs Union on HDM in the context of benefits (comparing benefits, if possible and feasible, is welcome).

In order to help assess – and measure – the difference (gap) between the national circumstances and the EU baseline as accurately as possible, each benchmark, in addition, is further explored in the form of two interlinked intermediary statuses to measure a degree of progress already made towards the stated EU baseline. The status 1 is closer but not equal to the EU baseline, while the status 2 is farther from it. If the answer is (3) Strongly disagree or (4) Disagree or (5) Uncertain, the interviewer should ask the respondent to choose one intermediary status that is most relevant in the context of a particular benchmark.

The proposed benchmarks are intermediary statuses are based on the assumption that the EaP countries are not yet on par with the EU baseline, i.e. there is a gap to be closed. At the same time, the EU baseline has been formulated in such a way that it is relevant and important (strategic) for all EaP countries (although to a different degree) in its own right where the progress can realistically be made. The essence of each EU baseline benchmark is described in detail in the Benchmark Notes field.

Structure of the Questionnaire

This Questionnaire consists of 2 parts. Part 1 contains three broader indicators that manifest the results that demonstrate what has already been achieved in practice and how relevant these results for making progress towards the established EU benchmarks. The benchmarks are grouped around indicators, which are as follows:

1. Legal frameworks (and related regulations/executive decisions).
2. Infrastructure.
3. Services.

Part 2 collects factual information on the organizations involved in developing digital markets in the country as far as Electronic Identification and Trust Services are concerned.

Part 1: Country's results

Indicator 1: Legal framework

Section 1.1: Benchmark 1 - Legal framework for electronic identification and trust services

Please select one of the answers below to demonstrate how close the benchmark statement presented below reflects upon the state of play in your country (avoid as much as possible selecting the first two answers which require additional explanation); if your answer ranges between options 3 and 5, please choose one the most appropriate intermediary status in relation to the EU baseline							
Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							
Benchmark 1	**<u>Benchmark statement</u>: Special legislation for electronic identification means and trust services contains specific provisions ensuring sufficiently high levels of trust services for secure electronic transactions across borders**						
Benchmark notes	This benchmark aims at assessing the level of trust in the online environment, which is key to economic and social development. The lack of trust, due to the actual or perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services. The Regulation No 910/2014 of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market creates such certainty by (a) setting the rules for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and						

	certificate services for website authentication; (b) laying down rules for trust services, in particular for electronic transactions; (c) establishing a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication. It defines trust services that are recognized by other countries as ***qualified*** trust services (the Member States still can define other types of trust services in addition to the qualified ones). According to the Regulation, the term 'trust service' (TS) means an electronic service normally provided for fee which consists of: (i) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or (ii) the creation, verification and validation of certificates for website authentication; or (iii) the preservation of electronic signatures, seals or certificates related to those services. A four-item list of the qualified TS includes (1) certificates for electronic signatures, (2) electronic signature creating devices, (3) certificates for electronic seals, and (4) certificates for website authentication, along with specific requirements (technology-neutral) set to make the above TSs qualified and thus mutually recognizable across borders. There are three assurances levels – low, substantial and high – applicable in relation to national electronic identification schemes/means (eID providers are still governed by national legislation), supported by minimum technical specifications, standards and procedures. These will govern the reliability and quality of (a) the procedure to prove and verify the identity of natural or legal persons applying for the issuance of electronic identification means; (b) the procedure for the issuance of the requested electronic identification means; (c) the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party; (d) the entity issuing the electronic identification means; (e) any other body involved in the application for the issuance of the electronic identification means; (f) the technical and security specifications of the issued electronic identification means. However, specific supervisory regimes are applied to TS providers only to ensure that the authentication procedure of an online service is mutually recognizable, while the access to such services and their delivery to the requesting user, including the right to receive such service, and still remains under the national supervisory regime. The obligation to recognize the online service is only possible if the electronic identification means are able to produce the identity assurance level equal to or higher than the level required for the requested online service (the high assurance level is needed specially with regard to identity proofing, verification and authentication for issuing qualified certificates). Comparing the availability and scope of the national legal and regulatory framework in the area of electronic identification means and trust services will help identify the existing gaps and find solutions to bridge them.
Please record relevant evidence in	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)*

support of the answer given by the respondent	*Rationale:* _____ *Supporting evidence:* _____						
Intermediate status 1 (closer to benchmark 1)	**The current legislation (including related regulatory framework) contains certain provisions that (a) governs in either specific or general terms both electronic identification means and trust services or (b) governs one of the above; plans exist to enhance such legislation in the near future**						
Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____						
Intermediate status 2 (farther from benchmark 1)	**The current legislation (including related regulatory framework) does not govern neither specially nor generally (a) electronic identification means and/or (b) trust services and no plans exist to have such legislation in the near future**						
Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____						

Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions: _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits: _____

for this benchmark between the partner countries and with the EU, as viewed by the respondent	Technological benefits: _____ Political benefits: _____ Other benefits: _____
For interviewers in Armenia and Belarus only: Please record the respondent's view on the role and impact of the Eurasian Economic Union and the Eurasian Customs Union on HDM; if needed, please refer to the role and impact in the fields above	*Role:* _____ *Impact:* _____ *Benefits comparison:* _____
Please record overall challenges, risks, opportunities/ benefits and impacts for implementing HDM in general, as viewed by the respondent	*Challenges:* _____ *Risks:* _____ *Opportunities/benefits:* _____

	Impacts: _____

Other remarks

_____

Section 1.2: Benchmark 2** - **Legal recognition and use of eSignature across borders

Please select one of the answers below to demonstrate how close the benchmark statement presented below reflects upon the state of play in your country (avoid as much as possible selecting the first two answers which require additional explanation); if your answer ranges between options 3 and 5, please choose one the most appropriate intermediary status in relation to the EU baseline

Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							
Benchmark 2	**<u>Benchmark statement</u>: Certification service-providers offer consumers and businesses opportunities to exchange information and trade electronically in a secure way, regardless of national frontiers and in a competitive environment**						
Benchmark notes	The objective of this benchmark is to ensure that national legislation and related regulations are approximated with that of the EU so as to ensure that (a) national digital signature products are interoperable and legally accepted in the EU countries by using recognised standards for electronic-signature products (compatible with STORK 2.0/PEPS requirements), and (b) certification service providers operate in a competitive environment striking a proper balance between consumer and business needs. This objective stems						

	from the provisions of and goals of the Directive 1999/93/EC and a follow-up Regulation No 910/2014 of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market aimed at facilitating the cross-border use of online services, with particular attention to facilitating secure electronic identification and authentication. Experimental participation in the STORK pilot is planned to help understand how different national eID systems can to talk to each other to access online services in other countries.						
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____						
Intermediate status 1 (closer to benchmark 1)	**National legislation and related regulatory frameworks (a) do contain some provisions that enable mutual legal recognition of national digital signatures and electronic identification schemes of other countries and/or (b) the work is under way/ planned to either introduce such provisions in the near future**						
Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____						
Intermediate status 2 (farther from benchmark 1)	**National legislation and related regulatory frameworks (a) do not contain any provisions that enable mutual legal recognition of national digital signatures and electronic identification schemes of other countries, and (b) no plans exist to introduce such provisions in the near future**						
Answer option (score)	1. Not	2. Don't	3. Strongly	4. Disagree	5. Uncertain	6. Agree	7. Strongly

	applicable	know	disagree				agree
Please tick one box only							
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____						
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____						
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____						
Please record required conditions and opportunities to achieve the EU baseline, as viewed by	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____						

the respondent	Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____
For interviewers in Armenia and Belarus only: Please record the respondent's view on the role and impact of the Eurasian Economic Union and the Eurasian Customs Union on HDM; if needed, please refer to the role and impact in the fields	*Role:* _____ *Impact:* _____ *Benefits comparison:* _____

above	
Please record overall challenges, risks, opportunities/ benefits and impacts for implementing HDM in general, as viewed by the respondent	*Challenges:* _____ *Risks:* _____ *Opportunities/benefits:* _____ *Impacts:* _____

Other remarks

_____

Section 1.3: Benchmark 3 - Trust in electronic services

Please select one of the answers below to demonstrate how close the benchmark statement presented below reflects upon the state of play in your country (avoid as much as possible selecting the first two answers which require additional explanation); if your answer ranges between options 3 and 5, please choose one the most appropriate intermediary status in relation to the EU baseline							
Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							
Benchmark 3	**Benchmark statement: Certification-service-providers and other providers of e-services observe data protection legislation and individual (online) privacy in order to increase user confidence in electronic communication and commerce and thus increase the uptake of e-services**						
Benchmark notes	Regulation No 910/2014 of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market shall be applied in full compliance with the principles relating to the protection of personal data provided for in Directive 95/46/EC of the European Parliament and of the Council (4). The principle of mutual recognition established by this Regulation, authentication for an online service will ensure that only adequate and relevant identification data will be processed (and exchanged) and thus prevent the unauthorized and excessive access to personal data online. Furthermore, Directive 95/46/EC requires that service providers and supervisory bodies guarantee confidentiality and security of						

	personal data processing. The objective of this benchmark is to ensure that (a) there is a sound national legislation and regulatory framework in the field of personal data protection, (b) such legislation is enforced, and (c) certification service providers strictly observe citizens' concerns about privacy protection, for the lack of such assurances hinders the uptake of e-services.						
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____						
Intermediate status 1 (closer to benchmark 1)	**There is a sound national legal and regulatory framework in place that (a) guarantees the protection of personal data from unauthorised access and (b) contains provisions concerning the implementation of the Authentication and Access Control (AAC) service by certification service providers and other relevant government bodies offering e-services**						
Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____						
Intermediate status 2 (farther from benchmark 1)	**National legislation and regulation (a) does not guarantee the protection of personal data according to international standards and (b) does not contain the provisions governing Authentication and Access Control (AAC) when providing electronic services**						
Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							
Please record	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.*						

relevant evidence in support of the answer given by the respondent	*Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____

Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____
For interviewers in Armenia and Belarus only: Please record the respondent's view on the role and impact of the Eurasian Economic Union and the Eurasian Customs Union on HDM; if needed, please refer to the role and impact in the fields above	*Role:* _____ *Impact:* _____ *Benefits comparison:* _____
Please record overall challenges,	*Challenges:* _____

risks, opportunities/ benefits and impacts for implementing HDM in general, as viewed by the respondent	*Risks:* _____ *Opportunities/benefits:* _____ *Impacts:* _____

Other remarks

_____

Section 1.4: Benchmark 4 - Use of electronic signature and identification for public procurement

Please select one of the answers below to demonstrate how close the benchmark statement presented below reflects upon the state of play in your country (avoid as much as possible selecting the first two answers which require additional explanation); if your answer ranges between options 3 and 5, please choose one the most appropriate intermediary status in relation to the EU baseline

Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							

Benchmark 4	**<u>Benchmark statement</u>: National legal and regulatory frameworks governing the use of electronic signature and electronic identification schemes (eIDs) guarantee free access electronic public procurement at all stages including across EU borders**
Benchmark notes	The objective of this benchmark is to promote the use of electronic signature and electronic identification management schemes in public procurement and thus support the creation of a national digital market. Special attention is given to the well-documented EU best practice of benchmarking eProcurement as a basic e-service in terms of the use of such specific ICT-based market instruments as eNotification (publication of procurement notices and electronic registration), eSubmission/eTendering (secure submission of tenders), eAwarding (online publication of awarded contracts, automated evaluation of tenders, electronic auctioning) at both pre-and post-award stages of public procurement (e.g. i2010 eGovernment Action Plan Progress Study. Final Report, 2009; Method paper 2010. Preparing the 9th Benchmark Measurement, June 2010. Capgemini, Rand Europe, IDC, Sogeti and DTi).
Please record relevant	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the*

evidence in support of the answer given by the respondent	*answer)* *Rationale:* _____ *Supporting evidence:* _____						
Intermediate status 1 (closer to benchmark 1)	**National legal and regulatory framework in the field of electronic signature and identification allows the use of the full spectrum of ICT-based market instruments of eProcurement (e.g. eInvoicing, ePayment) at both the pre- and post-award stages of public procurement**						
Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____						
Intermediate status 2 (farther from benchmark 1)	**National legal and regulatory framework in the field of electronic signature and identification either (a) does not allow the use of the full spectrum of ICT-based market instruments of eProcurement (e.g. eInvoicing, ePayment) at any stage of public procurement or (b) does allow such use in a limited manner at a pre-award stage of public procurement**						
Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____						

	Supporting evidence: _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____

other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____
For interviewers in Armenia and Belarus only: Please record the respondent's view on the role and impact of the Eurasian Economic Union and the Eurasian Customs Union on HDM; if needed, please refer to the role and impact in the fields above	*Role:* _____ *Impact:* _____ *Benefits comparison:* _____
Please record overall challenges, risks, opportunities/ benefits and impacts for implementing HDM in	*Challenges:* _____ *Risks:* _____ *Opportunities/benefits:*

general, as viewed by the respondent	_____ *Impacts:* _____

Other remarks

_____

Indicator 2: Infrastructure

Section 2.1: Benchmark 5 - Shared and secure infrastructure for e-government services

Please select one of the answers below to demonstrate how close the benchmark statement presented below reflects upon the state of play in your country (avoid as much as possible selecting the first two answers which require additional explanation); if your answer ranges between options 3 and 5, please choose one the most appropriate intermediary status in relation to the EU baseline							
Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							
Benchmark 5	**Benchmark statement: e-Government services requiring user authentication and authorization are provided via a secure, interoperable government-wide technology platform built on the principles of Service Oriented Architecture**						
Benchmark notes	This benchmark highlights the importance of building the e-government infrastructure that enables the provision of public services in a seamless, secure and cost-effective manner for all government agencies concerned; the latter also includes the Authentication and Access Control service (AAC) that, apart from identifying and authenticating end-users securely, authorizes their transactions based on the prescribed roles and rights related to the use of government information systems giving citizens' – as end-users – to be aware of the use by government officials of their personal information. One of the m main elements in this regard is the architecture of the technology platform for building such infrastructure. The Service Oriented Architecture (SOA) is of the most convenient and often used approaches to build the infrastructure for state information systems. SOA – and other similar concepts – does not only helps connect all the computers on a network and among various computer networks,						

	but makes them cooperate and exchange information needed for service provision without a need to change the underlying software programmes used by government agencies to produce such services. The SOA platform seamlessly integrates three main service delivery models – Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) that are essential for e-government service provision and access. SOA is technology neutral and does not depend on particular vendors and products, which is an important for cost-efficiency considerations as well. While there are various approaches to SOA implementation in practice, the Estonia's X-Road model (launched in 2001) is considered as an example of the European Best Practice (http://www.epractice.eu/files/eGovernmentEstonia.pdf) that provided its effectiveness and reliability over time (and has been replicated on other countries). It is a technical and organisational environment enabling a secure Internet-based data exchange between the state's information systems. The X-Road is linked to the national eID card (being issued since 2002) and allows institutions, citizens and enterprise to securely exchange data (using a two-level authorization model), as well as to ensure citizens to access their personal data maintained and processed in state databases. Public and private sector enterprises and institutions can connect their information system with the X-Road. This enables them to use X-Road services in their own electronic environment or offer their e-services via the X-Road. Joining the X-Road enables institutions to save resources, since the data exchange layer already exists. X-Road also enables public enquiries requiring user identification and authentication.						
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____						
Intermediate status 1 (closer to benchmark 1)	**The government has started building a common technology platform to provide access to information and services requiring user authentication and authorization in a secure manner via a dedicated interoperable service layer (similar to the Estonian X-Road model), including a possibility of electronic identification in mobile environment**						
Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							
Please record	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.*						

relevant evidence in support of the answer given by the respondent	*Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____						
Intermediate status 2 (farther from benchmark 1)	**The country does not have services requiring user authentication and authorization provided in a secure manner via a dedicated interoperable service layer (similar to the Estonian X-Road model), but intends to build a common technology platform, including a possibility of electronic identification in mobile environment**						
Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____						
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____						

Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____
For interviewers in Armenia and Belarus	*Role:* _____

only: Please record the respondent's view on the role and impact of the Eurasian Economic Union and the Eurasian Customs Union on HDM; if needed, please refer to the role and impact in the fields above	*Impact:* _____ *Benefits comparison:* _____
Please record overall challenges, risks, opportunities/ benefits and impacts for implementing HDM in general, as viewed by the respondent	*Challenges:* _____ *Risks:* _____ *Opportunities/benefits:* _____ *Impacts:* _____

Other remarks

_____

Indicator 3: Services

Section 3.1: Benchmark 6 - Priority services for citizens

Please select one of the answers below to demonstrate how close the benchmark statement presented below reflects upon the state of play in your country (avoid as much as possible selecting the first two answers which require additional explanation); if your answer ranges between options 3 and 5, please choose one the most appropriate intermediary status in relation to the EU baseline							
Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							
Benchmark 6	**Benchmark statement: Online maturity of 12 high impact (basic) e-services for citizens is constantly increasing (services are regularly monitored and benchmarked)**						
Benchmark notes	The objective of this benchmark is to highlight the importance of the EU-wide practice of benchmarking the online maturity of 12 key electronic services for citizens reflecting upon people's major life-cycle moments. These are: (1) Income taxes (declaration, notification of assessment); (2) Job search (services offered by labour offices); (3) Social security benefits (unemployment, child allowances, medical costs, including reimbursement and/or direct settlement; (4) Personal document (passport and driver's license); (5) Car registration (new, used, imported); (6) Building permission (application for permission); (7) Declaration to police (to report on incidents); (8) Public libraries (availability of catalogues, search tools); (9) Certificates (birth, marriage, death, request and						

	delivery); (10) Enrolment in higher education (university); (11) Announcement of moving (address change); (12) Health-related services (advice on service availability, appointments at various stages (from 0 to 5) of the 'sophistication' framework . Access to these e-services requires secure electronic identification schemes built on the principles of interoperable e-government architecture connected basic registers and databases.						
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____						
Intermediate status 1 (closer to benchmark 1)	**The government provides access to (a) at least 8-10 out of 12 basic e-services to citizens at the level of 'not full online availability' (stages 0 to 3 of the 'sophistication' framework) and (b) at least 5-6 basic e-services at the level of 'full online availability' (stages 4 and above of the 'sophistication' framework)**						
Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____						
Intermediate status 2 (farther from benchmark 1)	**The government provides access to (a) maximum 5-6 out of 12 basic e-services to citizens at the level of 'not full online availability' (stages 0 to 3 of the 'sophistication' framework) and (b) 2-3 or no e-services at the level of 'full online availability' (stages 4 and above of the 'sophistication' framework)**						
Answer option (score)	1. Not	2. Don't	3. Strongly	4. Disagree	5. Uncertain	6. Agree	7. Strongly

	applicable	know	disagree				agree
Please tick one box only							
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____						
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____						
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____						
Please record required conditions and opportunities to achieve the EU baseline, as viewed by	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____						

the respondent	Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____
For interviewers in Armenia and Belarus only: Please record the respondent's view on the role and impact of the Eurasian Economic Union and the Eurasian Customs Union on HDM; if needed, please refer to the role and impact in the fields	*Role:* _____ *Impact:* _____ *Benefits comparison:* _____

above	
Please record overall challenges, risks, opportunities/ benefits and impacts for implementing HDM in general, as viewed by the respondent	*Challenges:* _____ *Risks:* _____ *Opportunities/benefits:* _____ *Impacts:* _____

Other remarks

_____

Section 3.2: Benchmark 7 - Priority services for businesses

Please select one of the answers below to demonstrate how close the benchmark statement presented below reflects upon the state of play in your country (avoid as much as possible selecting the first two answers which require additional explanation); if your answer ranges between options 3 and 5, please choose one the most appropriate intermediary status in relation to the EU baseline

Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							

Benchmark 7	**<u>Benchmark statement</u>: Online maturity of 8 high impact (basic) e-services for businesses is constantly increasing (services are regularly monitored and benchmarked)**
Benchmark notes	The objective of this benchmark is to highlight the importance of the EU-wide practice of benchmarking the online maturity of 8 key electronic services for businesses reflecting upon key moments of doing business, such as (13) Social contributions (for employees); (14) Corporate tax (declaration, notification); (15) VAT (declaration, notification); (16) Company registration (of a new company); (17) Statistical data (submission of data to statistical office); (18) Custom declaration (submission); (19) Environment-related permits (obtaining and reporting); (20) Public procurement (tendering) at various stages (from 0 to 5) of the 'sophistication' framework. Access to these e-services requires secure electronic identification schemes built on the principles of interoperable e-government architecture connected basic registers and databases. A five-stage maturity model ('sophistication' framework) to assess a degree of the full online availability of government public services according to the following five stages: (i) information, (ii) one-way interaction, (iii) two-way interaction, (iv)

	transaction, and finally (v) targetisation.						
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____						
Intermediate status 1 (closer to benchmark 1)	**The government provides access to (a) at least 6-7 out of 8 basic e-services to businesses at the level of 'not full online availability' (stages 0 to 3 of the 'sophistication' framework) and (b) at least 2-3 basic e-services at the level of 'full online availability' (stages 4 and above of the 'sophistication' framework)**						
Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____						
Intermediate status 2 (farther from benchmark 1)	**The government provides access to (a) maximum 3-4 out of 8 basic e-services to businesses at the level of 'not full online availability' (stages 0 to 3 of the 'sophistication' framework) and (b) 1-2 or no e-services at the level of 'full online availability' (stages 4 and above of the 'sophistication' framework)**						
Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							
Please record relevant	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the*						

evidence in support of the answer given by the respondent	*answer)* *Rationale:* _____ *Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____

Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____
For interviewers in Armenia and Belarus only: Please record the respondent's view on the role and impact of the Eurasian Economic Union and the Eurasian Customs Union on HDM; if needed, please refer to the role and impact in the fields above	*Role:* _____ *Impact:* _____ *Benefits comparison:* _____
Please record overall challenges, risks,	*Challenges:* _____

opportunities/ benefits and impacts for implementing HDM in general, as viewed by the respondent	*Risks:* _____ *Opportunities/benefits:* _____ *Impacts:* _____

Other remarks

_____

Section 3.3: Benchmark 8 - Uptake of eProcurement

Please select one of the answers below to demonstrate how close the benchmark statement presented below reflects upon the state of play in your country (avoid as much as possible selecting the first two answers which require additional explanation); if your answer ranges between options 3 and 5, please choose one the most appropriate intermediary status in relation to the EU baseline

Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							

Benchmark 8	**<u>Benchmark statement</u>: 100% of all procurement made in the EU Member States by all public institutions at all governance levels is available for online use, with the at least of 50% realized via online instruments.**
Benchmark notes	The objective of the benchmark is to encourage online procurement for all goods and services undertaken by public authorities to prevent corrupted practices and increase trust transparency in business operations. The EU Manchester target 2010 requires that at least half of all public procurement is implemented online while all procurements is available for online use. That will ensure further development and enhancement of the national electronic identification schemes.
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____

Intermediate status 1 (closer to benchmark 1)	**At least 70-80% of all procurement made by all public institutions at all governance levels is available for online use, while at least 25% is realized in the online environment**						
Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____						
Intermediate status 2 (farther from benchmark 1)	**Maximum 50% of all procurement made by all public institutions at all governance levels is available for online use, while maximum 10-15% is realized in the online environment**						
Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____						
Please record main challenges and risks for	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges:						

achieving this EU baseline and implementing HDM in general, as viewed by the respondent	_____ Risks: _____
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____

with the EU, as viewed by the respondent	Political benefits: _____ Other benefits: _____
For interviewers in Armenia and Belarus only: Please record the respondent's view on the role and impact of the Eurasian Economic Union and the Eurasian Customs Union on HDM; if needed, please refer to the role and impact in the fields above	*Role:* _____ *Impact:* _____ *Benefits comparison:* _____
Please record overall challenges, risks, opportunities/ benefits and impacts for implementing HDM in general, as viewed by the respondent	*Challenges:* _____ *Risks:* _____ *Opportunities/benefits:* _____ *Impacts:* _____

Other remarks

_____

Section 3.4: Benchmark 9 - Sophistication and completeness of eProcurement

Please select one of the answers below to demonstrate how close the benchmark statement presented below reflects upon the state of play in your country (avoid as much as possible selecting the first two answers which require additional explanation); if your answer ranges between options 3 and 5, please choose one the most appropriate intermediary status in relation to the EU baseline							
Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							
Benchmark 9	**<u>Benchmark statement</u>: A balance exists between the pre- and post-award procurement stages within a fully automated eProcurement processes**						
Benchmark notes	The objective of the benchmark is to encourage a full digitalization of the entire procurement process, with a special emphasis placed on the post-award stage, which requires well-developed and secure national electronic identification schemes (it's been e dominant trend in all EU Member States over the past years). The following eProcurement services are distinguished at each stage. The pre-award stage includes eNotification (publication of procurement notices and electronic registration); eSubmission/eTendering (secure submission of tenders); eAwarding (online publication of awarded contracts, automated evaluation of tenders, electronic auctioning) regulation. The post-award stage encompasses electronic ordering (eOrdering), invoicing (eInvoicing), and paying (ePayment).						
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____						

Intermediate status 1 (closer to benchmark 1)	**The pre-award stage of the entire eProcurement process is almost fully automated to include publication of procurement notices and electronic registration, secure submission of tender documents, online publication of awarded contracts, while the post-ward stage includes as a minimum electronic invoicing**						
Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____						
Intermediate status 2 (farther from benchmark 1)	**The pre-award stage of the entire eProcurement process is automated to a certain extent to include at least publication of procurement notices and electronic registration, while the post-ward stage is not digitized but is planned for automation in the near future**						
Answer option (score)	1. Not applicable	2. Don't know	3. Strongly disagree	4. Disagree	5. Uncertain	6. Agree	7. Strongly agree
Please tick one box only							
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____						
Please record main challenges and risks for achieving this	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____						

EU baseline and implementing HDM in general, as viewed by the respondent	Risks: _____
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU,	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:*

as viewed by the respondent	_____ Other benefits: _____
For interviewers in Armenia and Belarus only: Please record the respondent's view on the role and impact of the Eurasian Economic Union and the Eurasian Customs Union on HDM; if needed, please refer to the role and impact in the fields above	*Role:* _____ *Impact:* _____ *Benefits comparison:* _____
Please record overall challenges, risks, opportunities/ benefits and impacts for implementing HDM in general, as viewed by the respondent	*Challenges:* _____ *Risks:* _____ *Opportunities/benefits:* _____ *Impacts:* _____

Other remarks

_____

7.3 eCUSTOMS

Study on the Harmonisation of the Digital Markets (HDM) in the Eastern Partnership

[Senior Expert 2, version 2.0]

QUESTIONNAIRE FOR eCUSTOMS

Introduction

eCustoms initiative conducted by the European Commission aims to replace paper format customs procedures with EU wide electronic ones, thus creating a more efficient and modern customs environment. The project's dual objective is to enhance security at the EU's external borders and to facilitate trade.

As part of this commitment, the Commission and Member States have undertaken a task to set up and operate secure, integrated, interoperable and accessible electronic Customs systems in order to facilitate end-to-end supply chain logistics and customs processes for the movement of goods into and out of the European Union, as well as to reduce the risks of threats to the citizens' Safety and Security by minimising the remaining differences between the Member States' customs processes.

The Community Customs Code has been providing the necessary legal basis (Legal framework) for the computerisation of customs procedures, declarations and data exchange (Infrastructure and Services).

EU baseline for eCustoms

As stated in the paragraph 2.3 of the project Terms of Reference, the EU baseline consists of relevant EU legislation, EU practices, standards and ICT platforms as appropriate for each HDM area. For eCustoms, this EU baseline has been defined in consultation with DG TAXUD.

The attached document describes the baseline for eCustoms to be used in conjunction with this questionnaire. The baseline is derived from three main sources;

- The EU legal and regulatory framework for electronic communications (see Annex of the EU baseline eCustoms document)
- The Association Agreements already signed between the EU and Georgia, Moldova, Ukraine
- Examples of EU practice already implemented by the European Commission at the central level or in selected member states.

Questionnaire

The Questionnaire aims at determining the current state of play in the EaP countries assessed in relation to the relevant EU baseline expressed in the form of key benchmarks. This "stock taking" stage will enable a gap analysis to be carried out.

The specific objectives of this questionnaire are;

- to establish (for each EaP country) the results already achieved in relation to the EU baseline for eCustoms as defined in the accompanying document

- to capture opinions on the enablers required for the achievement of the EU baseline
- to capture opinions on the conditions required for the achievement of full harmonization of digital markets with the EU in respect to electronic communications
- to identify possible areas (technological, political, economic) for any expected benefits from harmonisation
- to list the organisations involved with the development of digital markets, specifically in the field of electronic communications

Benchmarks and gap analysis

The questionnaire uses a number of benchmarks derived from the EU baseline for eCustoms and benchmarks related to enablers. Each benchmark in the questionnaire includes a statement that describes one of key feature of the EU baseline. The Results benchmarks (what to achieve) for 1) Legal framework, 2) Infrastructure, 3) Information services. The Enablers (what and how the country does) describe requirements for achievement of the EU baseline, such as leadership, policy, strategy resources, and implementation. The interviewees (respondents) should be asked by the National Experts to agree or disagree with the relevance of these benchmark statements to the state of play in their own countries. The level of relevance is measured on a five-point scoring scale, which comprises the following answering options: Strongly disagree; Disagree; Uncertain; Agree; Strongly agree. These answers should demonstrate the proximity of the national state of play to the EU Baseline on each specific benchmark.

By selecting one of the above answer options, respondents present their own opinion (judgment) based on the professional experience and should be prepared support their answers with evidence (which includes explaining the rationale behind the answer and relevant facts). The respondents should also be asked to provide other information including the existing risks, challenges, obstacles, opportunities, possible benefits both in relation to the specific benchmark area and, in general, as far as the implementation of the entire HDM initiative is concerned.

The proposed benchmarks statements in the questionnaire allow for the assumption that the EaP countries are not yet on par with the EU baseline, i.e. there is a gap to be closed. At the same time, the EU baseline has been formulated in such a way that it is relevant and important for all EaP countries in its own right where the progress can realistically be made. In other words, alignment to the baseline is expected to have real national benefits (technological, political, and economic) regardless of the need to harmonise with the EU per se.

Each EU baseline benchmark is described in the Benchmark notes. These have been written in a readable style. The benchmark notes should enable you to understand the key elements of each question. Detailed description of the EU baseline for eCustoms is presented in the separate document "**HDM EU baseline eCustoms**". Each benchmark presents the EU baseline's state of play and short to medium terms projected development.

Structure of the questionnaire

This questionnaire consists of 3 sections. The first section assesses the country's Results to be recorded and aims to collect opinions on the achieved progress for the harmonization of the country's digital markets. The second section assesses Enablers that describe what and how the country performs in order to progress on the HDM harmonisation process. The third section collects factual information on the Organisations involved in developing digital markets in the country.

The format of the questionnaire is a series of statements relating to the Baseline, for example **"National legal provisions are defined for secure, integrated, interoperable and accessible electronic customs systems for the exchange of data contained in customs declarations, documents accompanying customs declarations, certificates and the exchange of other relevant information",** (Benchmark 1.3 - Paperless environment for customs and trade). You are asked to say if you strongly agree, agree, are uncertain, disagree or strongly disagree. The notes that accompany each question describe what needs to be in place for "full introduction". For example, if legal provisions are defined only for electronic exchange of data, then you can agree with the statement. In addition, if the legislation defines electronic customs systems only for data contained in customs declarations (not for accompanying documents and for certificates), then this is not full implementation according to the EU Baseline. So, in this example, a correct response would be "disagree" because 2 of the most important elements are not yet in place. The spaces in the questionnaire for evidence, challenges, obstacles and conditions should be used to back up the answer, for example "the law on trade related to submission of data and documents in electronic format for the purposes of customs and international trade operations is in place since January 2008, and related government decree for electronic customs declaration was introduced in 2009".

Please complete the follow-up responses as comprehensively as you can – using specific evidence to support the response. For example, in the example above, the evidence would be a published law and government decrees. Other follow on responses concern risks, obstacles and conditions that are required to fully achieve the benchmark. Finally, a response is sought concerning the expected benefits that would arise if the benchmark was fully achieved.

Questions of clarification

If any of the statements below are not clear, please refer to the benchmark notes given below, and also please use the detailed description of the EU baseline given in the accompanying "HDM EU baseline eCustoms" document. If the benchmark or statement is still not clear, please refer back to Vladimir Abramytchev (vladimir@archev.net) for advice.

QUESTIONNAIRE FOR eCUSTOMS

Country name……

[Note: This questionnaire is intended to be completed by the National Experts in the HDM Study Team. It is not intended to be left with the officials in each country (e.g. in ministries and regulatory organisations) that are interviewed as part of the Study.]

Country's results

Part I consists of a set of separate statements relating to benchmarks required to achieve the EU baseline, as defined in the accompanying "HDM EU baseline eCustoms" document. Each statement describes a different benchmark as part of the EU baseline for eCustoms for 3 groups of indicators: 1) Legal framework, 2) Infrastructure, 3) Information services.

For each statement, please state whether the respondent in the country strongly agrees, agrees, is uncertain, disagrees or strongly disagrees with the statement. If a respondent is uncertain, or does not have an opinion, please try to obtain a further opinion from another credible respondent that can be more certain.

Part 1: Country's results

Indicator 1: Legal framework

Benchmark 1.1 – Common Risk Management Framework

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Common Risk Management Framework	A clearly defined national risk management framework in customs controls for goods brought into or out of the country is harmonised with the EU common criteria and priority control areas. Risk Information Form can be exchanged electronically with customs offices of the EU countries.				
Benchmark notes	The Common Risk Management Framework (CRMF) establishes common criteria and priority control areas - common Community risk profiles. The objective of the Risk Management Framework (RMF) is to provide for the rapid, direct and secure exchange of risk information to support targeting of consignments for customs controls and for the Commission to be able to disseminate information concerning Community-wide threats. The Framework defines commonly agreed standards and risk criteria for the selection of goods and economic operators. Customs controls, other than spot-checks, are based on risk analysis using automated data processing techniques, with the purpose of identifying and quantifying the risks and developing the necessary measures to assess the				

	risks, on the basis of criteria developed at national and Community level.
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ __
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please	*(Filled in by NEs during/after conducting interview(s) with national*

record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Benchmark 1.2 - Authorised Economic Operator (AEO) status

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Authorised Economic Operator (AEO) status	The customs authorities of the country apply common criteria and harmonised requirements for granting the status of authorised economic operators, allow the use of simplifications by authorised economic operators and recognise the status of AEOs registered in the EU member states or other countries. National system of identification and registration for economic operators interoperates with the Authorised Economic Operators EU system.				
Benchmark notes	A common approach is established for the risk assessment and accreditation of economic operators (Regulation (EC) 648/2005). Common criteria and harmonised requirements for authorised economic operators ensure a harmonised application of such criteria and requirements. The criteria for granting the status of authorised economic operator shall include: — an appropriate record of compliance with customs requirements, — a satisfactory system of managing commercial and, where appropriate, transport records, which allows appropriate customs controls,				

	— where appropriate, proven financial solvency, and — where applicable, appropriate security and safety standards. The status of authorised economic operator, once granted by one Member State, should be recognised by the other Member States. Member States should grant the status of authorised economic operator to any economic operator that meets common criteria relating to the operator's control systems, financial solvency and compliance record. An authorised economic operator shall benefit from facilitations with regard to customs controls relating to security and safety and/or from simplifications provided for under the customs rules.
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please	*(Filled in by NEs during/after conducting interview(s) with national*

record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Benchmark 1.3 - Paperless environment for customs and trade

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Paperless environment for customs and trade	National legal provisions are defined for secure, integrated, interoperable and accessible electronic customs systems for the exchange of data contained in customs declarations, documents accompanying customs declarations, certificates and the exchange of other relevant information.				
Benchmark	The electronic customs initiative (Decision No 70/2008/EC and Council				

notes	Regulation (EEC) No 2913/92) aims at establishing secure, interoperable electronic customs systems for the exchange of the data with the following main components: **Electronic customs systems** Secure, integrated, interoperable and accessible electronic customs systems are set up for the exchange of data contained in customs declarations, documents accompanying customs declarations and certificates and the exchange of other relevant information. **Data exchange** The electronic customs systems shall provide for the exchange of data between the customs authorities of the Member States and between those authorities and economic operators, the Commission, other administrations or official agencies involved in the international movement of goods.
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ __
Please record main obstacles obstructing achievement of the EU baseline, as	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____

viewed by the respondent	
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Indicator 2: Infrastructure

Benchmark 2.1 - Electronic interfaces to conduct all customs-related business

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Electronic interfaces to	Information systems of the country have a service of single access point				

conduct all customs-related business	enabling economic operators to use one single interface to lodge electronic customs declarations to the customs systems of other countries (the EU member state or others). For Belarus and Armenia, this can be within the Eurasian Economic Union.
Benchmark notes	The service of single access points enables economic operators to use one single interface to lodge electronic customs declarations, even if the customs procedure is carried out in another country. It allows traders to lodge their electronic pre-arrival/pre-departure, summary and full customs declarations via one single interface of their choice that connects their system with other countries' customs systems. The data is automatically made available to any customs office responsible for the place at which goods have been, or are to be, presented, irrespective of the country concerned.
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ __
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____

respondent	
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Benchmark 2.2 - Interoperating systems for import, export and transit

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Interoperating systems for import, export and transit	The country systems for import and export interoperate with the system for transit and enable the seamless flow of data. The service can ensures transfer of data between the national customs systems to/from customs				

	system of the EU member states.
Benchmark notes	Secure, integrated, interoperable and accessible electronic customs systems facilitate the exchange of data contained in customs declarations, documents accompanying customs declarations and certificates and the exchange of other relevant information. The main components of the interconnection is between the National Customs Declaration Processing Systems and the following EU systems: • Automated Import System (AIS) - The service ensures that import operations started in a country of import (EU Member State or other) can be completed in the country without re-submission of the same information. It assures handling of pre-arrival declarations and the link of the information with risk analysis. • Automated Export System (AES) - The service ensures that export operations started in the country can be finalised in a country of export (EU Member State or other) without re-submission of the same information. This includes the exchange of electronic messages related to the different stages of the operations amongst the various actors (traders, customs and other governmental administrations). • New Computerised Transit System (NCTS) - National transit system allows the use of an electronic transport document as a transit declaration. It provides control of the European TIR movements and facilitates the discharge of TIR (Transports Internationaux Routiers) operations within the country by replacing the return of Voucher No 2 with the sending of electronic messages.
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____

general, as viewed by the respondent	__
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Benchmark 2.3 - Integrated tariff information system

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Integrated tariff information system	The country has implemented a national centralised binding tariff information system that allows getting tariff classification for goods. The system is interconnected with other tariff related IT systems to facilitate re-use of data and functionality of one system to another.				
Benchmark notes	National Binding Tariff Information (BTI) system assists economic operators to obtain the correct tariff classification for goods they intend to import or export. Integrated tariff environment enables re-use of data through connection of import and export related systems, to the National Customs Declaration Processing Systems and the National Surveillance systems.				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____				
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ __				
Please	*(Filled in by NEs during/after conducting interview(s) with national*				

record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Benchmark 2.4 - Single Point for Entry or Exit of Data (SPEED) portal

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response					

(tick one box only)					
Single Point for Entry or Exit of Data (SPEED) portal	The country's computerised transit system (or other such as export, import or economic operators systems) is connected to SPEED portal and allows data exchange for electronic customs systems between the country and the EU				
Benchmark notes	Single Portal for Entry and Exit of Data (SPEED) is a secure portal connecting the private network Common Communications Network / Common Systems Interface (CCN/CSI) and the external world for system-to-system interfaces. Consequently, SPEED provides a technical infrastructure solution that enables automated data exchange between Member States' electronic customs systems and third countries that are not linked to CCN/CSI on the basis of EU bilateral or multilateral agreements. It is a key objective of the EU to facilitate trade with third countries and/or exchanges with non-Customs systems. To support this initiative, a generic technical solution has been developed which permits each partner (e.g. third country) to connect to a system developed centrally by DG TAXUD.				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____				
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ __				
Please	*(Filled in by NEs during/after conducting interview(s) with national*				

record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Benchmark 2.5 - Uniform user management & digital signatures

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response					

(tick one box only)					
Uniform user management & digital signatures	A common solution for electronic signatures (or a system based on mutual recognition of existing solutions) is operational in the country and enables the national economic operators to send information not only to other countries (EU member states), but also to other administrations than customs, and to enable these administrations to verify the authenticity of the author, of the sender and of the information. For Belarus and Armenia, this can be within the Eurasian Economic Union.				
Benchmark notes	A common solution for electronic signatures means that economic operators can use an electronic certificate delivered by one national authority and to use it for sending information to other administrations too. For example, a certificate provided by the customs to an economic operator is also accepted by veterinary agency, tax authority or any other to verify the authenticity of the author, of the sender and of the information. A system based on mutual recognition of existing solutions is a hybrid system where electronic certificates issued by different authorities (each has its own authentication centre) are mutually recognised by them. This system should allow economic operators to send information to other administrations than customs, and to enable these administrations to verify the authenticity of the author, of the sender and of the information. The advanced level of the uniform user management & digital signatures system allows economic operators to send information to administrations of foreign countries, such as EU member states or the countries of the Eurasian Economic Union.				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____				
Please record main challenges and risks for achieving this EU baseline	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____				

and implementing HDM in general, as viewed by the respondent	Risks: _____ __
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Indicator 3: Services

Benchmark 3.1 - Registered Exporters System

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Registered Exporters System	The country has established a Registered Exporters System (REX) that allows an automated verification of the exporters' registration number from the declarations in the national Customs declaration system. The country cooperates with the EU in order to register national exporters into the EU REX central database managed by the European Commission.				
Benchmark notes	The main purpose of the system is to replace the paper-based certification process by an IT-supported self-certification process. A central database contains the registered exporters' data. The system also allows verification of Registered Exporters System numbers in customs declarations contained in the National Customs Declaration System. The system is designated for economic operators from non-EU countries benefiting from preferential trade arrangements under the Generalised System of Preferences and exporting goods to the EU.				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____				
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ __				

viewed by the respondent	
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Benchmark 3.2 - Economic Operators Registration and Identification system

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Economic Operators Registration and Identification system	An electronic system for storing and exchanging Economic Operators Registration and Identification (EORI) numbers is operational in the country. The national system is interconnected with the EORI central database managed by the European Commission.				
Benchmark notes	Economic operators' registration and identification (EORI) number is assigned to each economic operator and, where appropriate, to other persons. It serves as a common reference in relations of economic operators with customs authorities throughout the country and for the exchange of information between the customs authorities and other authorities. EORI number is unique throughout the country and assigned by a customs authority or other designated authority. To ensure that it is unique, only one number should be used in respect of a given person. The country may use as an EORI number a number already assigned to an economic operator or to another person by the competent authorities for tax, statistical or other purposes.				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____				
Please record main challenges and risks for achieving this EU baseline and implementing	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks:				

HDM in general, as viewed by the respondent	_____ __
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Benchmark 3.3 - Exchange of data about Authorised Economic Operators

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Exchange of data about Authorised Economic Operators	The country has a registration and Identification information system of economic operators and has concluded an agreement of mutual recognition of the country's register of economic operators and the Authorised Economic Operators in the EU. System-to-system interface allows the economic operators' data received from the country to be disseminated to the EU member states and the validation of the county' AEO status in the EU transaction systems.				
Benchmark notes	The country should have an information system for registration and Identification of economic operators (traders). This system contains data about economic operators' profiles. Based on the profiles, the country's authorities can attribute different trust level status to different economic operators. In the EU, the status of Authorised Economic Operator (AEO) is defined and universally recognised by the national administrations. Centralised Economic Operators Registration and Identification information and communication system supporting the concept of the Authorised Economic Operators enables the national administrations of the Member States to grant AEO status (including online consultations) and provides access to the list of the AEOs for business needs. Third countries can conclude mutual recognition agreements with the EU and to ensure the exchange of AEO data in a uniform way to increase security and facilitation. The economic operator benefits from reduced physical and document based controls and priority treatment.				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____				
Please	*(Filled in by NEs during/after conducting interview(s) with national*				

record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*stakeholders.)* Challenges: _____ Risks: _____ __
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU,	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____

as viewed by the respondent	Other benefits: _____

Benchmark 3.4 - Summary electronic declaration

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Summary electronic declaration	An electronic summary declaration containing the required pre-arrival or pre-departure information is lodged before any goods are brought into or out of the territory of the country. All information is provided to the customs and other authorities in electronic format. Existing country's infrastructure allows such information to be shared electronically with third countries where an international agreement so provides.				
Benchmark notes	Required pre-arrival and pre-departure information in the form of summary declarations should be lodged by economic operators before any goods are brought into or out of the country customs territory. Data set and format for the summary declaration are defined by the national legislation and the regulatory framework, containing the particulars necessary for risk analysis and the proper application of customs controls, primarily for security and safety purposes. Summary declaration is filed electronically.				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____				
Please record main challenges	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)*				

and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	Challenges: _____ Risks: _____ __
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

respondent	

Benchmark 3.5 - National Single Window System

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
National Single Window System	The national single window and one-stop shop is in place and allows submission of all required information and documents in electronic format (application for certificates, customs declaration, required documents, and permits). Administrations or agencies deliver certificates required for import or export authorisation in electronic format.				
Benchmark notes	The Single Window is defined as a facility that allows parties involved in trade and transport to lodge standardised information and documents with a single entry point to fulfil all import, export and transit-related regulatory requirements. If information is electronic, then individual data elements should be submitted only once. The Single Window is managed by a central authority that ensures that the participating government agencies are either given access to the information or are actually given the information by the managing authority. It eliminates the need for the trader or transporter to submit the same data to several different border authorities or agencies.				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____				
Please record main challenges and risks for	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges:				

achieving this EU baseline and implementing HDM in general, as viewed by the respondent	_____ Risks: _____
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Benchmark 3.6 - Anti-Counterfeiting and Anti-Piracy System

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Anti-Counterfeiting and Anti-Piracy System	In the country, an electronic service is in place providing traders with the possibility to submit a claim asking the intervention of Customs in order to take measures against goods infringing certain intellectual property rights. The national Anti-Fraud Information System is connected with the centralised EU information system, which is accessible by all Member States.				
Benchmark notes	This electronic service is designed to protect the right holders against intellectual property rights (IPR) infringements. Through an electronic application, right holders can submit a claim and ask the intervention of Customs in order to take measures against goods infringing certain IPR. At an advanced level, data from the national information system is shared with information systems of other countries, thereby simplifying and reducing the workload of Customs administrations and improving the cooperation in the area of IPR enforcement. The national system can be connected to the EU centralised Anti-Counterfeiting and Anti-Piracy System which is accessible by all Member States. For Belarus and Armenia, data exchange can be within the Eurasian Economic Union's IPR information sharing agreements.				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____				

Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ __
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU,	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits:

as viewed by the respondent	_____

Part 2: Country's enablers

The enablers describe what the country does in order to achieve the EU baseline and produce the results of the harmonization of digital markets in eCustoms area. These benchmarks assess the capacities to define a policy, prepare a strategy, allocated resources and organize implementation of activities required for harmonization of the digital markets between the country and the EU in eCustoms area.

Indicator 1: Leadership

Score	**Strongly disagree**	**Disagree**	**Uncertain**	**Agree**	**Strongly agree**
Enter your response (tick one box only)					
Leadership	**The country has leaders who set and communicate a clear direction for the harmonisation of digital markets between the country and the EU in eCustoms area.**				
Benchmark notes	The country's leaders develop and facilitate the achievement of the vision and mission towards harmonisation of eCustoms with the EU digital market. They define values, set up organisational structures for sustainable success, and implement eCustoms harmonisation via their actions and behaviours. During periods of change, they retain a constancy of purpose. This leadership should be present and sound at legislative, executive (government) and business levels.				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders)* *Rationale:* _____ *Supporting evidence:* _____				
Please record main challenges, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____				
Please	*(Filled in by NEs during/after conducting interview(s) with national*				

record main obstacles, as viewed by the respondent	*stakeholders.)* Obstacles: _____

Indicator 2: Policy

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Policy	**The country has defined a comprehensive policy towards the harmonization of digital markets between the country and the EU in the area of eCustoms**				
Benchmark notes	The responsible authorities implement their mission and vision by developing an eCustoms harmonisation focused strategy that takes account of the market and sector. eCustoms harmonisation policy is based on the present and future needs and expectations of the country				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders)* *Rationale:* _____ *Supporting evidence:* _____				
Please record main challenges, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____				
Please record main obstacles,	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)*				

as viewed by the respondent	Obstacles: _____

Indicator 3: Strategy

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Strategy	**eCustoms strategy for harmonisation of the country and the EU digital markets is developed, published, reviewed and regularly updated.**				
Benchmark notes	The strategy is clearly based on the present and future needs and expectations of the country. The strategy is communicated and deployed through a framework of key processes				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders)* *Rationale:* _____ *Supporting evidence:* _____				
Please record main challenges, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____				
Please record main obstacles, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____				

Indicator 1: Resources

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Resources	**The country allocates sufficient resources in order to balance the current and future needs of eCustoms harmonisation process**				
Benchmark notes	The Leaders in eCustoms harmonisation plan and manage external partnerships, suppliers and internal resources in order to support policy, strategy and the effective operation of eCustoms harmonisation processes. Finances, technology, information and knowledge are efficiently managed				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders)* *Rationale:* _____ *Supporting evidence:* _____				
Please record main challenges, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____				
Please record main obstacles, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____				

Indicator 4: Implementation

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Implementation	**Legislation is drafted, infrastructure and information systems required for eCustoms harmonisation are designed, produced, delivered and serviced**				
Benchmark notes	People responsible for eCustoms design, manage and improve processes in order to fully achieve eCustoms harmonisation with the EU digital market. Legislation, infrastructure and information systems required for eCustoms harmonisation are designed and developed based on the country's needs and expectations				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders)* *Rationale:* _____ __ *Supporting evidence:* _____				
Please record main challenges, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____				
Please record main obstacles, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____				

ADDITIONAL QUESTIONS FOR ARMENIA AND BELARUS, MEMBERS OF THE EURASIAN ECONOMIC UNION

For interviews in Armenia and Belarus only

"eCustoms"

Please record the respondent's view on the role, benefits , risks and overall impact of the Eurasian Economic Union and the Eurasian Customs Union on the achievement of harmonisation of digital markets with the EU in the area of eCustoms	***(Filled in by NEs during/after conducting interview(s) with national stakeholders.)*** ***Role of the Eurasian Economic Union and Eurasian Customs Union regarding the topic of telecoms rules:*** _____ _ ***Supporting evidence:*** _____ ***Impact of the Eurasian Economic Union and the Eurasian Customs Union in the area of telecoms rules:*** _____ ***Supporting evidence:*** _____ ***Risks for achieving HDM with the EU in the area of telecoms rules:*** _____ _____ ***Supporting evidence:*** _____ ***Possible benefits of the Eurasian Economic Union and Eurasian Customs Union for HDM with the EU in the area of telecoms rules:*** ***economic:*** _____

technological:

_____

political:

_____

other benefits:

_____

_____

Other remarks: _____

The main benchmarks on eCustoms related to the membership of Belarus and Armenia in the Eurasian Economic Union

Benchmark	Statement
Electronic interfaces to conduct all customs-related business	Information systems of the country have a service of single access point enabling economic operators to use one single interface to lodge electronic customs declarations to the customs systems of other countries (the EU member state or others). For Belarus and Armenia, this can be within the Eurasian Economic Union.
Uniform user management & digital signatures	A common solution for electronic signatures (or a system based on mutual recognition of existing solutions) is operational in the country and enables the national economic operators to send information not only to other countries (EU member states), but also to other administrations than customs, and to enable these administrations to verify the authenticity of the author, of the sender and of the information. For Belarus and Armenia, this can be within the Eurasian Economic Union.
Anti-Counterfeiting and Anti-Piracy System	In the country, an electronic service is in place providing traders with the possibility to submit a claim asking the intervention of Customs in order to take measures against goods infringing certain intellectual property rights. The national Anti-Fraud Information System is connected with the centralised EU information system, which is accessible by all Member States.

	For Belarus and Armenia, this can be within the Eurasian Economic Union.

7.4 eCOMMERCE

Study on the Harmonisation of the Digital Markets (HDM) in the Eastern Partnership

Questionnaire for eCommerce for Small and Medium Enterprises

Introduction

eCommerce is a generic term used to describe trade over the internet. The activities concerned include selling goods online, offering online information or commercial communications, providing tools allowing for search of products and services, access and retrieval of data.

eCommerce brings to Small and medium enterprises (SMEs) more opportunities. They will have access to new markets beyond national borders. More intensive use of online services will improve the productivity of companies and access to new market niches.

EU baseline for eCommerce

As stated in the paragraph 2.3 of the project Terms of Reference, the EU baseline consists of relevant EU legislation, EU practices, standards and ICT platforms as appropriate for each HDM area. For eCommerce, this EU baseline has been defined in consultation with DG MARKT/CONNECT.

The attached document describes the baseline for eCommerce for SMEs to be used in conjunction with this questionnaire.

Questionnaire

The Questionnaire aims at determining the current state of play in the EaP countries assessed in relation to the relevant EU baseline expressed in the form of key benchmarks. This “stock taking” stage will enable a gap analysis to be carried out.

The specific objectives of this questionnaire are;

- to establish (for each EaP country) the results already achieved in relation to the EU baseline for eCommerce for SMEs as defined in the accompanying document
- to capture opinions on the enablers required for the achievement of the EU baseline
- to capture opinions on the conditions required for the achievement of full harmonization of digital markets with the EU in respect to eCommerce services
- to identify possible areas (technological, political, economic) for any expected benefits from harmonisation
- to list the organisations involved with the development of digital markets, specifically in the field of eCommerce for SMEs

Benchmarks and gap analysis

The questionnaire uses a number of benchmarks derived from the EU baseline for eCommerce for SMEs. Each benchmark in the questionnaire includes a statement that describes one of key feature of the EU baseline. The Results benchmarks (what to achieve) for 1) Internet security & privacy, 2) Consumer rights, 3) Competition, 4) E-payments, 5) E-logistics. The interviewees (respondents) should be asked by the National Experts to agree

or disagree with the relevance of these benchmark statements to the state of play in their own countries. The level of relevance is measured on a five-point scoring scale, which comprises the following answering options: Strongly disagree; Disagree; Uncertain; Agree; Strongly agree. These answers should demonstrate the proximity of the national state of play to the EU Baseline on each specific benchmark.

By selecting one of the above answer options, respondents present their own opinion (judgment) based on the professional experience and should be prepared support their answers with evidence (which includes explaining the rationale behind the answer and relevant facts). The respondents should also be asked to provide other information including the existing risks, challenges, obstacles, opportunities, possible benefits both in relation to the specific benchmark area and, in general, as far as the implementation of the entire HDM initiative is concerned.

The proposed benchmarks statements in the questionnaire allow for the assumption that the EaP countries are not yet on par with the EU baseline, i.e. there is a gap to be closed. At the same time, the EU baseline has been formulated in such a way that it is relevant and important for all EaP countries in its own right where the progress can realistically be made. In other words, alignment to the baseline is expected to have real national benefits (technological, political, and economic) regardless of the need to harmonise with the EU per se.

Each EU baseline benchmark is described in the Benchmark notes. The benchmark notes should enable you to understand the key elements of each question. Detailed description of the EU baseline for eCommerce for SMEs is presented in the separate document "**HDM EU baseline eCommerce for SMEs**". Each benchmark presents the EU baseline's state of play and short to medium terms projected development.

Structure of the questionnaire

This questionnaire consists of 3 sections. The first section assess the country's Results to be recorded and aims to collect opinions on the achieved progress for the harmonization of the country's digital markets in eCommerce area. The second section collects factual information on the Organisations involved in developing digital markets in the country.

The format of the questionnaire is a series of statements relating to the Baseline. You are asked to say if you strongly agree, agree, are uncertain, disagree or strongly disagree. The notes that accompany each question describe what needs to be in place for compliance.

Please complete the follow-up responses as comprehensively as you can – using specific evidence to support the response. Finally, a response is sought concerning the expected benefits that would arise if the benchmark was fully achieved.

Questions of clarification

If any of the statements below are not clear, please refer to the benchmark notes given below, and also please use the detailed description of the EU baseline given in the accompanying "HDM EU baseline eCommerce for SMEs" document. If the benchmark or statement is still not clear, please refer back to Vladimir Abramytchev (vladimir@archev.net) for advice.

Questionnaire for eCommerce for SMEs

Country ……

[Note: This questionnaire is intended to be completed by the National Experts in the HDM Study Team. It is not intended to be left with the officials in each country (e.g. in ministries and regulatory organisations) that are interviewed as part of the Study.]

Country's results

Part I consists of a set of separate statements relating to benchmarks required to achieve the EU baseline, as defined in the accompanying "HDM EU baseline eCommerce for SMEs" document. Each statement describes a different benchmark as part of the EU baseline for eCommerce for 5 groups of indicators: 1) Internet security & privacy, 2) Consumer rights, 3) Competition, 4) E-payments, 5) E-logistics.

For each statement, please state whether the respondent in the country strongly agrees, agrees, is uncertain, disagrees or strongly disagrees with the statement. If a respondent is uncertain, or does not have an opinion, please try to obtain a further opinion from another credible respondent that can be more certain.

Part 1: Country's results

Indicator 1: Internet security & privacy

Benchmark 1.1 - Allowance to process user traffic data by the provider of an electronic communication service

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Allowance to process user traffic data	**The national legislation defines the rules of processing of user traffic data by the provider of an electronic communication service for the purposes of marketing electronic communications services or for the provision of value added services.**				
Benchmark notes	For the purpose of marketing electronic communications services or for the provision of value added services, the provider of an electronic communications service may need to process the data to the extent and for the duration necessary for such services or marketing. This can be conditioned by the requirement if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers could be given the possibility to withdraw their consent for the processing of traffic data. This allowance can also concern processing of traffic data necessary for the purposes of subscriber billing and interconnection payments.				

	The legislation should indicate if the service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing.
Please record relevant evidence in support of the answer given by the respondent	*Rationale:* *Supporting evidence:*
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*Challenges:* *Risks:*
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*Obstacles:*
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*Conditions:* *Opportunities:*
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*Economic benefits:* *Technological benefits:* *Political benefits:* Other benefits:

Benchmark 1.2 - Specific liability regime for intermediary service providers

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Specific liability regime for intermediary service providers	**The national legislation clearly defines specific liability regimes for three categories of online service providers: transmission conduit operators, caching providers and hosting services providers.**				
Benchmark notes	The specific liability regime for three categories of essential services assuring the provision of eCommerce online services should be defined in the national legislation. These are the conditions for mere conduit operators (transmission in a communication network), caching providers (temporary storage of information) and hosting services. The legislation shall define the degree of liability of the service provider for the information transmitted in a communication network of information provided by a recipient of the service. The liability of service provider should be defined for the automatic, intermediate and temporary storage of that information, performed for making more efficient the information's onward transmission to other recipients of the service upon their request. Liability of the hosting service providers should be defined for the information stored at the request of a recipient of the service, with some clearly defined liability exceptions (does not have actual knowledge of illegal activity or information, and others).				
Please record relevant evidence in support of the answer given by the respondent	*Rationale:* *Supporting evidence:*				
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*Challenges:* *Risks:*				
Please record main obstacles	*Obstacles:*				

obstructing achievement of the EU baseline, as viewed by the respondent	
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*Conditions:* *Opportunities:*
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*Economic benefits:* *Technological benefits:* *Political benefits:* Other benefits:

Benchmark 1.3 – Obligation for providers to monitor transmitted or stored information

Score	**Strongly disagree**	**Disagree**	**Uncertain**	**Agree**	**Strongly agree**
Enter your response (tick one box only)					
Obligation for providers to monitor transmitted or stored information	**The national legislation does not impose requirements on information services providers to monitor information transmitted in order to detect illegal activities and to inform the competent public authorities.**				
Benchmark notes	The national legislation can include or not include any requirements and conditions on providers of eCommerce and other information services of transmission, caching and hosting, to monitor the information which they transmit or store in order to detect any illegal				

	activity. Type of illegal on-line activities should be defined. The legislation may establish obligations for information society service providers to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* *Supporting evidence:*
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*Challenges:* *Risks:*
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*Obstacles:*
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*Conditions:* *Opportunities:*
Please record expected economic, technological, political and other benefits of the harmonisation for	*Economic benefits:* *Technological benefits:* *Political benefits:* Other benefits:

this benchmark between the partner countries and with the EU, as viewed by the respondent	

Indicator 2: Consumer rights

Benchmark 2.1 - Online trustmarks for retail websites

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Online trustmarks for retail websites	**The country has established country-wide trustmark scheme(s) for electronic identification and trust services for electronic transactions which assure the trustfulness of qualified eCommerce service providers.**				
Benchmark notes	For the development of eCommerce, there is a definitive usefulness and benefits of the country-wide trustmark schemes that help to reassure consumers on the reliability of accredited online traders and service providers. A trust mark can be in form of a logo published on certified websites and linked to an accreditation website (trust mark providing third-party website identity validation). It can be also assured through another mean of trusted electronic identification (eID, electronic certificate). Another aim is also to encourage the establishment of price-comparison websites. Such certified sites will help consumers to make informed decisions when using online retail services. The next step would be harmonization of national trustmarks schemes with EU member states. The Commission is in process to elaborate different policy options for EU-wide trustmark schemes and the effectiveness of cooperation platforms in the governance of such trustmark systems.				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* *Supporting evidence:*				

Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*Challenges:* *Risks:*
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*Obstacles:*
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*Conditions:* *Opportunities:*
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*Economic benefits:* *Technological benefits:* *Political benefits:* Other benefits:

Benchmark 2.2 - Requirement to provide minimum general information by information society service provider

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick					

one box only)					
Minimum general information by information society service provider	**The national legislation imposes the obligation on the information service provider to render easily, directly and permanently accessible to both recipients of services and the competent authorities the defined scope of information about the service provider.**				
Benchmark notes	This obligation on the service provider can request the details of the service provider that allow it to be contacted rapidly and communicated with in a direct and effective manner. The required information may include the name of the service provider, geographical address, e-mail address, registration number if registered in a trade or similar public register. This information may be legally required to be published on the landing (home or first) page of the website of the information service provider or in a specially designated webpage. For information service providers and eCommerce traders providing online services to businesses, the legislation can require provision of VAT number and indication of professional insurance coverage (financial brokers, real estate).				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* *Supporting evidence:*				
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*Challenges:* *Risks:*				
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*Obstacles:*				
Please record required conditions and opportunities	*Conditions:* *Opportunities:*				

to achieve the EU baseline, as viewed by the respondent	
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*Economic benefits:* *Technological benefits:* *Political benefits:* Other benefits:

Benchmark 2.3 - Transparency requirement of commercial communications information to be provided

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Transparency of commercial communications information to be provided	**The national legislation imposes that advertisements on the Internet indicates natural or legal person responsible for commercial communication and any conditions attached to the offers.**				
Benchmark notes	This requirement emphasises the need for transparency when advertisements are displayed on the Internet. It can oblige to ensure that online commercial communications such as promotional offers, discounts, premiums, promotional competitions or games, meet certain transparency requirements. Both the commercial communication and the natural or legal person responsible for it should be clearly identifiable, and any conditions (price, delivery cost, delays of delivery, etc.) attached to the offers, discounts etc. must be easily accessible. For example, advertising originating from the operator of an online marketplace and displayed by a search operator discloses both the identity of the online marketplace operator and the fact that the trademarked goods advertised are				

	being sold through that online marketplace.
Please record relevant evidence in support of the answer given by the respondent	*Rationale:* *Supporting evidence:*
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*Challenges:* *Risks:*
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*Obstacles:*
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*Conditions:* *Opportunities:*
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*Economic benefits:* *Technological benefits:* *Political benefits:* Other benefits:

Benchmark 2.4 - Pre-contractual information required for distance contracts and off-premises contracts

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Requirements for distance contracts and off-premises contracts	**For distance (concluded online or by electronic means) or off-premises contract, the national legislation requires that the trader provides the consumer with a minimum of legally defined pre-contractual information and comprehensive explanation of contractual terms.**				
Benchmark notes	The requirement for pre-contractual information may include information requirements in relation to the product/service, address and identity of the seller, price, additional charges, acceptable payment mechanisms, delivery details, complaints policy, cooling-off period (where applicable) and after-sales services, and others. If a distance contract to be concluded by electronic means places the consumer under an obligation to pay, the trader shall be required to make the consumer aware in a clear and prominent manner, and directly before the consumer places his order. The obligations can include requirements for confirmation of the contract concluded on a durable medium (signed paper contract) within a reasonable time after the conclusion of the distance contract.				
Please record relevant evidence in support of the answer given by the respondent	*Rationale:* *Supporting evidence:*				
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*Challenges:* *Risks:*				
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the	*Obstacles:*				

respondent	
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*Conditions:* *Opportunities:*
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*Economic benefits:* *Technological benefits:* *Political benefits:* Other benefits:

Benchmark 2.5 - Consumer protection international cooperation mechanisms

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Consumer protection international cooperation mechanisms	**The country has established international cooperation mechanisms between the national public authorities and the authorities of other countries who are responsible for enforcement of consumer protection laws, including for eCommerce.**				
Benchmark notes	The international consumer protection cooperation brings together the public authorities in different countries who are responsible for the enforcement of consumer protection laws. Thanks to this cooperation, a national authority in a country where consumer interests are harmed can call on their counterpart in the country where the trader is located and ask for action to stop the infringement. Enforcement authorities can also alert each other to malpractices they have spotted which may spread to other countries. Consumer protection cooperation agreement can be set up, for				

	example, with neighbouring countries, countries with main trading volumes, EU member states, or with the Eurasian Economic Union. Especially for consumer protection in eCommerce field, the authorities can establish information systems for the exchange of information between competent authorities of different countries.
Please record relevant evidence in support of the answer given by the respondent	*Rationale:* *Supporting evidence:*
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*Challenges:* *Risks:*
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*Obstacles:*
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*Conditions:* *Opportunities:*
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*Economic benefits:* *Technological benefits:* *Political benefits:* Other benefits:

Benchmark 2.6 – Possibility for out-of-court dispute settlement

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Out-of-court dispute settlement	**The national legislation allows the use of out-of-court schemes for dispute settlement regarding provision of eCommerce services, including by appropriate electronic means.**				
Benchmark notes	The country's legislation shall clearly define the mechanisms of dispute resolution, in the event of disagreement between an information society service provider and the recipient of the service. The legislation can include prerequisites for the use of out-of-court schemes, available under national law, for dispute settlement, including by appropriate electronic means. Availability of such out-of-court dispute settlement mechanisms can significantly facilitate the development of eCommerce services, especially by SMEs, at the same time assuring a sufficient level of consumer protection.				
Please record relevant evidence in support of the answer given by the respondent	*Rationale:* *Supporting evidence:*				
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*Challenges:* *Risks:*				
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*Obstacles:*				
Please record required conditions and opportunities	*Conditions:* *Opportunities:*				

to achieve the EU baseline, as viewed by the respondent	
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*Economic benefits:* *Technological benefits:* *Political benefits:* Other benefits:

Benchmark 2.7 - Online dispute resolution system for consumers for eCommerce transactions

Score	**Strongly disagree**	**Disagree**	**Uncertain**	**Agree**	**Strongly agree**
Enter your response (tick one box only)					
Online dispute resolution system for consumers for eCommerce transactions	**The country has an online dispute resolution platform through which parties can initiate alternative dispute resolution in relation to disputes concerning online transactions.**				
Benchmark notes	Setting up of an online dispute resolution platform (an interactive website free of charge) facilitates and speeds up resolution of disputes related to eCommerce transactions. This tool can provide reassurance to both sides, service providers and consumers, and build trust in eCommerce transactions. Through this website, parties can initiate alternative dispute resolution procedure in relation to disputes concerning online transactions without going through traditional court legal procedures that are time and resources consuming. National entities responsible for settling alternative disputes receive the complaint electronically through the online platform and seek to				

	resolve the dispute through existing legal alternative dispute resolution mechanisms.
Please record relevant evidence in support of the answer given by the respondent	*Rationale:* *Supporting evidence:*
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*Challenges:* *Risks:*
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*Obstacles:*
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*Conditions:* *Opportunities:*
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*Economic benefits:* *Technological benefits:* *Political benefits:* Other benefits:

Benchmark 2.8 - Requirements for sending of unsolicited commercial communication (spam)

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Unsolicited commercial communication	**The national legislation clearly defines the requirements applied to sending of unsolicited commercial communications by e-mail.**				
Benchmark notes	Unsolicited commercial communications (spam) sent by e-mail is considered as a fundamental way of commercial promotion of products and services, and is an important factor for the development of eCommerce. The legal framework of the country may have the possibility to either prohibit or allow the sending of unsolicited commercial communications by e-mail. If the country permits unsolicited commercial communication, it should define the requirements applied to information service providers and describe the rights of consumers. This may ensure, for example, that such communication is clearly and unambiguously identifiable, and that service providers respect the opt-out registers to which consumers (natural or legal persons) not wishing to receive such commercial communications can sign up.				
Please record relevant evidence in support of the answer given by the respondent	*Rationale:* *Supporting evidence:*				
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*Challenges:* *Risks:*				
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*Obstacles:*				

Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*Conditions:* *Opportunities:*
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*Economic benefits:* *Technological benefits:* *Political benefits:* Other benefits:

Indicator 3: Competition

Benchmark 3.1 - Free movement of eCommerce services

Score	**Strongly disagree**	**Disagree**	**Uncertain**	**Agree**	**Strongly agree**
Enter your response (tick one box only)					
Free movement of eCommerce services	**The national legislation does not restrict the freedom to provide eCommerce services compliant to the national laws by a lawful service provider established in another country**				
Benchmark notes	The country ensures that eCommerce services provided by a service provider established on its territory comply with the national provisions. In general, the country's legislation may not restrict the freedom to provide eCommerce services by a provider from another country. If this freedom is limited, the national legislation should clearly define the requirements for provision of eCommerce services on its territory for any service provider lawfully established in another country.				
Please record relevant evidence	*Rationale:*				

in support of the answer given by the respondent	*Supporting evidence:*
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*Challenges:* *Risks:*
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*Obstacles:*
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*Conditions:* *Opportunities:*
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*Economic benefits:* *Technological benefits:* *Political benefits:* Other benefits:

Benchmark 3.2 - authorisation to pursuit the activity of eCommerce service provider

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your					

response (tick one box only)					
Authorisation to pursuit the activity of eCommerce service provider	**The country applies the principle excluding prior authorisation to pursuit the activity of eCommerce service provider**				
Benchmark notes	The legal framework of the country can ensure that the taking up and pursuit of the activity of an information society service provider, including eCommerce activities, may not be made subject to prior authorisation or any other requirement having equivalent effect. However, the country also can restrict starting of eCommerce activities by a condition of getting prior authorization in some particular sectors (financial services, online games, etc.) or for some products (medicine, arms, etc.). This principle shall be without prejudice to authorisation schemes which are not specifically and exclusively targeted at information society services, or which are covered by another legislation, such as a framework for general authorisations and individual licenses in the field of telecommunications services.				
Please record relevant evidence in support of the answer given by the respondent	*Rationale:* *Supporting evidence:*				
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*Challenges:* *Risks:*				
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*Obstacles:*				
Please record required conditions and opportunities to achieve the EU	*Conditions:* *Opportunities:*				

baseline, as viewed by the respondent	
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*Economic benefits:* *Technological benefits:* *Political benefits:* Other benefits:

Indicator 4: E-payments

Benchmark 4.1 - rules on the fees for the use of means of eCommerce payment

Score	**Strongly disagree**	**Disagree**	**Uncertain**	**Agree**	**Strongly agree**
Enter your response (tick one box only)					
Fees for the use of means of eCommerce payment	**The national legislation defines the requirements for eCommerce payments and defines the rules on the fees for the use of means of electronic payment.**				
Benchmark notes	The rise of eCommerce and the increasing popularity of smart phones has enabled new ways of making payments. A comprehensive national legislation for eCommerce payments by credit or debit card, on Internet, on phone, using mobile and other electronic payments presents a substantial benefit for eCommerce development and market integration in this field at European level. Rules on the fees for the use of certain means of payment (e.g. credit or debit cards, electronic valets) should prohibit traders from charging consumers excessive fees in respect of the use of a given means of payment.				
Please record relevant evidence in support of the	*Rationale:* *Supporting evidence:*				

answer given by the respondent	
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*Challenges:* *Risks:*
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*Obstacles:*
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*Conditions:* *Opportunities:*
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*Economic benefits:* *Technological benefits:* *Political benefits:* Other benefits:

Benchmark 4.2 - Equal treatment between paper and electronic invoices

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick					

one box only)					
Equal treatment between paper and electronic invoices	**The national legislation assures equal treatment between paper and electronic invoices (e-invoices) and defines the framework of a common national data model of e-invoicing format.**				
Benchmark notes	Removing of obstacles to the uptake of e-invoicing by creating equal treatment between paper and e-invoices assures that eCommerce transactions can be concluded faster. E-invoicing also significantly reduces the cost of business procedures related to keeping, processing, storing and delivery/postal expenses of paper invoices. A defined national legal framework and technical standards support the uptake of e-invoicing by ensuring legal certainty and promoting the development of interoperable e-invoicing solutions based on a common standard, paying particular attention to the needs of small and medium-sized enterprises. A single and clear semantic data model and a common e-invoicing format facilitate semantic interoperability, ensure technology neutrality and facilitate the uptake of e-invoicing for eCommerce transactions for SMEs.				
Please record relevant evidence in support of the answer given by the respondent	*Rationale:* *Supporting evidence:*				
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*Challenges:* *Risks:*				
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*Obstacles:*				
Please record required conditions and opportunities to achieve the EU	*Conditions:* *Opportunities:*				

baseline, as viewed by the respondent	
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*Economic benefits:* *Technological benefits:* *Political benefits:* Other benefits:

Indicator 5: E-logistics

Benchmark 5.1 - Equal validity of electronic contracting and contract concluded offline

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Equal validity of electronic and offline contracts	**The national legislation establishes the equal validity of electronic contracting and contract concluded offline together with defining the specific requirements to electronic contract**				
Benchmark notes	The legal validity of electronic contracting may impose several requirements on electronic contracts concluded for eCommerce services: equal treatment of contracts, information to be provided in electronic contract, conditions of placing of orders. Contracts concluded by electronic means can have the same validity as contracts concluded offline by "traditional" means (equivalence principle). This applies to all stages and acts of the contractual process, such as the contractual offer, the negotiation and the conclusion of the contract by electronic means. In case of the equal validity, legal provisions obliging hand-written contracts are no longer applicable. The national legislation may require that online traders provide the consumer with specific information prior to the order being placed.				

	This can be the steps to follow to conclude an electronic contract, the filing of the contract by the service provider, the technical means for identifying and correcting input errors prior to the placing of the order, the languages offered for the conclusion of the contract, availability of any relevant codes of conduct, contract terms and general conditions, and others. The rules applied for placing of orders can be also defined. The online contract may require to be concluded through an "order" placed by the consumer, followed by an electronic "acknowledgment" of the online trader without undue delay. The online trader may be requested to provide the consumer with the technical means allowing him/her to identify and correct input errors prior to the placing of the order.
Please record relevant evidence in support of the answer given by the respondent	*Rationale:* *Supporting evidence:*
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*Challenges:* *Risks:*
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*Obstacles:*
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*Conditions:* *Opportunities:*
Please record expected economic, technological, political and other	*Economic benefits:* *Technological benefits:* *Political benefits:*

benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	Other benefits:

Benchmark 5.2 - rules on the conditions for the risk of loss of or damage to the goods

Score	**Strongly disagree**	**Disagree**	**Uncertain**	**Agree**	**Strongly agree**
Enter your response (tick one box only)					
Conditions for the risk of loss of or damage to the goods	**The national legislation defines the conditions for the risk of loss of or damage to the goods purchased within eCommerce transaction and responsibilities of the parties involved.**				
Benchmark notes	These legal provisions should define the conditions for the risk of loss of or damage to the goods and responsibilities of the trader, the consumer, a third party indicated by the consumer, or the carrier. It also should stipulate the remedies available to consumers for damaged or faulty goods, entitlement of consumers to replacement or repair of goods, a refund or discount where specific circumstances apply.				
Please record relevant evidence in support of the answer given by the respondent	*Rationale:* *Supporting evidence:*				
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*Challenges:* *Risks:*				
Please record main obstacles	*Obstacles:*				

obstructing achievement of the EU baseline, as viewed by the respondent	
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*Conditions:* *Opportunities:*
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*Economic benefits:* *Technological benefits:* *Political benefits:* Other benefits:

Benchmark 5.3 - Rights on delivery of goods

Score	**Strongly disagree**	**Disagree**	**Uncertain**	**Agree**	**Strongly agree**
Enter your response (tick one box only)					
Rights on delivery of goods	**The national legislation defines the requirements for time of delivery of goods purchased through eCommerce transaction**				
Benchmark notes	The legislation should define the time of delivery when the trader shall deliver the goods by transferring the physical possession or control of the goods to the consumer. This is usually without undue delay, but not later than a defined maximum number of days from the conclusion of the contract (30 days in the EU). The legislation should also clearly define the conditions when the trader fails to fulfil his obligations to deliver the goods at the time agreed, additional period of time and the right of the consumer to				

	terminate the contract and get reimbursement of all sums paid under the contract.
Please record relevant evidence in support of the answer given by the respondent	*Rationale:* *Supporting evidence:*
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*Challenges:* *Risks:*
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*Obstacles:*
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*Conditions:* *Opportunities:*
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*Economic benefits:* *Technological benefits:* *Political benefits:* Other benefits:

ADDITIONAL QUESTIONS FOR ARMENIA AND BELARUS, MEMBERS OF THE EURASIAN ECONOMIC UNION

For interviews in Armenia and Belarus only

"eCommerce for SMEs"

Please record the respondent's view on the role, benefits , risks and overall impact of the Eurasian Economic Union on the achievement of harmonisation of digital markets in the area of eCommerce	***(Filled in by NEs during/after conducting interview(s) with national stakeholders.)*** ***Role of the Eurasian Economic Union and Eurasian Customs Union regarding the topic of eCommerce for SMEs:*** _____ _ ***Supporting evidence:*** _____ ***Impact of the Eurasian Economic Union and the Eurasian Customs Union in the area of eCommerce practices:*** _____ ***Supporting evidence:*** _____ ***Risks for achieving HDM with the EU in the area of eCommerce for SMEs:*** _____ _____ ***Supporting evidence:*** _____ ***Possible benefits of the Eurasian Economic Union and Eurasian Customs Union for HDM with the EU in the area of eCommerce for SMEs:*** ***economic:*** _____

technological:

_____

political:

_____

other benefits:

_____

_____

Other remarks: _____

7.5 DIGITAL SKILLS

Study on the Harmonisation of the Digital Markets (HDM) in the Eastern Partnership

[Senior Expert 3 version 5th March 2015]

QUESTIONNAIRE FOR "Digital Skills"

Introduction

The Questionnaire aims at determining the current state of play in the EaP countries assessed in relation to the relevant EU baseline (see below) expressed in the form of key benchmarks. This "stock taking" stage will enable a gap analysis to be carried out (see below).

The specific objectives of this questionnaire are;

- to establish (for each EaP country) the results already achieved in relation to the EU baseline for "Digital Skills" as defined in the accompanying document

- to capture opinions on the enablers required for the achievement of the EU baseline

- to capture opinions on the conditions required for the achievement of full harmonization of digital markets with the EU in respect to electronic communications

- to identify possible areas (technological, political, economic) for any expected benefits from harmonisation

- to list the organisations involved with the development of digital markets, specifically in the field of electronic communications

EU baseline for "Digital Skills"

As stated in the paragraph 2.3 of the project Terms of Reference, the EU baseline consists of relevant EU legislation, EU practices, standards and ICT platforms as appropriate for each HDM area. For Digital Skills, this EU baseline has been defined in consultation with DG CONNECT.

There are two main sources for the proposed definition of the EU baseline for Digital Skills:

- The EU policies and initiatives for Digital Skills (see Annex A)
- Examples of practices, enablers and initiatives in EU member states (see Annexes B and C)
-

The spread of ICT (information and communications technologies) throughout the economy and society is leading to the need of everyone in society to have at least basic digital skills in order to live,

work, learn and participate in an increasingly digital society. Not only in the world of work, but almost everywhere else too, ICTs are playing a bigger and bigger role in our daily lives. Besides, ICT changes the way we learn by fostering online communities, by enabling personalised learning experiences, by supporting the development of soft skills such as problem solving, collaboration and creativity, and by making learning fun.

For the purposes of this baseline, ***Digital Skills are broadly defined***[113] ***as ICT-related skills for the labour force, including ICT professionals, digital learners and citizens).*** *Moreover, digital skills could be classified as follows:* ***ICT user skills*** *– required for effective application of ICT systems and services by the individual;* ***ICT practitioner skills*** *required for researching, developing and designing, managing, consulting, marketing and selling, integrating, installing and administrating, maintaining, supporting and servicing ICT systems; and* ***E-business skills*** *needed to exploit opportunities provided by ICT, notably the Internet, to ensure more efficient and effective performance of different types of organisations, to explore possibilities for new ways of conducting business and organisational processes, and to establish new businesses.*

Benchmarks and gap analysis

The questionnaire uses a number of benchmarks derived from the EU baseline for Digital Skills (see above) Each benchmark in the questionnaire includes a statement that describes a key feature of the EU baseline, namely benchmarks for policy, leadership, best practices, resources and relevant initiatives. The interviewees (respondents) should be asked by the National Experts to agree or disagree with the relevance of these benchmark statements to the state of play in their own countries. The level of relevance is measured on a five-point scoring scale, which comprises the following answering options: Strongly disagree; Disagree; Uncertain; Agree; Strongly agree. These answers should demonstrate the proximity of the national state of play to the EU Baseline on each specific benchmark.

By selecting one of the above answer options, respondents present their own opinion (judgment) based on the professional experience and should be prepared support their answers with evidence (which includes explaining the rationale behind the answer and relevant facts). The respondents should also be asked to provide other information including the existing risks, challenges, obstacles, opportunities, possible benefits both in relation to the specific benchmark area and in general as far as the implementation of the entire HDM initiative is concerned.

The proposed benchmarks statements in the questionnaire allow for the assumption that the EaP countries are not yet on par with the EU baseline, i.e. there is a gap to be closed. At the same time, the EU baseline has been formulated in such a way that it is relevant and important for all EaP countries in its own right where the progress can realistically be made. In other words, alignment to the baseline is expected to have real national benefits

[113] See also http://eskills-monitor2013.eu/fileadmin/monitor2013/documents/MONITOR_Final_Report.pdfwww

(technological, political, and economic) regardless of the need to harmonise with the EU per se.

Each EU baseline benchmark is described in detail in the Benchmark notes. These have been written in a readable style, not too jargon filled. The benchmark notes should enable you to understand the key elements of each question without having to read the vast volume of EU Directives, Commission recommendations etc. that are referred to in the baseline.

Structure of the questionnaire

This questionnaire consists of two sections. The first section enables the country's results and enablers to be recorded and aims to collect opinions on the required conditions for the harmonization of the country's digital markets. The second section collects factual information on the organisations involved in developing digital markets in the country.

The format of the questionnaire is a series of statements relating to the Baseline, for example: **"Your country has already commenced sufficient initiatives to ensure a full supply of the required digital skills for all the country's requirements well into the future"** (Initiatives benchmark). You are asked to say if you strongly agree, agree, are uncertain, disagree or strongly disagree. The notes that accompany each question describe what needs to be in place for "commenced sufficient initiatives". For example, only if all the initiatives mentioned in the notes have been commenced (and evidenced), can the answer be "strongly agree". If none of these aspects is evident, then the only response can be "strongly disagree". If some initiatives have and the others have not been commenced, then you have to grade your answer. The spaces in the questionnaire for evidence, challenges, obstacles and conditions should be used to back up the answer, for example "*In our country we have measured our skills gap and published the results together with our priority areas for improving Digital Skills - see document ref xxxxx*"; "*In our country we have not started a National Coalition*" ; "*In our country we have training for coding only at universities as part of ICT based degree courses" ; "We do not have a web entrepreneurs leaders' club" etc.* In the case of this (example) evidence, a correct response would be "disagree".

Please complete the follow-up responses as comprehensively as you can – using specific evidence to support the response. For example, in the example above, the evidence would be a published document by a responsible ministry that has the active participation of the sector participants. Other follow on responses concern risks, obstacles and conditions that are required to fully achieve the benchmark. Finally, a response is sought concerning the expected benefits that would arise if the benchmark was fully achieved.

Questions of clarification

Any questions about the structure and requirements of this questionnaire should be referred to peter.lundy@btopenworld.com

DIGITAL SKILLS

Country name……

[Note: This questionnaire is intended to be completed by the National Experts in the HDM Study Team. It is not intended to be left with the officials in each country (e.g. in ministries and regulatory organisations) that are interviewed as part of the Study.]

Part I: Country's results and enablers

Part I consists of a set of separate statements relating to benchmarks required to achieve the EU baseline, as defined in the accompanying document. Each statement describes a different benchmark as part of the EU baseline for "Digital Skills". For each statement, please state whether the respondent in the country strongly agrees, agrees, is uncertain, disagrees or strongly disagrees with the statement. If a respondent is uncertain, or does not have an opinion, please try to obtain a further opinion from another credible respondent that can be more certain.

If any of the statements below are not clear, please refer to the benchmark notes given below, and also please use the examples of "best practice" given in Annex C of the accompanying document. If the statement or benchmark is still not clear, please refer back to peter.lundy@btopenworld.com for advice.

Section 1: Answer frame: Benchmarks for "Digital Skills"

Benchmark for "Measuring the Digital Skills Gap"

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Measuring the Digital Skills Gap benchmark	Your country has carried out a thorough survey to measure the "Digital Skills gap" and published the results. The survey has measured the supply and demand of digital skills nationally, and collected information on the digital skills required by enterprises and by the education sector.				
Benchmark notes	The starting point for any policy making and implementation on digital skills is the measurement of the "skills gap" between the supply of individuals with digital skills and the demand for these skills. The demand is mostly from enterprises across all sectors of the economy, not just enterprises in the ICT sector. The demand is also for persons in the education sector (teachers and education providers) to possess the skills. For a definition of digital skills used in the EU surveys, see http://eskills-monitor2013.eu/fileadmin/monitor2013/documents/MONITOR_Final_Report.pdfwww which includes the following categories of skills; • **ICT practitioner skills**: the capabilities required for researching, developing, designing, strategic planning, managing, producing, consulting, marketing, selling, integrating, installing, administering,				

maintaining, supporting and servicing ICT systems.

- **ICT user skills**: the capabilities required for the effective application of ICT systems and devices by the individual. ICT users apply systems as tools in support of their own work. User skills cover the use of common software tools and of specialised tools supporting business functions within industry. At the general level, they cover "digital literacy": the skills required for the confident and critical use of ICT for work, leisure, learning and communication.
- **e-Leadership skills**: these cover a range of skills, attributes and attitudes related to: knowledge of the capabilities and limitations of software systems and information systems in use; ability to quickly assess new capabilities of existing systems and the relevance of offers of software and web services emerging on the market; ability to describe prototype solutions; understanding of the fundamentals of alignment of business and IT functions in an organisation.

As well as measuring the supply and demand for digital skills, the survey also makes an assessment and validation of;

- the existing policies, initiatives and multi-stakeholder partnerships
- the expectations as to the development of the supply of ICT practitioners and professionals from the education sector and the industry demand of these until 2020
- Finally, questions on the role of the national governments and other relevant stakeholders where asked

In the EU, the research methodology typically involves data gathering mainly through an online survey accompanied by telephone interviews with different types of institutions, targeting experts from national governments or governmental institutions which had already been involved as part of the activities for the identification and description of relevant digital skills policies, initiatives and multi-stakeholder partnerships, experts from higher education, research and academia, industry and ICT industry, associations of different type, consultants and other types of experts including those from social partners.

The ICT workforce measurement (supply of ICT professionals) uses the occupational categories from the ISCO –International Standard Classification of Occupations 2008 [114] . The counted ICT workforce includes:

- Management, architecture and analysis level positions (ISCO level 1+2)
- ICT practitioners in professional level positions (ISCO level 2)

[114] See: http://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/---publ/documents/publication/wcms_172572.pdf

	• ICT practitioners in associate or technician level positions (ISCO level 3) Demand potential up until 2020 is calculated and estimated using the following observations: • The long term trend of ICT workforce growth over the past decade • Annual growth of ICT employment has remained very robust throughout the crisis • The correlation between the ICT workforce growth rates, GDP growth rates and IT investment growth rates have been disappearing somewhat during recent years • There seems to be less influence of economic cycles and a stronger indication of a "megatrend" • Consequence for foresight: Heavier weighting of "trend" in favour of "economic situation" Several assumptions for forecasting the future digital skills developments in Europe have been developed which build the basis for the calculation of digital skills demand and supply for the period up until 2020. The assumptions and other factors used in estimating digital skills demand are contained in the report "e-Skills for jobs in Europe: Measuring progress and moving ahead" (February 2014) on; https://www.google.co.uk/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=e-skills%20for%20jobs%20in%20europe%20february%202012
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ __ *Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks:

HDM in general, as viewed by the respondent	_____
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Policy Benchmark for "Digital Skills"

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Policy benchmark	Your country has a clear recognition that a strong digital economy is vital for innovation, growth, jobs and competitiveness. Therefore there is a clear long-term Digital Skills policy for developing digital literacy for employability, e-inclusion and lifelong acquisition of Digital Skills.				
Benchmark notes	Digital technology is changing the way we work, learn and live. The spread of digital is having a massive impact on the labour market and the type of skills needed in the economy and in the society: • Firstly, it is changing the structure of employment, leading to the automation of "routine" tasks and to the creation of new and different types of jobs. • Secondly, it is leading to the need for more skilled ICT professionals in all sectors of the economy. It is estimated that across the EU there will be 825,000 unfilled vacancies for ICT professionals by 2020. • Thirdly, it is leading to the need for digital skills for nearly all jobs where ICT complements existing tasks. In the near future 90% of jobs - in careers such as engineering, accountancy, nursing, medicine, art, architecture, and many more - will require some level of digital skills. • Fourthly, it changes the way we learn by fostering online communities, by enabling personalised learning experiences, by supporting the development of soft skills such as problem solving, collaboration and creativity, and by making learning fun. • Finally, it is leading to the need for every citizen to have at least basic digital skills in order to live, work, learn and participate in the modern society. Digital Skills requires a co-ordinated policy approach, within the context of national policies for uptake of ICT for competitiveness, growth, employment, education, lifelong training and social inclusion. Digital Skills must be elevated to have an important place in long-term national policy. Each country should take a central role in developing these national policies and actions, within which a long-term Digital Skills agenda is launched, to improve cooperation and mobilisation of all stakeholders and to adopt best strategies and practices in order to better face global competitive challenges. Countries should therefore ensure that they develop, with national and local stakeholders, clear long-term Digital Skills policies. Within the national policy, the key components of action should be defined – long term co-operation, human resources investment, making science, maths and ICT attractive, developing digital literacy for employability and e-inclusion and lifelong acquisition of				

	Digital Skills.
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ __
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please	*(Filled in by NEs during/after conducting interview(s) with national*

record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Leadership Benchmark for "Digital Skills"

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Leadership benchmark	**Your country has an approach aligned to the EU's "Grand Coalition for Digital Jobs" whereby stakeholders "pledge" concrete actions within and overall leadership framework of a National Coalition for Digital Jobs.**				
Benchmark notes	**Pledges** are concrete commitments by companies, universities, and other stakeholders to address the digital skills gap. Actions such as industry-led training, encouraging cross-border mobility for ICT workers, certifying skills, modernising school and university curricula and raising awareness need the active engagement of all stakeholders at national level. Some countries are forming **National Coalitions for Digital Jobs**. These are partnerships that bring together the government (e.g. education and employment ministries) with ICT and ICT-using businesses, education and training providers, public and private employment services, associations, NGOs, social partners and many more, in order to achieve high-impact action on the ground. So far 8 national coalitions have been launched (see examples at Annex B of the Digital Skills Baseline document) and many more are under formation. National and Local Coalitions are described below under the Initiatives Benchmark. For **examples of the pledges** made in EU countries under National Coalitions, see http://ec.europa.eu/digital-agenda/en/make-pledge#how-are-we-doing This gives examples of companies that have pledged support for; • Training and matching for digital jobs • Certification, including promoting the adoption and take-up of the e-Competences Framework [115] (see also "Best Practices Benchmark" below) • Innovative learning and teaching (see also "ICT for better Education Benchmark" below) • Mobility; e.g. showcasing opportunities in the technology sector to a global audience and providing information to assist people in moving to the country • Awareness raising; e.g. the engagement between business representatives and educational players focusing in the fields of STEM (science, technology, engineering and mathematics) education and entrepreneurship skills				
Please record relevant	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)*				

[115] See also http://www.ecompetences.eu/

evidence in support of the answer given by the respondent	*Rationale:* _____ _ *Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ __
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological,	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____

political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	Technological _____	benefits:
	Political _____	benefits:
	Other _____	benefits:

Best Practices Benchmark for "Digital Skills"

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Best Practices benchmark	**Your country has provided a platform for exchange of best practices, promoting a regular dialogue on Digital Skills, and has developed an e-Competence Framework.**				
Benchmark notes	One of the key steps for effective stimulation of digital skills across the EU has been the creation of a focal point that co-ordinates and supports various initiatives. Under the Grand Coalition on Digital Jobs (see Leadership Benchmark above and the Initiatives Benchmark below). A Grand Coalition Secretariat focuses on encouraging action and local implementation. It aims at amplifying successful local and national programmes and initiatives and seeks to export these to other parts of Europe. It builds and promotes local coalitions to facilitate action towards enhanced digital skills at national, regional or local level. In this way, the sharing of best practice by recognition, awareness raising and publicity acts to promote more local action and implementation. The platform for sharing best practice could reside in a government or non-governmental organisation and provide a recognised focal point for information, advice and support. The EU Secretariat has produced a **Toolkit for National and Local Coalitions**[116]. The Toolkit defines the role of National and Local Coalitions and clarifies the support available from the Secretariat. Information about available funding opportunities to develop the activities of National and Local Coalitions are also provided in the Toolkit. Stakeholders involved with the Grand Coalition for Digital Jobs now benefit from a clear set of guidelines and recommendations on how to implement successfully the Grand Coalition in their country of interest. The EU has also developed a **European e-Competence Framework (e-CF)**[117] which provides a reference of 40 competences as required at the ICT workplace, using a common language for competences, skills and proficiency levels that can be understood across Europe. A user guide for the application of the e-CF is also available.[118]				
Please	*(Filled in by NEs during/after conducting interview(s) with national*				

[116] This is downloadable from: http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=913&PortalId=0&TabId=353

[117] The e-CF framework definition is downloadable on:

www.ecompetences.eu/wp-content/uploads/2014/02/European-e-Competence-Framework-3.0_CEN_CWA_16234-12014.pdf

[118] The user guide for the application of the e-CF is downloadable on;

www.ecompetences.eu/wp-content/uploads/2014/02/User-goide-for-the -application-of-the-e-CF-3.0_CEN_CWA_16234-1-2014.pdf

record relevant evidence in support of the answer given by the respondent	*stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ __
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)*

economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	Economic _____	benefits*:*
	Technological _____	benefits*:*
	Political _____	benefits*:*
	Other _____	benefits:

Resources Benchmark for "Digital Skills"

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Resources benchmark	**Your country has already created, or has access to, sufficient funding to drive the activities of National and Local Coalitions for Digital Jobs and promote Digital Skills initiatives and advancement.**				
Benchmark notes	The European Commission encourages Member States to use available funding (e.g. from ESF, Youth Employment Initiative, Horizon 2020, Erasmus+, etc.) to fund activities of national coalitions aimed to digital skills development. Although The Grand Coalition does not have a specific budget line to support its activities, there are several funding sources at European and national level to support projects boosting digital skills. A website [119] gives a number of funding instruments that are available to stakeholders as well as the non-financial support that can be obtained. Each country could ensure that it creates, or has access to, sufficient funding to drive the activities of national and local coalitions and promote Digital Skills development. Examples of committed resources for national coalitions are pledges by coalition partners for training, awareness raising events, job fairs, and incubator initiatives; sponsorships and private funding, government funding. Open Educational Resources (OER), ensures that educational materials produced with public funding are available to all, so that learning can happen anytime, anywhere. Massive Open Online Courses (MOOCs) allow students, practitioners and educational institutions to share free-to-use course material and the EU-funded Open Education Europa portal provides access to the many resources available. In addition, large scale pilot projects such as Open Discovery Space, co-funded by the European Commission, are working with teachers to create and make better use of OER. Initiatives linked to the Opening up Education will be funded with support from Erasmus+, the new EU programme for education, training, youth and sport, and Horizon 2020, which is the financial instrument implementing the Innovation Union, a Europe 2020 flagship initiative aimed at securing Europe's global competitiveness. *Note: The extent to which these EU based resources are available to the EaP countries will be clarified during the implementation phase of the HDM project. This questionnaire is seeking to determine what existing funding and resources are already in place for the advancement of Digital Skills in each EaP country.*				
Please record relevant evidence in support of the	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:*				

[119] https://ec.europa.eu/digital-agenda/en/potential-funding

answer given by the respondent	_____ _ *Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ __
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____

of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	Technological _____	benefits:
	Political _____	benefits:
	Other _____	benefits:

Initiatives Benchmark for "Digital Skills"

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Initiatives benchmark	**Your country has already commenced sufficient initiatives to ensure a full supply of the required digital skills for all the country's requirements well into the future**				
Benchmark notes	In order to ensure that the country has sufficient digital skills for all its needs well into the future, it is first necessary to have measured the likely demand (from all sectors including business, government and education) and supply of digital skills – see also Measurement of Digital Skills Gap benchmark above). Having measured the "digital skills gap" and determined the priorities for action, the country will commence a number of relevant initiatives to remove the digital skills gap. In the EU the main current initiatives are The **Grand Coalition for Digital Jobs**, which is the largest collaborative effort in Europe to date to address the digital skills shortage. So far 80 stakeholders, representing large and smaller companies, education providers and NGOs have made pledges, i.e. concrete commitments to act to reduce digital skills gaps. Likewise, national coalitions for digital jobs aimed to facilitate high-impact actions at local level have already been (see below and examples in Annex B). **National Coalitions** have the following key objectives: Innovative learning and teaching, Increase the number of ICT specialists, Fostering digital entrepreneurship, Certification of digital skills, Improved digital literacy, Awareness raising. Broadly speaking, the goals of national coalitions are same as of the Grand Coalition. So far 8 national coalitions have been launched (in Bulgaria, Greece, Italy, Malta, Latvia, Lithuania, Poland, Romania) and many more are under formation (see also Annex B). There are also some **Local Coalitions**, which either focus on a specific geographical region or have particular objectives, e.g.: Italy: multi-sector network on educational robotics (ER) WGGD Greece: equal employment opportunities for women in ICT, attract more girls to Science, Technology, Engineering and Mathematics (see also Annex C). **Coding** has become the focus of a specific work stream under the Grand Coalition aimed to encourage coding and computer science across Europe, both within schools and beyond. Europe is promoting coding through various initiatives, such as the EU code Week and the European Coding Initiative and through pilot projects on digital learning in schools. In January 2013, the Commission adopted the **Entrepreneurship 2020 Action Plan** to unleash Europe's entrepreneurial potential. This Action Plan includes a set of actions, such as a Start-up Europe Partnership, to unlock expertise, mentoring, technology and services; work with European investors in order to increase the flow of venture capital and crowd-funding (in particular for web start-ups); and stimulate the emergence of Massive Online Open Courses (MOOCs) and the setting up of platforms for mentoring, and skill building.				

	The **Web Entrepreneurs Leaders Club** brings together world-class web entrepreneurs to strengthen the web entrepreneurial culture in Europe as well as a European network of web business accelerators.
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ __
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____

respondent	
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

ICT for Better Education Benchmark for "Digital Skills"

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
ICT for Better Education benchmark	**Your country has highly digitally equipped schools – i.e. ICT in classrooms with broadband connections, giving non-discriminatory access to quality content and innovative teaching methodologies for students of all ages**				
Benchmark notes	While digital technologies gradually embrace wider parts of everyday life, it is estimated that in the EU, 60% of students never use digital equipment in classroom. The full potential for improving education through ICT in Europe remains yet to be discovered and this is why the European Commission is developing policy and supporting research to make learners fit for 21st century life and work. The Communication on **Opening Up Education** and research and innovation programmes both aim at enabling opportunities for better learning through use of modern devices, wider connectivity and interoperability, non-discriminatory access to quality content and innovative teaching methodologies which are responsive to learner's individual needs. A learner-centred pedagogy using ICT and interdisciplinary research makes personalised and adaptive learning possible. For instance, learning analytics tools support teachers' work by providing individual feedback and recommendations to students and educational games are powerful tools to engage kids (and students of all ages) in learning. Fostering of online teachers' communities across Europe empowers them to use and co-create the wealth of educational repositories. The essential pre-condition for innovative learning ecosystems are **Connected Classrooms** - in 'highly digitally-equipped school' – with recent equipment, fast broadband (10Mbps plus) and high 'connectivity' (website, email for students and teachers, local area network, virtual learning environment). They can only happen if broadband can reach even remote areas - as a recent EU report shows[120], Policies and action at infrastructure level are still needed to enable the large majority of students, at all grades, to be in highly digitally equipped schools.				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:*				

[120] "Survey of Schools: ICT in Education Benchmarking Access, Use and Attitudes to Technology in Europe's Schools" http://europa.eu/rapid/press-release_IP-13-341_en.htm

	_____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ __
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:*

partner countries and with the EU, as viewed by the respondent	_____ Other benefits: _____

Section 2: National organisations involved in development of digital markets

Organisation	Level of involvement (High, Medium or Low)						Description	Key functions in relation to HDM
	EU cooperatio	National policy	Strategy	Legislation	Executive	Regulatory body		
Organisation 1 (enter name)								
Organisation 2 (enter name)								
Organisation 3 (enter name)								
Organisation 4 (enter name)								

ADDITIONAL QUESTIONS FOR ARMENIA AND BELARUS, MEMBERS OF THE EURASIAN CUSTOMS UNION

For interviews in Armenia and Belarus only

"Digital Skills"

Please record the respondent's view on the role, benefits , risks and overall impact of the Eurasian Economic Union and the Eurasian Customs Union on the achievement of harmonisation of digital markets with the EU in the area of Digital Skills	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* *Role of the Eurasian Economic Union and Eurasian Customs Union regarding the topic of digital skills:* _____ *Supporting evidence:* _____ *Impact of the Eurasian Economic Union and the Eurasian Customs Union in the area of digital skills:* _____ *Supporting evidence:* _____ *Risks for achieving HDM with the EU in the area of digital skills:* _____ _____ *Supporting evidence:* _____ *Possible benefits of the Eurasian Economic Union and Eurasian Customs Union for HDM with the EU in the area of digital skills:* *economic:* _____ *technological:* _____

	political: _____ *other* *benefits:* _____

7.6 TELECOM RULES

Study on the Harmonisation of the Digital Markets (HDM) in the Eastern Partnership

[Senior Expert 3 version 27th January 2015]

QUESTIONNAIRE FOR "TELECOMS RULES"

Introduction

The Questionnaire aims at determining the current state of play in the EaP countries assessed in relation to the relevant EU baseline (see below) expressed in the form of key benchmarks. This "stock taking" stage will enable a gap analysis to be carried out (see below).

The specific objectives of this questionnaire are;

- to establish (for each EaP country) the results already achieved in relation to the EU baseline for "Telecom Rules" as defined in the accompanying document

- to capture opinions on the enablers required for the achievement of the EU baseline

- to capture opinions on the conditions required for the achievement of full harmonization of digital markets with the EU in respect to electronic communications

- to identify possible areas (technological, political, economic) for any expected benefits from harmonisation

- to list the organisations involved with the development of digital markets, specifically in the field of electronic communications

EU baseline for "Telecom Rules"

As stated in the paragraph 2.3 of the project Terms of Reference, the EU baseline consists of relevant EU legislation, EU practices, standards and ICT platforms as appropriate for each HDM area. For Telecom Rules, this EU baseline has been defined in consultation with DG CONNECT.

The attached document describes the baseline for "Telecoms Rules" to be used in conjunction with this questionnaire. The baseline is derived from three main sources;

- The EU legal and regulatory framework for electronic communications (see Annex A of the attached document)
- The Association Agreements already signed between the EU and Georgia, Moldova and Ukraine (see relevant extracts at Annex B of the attached document)
- Examples of EU practice already implemented in selected member states. (It is highly recommended that the National Experts read a document available from peter.lundy@btopenworld.com that provides extracts from the recent report

"Benchmarking Electronic Communications Markets in EaP countries". These extracts give examples of implemented practices in selected EU countries for each of the questionnaire sections below.)

The definition of "Telecoms" *for the purposes of this questionnaire (arising from the baseline for "Telecoms Rules") is that part of the electronic communications market that provides infrastructure and services (on a wholesale or retail basis) for fixed and mobile communications including voice and data services. The "Telecoms" definition also applies particularly to fixed and mobile broadband services capable of providing stand-alone and bundled services comprising voice, internet and media services. For the purposes of this questionnaire, broadband services are defined as services (wholesale or retail) capable of presenting data transmission rates of at least 2Mbps to an end users. "High speed broadband" is similarly defined for data transmission of at least 30Mbps.*

Benchmarks and gap analysis

The questionnaire uses a number of benchmarks derived from the EU baseline for Telecoms Rules (see above) Each benchmark in the questionnaire includes a statement that describes a key feature of the EU baseline, namely benchmarks for leadership, policy, strategy resources, implementation, legal framework, infrastructure and services. The interviewees (respondents) should be asked by the National Experts to agree or disagree with the relevance of these benchmark statements to the state of play in their own countries. The level of relevance is measured on a five-point scoring scale, which comprises the following answering options: Strongly disagree; Disagree; Uncertain; Agree; Strongly agree. These answers should demonstrate the proximity of the national state of play to the EU Baseline on each specific benchmark.

By selecting one of the above answer options, respondents present their own opinion (judgment) based on the professional experience and should be prepared support their answers with evidence (which includes explaining the rationale behind the answer and relevant facts). The respondents should also be asked to provide other information including the existing risks, challenges, obstacles, opportunities, possible benefits both in relation to the specific benchmark area and in general as far as the implementation of the entire HDM initiative is concerned.

The proposed benchmarks statements in the questionnaire allow for the assumption that the EaP countries are not yet on par with the EU baseline, i.e. there is a gap to be closed. At the same time, the EU baseline has been formulated in such a way that it is relevant and important for all EaP countries in its own right where the progress can realistically be made. In other words, alignment to the baseline is expected to have real national benefits (technological, political, and economic) regardless of the need to harmonise with the EU per se.

Each EU baseline benchmark is described in detail in the Benchmark notes. These have been written in a readable style, not too jargon filled. The benchmark notes should enable you to understand the key elements of each question without having to read the vast volume of EU Directives, Commission recommendations etc. that are referred to in the baseline.

Structure of the questionnaire

This questionnaire consists of 2 sections. The first section enables the country's results and enablers to be recorded and aims to collect opinions on the required conditions for the harmonization of the country's digital markets. The second section collects factual information on the organisations involved in developing digital markets in the country.

The format of the questionnaire is a series of statements relating to the Baseline, for example: ***"Your country has fully introduced number portability for both mobile and fixed numbers"*** (Implementation benchmark 3a). You are asked to say if you strongly agree, agree, are uncertain, disagree or strongly disagree. The notes that accompany each question describe what needs to be in place for "full introduction". For example, if only mobile number portability has been implemented (and not fixed number portability), then you cannot fully agree with the statement. If the time to port a number is greater than one day, again, this is not full implementation according to the EU Baseline. If there are restrictions to porting (for example a maximum number per year for any customer), again this is not full implementation. So, in this example, a correct response would be "disagree" because many of the most important elements are not yet in place. The spaces in the questionnaire for evidence, challenges, obstacles and conditions should be used to back up the answer, for example "Mobile number portability was introduced in 2013";"No fixed number portability until at least 2016"; "Average porting time is 4 days"; "Customers can only port once a year", etc.

Looking at another example, ***"Your country has an adopted strategy promoting high speed broadband infrastructure investment with clearly defined targets for the achievement of universal fast broadband access and take-up"*** (Infrastructure benchmark 2), the notes to the question provide guidance as to what constitutes an adopted strategy. This includes a set of specific published targets for broadband, rules governing state aid for broadband investments and a clear market-driven strategy for releasing spectrum to promote universal broadband access. Only if there is clear evidence on these aspects can the answer be "strongly agree". Only if all the elements described in the benchmark notes are actually in place (implemented and evidenced) can the answer be "strongly agree". If none of these aspects is evident, then the only response can be "strongly disagree". Again, the spaces in the questionnaire for evidence, challenges, obstacles and conditions should be used to back up the answer, for example "There a target for at least 30Mbps to be available in the entire territory of the country by 2020 (see www.etc)" "Spectrum was assigned to 3 operators for 4G/LTE services in 2014"; "No state aid has been allocated specifically for broadband infrastructure investment".

Please complete the follow-up responses as comprehensively as you can – using specific evidence to support the response. For example, in the 2nd example above, the evidence would be a published document by a responsible ministry that has the active participation of the sector participants. Other follow on responses concern risks, obstacles and conditions that are required to fully achieve the benchmark. Finally, a response is sought concerning the expected benefits that would arise if the benchmark was fully achieved.

Questions of clarification

Any questions about the structure and requirements of this questionnaire should be referred to peter.lundy@btopenworld.com

QUESTIONNAIRE FOR "TELECOMS RULES"

Country name……

[Note: This questionnaire is intended to be completed by the National Experts in the HDM Study Team. It is not intended to be left with the officials in each country (e.g. in ministries and regulatory organisations) that are interviewed as part of the Study.]

Part I: Country's results and enablers

Part I consists of a set of separate statements relating to benchmarks required to achieve the EU baseline, as defined in the accompanying document. Each statement describes a different benchmark as part of the EU baseline for "Telecoms Rules". For each statement, please state whether the respondent in the country strongly agrees, agrees, is uncertain, disagrees or strongly disagrees with the statement. If a respondent is uncertain, or does not have an opinion, please try to obtain a further opinion from another credible respondent that can be more certain.

If any of the statements below are not clear, please refer to the benchmark notes given below, and also please use the examples of "best practice" given in Annex C of the accompanying document. If the statement or benchmark is still not clear, please refer back to peter.lundy@btopenworld.com for advice.

Section 1: Answer frame: Benchmarks for "Telecoms Rules"

Leadership Benchmarks for "Telecoms Rules"

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Leadership benchmark 1	**Your country has a clear separation of functions between policy making, regulation and operational functions for the electronic communications sector**				
Benchmark notes	The function of **policy making** is normally undertaken by a competent ministry with clear powers to set forward policy for the electronic communications sector. This ministry should not be involved in, and should not unduly influence the day-to-day regulation of electronic communications markets, nor should the ministry exercise control or ownership over any operators or service providers deriving revenues from providing services in the sector, either on a wholesale or retail basis. The function of **regulation** is normally undertaken by an independent organisation from any ministry or operator and should not be unduly influenced in its decision-making by government or by operators The function of **operations** is normally carried out by commercial entities serving the market as networks and service providers at both wholesale and retail level. If any operating/ service providing entity is owned or part-owned by the state, then the state entity that represents that ownership share should not be the same state entity responsible for policy making or regulation and should not unduly influence policy				

	making or regulatory functions.
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ __
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please	*(Filled in by NEs during/after conducting interview(s) with national*

record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Leadership benchmark 2	**Your country always ensures that any proposed new policies and any proposed new regulations that could impact the electronic communications sector are published in draft form first, allowing a reasonable period for public comment and discussion before decisions are taken. The results of this public consultation are published.**				
Benchmark notes	The purpose of public consultation is to allow comment to be expressed by any party before decisions are taken that may affect any parties, including consumers, businesses, market investors, operators and service providers. If forward-looking policy (e.g. by a responsible ministry) or regulatory decisions (e.g. by the sector regulator or the competition/ anti-monopoly entities) are made without this transparency and without an opportunity to express consumer, business and investor interests, then the credibility and effectiveness of the policy/ regulatory decision is diminished. A reasonable period for public consultation would be at least 2 weeks, normally 4. Publication of the results of the public consultation should include a list of the key issues involved, the comments received regarding each issue and response of the decision making body – i.e. a revised decision or clear reasons for rejection of opinions received.				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____				
Please record main challenges and risks for achieving this EU baseline and implementing HDM in	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____				

general, as viewed by the respondent	__
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Leadership benchmark 3	**Your country has a clear and actively promoted policy towards consumers - including the protection of their rights for access to electronic communications services, the right to privacy in electronic communications and the right of freedom of expression for electronic communications services and their use**				
Benchmark notes	Consumers should have the right of access to electronic communications including; -a connection supporting data communications at rates sufficient for access to online services such as those provided via the public Internet -the right to clear information on services, quality and price -the right to have a contract with a supplier stating the duration of the contract, any limitations on use and complaints procedures -public pay-telephones and/or alternative public access points -access to emergency services numbers free of charge -access for disabled users to equivalent services as other users Additional users' rights include the protection of fundamental rights and freedoms, in particular; -the right to privacy and confidentiality of electronic communications -end users should be able to decide what content they want to send and receive and which services, applications, hardware and software they want to use -the personal data of users should not be disclosed to third parties without the expressed permission of the user -end users should be informed of their rights with respect to the use of their personal information in subscriber directories -free movement of electronic communications equipment and services across national boundaries				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____				
Please record main challenges and risks for	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges:				

achieving this EU baseline and implementing HDM in general, as viewed by the respondent	_____ Risks: _____
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Policy Benchmarks for "Telecoms Rules"

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Policy benchmark 1	**Your country has a clear Universal Services approach containing a competitively neutral policy for the provision, to any requesting person, of a defined set of services, including internet access, at affordable prices**				
Benchmark notes	A **universal service policy** ensures that anyone that requests a basic service should be able to receive it from at least one service provider at a reasonable price – normally the published uniform price for the service without geographical discrimination or discrimination of tariffs between different types of user. A typical universal service policy would include the procedures for the regulator to designate at least one service provider with the obligation to provide a defined basic set of services, with a financial compensation mechanism to the designated providers if it is calculated that having this obligation results in a net economic loss when compared with not having the obligation, taking into account the actual costs and benefits to each service provider. **The definition of basic service** normally includes access at a fixed location (regardless of the technology used, which could also be mobile service), all types of voice calls, public access points, emergency services and access to data communications at rates sufficient for online services such as those provided via the public Internet. The minimum data rates for efficient internet access should normally be defined taking due account of specific circumstances in national markets, for instance the prevailing bandwidth used by the majority of subscribers. A typical minimum rate in the EU is now 2Mbps. **A competitively neutral policy** for universal service means that the service providers that are obliged to provide service do not derive any consequent competitive advantage or exclusive right to provide service at any locations as a result of having the universal service obligation or access to universal service funding. This rules out a policy that simply subsidises any operators to keep all monthly rental charges at below the cost of supply, which for a typical fixed access line is at least EUR 10 per month.				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _				

	Supporting evidence: _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____

benchmark between the partner countries and with the EU, as viewed by the respondent	Political benefits: _____ Other benefits: _____

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Policy benchmark 2	**Your country has a clear policy towards increased effectiveness of broadband competition and for enhancing investment in infrastructure for high speed broadband services**				
Benchmark notes	A **policy for effective broadband competition** would typically include that any operator or service provider can; - freely enter the market and use whatever technology they chose - have access to other operators' network elements and infrastructure on a wholesale basis in order to provide end users with their own competing broadband offerings. Note that this policy should contain regulatory safeguards (with compliance monitoring) that will ensure that access to the networks of operators with significant market power (SMP) gives the requesting operator/ service provider an equivalent wholesale service to the service that is self-supplied to the SMP operator's own retail operation (equivalent in cost, quality and timeliness) A **policy for encouragement of broadband investment** would typically include; -access to state aid for the acceleration of planned investments in broadband infrastructure to currently uneconomic areas in order to meet government targets for broadband coverage -state funding and facilitation to assist in the creation of specific infrastructure projects that will allow operators/ service providers to have access, at cost related wholesale charges, to extend their retail services beyond their current geographical scope -the promotion and facilitation of measures to enable cost sharing agreements for the construction and joint use of networks and passive infrastructures (ducts, manholes, street cabinets, poles, masts, towers, buildings, power supplies and other supporting elements). This type of cost sharing opportunity should extend beyond just the providers of electronic communications infrastructure, also to other utilities that construct and operate infrastructure (e.g. sharing of trenching costs between electricity, water and telecoms providers)				
Please	*(Filled in by NEs during/after conducting interview(s) with national*				

record relevant evidence in support of the answer given by the respondent	*stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ __
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)*

economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	Economic _____	benefits:
	Technological _____	benefits:
	Political _____	benefits:
	Other _____	benefits:

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Policy benchmark 3	**Your country has clear policy and regulations ensuring the harmonised availability and efficient use of spectrum, taking account of the market needs and the optimal use of scarce resources**				
Benchmark notes	**Radio spectrum policy** should have a defined objective that contributes to freedom of expression, including freedom of opinion and freedom to receive and disseminate information and ideas, irrespective of borders, as well as freedom and plurality of the media taking account of the democratic, social, linguistic and cultural interests related to the use of the frequency spectrum. The policy should also specifically support a universal high-speed broadband strategy, thus exploiting the huge potential of wireless services to promote a knowledge-based economy, develop and assist sectors relying on information and communications technologies and overcome the digital divide. The spectrum policy must therefore be market-driven such that if there is spectrum available, it should be offered to the market for economic exploitation rather than retained in inefficient usage or withheld in order to create an artificial shortage. The policy must also recognise that spectrum management may affect competition by changing the role and power of market players, for example if existing users receive undue competitive advantages. Limited spectrum access, in particular when appropriate spectrum becomes scarcer, can create a barrier to entry for new				

	services or applications and hamper innovation and competition. Acquisition of new rights of use of spectrum, including through spectrum transfer or leasing or other transactions between users, and the introduction of new flexible criteria for spectrum use can have an impact on the existing competitive situation. The spectrum policy should therefore explicitly allow the regulator to take appropriate ex-ante or ex-post regulatory measures such as; - action to amend existing rights, to prohibit certain acquisitions of rights of use of spectrum, to impose conditions on spectrum hoarding -to limit the amount of spectrum available for each undertaking, or to avoid excessive accumulation of rights of use of spectrum -to avoid distortions of competition in line with the principles for public pan-European cellular digital land-based mobile communications The policy should include the need for strategic planning and harmonisation of the use of radio spectrum taking into consideration inter alia economic, safety, health, public interest, freedom of expression, cultural, scientific, social and technical aspects as well as the various interests of radio spectrum user communities with the aim of optimising the use of radio spectrum and of avoiding harmful interference. The policy should also emphasise an economic and social approach with regard to the management, allocation and use of spectrum with particular focus on ensuring greater spectrum efficiency, better frequency planning and safeguards against anti-competitive behaviour plus the creation of opportunities for innovation and employment creation, economic growth and social integration. Other specific aspects that should be included in spectrum policy are the need for international coordination in particular with regard to; -the provision of international roaming facilities -trans-border services without requiring the movement of persons, such as satellite communications services -the avoidance of cross-border interference -other international agreements which may affect radio frequency bands usage and sharing plans and which may address issues such as trade and market access, including in the World Trade Organisation framework, free circulation and use of equipment, communications systems of regional or global coverage such as satellites, safety and distress operations, transportation systems, broadcasting technologies, and research applications such as radio astronomy and earth observation. -**Radio spectrum regulations** should cover clear, transparent and non-discriminatory procedures for the allocation of radio spectrum, assignment and licensing procedures, including the use competitive selection procedures for the assignment of radio frequencies. Other requirements require the publication of the existing state of allocated radio frequency bands and with regard to mobile and personal communications, the publication of plans for future extension of such frequencies. Regulation should promote easy access to spectrum and define innovative types of authorisation such as collective use of spectrum, infrastructure sharing and spectrum secondary trading.
Please record relevant evidence in support of the answer given	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____

by the respondent	_ *Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ __
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:*

harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	_____ Political benefits: _____ Other benefits: _____

Strategy benchmarks for "Telecoms Rules"

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Strategy benchmark 1	**Your country has clear procedures for the identification, definition and analysis of relevant markets that are subject to ex-ante regulation in order to determine if significant market power (SMP) exists**				
Benchmark notes	**Ex-ante regulation** is the standard type of regulation applied to markets that are not yet sufficiently competitive. The regulator should use this approach to anticipate any likely abuse by an operator with a dominant market position (significant market power) against its less dominant competitors. The application of ex-ante regulation has already achieved far more effective markets in electronic communications in all EU (and many other) countries. The procedures involve the identification of "relevant" markets in each country that should be subjected to ex-ante regulation, followed by detailed definitions of these markets then formal analysis of each defined market to determine if SMP exists and finally the intervention by the regulator using market remedies that will reduce SMP in each market and therefore make the markets more competitive. This type of regulation is termed "asymmetric" because it is applied only to players with SMP and not to the other players in each market. In some relevant markets (for example call termination on individual operators' networks) there are likely to be more than one SMP operator. In other markets (for example the provision of a line at a fixed location) there will normally be only one SMP operator (usually the incumbent operator/ service provider in the case of electronic communications markets). In 2003, the EU recommended 18 relevant markets (5 retail and 13 wholesale markets). By 2007, the use of ex-ante regulation had made 11 of these markets sufficiently competitive, leaving only 7 recommended markets that are susceptible to ex-ante regulation (1 retail and 6 wholesale). In 2014, the EU further reduced the number of recommended markets to 5 wholesale markets. This means that out of 18 markets within the electronic communications sector, only 5 in the EU remain insufficiently competitive. It is unlikely that this situation exists in the EaP countries and so each country should have clear procedures (see notes below) to identify, define and analyse relevant markets and then apply formal ex-ante regulation to ensure that each market becomes sufficiently competitive. If a country does not have procedures in place (and regularly used by the sector regulator) to define, analyse and apply market remedies, then it is unlikely that the whole electronic communications sector is effective in terms of consumer choice and competitive safeguards for investors. **Identification of relevant markets.** The defined procedures should normally be derived from competition law (anti-monopoly law), rather than sector-specific law, because the principles of ex-ante regulation for improving the effectiveness of competitive markets are generic. The standard (best practice) test used to determine if markets are sufficiently competitive (and therefore not susceptible to ex-ante regulation) is the so called "3 Criteria Test" which should be explicitly stated in the procedures. For electronic communications, the starting point should be the 2007 list of 7 relevant markets as recommended in the EU. The procedures should					

	allow other markets to be added to the list where the results of the "3 Criteria Test" justifies their inclusion. **Definition of relevant markets.** The defined procedures should be based on best practice, as recommended and used in the EU. These procedures use standard tests (for example the SSNIP test) to determine what services are actual substitutes within a relevant market and therefore should be included in the market definition. Only when the relevant market is fully defined in terms of a set of substitutable services and in terms of geographical scope can it be analysed for competitiveness. **Analysis of relevant markets to determine SMP.** The defined procedures should follow the best practice recommendations applied in the EU. These involve the examination (for each relevant market in turn) of a number of demand side and supply side features of the market based on data on the market and observations of the behaviour of customers and suppliers. The objective of the analysis in each market in turn is to determine if SMP exists in that market, based on objective and transparent criteria. The results of the market analysis for each defined relevant market should be published for public consultation before any regulatory decisions are made. The results of the public consultation, taking account of the responses received, should also be published and used to objectively justify any regulatory decisions regarding market remedies (see also Implementation Benchmark 1 below).
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ __
Please record main obstacles obstructing	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles:

achievement of the EU baseline, as viewed by the respondent	_____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Score	**Strongly disagree**	**Disagree**	**Uncertain**	**Agree**	**Strongly agree**
Enter your response (tick one box only)					
Strategy	**Your country has an effective means to ensure that operators have**				

benchmark 2	**access to public and private property for the purposes of building and operating electronic communications infrastructure ("rights of way") using simple, efficient, transparent procedures, applied without discrimination or delay**
Benchmark notes	The **"rights of way" procedures** should ensure that the granting of permission to install and maintain electronic communications facilities on public or private property are timely, non-discriminatory and transparent, in order to guarantee the conditions for fair and effective competition. The procedures should apply when a competent authority (national, regional or local government or private owner) considers a request from an electronic communications provider to install equipment in, under or above public or private property for the purposes of providing public or private telecommunications services. The procedures should guarantee that the competent authority acts efficiently, non-discriminately and without delay. Any conditions related to the permission should be made transparent. There should also be a simple mechanism for a permission seeker to appeal to an independent entity (for example the regulator) against any adverse decisions of the competent authority. Also, if the competent authority responsible for the property also has ownership of any electronic communications entity (for example where the state has some ownership of an operator), then the two ownership functions must be functionally separated in order not to provide the perceived conditions for discrimination or conflict of interest.
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ __
Please record main	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)*

obstacles obstructing achievement of the EU baseline, as viewed by the respondent	Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Score	**Strongly disagree**	**Disagree**	**Uncertain**	**Agree**	**Strongly agree**
Enter your response (tick one					

box only)					
Strategy benchmark 3	**Your country has a general authorisation procedure, allowing any person to start and operate an electronic communications service without the need to obtain any permission. All that is required when entering the market is a simple notification procedure. The need for individual licences is restricted only to specific, objectively justified cases.**				
Benchmark notes	A **general authorisation procedure** is one that applies to all market participants for market entry, removing the need for new entrants to obtain permission. The way this normally works is that after a **simple notification procedure**, the market player receives an acknowledgement from the regulator and stating the legal and regulatory framework which applies, with reference to the current set of primary and secondary legislation. No fee should be charged for the simple notification. The notification itself should be submitted by the new entrant to the regulator containing only the minimum of information about the new entrant's identity, contact details and perhaps a brief outline of the proposed service. The new entrant should not have to wait for any decision or confirmation of receipt, its services can start immediately. The purpose is to remove any unnecessary administrative barriers to market entry or any perception that the regulator has to power to refuse entry. If the market entrant requires **numbering or spectrum resources** to operate any part of its services, these resources should be made available without delay, on payment of a fee for the use of these resources which is published and related to the administrative costs incurred by the body competent to issue and manage frequency and numbering resources (normally the regulator). Only if these resources are deemed to be scarce (by some objectively justified decision of the competent body) should there be an additional procedure for specific authorisation for the use of the scarce resource. In these circumstances, the limited spectrum or numbering resource available should be assigned to operators using fully transparent competitive procedures, allowing all interested parties to submit bids and for the decision to be made in accordance with pre-published and objective criteria. The results of such competitive contests should be published and any fees charged for the use of the resources must be objectively justified. Any conditions attached to the licences/ authorisation documents associated with the assigned resources should be clear to all bidders before the contest. All such conditions should be objectively justified by the competent body.				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____				
Please record main	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)*				

challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	Challenges: _____ Risks: _____ __
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits:

the respondent	_____

Resources Benchmarks for "Telecoms Rules"

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Resources benchmark 1	**The country has adequate human and financial resources to carry out an effective independent regulatory function**				
Benchmark notes	The legal framework should guarantee that a national regulator shall exercise their powers impartially, transparently and in a timely manner. In order to achieve this, the country should ensure that the national regulatory authority has adequate financial and human resources to carry out the task assigned to them. The normal method of regulatory funding is from the electronic communications sector itself, based on the estimated administrative cost, the calculation of which is transparent for public scrutiny and based on a statement issued by the regulator of its annual programme of regulatory work and a resources budget that clearly supports that programme. Within the overall amount requested from the sector, the individual amounts to be paid by each market participant should be clearly pre-defined and justified using a fair, proportionate, transparent and non-discriminatory basis. The contributions made and the basis of their calculation (for example the publicly auditable gross revenue of each market entity) should be published. Any unused surplus of the contributions should either be returned to the contributing entities, or carried forward to the next year with an adjustment to that next year's contributions, or set aside for defined purposes related to the development of the sector after public consultation to determine that purpose. The possible alternative funding mechanism, where the regulator receives financial resources from the state budget has to be equally transparent and not subject to restrictions arbitrarily imposed by the state. The budget of the regulator should be relatively stable and consistent with the need for independence of the regulator and the need for market predictability. Any other payments made to the regulator or to the state (for example numbering or spectrum fees or contributions to a universal service fund) should be separately accounted for and separately justified from the funding of the administrative costs of the regulator. Apart from ordinary retail taxes (e.g. VAT) on services provided to end-users and corporation (profit) taxes on market entities supplying services, the imposition of any additional or sector-specific taxes (for example on Internet or mobile phone revenues or usage) is not permissible under the EU legal and regulatory framework.					
Please record relevant evidence in support of the answer given by the	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _				

respondent	*Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ __
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisatio	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____

n for this benchmark between the partner countries and with the EU, as viewed by the respondent	Political benefits: _____ Other benefits: _____

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Resources benchmark 2	**Your country provides access to state funding for investment in broadband infrastructure and chooses projects that pass clear "state aid" rules to ensure that the state subsidy does not distort a competitive market**				
Benchmark notes	Following the wave of privatisations in the last 30 years, the electronic communications market now relies mainly on private investors, although in some countries one or more operators are still fully or partly owned by the state. Because private investors are profit seekers, their network investments tend to prioritise in geographical areas (mainly urban centres of population) where revenues are highest, and lower priority is given to the expansion of infrastructure into the more rural areas. There is also a legacy in some countries of significantly lower penetration of traditional telecommunications services in rural areas. Although the situation has improved with the roll-out of mobile networks, there remain many rural areas that are not well served, particularly with competitive high-speed broadband services. At EU level, funding has been made available to accelerate high-speed broadband infrastructure investment into inadequately served rural areas ("White Areas"). Many EU member states have also make public funding available for this purpose. A typical project that qualifies for "state-aid" (either using EU or national funds) would be an investment in high-speed broadband infrastructure (for example a regional fibre network connecting all villages into the main core network). By making **state funds** available to private operators, their investment plans are accelerated because the additional subsidy (together with their own financial input) will turn an unprofitable project into a profitable one. To make the funding process efficient, clear public/private mechanisms have to be stated and applied, for example investors should have to compete for the state subsidies (to ensure that only the minimum subsidy schemes win the money). Also, to ensure that a competitive market results, the winning operator has to allow open (wholesale) access to other service providers. If the operator is itself a state-owned entity, then					

	additional safeguards have to be built in to ensure that the state does not become a distorting influence on the market. To ensure the utmost transparency and market effectiveness (whether the investor is private/ state-owned or a public/ private partnership), a set of **"state aid" rules** have to exist so that only projects that pass the test can receive the funding. The European Commission has defined a set of "EU Guidelines for the application of State aid rules in relation to the rapid deployment of broadband networks" which should be taken as best practice when considering the use of state funds for broadband infrastructure projects. A more traditional example of telecommunications networks subsidy arrangements has been the **"Universal Service Fund"** (USF) that has been established in many countries to promote the expansion of basic telecommunications services. If the USF exists, the mechanism needs to be updated for the broadband era in order to ensure that any funding does not distort a competitive broadband market in the same way that it often has in the traditional market. An example of misuse of USF is the practice of subsidising an incumbent to keep the tariff for all existing fixed lines below cost. Instead, subsidies should be clearly targeted only for the defined purpose of network expansion, or to allow access for disadvantaged consumers, e.g. disabled or economically excluded persons. The use of competitive mechanisms to assign state funds and the obligation to open all funded infrastructure for wholesale access to competitors, are the basic safeguards required in the broadband era. Other safeguards are necessary if the operator receiving state funds is itself a state owned entity, for example to establish a separate entity to manage the project and to set a date in the future where the project assets will be privatised. Other possible enabling mechanisms for facilitating access to funds for broadband investment are government guarantees to private banks that offer to lend money for broadband projects that pass the "state aid" rules.
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ __

viewed by the respondent	
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Implementation Benchmarks for "Telecoms Rules"

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Implementation benchmark 1	**Your country has clear mechanisms for affected parties to appeal decisions made by the regulator**				
Benchmark notes	The regulator for electronic communications should be responsible for taking appropriate steps in the market in accordance with the legal and regulatory framework (primary and secondary legislation relating to the sector). These actions will normally be initiated by regulatory decisions carried out in accordance with the responsibilities (competences) of the regulator, as defined in the framework. Best regulatory practices require the regulator to publish draft decisions in advance to allow full public consultation (see also "Leadership Benchmark 2" above). This practice of public consultation allows any potentially affected party (for example consumers, investors, operators and service providers, business groups, other agencies) to express their opinion about the decision. The regulator in turn should acknowledge the responses and consider them. This may lead to a revised decision or a change in the method of implementing the decision. The regulator should summarise its views and announce any changes plus the reasons for rejecting opinions where relevant. Having passed this public consultation stage, the regulator should announce its final decision and commence implementation. The requirement for a mechanism for affected parties to **appeal the final decision of the regulator** should be a fundamental right of any affected party. In this way, an independent appeal body (for example a court or an ombudsman) should consider the appeal, taking evidence from both parties (the appellant and the regulator). Although the details of the conduct of an appeal may differ in each country's administrative legal code, it is preferable that while the appeal is being considered, the regulator's decision should stand – i.e. implementation should be continued. If this is not the case, then any party that does not agree with the decision would jump to appeal in order to delay implementation and the overall regulatory process would be less effective. At the end of the appeals process – which itself should be simple to access – the regulator's decision is either upheld or overturned. In the case that it is overturned, the regulator has to remove the decision and cease implementation. It is up to the appeal body to decide if the regulator (or the appellant) should pay for any eligible costs of the appeal, or whether is any case for compensation arising from the decision.				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ __				

	Supporting evidence: _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ ___
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____

between the partner countries and with the EU, as viewed by the respondent	Political benefits: _____ Other benefits: _____

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Implementation benchmark 2	**Your country has clear provision for the regulator to impose access obligations on operators found to have significant market power (SMP) in relevant markets under implemented market analysis procedures carried out in accordance with the EU Framework Directive (see also "Strategy Benchmark 1" above). The access obligations that are clearly defined are:** – **access to, and use of, specific network facilities** – **price controls on access and interconnection charges, including obligations for cost orientation** – **transparency, non-discrimination and accounting separation**				
Benchmark notes	Regulatory obligations for **access to specific network facilities** are a fundamental means for the promotion of a competitive market in electronic communications. Without such obligations, the operators with significant market power (SMP) could use their market position to deny any alternative operators the chance to serve retail markets in any geographical areas where the alternative operator has not yet installed its own infrastructure. If this was the case, competition and consumer choice would be very limited, especially in the early stages of a competitive market. In order to promote competition, accelerate expansion and investment by alternative operators and to give consumers the earliest benefits of better choice and innovation, then the regulator should impose proportionate access obligations on operators that have SMP. In practice, this normally means that the incumbent fixed operator cannot refuse any requests from alternative operators to use parts of its network that are defined in relation to the relevant market definition, using best practice market analysis procedures (as defined in "Strategy Benchmark 1" above). For example, in the relevant market for the provision of a fixed line for basic voice calls, the obligation for access should include the access and use of the incumbent's local loop by any requesting alternative operator so that the alternative operator can use the loop (under a wholesale agreement) to provide a retail service to the end-user who is already				

	connected to the incumbent's network. This kind of wholesale arrangement is called "wholesale line rental". Another example comes from the relevant market for calls from a fixed line. By allowing access (interconnection) for an alternative operator at the incumbent's local exchange, the alternative service provider can offer a competing call service. This type of wholesale access is normally called "carrier selection" and "carrier pre-selection". In the broadband era, the access types are normally called "wholesale broadband access", "bit-stream access" or "local loop unbundling" depending on the exact requirements of the access seeker. Further examples include access to physical infrastructure including ducts, street cabinets and manholes, poles, fibres, towers, masts, buildings (co-location) and spectrum (including national roaming). The regulatory intervention is designed to liberalise the market by making it possible for new operators/ service providers to enter and expand their market with low entry costs and gain revenues that can be used for further infrastructure investments of its own. This has been called the "ladder of investment approach". Clearly, the regulatory interventions have to include obligations on the SMP operator to allow access of the above types under wholesale agreements that contain **price controls on access and interconnection charges including obligations for cost-orientation.** This type of obligation ensures that the alternative operator does not have to pay more than the cost (plus a reasonable margin) for the wholesale service provided by the SMP operator. Modern regulatory practice is to base the correct level of charges on "Incremental Costs" (for example "Forward-Looking Average Incremental Costs") which are determined by cost modelling of an efficient network, rather than the legacy network of the incumbent. These cost models, for a variety of access and interconnection services (fixed and mobile) are a desired tool of modern regulators. Further obligations should form part of the regulatory mechanisms to ensure **transparency, non-discrimination and accounting separation** such that the SMP operator's wholesale access service is clearly defined (normally in the form of an "Reference Access Offer" or "Reference Interconnection Offer"), to ensure that the service provided to the access seeker is not inferior to the service that the SMP operator uses in its own retail service offerings, and finally to ensure that there is no cross subsidy distortions within any SMP operator's accounting system that would give it an unfair competitive advantage (for example by allowing it to squeeze the margins of the alternative operators using its own retail tariffs and wholesale charges to make a competing service unattractive to consumers or uneconomic for the alternative provider). All these regulatory measures for access have been used extensively in the EU and elsewhere to help create more competitive and efficient markets in electronic communications.
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ __ *Supporting evidence:*

	_____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ ___
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____

with the EU, as viewed by the respondent	Other benefits: _____

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Implementation benchmark 3	**3a) Your country has fully introduced number portability for both mobile and fixed numbers** **3b) Your country has fully introduced the single European Emergency Call number 112**				
Benchmark notes	**Number portability** is a very important enabler to a competitive market because it removes one of the main reasons why existing customers do not want to switch from their current service provider to take an alternative offering in the market. This is because, without number portability, the customer would have to change their telephone number, meaning that as an individual they will have to inform all their contacts of the new number and as a business, they would face loss of demand because customers cannot contact them on their old number after the change. **Mobile number portability** allows the customer to keep their existing number (the full number, not just the last digits) even though they are served by a different mobile operator. Under best practice, all the customer has to do is go to their desired mobile operator and sign up for service, the new operator arranges everything with the old operator, including the use of the old number, without the customer having to deal with the old operator. The maximum amount of time that it should take to "port" a number is one day from the customer's request. **Fixed number portability** allows numbers to be retained within defined geographical areas of the country, and under best practice the procedure is the same as mobile number portability including the maximum time of one day for porting. The regulator should ensure that any charges made to customers for the number portability service is related to costs, so that the consumer is not exploited in what is basically a supplier dominated process. The regulator should also ensure that the service is actively promoted to consumers so that it encourages competition and also that the operators do not impose anti- competitive conditions on consumers for example to limit the number of occasions that they can port. **The single European emergency call number 112** has been fully implemented as a free service to consumers from any fixed or mobile telephone number to reach emergency services (ambulance, fire and rescue, police) in the whole of the EU and many others. In some countries the previously used numbers continue to be available for the same purpose and in the USA some operators recognise the number 112 and translate it to their emergency number 911.				

Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions: _____ Opportunities: _____
Please record expected economic,	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)*

technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	Economic benefits: _____ Technological benefits: _____ Political benefits: _____ Other benefits: _____

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Implementation benchmark 4	**Your country has implemented effective measures for ensuring quality of service in a broadband environment, taking account also the context of net-neutrality**				
Benchmark notes	The **quality of service** in broadband markets is determined by more complex factors than the traditional voice market. Broadband services (both fixed and mobile) can be used to access voice, Internet, media and a large number of application-based services. The overall quality experienced by the customer depends on a number of factors, most of which are determined by the technical features of the data transmission systems used to transfer the service from the providers (including telecommunications operators, Internet service providers, radio and TV content providers) to the users. Consumers are aware that the quality of service experienced can vary significantly, not just between different broadband service providers but also with one broadband service at different times of day. For example, a broadband service sold as being “8Mbps” could experience significantly less data transmission rates depending on the network loading at different times. The data transmission speed desired for efficient internet access or satisfactory TV viewing can vary between different users. For this reason, broadband service providers typically offer a range of different services, for example 2Mbps up to 1,000Mbps at different tariffs. Regulatory intervention could be required if consumers are generally not happy that the services offered are not matched by their user experience. If one of many broadband service providers has a poor service, then consumers should be able				

	to switch to better providers. In this case regulatory intervention may not be required because the market has been efficient in delivering good alternative choices and services. In the case where the networks overall are not effective in dealing with broadband service demand, the regulator should have powers to intervene so that the general level of quality is maintained, avoiding deterioration due to the existing congestion. In some cases, Internet service providers try to deal with challenging demand conditions by giving priority to certain Internet traffic or priority to certain users. The general regulatory policy towards this behaviour allowing some traffic to pass and other traffic to be restricted is to impose **"net-neutrality"** on the market such that the Internet service providers do not discriminate between different types of traffic as a means of dealing with changing market demands. Internet service providers can however offer different "high user" services to the market at a price premium if this is their market strategy, but they should not be able to discriminate between different types of carried traffic. There are several possible regulatory interventions that can be used to **ensure better quality performance** in the broadband market. The first is to define a minimal level of universal broadband service (for example 2Mbps). The second regulatory measure is to insist that broadband service providers do not exaggerate their broadband speeds, meaning that if it is sold as an 8Mbps service, then that is the speed that is delivered the majority of the time, otherwise the user can cease the contract without penalty. A third method is to oblige the operators to submit plans for the security of their networks, including the measures that they are taking to ensure the maintenance of data transmission rates to their customers under network load conditions. These operators' plans should be submitted for inspection by the regulator. Further measures should require operators to report to the regulator when significant security breaches (either in terms of network outage or breaches of data security) occur. These regulatory interventions regarding broadband quality should only be taken if they are proportional to a measured problem with broadband service that is common across most providers, meaning that consumers do not have sufficient competitive choices to seek and secure a quality service matching their needs. The **measurement of actual broadband quality** of service can best be done by "crowd sourcing". This asks a sample of consumers to use measurement devices (or downloadable applications) and to report the results to the regulator. This modern measurement technique is far more cost effective because it largely replaces the need for the regulator to purchase and operate expensive monitoring equipment.
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ __ *Supporting evidence:* _____

Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ ___
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____

respondent	Other benefits: _____

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Implementation benchmark 5	**Your country has adopted measures to impose price control and cost-accounting on the markets for wholesale voice call termination on individual public telephone networks based on the costs incurred by an efficient operator, using current cost and a bottom-up modelling approach with long-run incremental costs (LRIC) as the relevant cost methodology**				
Benchmark notes	The relevant EU regulation is contained in Commission Recommendation 2009/396/EC on the Regulatory Treatment of Fixed and Mobile Termination Rates in the EU. **The markets for wholesale voice call termination** are the services required in order to terminate calls to called locations (in fixed networks) or subscribers (in mobile networks). The charging system in the EU is based on Calling Party Network Pays, which means that the termination charge is set by the called network and paid by the calling network. The called party is not billed for this service and generally has no incentive to respond to the termination price set by its network provider. In this context, excessive pricing is the main competition concern of regulatory authorities. The fixed and mobile **markets for voice call termination on individual public telephone networks** are included in the EU's recommended list of markets that are subject to ex-ante regulation (see also Strategy Benchmark 1 above). Most regulators have designated a number of market players (fixed and mobile) with SMP in these markets because market players have no other choice but to interconnect with the individual operator that terminates the call. For example, a fixed operator that wants to terminate a call on a particular mobile operator's network has no choice but to use that operator under a wholesale agreement providing call termination on that individual mobile network. Regulator intervention is required because if individual operators are allowed to set their own market rates, they will use their position of SMP to disadvantage the other operators. Existing operators in the market could also use their collective position in this way to discourage new entrants. Lack of regulatory intervention has also led to distorted tariff structures (for example low tariffs for on-net calls and high tariffs for off-net calls) which further acts to decrease overall market competitiveness. **Measures to impose price control and cost accounting** should normally be applied at wholesale level so that fixed and mobile termination rates can be based on the cost of providing the wholesale service, where individual operators have				

	SMP. Basing termination rates on cost also ensures that there is no discrimination. For example, if individual mobile operators were allowed to charge different rates for the same terminating service (i.e. use rates not based on costs) then further market distortions would inevitably apply – a higher charge to a new entrant would restrict the new entrant's growth, a higher charge to a fixed operator than a mobile operator would artificially encourage fixed to mobile migration, a higher charge to terminate international incoming calls would be an unfair subsidy. The regulator should therefore define obligations based on access to call termination service, transparency and cost orientation of prices based on separated accounts (see also Implementation Benchmark No 2 above). **Costs incurred by an efficient operator, using current cost.** In a competitive environment, operators would compete on the basis of current costs and would not be compensated for costs which have been incurred through inefficiencies. Historic cost figures therefore need to be adjusted into current cost figures to reflect the costs of an efficient operator employing modern technology. Operators which are compensated for actual costs incurred for termination have few incentives to increase efficiency. The implementation of a **bottom-up model** is consistent with the concept of developing a network for an efficient operator whereby an economic/engineering model of an efficient network is constructed using current costs. It reflects the equipment quantity needed rather than that actually provided and it ignores legacy costs. This ensures that the operator buying the service is not disadvantaged by any inefficiencies in the operator providing call termination due to out of date technologies or poor working practices. Modern regulators typically use **cost models** based on the above methodologies to regulate wholesale call termination charges. The cost models (generally separate for fixed and mobile) should be based on the efficient technological choices available in the time frame considered by the model, to the extent that they can be identified. Hence, a bottom-up model built today could in principle assume that the core network for fixed networks is Next-Generation-Network (NGN)-based. The bottom-up model for mobile networks should be based on a combination of 2G, 3G and 4G/LTE employed in the access part of the network, reflecting the anticipated situation, while the core part could be assumed to be NGN-based. Taking account of the particular characteristics of call termination markets, the costs of termination services should be calculated on the basis of forward-looking **long-run incremental costs (LRIC).** In a LRIC model, all costs become variable, and since it is assumed that all assets are replaced in the long run, setting charges based on LRIC allows efficient recovery of costs. LRIC models include only those costs which are caused by the provision of a defined increment. An incremental cost approach which allocates only efficiently incurred costs that would not be sustained if the service included in the increment was no longer produced (i.e. avoidable costs) promotes efficient production and consumption and minimises potential competitive distortions. If call termination rates are not set in this way by the regulator, the overall markets for voice calls Fixed and mobile) are unlikely to be effectively competitive, leading to price distortions in both the wholesale and downstream retail markets for call services.
Please record relevant evidence in support of the	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)*

answer given by the respondent	*Rationale:* _____ __ *Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ ___
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____

harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	Technological _____	benefits:
	Political _____	benefits:
	Other _____	benefits:

Legal Framework Benchmarks for "Telecoms Rules"

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Legal framework benchmark 1	**Your country has adopted a legislation action plan with a clear date defined for alignment of the legal and regulatory framework for electronic communications with the EU acquis, including;** **1a) full alignment of the national legislation with the EU acquis** **1b) full alignment with European recommendations and decisions on spectrum and broadband** **1c) full alignment of the relevant regulations (by-laws) with the EU acquis**				
Benchmark notes	A **legislation action plan** is a document, approved by the competent ministry responsible for drafting primary legislation and also agreed by the regulatory body for the sector which is responsible for issuing secondary legislation. The document lists the existing legal acts and by-laws that are required to be updated plus any new legislation that needs to be written. The document should also be sent to the European Commission for their comment. For each law or bylaw that needs revision, a responsible person should be shown, who is tasked to ensure, by a defined date, that the draft is prepared, issued for public consultation and then presented or adoption by the relevant body (e.g. parliament, government, ministry or regulator as appropriate). The alignment process should seek to transpose the EU legal and regulatory framework (**the acquis**) into the appropriate legal instruments in the country. The current acquis for electronic communications is defined in the attached "Telecoms Rules Baseline" document. The legislation action plan should also include alignment with the **European recommendations and decisions on spectrum and broadband**. The references for these texts are also defined in the attached document.				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____				
Please	*(Filled in by NEs during/after conducting interview(s) with national*				

record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*stakeholders.)* Challenges: _____ Risks: _____ __
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU,	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____

as viewed by the respondent	Other _____	benefits:

Infrastructure Benchmarks for "Telecoms Rules"

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Infrastructure benchmark 1	Your country has a clear plan with a defined completion date for the adoption of the obligations on non-discrimination and costing methodologies for promoting broadband competition and investment				
Benchmark notes	The **Commission recommendation on promoting broadband competition and investment** has the full title "Recommendation on consistent non-discrimination obligations and costing methodologies to promote competition and enhance the broadband investment environment - C(2013) 5761". It seeks to update the regulatory measures to improve competition and investment in the broadband era, taking account of the latest "Next Generation Access" technologies (NGA). The topics that are covered are the regulatory approach to; - the application of the non-discrimination obligation (see also "Implementation Benchmark 2" above) by ensuring equivalence of access between the wholesale access offered by an operator with significant market power (SMP) to alternative access seekers on the one hand and the same service used by the SMP operator to serve its own downstream service offering. - the application of the non-discrimination obligation to ensure the technical replicability of the SMP operator's new retail offering as a minimum - compliance monitoring of non-discrimination obligations by means of Key Performance Indicators (KPIs), Service Level Agreements (SLAs) and Service Level Guarantees (SLGs) - costing methodology approach and implementation - non-imposition of regulated wholesale access prices on NGA networks Together, the application of these defined regulatory approaches seeks to achieve the right balance between the need to promote innovation and competition on the one hand and the need for existing network operators to have confidence in new investments in NGA infrastructure (including fibre access networks) for the future.				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ _ *Supporting evidence:* _____				

Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____ __
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU,	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____

as viewed by the respondent	Other benefits: _____

Score	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
Enter your response (tick one box only)					
Infrastructure benchmark 2	**Your country has an adopted strategy promoting high speed broadband infrastructure investment with clearly defined targets for the achievement of universal fast broadband access and take-up**				
Benchmark notes	The EU has adopted a "Digital Agenda for Europe" strategy, a flagship initiative of the "Europe 2020 strategy for a smart, sustainable and inclusive economy". The strategy has established broadband targets for Europe. These **promote high speed broadband infrastructure investment.** The targets are: - Basic broadband for all citizens by 2013 (target met) - Coverage: Next Generation Access (NGN) giving 30Mbps or more for all by 2020 - Uptake: 50% of households having 100Mbps subscriptions or higher To support the universal coverage target in areas where the competitive market fails to invest sufficiently, the European Commission has adopted "**State aid broadband guidelines**" (see also "Resource Benchmark 2" above). Also, Europe has developed a **market-driven spectrum policy** to help satisfy the expected broadband demand (see also "Policy Benchmark 3" above). A clear and co-ordinated strategic approach is required to achieve universal high-speed broadband. On the supply side, investment has to be made even in unprofitable areas to achieve the coverage target and remove the "digital divide". On the demand side a range of measures have to be defined and implemented to promote the use of broadband-enabled services by citizens and businesses.				
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the findings.)*				
Please record main challenges and	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)*				

risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)*
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)*
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)*

Services Benchmarks for "Telecoms Rules"

Score	Fixed broadband (national penetration per 100 population)	Mobile broadband (national penetration per 100 population)	Fixed broadband (urban penetration per 100 urban population)	Mobile broadband (urban penetration per 100 urban population)	Fixed broadband (rural penetration per 100 rural population)	Mobile broadband (rural penetration per 100 rural population)
Enter figures for broadband penetration						
Please enter the date that the figure applies (e.g. September 2014)						
Services benchmark 1	**Please provide the latest estimate of the national uptake of broadband services (separate figures for fixed and mobile broadband market penetration and also if available the estimates for urban and rural areas of the country).**					
Benchmark notes	Please provide in all cases the latest figures or estimates available. If the responsible ministry or regulator does not have these figures, then the National Expert should contact the main market players to obtain their figures, then make estimates of the total market figures based on this data. The definition of **fixed broadband penetration** is the total number (aggregate of all fixed retail broadband service providers) of broadband subscriptions sold to end-users divided by the total population of the country. Broadband service is a service that provides at least 2Mbps data transmission speed to the end-user. The broadband connection may use any technology – fibre, copper with xDSL, leased line, ISDN or wireless broadband access. The broadband subscription should be either specifically for data service separately from voice or as a defined (itemised) part of a bundled mobile broadband service. The figure should exclude wholesale service arrangement numbers (e.g. unbundled local loops, wholesale broadband access, bit-stream services because these are not retail services sold to end users). Only the numbers of broadband connections taken up by end users should be included. The definition of **mobile broadband penetration** is the total number (aggregate of all mobile retail broadband service providers) of mobile broadband subscriptions sold to end users divided by the total population of the country. Retail mobile broadband subscriptions should include all subscriptions for use					

	with data modems or by smartphones. The subscription should be either specifically for data service separately from voice or as a defined (itemised) part of a bundled mobile broadband service. The mobile access technology can be any technology that can deliver at least 2Mbps data transmission rates, including 3G and LTE/4G. It should be noted that a figure that simply gives the population coverage of 3G or 4G service in the country is not the required figure – what is required is the actual number of subscribers who have taken up a mobile data subscription. The **urban and rural figures** are required to check the extent to which broadband services are universal. For example a national penetration figure of 60% might hide the fact that this means 80% penetration in urban areas but only 30% in rural areas. The figures or estimates required are the number of subscriptions (separately for fixed and mobile) in urban and rural areas divided by the population living in urban and rural areas respectively.
Please record relevant evidence in support of the answer given by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders. Also please provide reference to documentation or records that justify the answer)* *Rationale:* _____ *Supporting evidence:* _____
Please record main challenges and risks for achieving this EU baseline and implementing HDM in general, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Challenges: _____ Risks: _____
Please record main obstacles obstructing achievement of the EU baseline, as viewed by the	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Obstacles: _____

respondent	
Please record required conditions and opportunities to achieve the EU baseline, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Conditions*:* _____ Opportunities: _____
Please record expected economic, technological, political and other benefits of the harmonisation for this benchmark between the partner countries and with the EU, as viewed by the respondent	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* Economic benefits*:* _____ Technological benefits*:* _____ Political benefits*:* _____ Other benefits: _____

Section 2: National organisations involved in development of digital markets

Organisation	Level of involvement (High, Medium or Low)						Description	Key functions in relation to HDM
	EU cooperation	National policy	Strategy	Legislation	Executive	Regulatory body		
Organisation 1 (enter name)								
Organisation 2 (enter name)								
Organisation 3 (enter name)								
Organisation 4 (enter name)								

ADDITIONAL QUESTIONS FOR ARMENIA AND BELARUS, MEMBERS OF THE EURASIAN CUSTOMS UNION

For interviews in Armenia and Belarus only

"Telecoms Rules"

Please record the respondent's view on the role, benefits , risks and overall impact of the Eurasian Economic Union and the Eurasian Customs	*(Filled in by NEs during/after conducting interview(s) with national stakeholders.)* *Role of the Eurasian Economic Union and Eurasian Customs Union regarding the topic of telecoms rules:* _____ *Supporting evidence:* _____

Union on the achievement of harmonisation of digital markets with the EU in the area of Telecoms Rules	*Impact of the Eurasian Economic Union and the Eurasian Customs Union in the area of telecoms rules:* _____ *Supporting evidence:* _____ *Risks for achieving HDM with the EU in the area of telecoms rules:* _____ _____ *Supporting evidence:* _____ *Possible benefits of the Eurasian Economic Union and Eurasian Customs Union for HDM with the EU in the area of telecoms rules:* *economic:* _____ *technological:* _____ *political:* _____ *other benefits:* _____

Other remarks: _____

_____