ISSN 2228-0391

No. 16
December 2013

Eastern Partnership Review

Comparative Study of Open Governance and Data Security in Eastern Partnership Countries

Ivar Tallo
Liia Hänni
Arvo Ott
Raul Rikk
Mari Pedak

e-Governance Academy

Global Information Society Initiative

Eesti Idapartnerluse Keskus
Estonian Center of Eastern Partnership

Contents

Biographical notes

Ivar Tallo

Ivar Tallo is one of the founders and the first director of e-Governance Academy. Before that, he was a Member of Parliament of Estonia and Member of the Parliamentary Assembly of the Council of Europe. He has also worked as a foreign policy advisor to the President of Estonia and he has been lecturing on public policy and public administration at Tartu University. He was the author of the Basic Principles of Information Policy of Estonia, Code of Conduct for Civil Servants and co-authored Public Information Act. He has also served at UNDP regional office in Bratislava and at UNITAR in Geneva.

Ivar Tallo has been promoting the use of the information and communication technologies for the public sector leaders in the Central and Eastern European countries, Balkan states, the CIS, the Arab countries and in Africa and Asia.

He has given e-gov lectures to presidents of Kazhastan and Armenia, Cabinets and Ministers of Uzbekistan, Moldova, Ukraina, Azerbajian, Northern Cyprus, Palestinian Authonomy, Namibia and Rwanda, Speakers and MPs from Macedonia, Afganistan, and Kazahstan and to many others.

Liia Hänni

Liia Hänni is a physicist by education, she holds a Ph.D degree. During revolutionary events in Estonia she became actively involved in politics. From 1990 to 2003 Liia was a Member of Parliament and Cabinet Minister responsible for ownership reform (1992-1995). From the beginning of 2005, Liia had lead the e-democracy programme at the e-Governance Academy. She promotes the use of ICT for democratic governance and the empowerment of citizens. Her activities have been acknowledged by state decorations.

Arvo Ott

Arvo Ott joined the e-Governance Academy on November 1st, 2005. His main responsibilities include the coordination of e-governance studies (eGovernment and eDemocracy aspects), training programmes and general management.

Prior to joining the e-Governance Academy, Arvo Ott served as the Head of Department of State Information Systems (head of e-government office) at the Ministry of Economic Affairs and Communications for 12.5 years. He was responsible of Estonia Information Society and e-Government strategy planning and implementation. For the last several years Arvo Ott has taken part in many international projects and programs on e-governance (information society policy and e-participation advice, e-government interoperability aspects, etc). Arvo Ott is a member of the Estonian Informatics Board.

Raul Rikk

Raul Rikk is one of the founders of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn. He was leading the establishment of the Centre from 2004 to 2008. Currently he is the Cyber Security Program Director at the e-Governance Academy in Estonia and is engaged in strategic cyber security development in many countries and international programs.

He holds a master-level degree (military science) form Finnish National Defence University and master's degree (management of information technology) from Tallinn University. He is also a graduate of the US Army Command and General Staff College.

Raul Rikk has worked as an advisor to the Georgian National Security Council Office and NATO Liaison Office and has been involved in Georgian cyber security capacity building for many years. Also, he has been a leading expert in developing Moldovan national cyber security roadmap in 2013. In Estonia he is a member of the Cyber Defence Commission of the Academy of Science and a member of the National Cyber Security Strategy working group.

Mari Pedak

Mari Pedak has 22 years of experience in public sector in local, regional and central government including 14 years as top manager directing Estonian Citizenship and Migration Board and IT and Development Centre, Ministry of the Interior. She has 12 years of experience in development and implementation of digital documents incl national ID-card, digital ID-card, mobile-ID and in e-government framework development. Mari Pedak joined the e-Governance Academy in 2012.

Estonian E-Governance Academy

The e-Governance Academy (EGA) is a non-profit organization, founded for creation and transfer of knowledge concerning e-governance and transition experience.

EGA is jointly brought into existence by United Nations Development Program (UNDP), Open Society Institute (OSI) and the Government of Estonia in 2002.

EGA implements its mission through training provision, organizing research, networking and facilitating exchange of experience. Located in Estonia the academy is drawing on both the experiences of the country as well as the achievements from other, both developed and transition, countries.

EGA's competencies are divided into five program areas:

- e-Governance program for central governments;
- e-Government program for local and regional governments;
- e-Democracy and e-Participation program;
- ICT in education;
- Mobile governance.

EGA strong competences are based on the international experience of the experts, having remarkable expertise and long track record in the public sector ICT development.

Together with EGA core staff EGA is using wide network of e-governance experts, working in governmental institution, academic research institutions or private companies.

The academy has the legal form of a foundation. It is governed by a supervisory board composed of representatives of main stakeholders of international organizations, having eGovernance issues in their agendas as well as representatives from Estonian Foreign Ministry and Ministry, responsible on ICT coordination.

EGA's main services are:

- Consultancy
- Training
- Research

As EGA field of expertise is wide, consultancy and training program could be composed in the same project as usually together with consultancy training is necessary.

EGA also provides consultancy and training in specific e-Government topics:

- Implementation of national ID-cards with electronic chip;
- Implementation of governmental gateway (x-road), interoperability;
- Digital registries and databases;
- Governmental systems for digital land management;
- Governmental digital systems for pension management;
- Legal framework of information society;
- Cyber security policy development and implementation;
- Public-private partnership challenges in information society systems.

EGA has successfully undertaken and completed contracts with distinguished clients as Open Society Institute, UNDP, World Bank, USAID, Estonian Government, European Commission, various international organizations and companies.

EGA geographical focus has been broaden from the countries of the Caucasus and Central Asia, Ukraine, Moldova, Mongolia to South Eastern Europe (Albania, Macedonia, Kosovo, Serbia, etc.). Today EGA is also implementing projects in the European Union member countries, Arabic countries and in West Africa.

Since its inception, EGA has worked closely with a wide variety of government organizations and ministries on more than hundred international projects with more than 25 countries. All projects are successfully completed. EGA has always been aware of the high standards of integrity and performance required for these efforts. EGA has ensured that these standards are maintained.

Office and mailing address:

eGovernance Academy
Tõnismägi 2
10122 Tallinn
Estonia
Phone +372 6 411 313
Fax +372 6 411 314
info@ega.ee
www.ega.ee

Executive Summary

Open Governance Partnership has brought a renewed political attention to the questions of transparency and good governance into international arena. While we have heard a lot from the Digital Agenda of the European Commission and best practices from developed countries, these questions are also addressed by our neighbours to the East.

The present report aims to provide a first coherent overview of a multitude of initiatives undertaken by the 6 Eastern Partenship countries – Ukraine, Moldova, Belarus, Georgia, Armenia and Azerbajian – in modernisation of their public administrations with the help of new technologies, usually referred to as e-governance.

The report is divided into three main chapters: E-Government; Open Government, e-Participation and e-Democracy; Cyber Security and Data Protection. They reflect and generalize the results of answers to the Questionnaires sent to Eastern Partnership countries during the summer 2013. The report also utilized various information resources from Internet and benefited from the experience and a first-hand knowledge of the experts from e-Governance Academy.

The main outcome of the work is clear understanding that all countries pay considerable attention to developing e-society and e-services. There are clear signs of progress and improvements in shaping e-societies in all Eastern Partnerhip Countries. Progress varies from country to country and from topic to topic. Our aim was not to rank the countries based on different parameters, this has been done in numerous international e-governance surveys. Rather, we tried to provide an in-depth look into what is happening in key areas of e-government and cyber security and whether, from the point of view of the European Union, we could generate some policy recommendations for future assistance projects.

Despite the encouraging signs of progress, a lot of work still needs to be done in all these countries, and there are indeed common themes where our help could have the benefit for both the EU and the Eastern Partnership countries.

The survey was designed and the text written as a collective exercise by the experts from the e-Governance Academy: Arvo Ott, Ivar Tallo, Liia Hänni, Raul Rikk and Mari Pedak.

Authors of the study would like to acknowledge the financial support of the development co-operation funds of the Ministries of Foreign Affairs of Finland and Estonia. This support was used for carrying out the research activities and publishing the final version of the report.

Background

Cooperation between the EU and it's Eastern European partners - the Republic of Armenia, the Republic of Azerbaijan, the Republic of Belarus, Georgia, the Republic of Moldova and the Ukraine – is an important part of the Union's external relations. The main goal of the Eastern Partnership is to create the conditions to accelerate political association and deepen economic integration between the EU and the Eastern European partner countries[1].

Collaboration between EU and the Eastern European partner countries occurs in many areas. Open governance and data protection are two central themes passing through other fields.

People all over the world demand more openness from their governments. Greater involvement of citizens in public relations is requested and methods are searched to change governments into being more transparent, responsive, accountable and effective. Involvement of citizens and implementation of new technologies make governments more efficient. New technologies offer opportunities for sharing information, public participation and collaboration. By applying new technologies more information can be made public in ways that allow people to understand what their governments are doing and to influence respective decisions. Accessible and secure Web environments function as platforms for provision of services, community involvement, and sharing information and ideas.

European Union digital priorities for 2013-2014 include priority "New public digital service infrastructures through Connecting Europe Facility" and the Commission will fast-track the roll out of digital services (especially their cross border interoperability) in eIDs and eSignatures, business mobility, eJustice, electronic health records and cultural platforms. It is important to assess the level of Eastern European partner countries' e-governance infrastructure and provision of e-services to ensure the functioning of the common digital agenda.

One of the cornerstones of the goals set is data protection on every level: personal data protection, information systems security and cyber security.

Personal data protection is a fundamental right, and is also enshrined in the Lisbon Treaty. The Charter of Fundamental Rights of the European Union provides that "Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified"[2]. Every individual has the right to adequate protection of his personal data and the right to receive information[3].

In addition to the research challenges listed above, a large number of additional issues can be listed. Most prominently the security and privacy concerns, covering the full range from legal aspects over regulatory issue down to the organizational and technical level. Data Processing Agreements beyond Europe are already in discussion though and their technological impact will have to be assessed over the next years.[4]

The survey on open government and data protection supports the implementation of goals set in the roadmap to the autumn 2013 Summit in the section of the "Freedom, justice and security" (data protection) and the section of the "Democracy, good governance and stability" (cyber-crime). Both areas also have an important role in supporting these over-arching goals, like forge new, deeper contractual relations between the EU and partner countries; support the mobility of citizens and visa liberalization in a well managed and secure environment; enhance sector cooperation and facilitate the participation of partner countries in EU programs and agencies.

As efforts of Eastern European partner countries in promoting openness of their governments and the data protection supporting it are in relatively early stage, it is now the right time to carry out a comparative analysis based on what it is possible to provide a comparative assessment and to design common activities as well as to give separate recommendations to states.

1 European Commission High Representative of the European Union for Foreign Affairs and Security Policy. Brussels, 15.5.2012. Join(2012) 13 final. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Eastern Partnership: a Roadmap to the Autumn 2013 Summit.

2 Treaty of Functioning of the European Union, Article 16. Charter of Fundamental Rights of the European Union, Article 8.

3 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, Articles 6, 8 12 and 15.

4 Advances in Clouds. Expert Group Report Public version 1.0. Editors Lutz Schubert [USTUTT-HLRS], Keith Jeffery [STFC], Research in Future Cloud Computing.

Survey Methodology

Current survey is based on information available in different national and international sources. First phase of the study was dedicated to analyzes of relevant EU strategy papers, indicative programs, annual national action programs and progress reports, national policy documents, relevant legal acts etc. Analysis of the documents by countries was the input for compilation of survey questionnaire and ensured the relevance and actuality of the questionnaire.

In the next step experts compiled the survey questionnaire taking into account also experience gained from different e-government projects which were made by e-Governance Academy. Based on the results of previously conducted table-study it was decided, that it is sufficient to have common and uniform questionnaire for all countries.

The questionnaire consisted of four chapters: 1) country policies; 2) e-government; 3) open governance, e-democracy and e-participation; 4) data protection.

The objective of the first chapter questions was to understand countries' overall framework for information society policies, strategies, etc. that are an essential prerequisite for the developments in relevant areas. We were interested in government policies, strategies and action plans, i.e. documented evidence of the importance and the place of information society development for any country.

Second chapter questions were directed to get a factual overview of the e-government development. Through these questions an overview was obtained about legislation and regulatory environment, organisational framework, e-government infrastructure (electronic registries and databases, data exchange, digital identity etc) and e-services.

The aim of the third chapter was to provide an overview how ICT is used to advance open governance and participatory governance.

The fourth chapter focused on the issues of data protection: personal data protection, cyber security and cybercrime regulation.

During the period of July-August 2013 6 questionnaires were conducted by local partners of the e-Governance Academy in Eastern Partnerhip countries. During September-October 2013 experts analyzed the situation in all 6 countries – this work continues till December 2013. Unfortunately, due to lack of financing it was not possible to carry out fact-finding missions, which undoubtedly would have increased the quality of survey.

Then the primary analysis of the questionnaire responses was carried out, which resulted in an initial survey report, but also clarifying or supplementary questionnaires were formulated, the fulfillment of which, in turn, was conducted through the cooperation partners.

After conducting the initial survey, the results were discussed in the 8th Eastern Partnership Public Administration Reform Seminar "Open Governance and Data protection" (Tallinn-Helsinki 21-23 October, 2013) organised by the Estonian Center of Eastern Partnership in co-operation with the Ministry of Foreign Affairs of Finland, the European Commission and the Estonian Ministry of Foreign Affairs.

After the seminar and next round of clarification questions the current survey report was compiled. Survey focussed both on finding similar development characteristics and bringing out the differences of countries. Survey provides recommendations to states.

The final version of the study report will be published on webpage of Eastern Partnership and on the home page of e-Governance Academy.

Political and Legal Framework of Information Society

In the last decade all Eastern Partnership countries dealt with in this report (Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine) have gone through remarkable information-society development[5]. There is noticeable progress in national information and communication infrastructure, e-government and e-services. In most answers of the survey information society development and e-government development were used as synonyms.

Countries have taken different paths in the development of use of ICTs in the public sector but it seems that at some point they start to converge. There is quite a clear evidence to suggest that we could speak of the e-government infrastructure to consist of four basic pillars: access, digital data, interoperability and digital identity.

This information society development needs both political will and systemic approach in order to be successful. Thus the importance of the political and legal frameworks.

A separate Information Society Development Policy has been approved in Armenia (2010-2012[6]), Belarus (2010-2015[7]) and the Ukraine (2007-2015) and in Moldova[8]. In Georgia and Azerbaijan[9] no separate document has been adopted, but information society development is often implied in the documents related to e-government strategy or ICT policy.

One can observe that different countries are using different terminologies when regulating the area of information society. Also, the structure of national legislation and norms used in strategy planning (concepts, strategies, policies and related definitions) are somewhat different. It means that even if the titles of national level strategy documents are different, the content is often similar. So, if in this survey there are mentioned different strategy papers, it does not mean that one or another country has strategy document which another does not have. It can simply mean that a country has document with different name. In scope of current survey the aim was not to propose deep analyzes of strategy papers and legal regulations but understand whether the documents are available for future analyzes.

Internet among citizens

A main indicator for the information society and the prerequisite for development of e-government is access to Internet by the population. While the uptake of Internet was initially slow in all these countries, the situation has improved considerably over the last 5 years. The number of Internet users is still not big enough to focus solely on developing e-services, however, especially in metropolitan areas there are enough of Internet savvy users who would benefit directly from the e-government developments. Increasing the number of Internet users is accompanied by the raising public awareness of the importance of the access to Internet. At the same time, the bandwith of internet connection is not sufficient for e-services in many of the countries (see Figure 1).

Access to Intenet in other towns and rural areas, especially in Armenia, Belarus, and Georgia is still a problem but all countries have plans to develop access in rural areas. Also in all the countries internet is used more among youngsters, so there is a clear generational digital divide. In addition to increasing access a substantial rise in quality is planned.

Price policy promoting internet usage is planned in Moldova[10] and Ukraine[11], connecting schools to the internet has taken place in Moldova, Georgia[12] and Ukraine[13] etc. Good practice from Moldova is access to information through public libraries[14].

5 Often it means preferential development of one or another component contributing to the information society, not development of information society as a whole.

6 http://www.e-gov.am/u_files/file/decrees/kar/2012/06/MAR-740.pdf

7 http://pravo.by/main.aspx?guid=3871&p2=5/32317

8 http://lex.justice.md/viewdoc.php?action=view&view=doc&id=350246&lang=2

9 National ICT Strategy for 2003 – 2012, Ministry of Communication and IT are preparing a Strategy for the years 2013 – 2018. Executive Order of the President of the Republic of Azerbaijan on the approval of the State Program on the Development of Communications and Information Technologies of the Republic of Azerbaijan in 2010-2012 (Electronic Azerbaijan). August 11, 2010.

10 In terms of cost per Mbps, Moldova ranks 5th, with a price of USD 1,15 per 1 Mbps. http://www.netindex.com

11 According to "The Global Information Technology Report 2013" Ukraine is on the 6th place among 144 countries.

12 Georgian schools are connected to the Internet via mixed technologies. Large schools in urban areas have a broadband connection (100 mb/s) but schools in smaller settlements and villages are connected through EVDO with significantly less speed (2mb/s).

13 According to the national project „Open world" or «Открытый мир» all schools will be connected to internet by the end of the year 2015.

14 http://www.irex.org/sites/default/files/Access%20to%20Information%20Through%20Public%20Libraries%20in%20the%20Republic%20of%20Moldova_eng.pdf

Figure 1. Percentage of Individuals using the Internet and Household Download Index

Country	Percentage of Individuals using the Internet 2012 (rank of 211)	Household Download Index Mbps (rank of 186)
Armenia	39.16 /(112)	10.80 (60)
Azerbaijan	54.20 (78)	4.56 (118)
Belarus	46.91 (93)	7.32 (82)
Georgia	45.50 (95)	16.43 (40)
Moldova	43.37 (101)	29.74 (16)
Ukraine	33.70 (127)	20.13 (32)
Estonia	79.00 (34)	24.99 (23)

Sources: http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls and http://www.netindex.com/download/allcountries/

According to figures provided by the Ministry of Information Technology and Communications of the Republic of Moldova, in April 2013, „every second citizen is an Internet user, more than half of households have at least one computer connected to the Internet. In terms of Internet access speed, Moldova ranks among **the top-20 countries** in the word." The sector of information technology and communications (ICT) is one of the few economy areas, where the Republic of Moldova is making good progress. This fact is confirmed by national assessments and global ratings. The ICT contribution rate in Gross Domestic Product (GDP) of the country is about 9%, with a market value of over 6 billion annually. Every second citizen is an Internet user, more than half of households have at least one computer connected to the Internet. In terms of Internet access speed, Moldova ranks among the top-20 countries in the world.

In addition to internet access there is very high mobile penetration rate in Moldova[15] and Azerbaijan, which is a good prerequisite for developing mobile services.

Public awareness

A cornerstone of information society development is the awareness of citizens of the new possibilities. This has not received sufficient attention to in most of these countries and clearly, countries have not allocated sufficient means for that. There are relevant conferences, seminars, training campaigns and some countries have paid more attention to awareness raising than others, organizing the events also in regional and local levels.

In Georgia the past communication campaigns in TV and media were managed by the Ministry of Justice and its agencies. Impactful communication campaign was performed by the Data Exchange Agency on Cyber Security and prevention topics. That includes TV ads, printed calendars and other ways of communicating information to the public. In Moldova communication/awareness campaigns have been organised in the context of a number of existing policy papers.

In Azerbaijan and Belarus there have been no communication or awareness campaigns of significant scale.

Followingly a couple of examples of the best practice.

In Armenia widely known public awareness campaign was called "**I know**" (esgitem.am)[16] , which was launched in 2011. "Developed and implemented by "America" consulting company with the World Bank's support, the first stage of the

15 In November 2012, the Republic of Moldova issued the first two licenses for mobile telephony of fourth generation (4G). Licenses were offered to the companies Moldcell and Orange, which already provide mobile services on Moldovan markets and shall ensure the upgrade existent networks based on LTE technology standards (Long Term Evolution). Both operators launched 4G network in commercial regime in less than a month after issuance of the license. The mobile electronic signature, launched in September 2012, places Moldova among seven countries in the world, which are implementing similar innovative technologies and the use of this tool will boost access to secure electronic services.

16 Eng_ http://www.gov.am/en/press-conference/item/6113/. Official page: http://esgitem.am/

"I know" public awareness campaign was completed on March, 1, 2013. "Meant to foster participation in public sector and institutional reforms, as well as to achieve wide awareness of those 25 reforms carried out by the government in the period from 2007 to 2012, the initiative was highly appreciated as evidenced by numerous phone calls and social network users' positive feedback," David Sargsyan said. 11,698 calls came from both Yerevan and different marzes to the (010) 527 000 hotline phone number. Over 4000 Facebook users hailed the campaign's web page and its content, with a daily average of one thousand people involved in active discussions about the campaign: The official website of the "I know" campaign had 40 million visitors during this period. Most of the calls related to the reforms in the field of real estate registration, delivery of driver's licenses and technical overhaul of vehicles. "According to the Chief of Government Staff, only 33 out of a total of 11.000 calls represented complaints.",-abstract from press conference before the launch of the second phase of the campaign.

In Ukraine regular Social Camps are held with the support of UNDP on the topic of „Libraries – a bridge to e-government"[17], through which citizens and NGO representatives are trained.

E-Government

Legislation and regulatory environment

Laws do not create e-government nor information societies but they are important as reflections on what consensus any given society has reached or as a direction what has been chosen in this area of development. All the Eastern Partnership countries have a variety of legal regulation to support the functioning of e-government, demonstrating at least that the topic has come before the legislature quite often and in substantial ways.

Our concern looking at regulatory environment was to find whether there are obvious gaps in legal framework for e-government in these countries. We were looking for the regulation backing up e-government infrastructure, i.e. access, digitization, interoperability and digital identity that allow governments to start providing electronic services. Of particular interest to us were the laws regulating the movement of information, i.e. public information laws in any form, digital identity laws, e-government framework laws or action plans passed by the government and reflections on organisational structure of responsibilities for e-government in government. As there are variety of names and scopes of these regulations even if they have similar names, we have included the multitude of references in footnotes, limiting the main body of the text with most important country based generalizations.

As the questions on transparency have wider implications, they are also reflected in the next chapter, in this chapter we just provide an overview of the legislation. We have taken the following topics as separate sub-chapters for the easier reference:

a) e-government frameworks;
b) e-government at local level;
c) organisational structure;
d) interoperability;
e) digital identity;
f) electronic service provisjon.

The use of public information (often referred also as Freedom of Information Act) has been regulated by law in Azerbaijan since 1998[18], in Moldova since 2000[19], in Armenia since 2003[20], in Belarus since 2008[21] and in Ukraine since 2011[22]. Although in Georgia no act named like this has been adopted, the necessary provisions exist in General Administrative Code.

Act regulating the processing and use of personal data (often referred also as Personal Data Protection Act) have been in force in Armenia since 2002[23], in Azerbaijan since 2010[24], in Ukraine since 2011[25], in Georgia since 2011[26] and in Moldova

17 http://www.library.lg.ua/eng/kollegam_programs.php?filename=2010_12_20_14_15_22.html&name=International+Program+%22BIBLIOMOST%22

18 http://www.azerbaijan.az/portal/Society/MassMedia/massMedia_03_e.html

19 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=311759

20 http://www.genproc.am/am/219/;http://www.ictparliament.org/node/2007/

21 http://www.pravo.by/main.aspx?guid=3871&p2=2/1552

22 http://zakon1.rada.gov.ua/laws/show/2939-17

23 http://www.parliament.am/legislation.php?sel=show&ID=1331&lang=arm&enc=utf8]; http://www.parliament.am/legislation.php?sel=show&ID=1331&lang=eng

24 http://archive.president.az/articles.php?item_id=20100606093305718&sec_id=67

25 http://zakon4.rada.gov.ua/laws/show/2297-17

26 http://www.coe.int/t/dghl/standardsetting/dataprotection/National%20laws/Georgia%20%28Law%20of...%29%20on%20Personal%20Data%20Protection%20as%20amended%2014%2005%202013.pdf

since 2012[27]. In Belarus there is no separate law that addresses this but some provisions inwith regard to this issue have already been added to other acts.

Act regulating use of digital signature exist in all the countries: Ukraine (2003[28]), Moldova (2004[29]), Azerbaijan (2004[30]), Armenia (2005[31]), Georgia (2008), Belarus (2009[32]).

The main legal acts concerning e-identity management systems are acts regulating identity documents (ID-cards) and the digital signature (regarding ID-card certificates), also acts that regulate the population register. There are no general regulations about authentication or legal acts which would define the hierarchy of the different authentication systems. The existing regulations are usually related to a specific application or they define the approved authentication systems in the specific area.

Act regulating public databases and information systems exists separately in Armenia (2000[33]), Azerbaijan (2004[34]), Belarus (2008[35]) and in Georgia (2013[36]). In Moldova the field is regulated with several acts since 2000.

E-services are not regulated by law but lower level regulations concerning this exist in all of these countries.

We were particularly interested in seeing if the principle is established in law that no government institution is allowed to ask a person for information that one or another government institution already has and then to see how the implementation of it is actually monitored. Establishing this principle is a good reason/impulse to develop e-government. The establishing of this requirement would also be welcomed by the citizens of these countries, because the requirement for certificates or spravka's in the procedural process is very burdensome one and one that also promotes corruption. It appeared that this requirement has not been established by law in any of these countries, but in Moldova this principle is only included in a secondary act concerned with e-Transformation.

Armenia. The Law on Freedom of Information was adopted by the National Parliament[37] on September 23, 2003, the Law on Personal Data[38] on October 8, 2002 and a Government of Armenia Decision "On the introduction of the Migration System of the Republic of Armenia and the System of eE-passports and Identification Cards with Biometric Parameters in the Republic of Armenia[39]" on April 25, 2008 and the Law on Electronic Document and Electronic Signature was approved be President on January 15, 2005[40].

Azerbaijan. The State Program on the Development of Communications and Information Technologies of the Republic of Azerbaijan in 2010-2012 (Electronic Azerbaijan) was approved by the President on August 11, 2010[41]. To speed up the implementation of the plans of the State Program Election Azerbaijan, the decree of the President of the Republic of Azerbaijan on the Provision of Electronic Services by State Bodies was passed on May 23 2012[42].

Acts regulating the use of public information (often referred to as Freedom of Information Act) was past in 1998[43]. An act regulating the processing and use of personal data (often referred to as Personal Data Protection Act) was past in 2010.[44] An act regulating public databases and information systems - Law on legal protection on Databases - was past in 2004.[45] There is no separate act regulating the establishment and the use of electronic

27 http://zakon4.rada.gov.ua/laws/show/2297-17

28 http://zakon2.rada.gov.ua/laws/show/852-15

29 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=313061

30 http://www.e-imza.az/downloads/qanunlar/E-signature%20law/e-Signature%20Law%20English.pdf

31 http://www.parliament.am/legislation.php?sel=show&ID=2252; http://www.parliament.am/legislation.php?sel=show&ID=2252&lang=eng

32 http://www.pravo.by/main.aspx?guid=3871&p2=2/1665

33 http://www.armstat.am/am/?nid=183, http://www.armstat.am/en/?nid=183

34 http://www.wipo.int/wipolex/en/text.jsp?file_id=223022

35 http://www.pravo.by/main.aspx?guid=3871&p2=2/1552

36 http://dea.gov.ge/uploads/Law%20on%20Unified%20State%20Registry%20of%20Information.pdf

37 http://www.genproc.am/am/219/;http://www.ictparliament.org/node/2007/

38 http://www.parliament.am/legislation.php?sel=show&ID=1331&lang=arm&enc=utf8]; http://www.parliament.am/legislation.php?sel=show&ID=1331&lang=eng

39 http://www.arlis.am/DocumentView.aspx?docID=83326

40 http://www.parliament.am/legislation.php?sel=show&ID=2252; http://www.parliament.am/legislation.php?sel=show&ID=2252&lang=eng

41 Executive Order of the President of the Republic of Azerbaijan on the approval of the State Program on the Development of Communications and Information Technologies of the Republic of Azerbaijan in 2010-2012 (Electronic Azerbaijan). August 11, 2010.

42 the Decree of the President of the Republic of Azerbaijan On the Provision of Electronic Services by State Bodies. May 23, 2012.

43 http://www.azerbaijan.az/portal/Society/MassMedia/massMedia_03_e.html

44 http://archive.president.az/articles.php?item_id=20100606093305718&sec_id=67

45 http://www.wipo.int/wipolex/en/text.jsp?file_id=223022

identification by the population. With regard to the topic of e-identification, it is processed through the e-signature. An act regulating the use of digital signatures was past in 2004.[46] There was a the National ICT Strategy for 2003-2012[47]. Now the Government is finalizing the new version of their strategy for the near future - untill 2020. Also, in parallel with this, the Government has implemented the E-Azerbaijan Action Plan and in addition an Open Governance and Anticorruption Action Plan has recently been adopted.

Belarus. A law on information and informatization was past on 2008[48]. There are no special acts regulating the processing and use of personal data. A law on Electronic Document and Electronic Digital Signature (2009)[49] was amended in May 2013[50]. E-services are regulated through the Council of Ministers Resolution on electronic services and governmental functions in electronic form through the state automatic information system (August 9, 2011 no 1074)[51] , the Council of Ministers Resolution On Basic e-Services (Feruary 10, 2012 no 138)[52] and the Council of Ministers Resolution On E-Services rendered by the National Center of Electronic Services to government and to citizens free of charge and on some measures for the provision of e-services (May 31, 2012 no 509). Public databases and information systems are regulated by the law on information and informatization (2008)[53] and the law on the public register (2008, came into force in July, 2013)[54] .

Georgia. There is no Freedom of Information Act, but it is being actively developed with involvement of various watchdog organizations and experts. Currently the access to public information is regulated by the General Administrative Code (see more in the p 9). The Decree of Georgian Government regulating the proactive publishing of public information was adopted at the end of August, 2013, and it has been in force since September 01, 2013. A Personal Data Protection Act[55] was adopted in December 2011 but its practical implementation has just recently been started from July 2013 through the appointment of a Personal Data Protection Inspector and the respective administrative support structure. A law concerning the Unified State Registry of Information[56] has been in force since June 01, 2013. It regulates state information systems and databases. The electronic identification of the population is currently regulated by the Law on Public Services Development Agency (in force since June 2012) that is responsible for the creation and maintenance of the Population Civil Registry and also by internal regulations of the Ministry of Justice. The use of digital signatures is regulated by the law on Electronic Document and Electronic Signature in force since March 2008. An e-government act does not currently exist. The DEA is preparing a draft law (September, 2013) which will contain definitions of such important concepts as authentication, authorization, transaction and its proof, and this law will also make it mandatory to publish all e-services on the my.gov.ge central government portal.

Moldova. On May 11, 2000 the Law on Access to Information[57] was adopted. On December 26, 2012 the Law on the Reuse of Public Sector Information[58] was adopted. On April 14, 2012 the Law on Personal Data Protection[59] came into force. There are a number of acts, which apply in these cases (public databases and information systems), namely: (a) the Law no.71 of 22.03.2007 on Registries[60], (b) the Law no.1069-XIV of 22.06.2000 on Informatics[61]; (c) the Law no.467 of 21.11.2003 on Information and the State Information Resourses[62];

46 http://www.e-imza.az/downloads/qanunlar/E-signature%20law/e-Signature%20Law%20English.pdf

47 http://www.itu.int/wsis-implementation/national/flash/reports/azerbaijan/1175150268-National%20Strategy%20%282003-2012%29%20%282%29.pdf

48 http://www.pravo.by/main.aspx?guid=3871&p2=2/1552

49 http://www.pravo.by/main.aspx?guid=3871&p2=2/1665

50 http://www.pravo.by/main.aspx?guid=3871&p0=H11300027&p1=1

51 http://pravo.by/main.aspx?guid=3871&p2=5/34288

52 http://pravo.by/main.aspx?guid=3871&p2=5/35264

53 http://www.pravo.by/main.aspx?guid=3871&p2=2/1552

54 http://www.pravo.by/main.aspx?guid=3871&p0=H10800418&p2={NRPA}

55 http://www.coe.int/t/dghl/standardsetting/dataprotection/National%20laws/Georgia%20%28Law%20of...%29%20on%20Personal%20Data%20Protection%20as%20amended%2014%2005%202013.pdf

56 http://dea.gov.ge/uploads/Law%20on%20Unified%20State%20Registry%20of%20Information.pdf

57 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=311759

58 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=347200

59 http://lex.justice.md/viewdoc.php?action=view&view=doc&id=340495&lang=1 http://datepersonale.md/file/Data%20Protection%20Law%20133.pdf

60 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=325732

61 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=312902

62 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=313189

(d) the Law no.133 of 8 July 2011 on the Protection of Personal Data[63]; (e) the Requirements for the assurance of personal data security during their processing within the information systems of personal data were approved on 14 December 2010 by Government Decision no.1123 and entered into force 1 year later.[64]A law on Electronic Document and Digital Signature[65] was adopted on April 15, 2004. The Ministry of Information Technologies and Communications has also drafted a new law in this area and it has been published for consultations. Government Decision no.329 on Electronic Governmental Service for Electronic Payment was adopted on 28 May[66]. Government Decision no.330 on the Creation and Administration of the Unique Governmental Public Services Portal was adopted on 28 May 2012[67].There are no specific legislative acts on e-government/e-governance, e-ID, e-service, etc. Most of acts, adopted in this context and for the implementation of projects which result from the e-Government Agenda of the Government of Moldova, are secondary acts. The legal basis for these secondary acts adopted (2011-2013) in the context of the e-Government Agenda is the Law no.173 of 28 July 2011[68].

Ukraine. Ukraine has adopted an essential part of the necessary legislation: act regulating use of public information (often referred to as Freedom of Information Act) was passed in 13.01.2011[69], the Law on Protection of Personal Data was passed 01.06.2010[70], the Digital Signature Act was passed 22.05.2003[71], Law on Information was already passed 02.10.1992[72]. In addition to the laws the different areas are regulated by the decree of the Supreme Council of Ukraine *(Verkhovna Rada)*[73] and the decrees and ordinances of the Cabinet of Ministers of Ukraine[74].

E-government frameworks and action plans

The adoption of e-government frameworks and action plans usually provides the best picture if not of the reality, then at least of the desired state of affairs of e-government in any given country. It usually also indicates the importance the political leadership attaches to the development of e-government and information society.

All of these countries have an e-government development plan in one form or another. In Armenia[75] and Beloarus it is a part of an overal information society development plan. All these countries excluding Belarus have joined the Open Government Partnership and this act in itself entails the development of e-government. Moldova has had a separate program „e-Transformation“ since 2011. In Georgia an „e-Georgia“ program is being widely

63 http://lex.justice.md/viewdoc.php?action=view&view=doc&id=340495&lang=1

64 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=337094 http://datepersonale.md/file/hotariri/cerinte_securitate%20eng_101228.pdf

65 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=313061

66 2012.http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=343404

67 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=343406

68 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=339783

69 Закон Украины «Про доступ к публичной информации». http://zakon1.rada.gov.ua/laws/show/2939-17

70 Закон Украины «О защите персональных данных», http://zakon4.rada.gov.ua/laws/show/2297-17

71 Закон Украины «Об электронной цифровой подписи», http://zakon2.rada.gov.ua/laws/show/852-15

72 Закон Украины «Про информацию», http://zakon4.rada.gov.ua/laws/show/2657-12

73 Постановление Верховного Совета Украины «О рекомендациях парламентских слушаний по вопросам развития информационного общества в Украине» от 1.01.2005 №3175-IV [http://zakon4.rada.gov.ua/laws/show/3175]

74 Постановление Кабинета Министров Украины «Об утверждении Положения о Национальном реестре электронных информационных ресурсов» от 17.03.2004 №326 [http://zakon1.rada.gov.ua/laws/show/326-2004-%D0%BF/print1331022139701229], Постановление Кабинета Министров Украины «Об электронном обмене служебными документами в органах исполнительной власти» от 17.07.2009 №733[http://zakon4.rada.gov.ua/laws/show/733-2009-%D0%BF], Постановление Кабинета Министров Украины «Об утверждении Порядка применения электронной цифровой подписи органами государственной власти, органами местного самоуправления, предприятиями, учреждениями и организациями государственной формы собственности» от 28.10.2004 №1452 [http://zakon4.rada.gov.ua/laws/show/1452-2004-%D0%BF]. Постановление Кабинета Министров Украины «Об утверждении Классификатора обращения граждан» от 24.09.2008 №858 [http://zakon4.rada.gov.ua/laws/show/858-2008-%D0%BF], Распоряжение Кабинета Министров Украины «Об утверждении Концепции формирования системы национальных электронных информационных ресурсов» от 5.05.2003 №259-р [http://zakon1.rada.gov.ua/laws/show/259-2003-%D1%80/print1331022139701229], Распоряжение Кабинета Министров Украины «Об одобрении Концепции создания и функционирования автоматизированной системы «Единое окно подачи электронной отчетности»» от 7.08.2013 №587-р [http://zakon4.rada.gov.ua/laws/show/587-2013-%D1%80], Распоряжение Кабинета Министров Украины «Об одобрении плана действий по внедрению в Украине инициативы «Партнерство «Открытое Правительство»» от 5.04.2012 №220-р [http://ogp.gov.ua], Распоряжение Кабинета Министров Украины «Об утверждении плана мероприятий по внедрению Инициативы «Партнерство «Открытое правительство»» от 18.07.2012 №514-р [http://ogp.gov.ua].

75 http://www.gov.am/files/meetings/2010/4655.pdf

discussed now, and it will probably be approved some time this year.

In all these countries several sectoral programs and action plans have been adopted and put into practice. In all these countries there are so-called e-field champions for example in Armenia there are e-Business, e-Tax and e-Cadastre; in Azerbaijan e-Tax, e-Social Services and e-Customs; in Belarus e-Education, e-Health and e-Commerce; in Georgia e-Health, e-Business and e-Education; in Moldova e-Education and e-Health and in Ukraine e-Commerce, e-Education and e-Health.

In all of these countries the development of this sector has depended on role of enthusiasts and therefore there has been an uneven development of e-services. At the same time, the bottom-up - implementing agencies – the original initiatives benefited from the "green light" given to innovation in the design and delivery of e-services.

Armenia. The Information Society development policy 2010-2012 (approved on February 25, 2010) Annex 1 is the "E-governance development action plan"[76]. The action plan include: the development of the principles of e-government interoperability, the adjustment of e-government system software and standards, e-government system legal framework analysis and proposals, etc.

Azerbaijan. There is a National Action Plan (2012-2015) on the development of Open Government in the country, which was approved by a decree of the President on Sept. 5, 2012[77]. Also prior to this, there were 2 stages of an E-Azerbaijan State Programme, for the years 2005-2008 and 2010 – 2012. Currently there are ongoing activities for the next stage of the programme up to 2015.

Belarus. There is no coherent e-government strategy, however e-government is included as a subprogram in: 1) Information Society Strategy[78] (2010); 2) National programme for accelerated development of services in the ICT sphere for 2011-2015[79] (2011) amended in 2012.

Georgia. The draft e-government strategy called e-Georgia is undergoing an approval process. It was developed with in the framework of the e-Twinning program of the EC. The draft document (120 pages) is available[80] and it has been widely distributed for public comments and consultations. The expected approval time is some time before the end of 2013.

Moldova. The Strategic Programme for Governance, Technological Modernisation (e-Transformation)[81] was approved by Government Decision no.710 on September 20, 2011. Every year the Government of the Republic of Moldova adopts Action Plans to implement the Strategic Programme for Governance, Technological Modernisation of the Government: a) Government Decision no.972 of 21.12.2012 on the approval of the Action Plan for 2013 in terms of implementing the technolocal modernization of the Government (e-transformation)[82] was adopted on 21.12.2012; b) Government Decision no.44 on the approval of the Action Plan for 2012 in terms of implementing the technological modernisation of the Government (e-trasformation)[83] was adopted on 21.01.2012.

Ukraine. The National Development Plan for the year 2013 includes the subtopic "Digital Management"[84]. With the ordinance of the Cabinet of Ministers of Ukraine „Concept of Digital Management of Ukraine"[85] and „Development Strategy of Information Society"[86] have been approved. Open Government Partnership has been approved as of 18.07.2012[87].

76 http://www.gov.am/files/meetings/2010/4655.pdf

77 http://az.president.az/articles/5712

78 http://pravo.by/main.aspx?guid=3871&p2=5/32317

79 http://www.pravo.by/main.aspx?guid=3871&p2=5/33546

80 http://dea.gov.ge/uploads/20130706%20eGeorgia_%20final_DRAFT%20for%20public%20consultation.pdf

81 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=340301

82 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=346058

83 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=342049

84 Указ Президента Украины «О Национальном плане действий на 2013 год по внедрению Программы экономических реформ на 2010-2014 года «Зажиточное общество, конкурентоспособная экономика, эффективное государство» от 12.03.2013 №128/2013 (Раздел «Электронное управление»). http://zakon0.rada.gov.ua/laws/show/128/2013

85 Распоряжение Кабинета Министров Украины «Об одобрении Концепции развития электронного управления в Украине» от 13.12.2010 №2250-р, http://zakon2.rada.gov.ua/laws/show/2250-2010-%D1%80

86 Распоряжение Кабинета Министров Украины «Об одобрении Стратегии развития информационного общества в Украине» от 15.05.2013 №386-р (раздел «Электронное управление», «Электронная демократия»), http://zakon4.rada.gov.ua/laws/show/386-2013-%D1%80?test=qY4Mfbtc78fVAZBUZiTuFSn9HI4R2s80msh8Ie6

87 Распоряжение Кабинета Министров Украины «Об утверждении плана мероприятий по внедрению Инициативы «Партнерство «Открытое правительство»» от 18.07.2012 №514-р (раздел «Внедрение электронного управления и развитие электронной демократии»), http://ogp.gov.ua

E-government at local level

As most of the reform and reconstruction efforts in the Eastern Partnership countries have been concentrated on the capitals and central level of government, it is quite understandable that developments at the local government levels are lacking behind. When looking at the e-gov developments, we could not find any programs directed separately towards local authorities.

While no specific programs directed towards local authorities have been drawn up in these countries it does not mean that nothing has yet been done with regard to this area.

The best practice with regard to the local level is found in Georgia. The Public Service Development Agency that has become the Government's arm for consulting and assisting its agencies to implement reforms in the public service has been developing municipal e-government services modules. Plans for the establishing of physical one-stop-shops – Village Service Halls were promoted by the previous government, and have been partially supported by the new government.

In Moldova one project was implemented at the regional level by the UNDP, another one was implemented together with German partners[88].

In Ukraine e-service development programs have been adopted in several big cities, for example in Mykolaiv (in 2010 for 2011-2015), in Dnipropetrovs'k (2011-2014), in Kiev (2012-2014), in Luhans'k (2012), in Chernivtsi (2012), in Volyns'ka oblast (2012), in Lviv (2013-2014), in Novohrad-Volyns'kyi (2013)[89].

As several countries (Armenia, Azerbaijan, Georgia) are now in the process of planning the reforms of the municipalities it is presumed that the rapid development of e-services in local authorities will take place after that.

The role of the Associations of Municipalities in e-government development were not mentioned but in several countries joint actions are underway. In Ukraine for example there is agreement between cities to focus on e-government developments and they have created a common framework for this cooperation.

The main problems with regard to the development of ICT in the municipalities lie in their large numbers but also in the fact that many small municipalities are not able to run their own strategies and development projects. This means that some form of cooperation is needed and it does not matter whether it is done by central government associations of the municipalities or by voluntary groups or agreements between separate municipalities. It would be a good thing to encourage the establishment of cooperation frameworks for the joint development and coordination of e-government.

Organizational framework

It has been observed since the beginning of the XXI century that political leadership is the most important ingredient of e-government development. Consequently, one of the most telling signs of e-government development is the organisational framework for its implementation.

When we look at the Eastern Partnership countries, we can see that developing e-government is not a responsibility of a single insitution in any of these countries but rather, e-government development is carried out by several institutions coordinated in variety of ways.

The best practice is for the coordination to be done at either the Presidential or Governmental level as lower level insitutions often do not have the sufficient powers to actually coordinate the development of e-government. Another option is that the development of e-government is treated as a technical field and that the development of e-government is carried out by the so-called technical ministries, for example ministries responsible for IT and communication. In Moldova and Armenia the coordination of e-government has been done by an institution servicing the Government, which therefore had the necessary powers – which has guaranteed success and can be considered as the best practice for others to follow.

In all of these countries there are institutions that are responsible for developing the e-infrastructure, which due to the circumstances often means that they are dealing with and coordinating their actions with other institution operating in the corresponding field: in Armenia the EKENG, in Azerbaijan the EHDIS, in Belarus the Ministry of Communication and IT and the Operative Analytical Center (OAC), in Georgia the Data Exchange Agency and in Moldova the Ministry of Communication and IT together with the E-government Centre and the State Enterprise „Center of Special Telecommunications."

There has been the emergence of a new tendency

88 http://www.serviciilocale.md/lib.php?l=ro&idc=69&nod=1&t=/Rapoarte-de-progres&

89 Николаев – Mykolaiv; Вознесенск - Voznesens'k; Днепропетровск - Dnipropetrovs'k; Киев – Kiev; Львов – Lviv; Новоград-Волынский - Novohrad-Volyns'kyi; Луганск - Luhans'k; Черновцы – Chernivtsi; Волынская область - Volyns'ka oblast; Славутич – Slavutych.

to establish institutions that are responsible for the development of e-services development, for example in Azerbaijan (ASAN), in Belarus (the National Center for e-Services) and in Georgia the Agency for Public Services under Ministry of Justice.

In all of these countries the development of e-government has substantially been dependent on and is still dependent on political leaders. For example in Armenia and Georgia coordinating has been done at the head of state level: the Armenian E-Governance Council is directed by the Prime Minister, in Ukraine the Information Society Council is directed by the Deputy Prime Minister and in Georgia the development engine of e-government has been the President.

As a rule CIO's are not included in the make up of the ministries today. Often the role of IT management is given to some unit or person but in most cases these tasks are considered to be purely technical and not connected to the changes of processes and changes at the ministry level.

One of greatest challengies may prove to be getting support from the political level to nominate CIO-s with concrete roles into management positions including the important role in the management of change in these ministries.

An example of best practice in this area can be found in Moldova where they recently made strong efforts to establish a stable e-government IT organization including a central coordination unit and the institution of a CIO. Pursuant to Government Decision no.499 of 06.07.2012, „all ministries, other than the central administrative authorities will institute the subdivision on e-Transformation as a mandatory subdivision." It will be subordinated to the head of the authority. The head of the Sub Division is responsible for the implementation and coordination of the e-Transformation process within the authority. This sub-division will be formed out of a number of specialist in areas, such as: Large-scale Architecture Infrastructure and Information Resources, the Management of IT Projects, Information and Data Analyses.[90]

The best practice example of PPP and science cooperation also comes from Moldova. The E-government Center organizes monthly meetings with the business sector. At these meetings the E-government Center's representatives speak about new projects, tenders, etc. The E-government Center has signed a Memorandum of Understanding with the Academy of Sciences of the Republic of Moldova.

Unfortunately Civil Society Organizations have not played a significant role in the development of e-government in any of the countries and while IT business associations are consulted sporadically, there seem to be no institutionalized involvement of such organisations in the overall e-government development. At the same time, we feel that the scope of required change is such that these types of arrangements for information exchange and feedback from the society are absolutely necessary for the successful reform programs.

Armenia. The e-Governance Council is the key organisation that is responsible for the development of e-government in Armenia. The members of the e-Government Council are: the Prime Minister, the Chairman of the Board; the Deputy Prime Minister, the Minister of Territorial Administration; the Minister of the Economy; the Minister of Transport and Communications; the Minister of Education and Science; the National Security Service Officer; and the Chief of Police. The e-Government Council was created on 28.06.2010 in accord with the decision document N 475-Ա of the Prime Minister[91].

The e-Government Council can be considered as the e-government coordination unit. In the document it is stated that the objectives are: 1) The implementation, coordination, monitoring and evaluation of all related activities; 2) The reporting on the development trends and the implementation of programs; 3) The adjustment and revision of policies and under the framework of the e-society development policy the implementation of strategic coordination and other legislative support; 4) The coordination of the annual and mid-term development plans; 5) Support to both the public and private sectors and international cooperation; 6) Coordinating and management the "e-Governance Infrastructure Implementation Unit" Open Joint Stock Company; 7) The submission of proposals to the Government for the development of the Cyber Security Council.

There is no official e-Government Council web page, but the www.e-gov.am (e-government official web-page) is an official platform for communicating with the public.

The E-Governance Infrastructure Implementation Unit is EKENG[92], which is coordinating the overall implementation of the strategy for the devel-

90 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=344035

91 http://acts.legalportal.am/show/NTkxOTE=/HH+VARChAPETI+OROShUM@+HH+ELEKTRONAYIN+KARAVARMAN+KhORHURD+STEGhTsELU+DRA+KAZM@+EV+AShKhATAKARG@+HASTATELU+MASIN/

92 http://www.ekeng.am/

opment of e-government. The company makes citizen and businesses interaction with the state bodies easier in the e-governance sphere.

Azerbaijan. The main entity for leading the drive towards e-government is the Ministry of Communication and IT. Azerbaijan needs a strong leader for the development of e-services and this is a challenge for the State Agency for Public Service and Social Innovations, whose first major task was the establishment of the ASAN service centres in order to ensure that all services awere made availiable to all citizens from a single source, and that these services were to be of the highest quality and very convienent for its users.

The central e-government coordination unit is currently the Ministry of Communications and IT. In the Regulation of the Ministry, approved by the Government, it is clearly stated, that „(2). The Ministry is the central executive body which formulates and implements state policy, secures the legal normative regulations and over sees the development of communications and information technologies, coordinates the activities of other government agencies in the areas of communications (telecommunication, post) and information technologies in the Republic of Azerbaijan."[93]. The e-government Web portal[94] is also implemented by the Ministry.

Belarus. In Belarus e-government is still considered to be a technical and not political matter, which means that the Ministry of Communications and Informatization is the key institution. According to the national program for the accelerated development of the ICT services sphere for 2011-2015[95] (2011) the implementing agencies responsible for the e-government subprogram is to be determined on a competitive basis by the Ministry of Communication and Informatization. The Ministry of Communications and Informatization is responsible for the coordination of the e-government projects. The Operative Analytical Center[96] (OAC) is responsible for information protection issues and for the PKI infrastructure. OAC subdivision the Research Institute for information protection[97] is working on information security issues. The OAC subdivision the National Center for data exchange [98]is responsible for the provision of protection from unauthorized access to data transmission network, for state agencies, organizations, the interoperability between legal entities and individual entrepreneurs, and for online access to the state bodies and organizations. The National Center for E-Services, a subdivision of the Operative Analytical Center, is responsible for the functioning of interdepartmental information systems. It is here that we can see one of the problems related to the current structure. When an E-Delegation (the Public council for e-business development) turned to the Operative Analytical Center (responsible for data protection and public key infrastructures) with the comments related to key public procedures the OAC reacted in the following manner: the Ministry of Communications and Informatization has developed Law on digital signatures and therefore all comments on this matter should be addressed to it.

There is no special law, which underpins the coordination unit and defines its responsibilities. Formally, The Council of Ministers was the major coordinating unit. Historically the Ministry of Communications and Informatization have been developing and supervising the informatization programs and it has preserved this function up till now. The National program for the accelerated development of services in the ICT sphere for 2011-2015[99] (2011) states that the key agency for overseeing the e-government sub program ("customer" - "заказчик") is the Department for Informatization at the Ministry of Communication and Informatization: the customer-coordinator of the National program is the Ministry for Communication and Informatization[100] in the person of the Department of Communications and Informatization.[101] The National program customer-coordinator can at any stage form the Council /Board to ensure the coordination of activities, to consider proposals on amendments, and the redistribution of the budget for the program. The tasks and functions of the Council should be defined by the customer-coordinator Ministry of Communication and Informatization. The Ministry of Communications and Informatization has formed a Coordination Council for the e-Government Subprogram of the National Program for its accelerated development (information on the meetings of the Council[102] and

93 http://www.mincom.gov.az/ministry/regulations

94 https://www.e-gov.az/

95 http://www.pravo.by/main.aspx?guid=3871&p2=5/33546

96 http://oac.gov.by

97 http://www.niitzi.by/index.php?lang=en&Itemid=108

98 http://www.ncot.by/

99 http://www.pravo.by/main.aspx?guid=3871&p2=5/33546

100 http://www.mpt.gov.by/ru/

101 http://www.mpt.gov.by/ru/department/

102 http://www.mpt.gov.by/ru/new_page_8_1_15288/

members of the Council[103]).

Georgia. It is a peculiarity of the development of e-government in Georgia that until recently there was no centralized e-government organizational framework, but at the same the country has developed sound e-services and information systems (some of them awarded by the UN). Different agencies have often competed with each other in the development of e-services, but the overall e-government picture remains quite spotty and uneven. The champions of e-government developed and maintained highly functional e-registries and electronic taxation systems, while some Ministries would not update parts of their websites for months. The Minister of Justice supports the initiatives in e-government, especially those concerning e-identity and other e-services under control of her ministry.

As of August 2013 the coordination unit has not yet been established. Presumably the ICT and Innovations Council will serve as the central e-government coordination unit. Currently the Data Exchange Agency (DEA)[104] could be considered the de-facto coordinator of such activities, but the DEA often lacks the ability to leverage high-level decision making, thus it is still unclear if the creation of the ICT and Innovations Council will amend the e-Georgia plans.

Moldova. In the process of the implementation of the e-Governance Agenda, the Government of the Republic of Moldova has delegated powers to a number of actors, namely, the State Chancellory, the relevant Ministries, the Public Institution „e-Government Center", the State Enterprise "Center of Special Telecommunications" among others, (Government Decision no.709 of 20 september 2011 on some measures in the field of the Governance e-Transformation[105]). Pursuant to the Law no.173 of 28.07.2011 on the ratification of the Financing Agreement Between the Republic of Moldova and the International Development Association for the Implementation of the „Governance e-Transformation" Project, „the Government of the Republic of Moldova will take the necessary measures to implement the provisions of the Agreement" (Article 2)[106] . According to Government Decision no.709 of 20 September 2011, the State Chancellory, in cooperation with the Public Institution "e-Government Center" and the State Enterprise "Center of Special Telecommunications", is responsible for a number of projects which result from the Strategic Programme for Governance and Technological Modernisation (e-Transformation), which was approved by Government Decision no.710 of 20 September 2011[107]. According to Government Decision no.710 of 20 September 2011 on the adoption of the Strategic Programme for Governance and Technological Modernisation (e-Transformation), "The implementation of the Strategic Program shall be coordinated by the National Commission for e-Transformation and will be ensured by the State Chancellery, together with the Center for Electronic Government, the Ministry of Information Technology and Communications, other ministries and other central administration authorities. These Ministries and the other central administrative authorities: a) will generate annual plans to meet the objectives of the e-transformation of governance, including the modernization of the public services and the modernization of governance through the implementation of information technology (IT); b) will appoint individuals (at the level of of deputy ministers) who in collaboration with the Coordinator for e-Transformation, the various IT managers and the Divisions responsible for Analysis, Monitoring and Evaluation will be responsible for the implementing of the above-mentioned strategic program. The State Chancellory will be responsible for control over the implementation of this decision."[108].

Pursuant to Government Decision no.222 of 1 April 2011, members of the Council of Coordinators for e-Transformation will "a) will participate in the implementation of policies, standards and technical regulations for the technological transformation of government and the implementation of e-governance; b) will coordinate, jointly with the Center,electronic public services in each public authority; c) coordinate the use of modern technology to streamline the work of the Government, ministries and other central administrative authorities; d) coordinate the effective implementation of information and communication technologies to provide high quality public services and increasing increasing the performance of the public sector through ICT."[109].

103 http://www.mpt.gov.by/be/new_page_8_1_15287/

104 http://www.dea.gov.ge

105 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=340300

106 http://lex.justice.md/viewdoc.php?action=view&view=doc&id=339783&lang=1

107 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=340301 and http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=340300

108 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=340301

109 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=338053

The National Commission for e-Transformation has a consultative role. According to Government Decision no.632 of 8.06.2004, the Commission was established „for building an Information Society in Moldova and for adjusting the national strategy on information technologies to other strategies which are being developed and implemented“[110].

Ukraine. Project of the Annual Report “Informatization and information society development in Ukraine over the year of 2013” states: “It should be noted that the development of e-government in Ukraine is carried out on the basis of different mechanisms of state governance that are not consistent with each other on the principles, priorities, objectives, subjects, objects, procedures, terms and resources, in a significant measure duplicate each other and sometimes contradict each other.

Key figures (personnel and structures), which work in the field of e-governance: 1) Coordination Center for the implementation of economic reforms under President of Ukraine[111]; 2) Deputy Prime Minister of Ukraine, responsible for the implementation of reforms in the field of “e-government”; 3) Deputy Prime Minister responsible for implementing the informatization, the information society, initiative “Open Government”; 4) State Committee for Science, Innovation and Informatization of Ukraine; 5) National Centre for e-Governance of Ukraine as a structural subdivision of the state enterprise “State Center of Information Resources of Ukraine.”.

At the moment the interdepartmental Council for the Development of the Information Society is operating[112], it is planned to establish an interdepartmental Council on e-government at the profile of the Deputy Prime Minister of Ukraine.

Interoperability framework

In order to provide complex electronic services, a country needs to have a functioning interoperability framework, i.e. the way data could travel between different information systems belonging to different public institutions. The existence and the sophistication of such framework indicates also the level of e-government development.

The exchange of data between different institutions takes place in all of these countries, and there is also a system of automatic data exchange between databases in many of these countries. The most common form of data exchange is a bilateral data exchange arrangement based on specific bilateral agreements.The goal of creating a modern and secure Data Exchange Layer is in the process of being developed in Georgia, Moldova and Azerbaijan. In Belarus and Ukraine the plans are being put into practice, and in Armenia the decision to establish a data exchange layer is under preparation (EKENG).

The example of best practice in this respect is found in Georgia, where the data exchange infrastructure is almost in place. There is ongoing framework of cooperation with in the Twinning project to make the Georgian registries compatible with EU standards, including GIS. The automatic exchange of data between the various registers and databases is also being developed inside the country; the creation of an interoperability framework with EU countries is part of the current agenda. More information on this subject is available in the draft eGovernment strategy – eGeorgia. The DEA is currently developing a standard catalogue of e-services for requests by the interested state agencies to implement an automated exchange of information. The most commonly used government data base is one that contains data about individuals. Interfaces with the Civil (Population) Registry are being implemented by all the public organizations that need to identify individuals or process personal data. Notaries and commercial banks also have access to the Civil Registry data.The second most popular service is the Register of Businesses. The open online database (and respective interfaces) are used by the commercial organizations for identification and tax documentation.

A good example of this can be found in Azerbaijan. To enable the interoperability between the different IT systems in Government “The state of e-government information system - EHDİS» project was recently initiated by the Ministry of Communications and Information Technologies. Under the EHDİS several government databases are already connected enabling the exchange of data between different government agencies. EHDİS is a complete system consisting of a certification Centre, central servers, a monitoring system, security servers, an adaptive server, and a support and official communications system. EHDİS is an extremely

110 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=296594

111 Национальный план действий на 2013 год по внедрению Программы экономических реформ на 2010-2014 года «Зажиточное общество, конкурентоспособная экономика, эффективное государство»; реформы в сфере «э-управления»

112 Постановление Кабинета Министров Украины от 14.01.2009 г. №4.

secure system, it meets the ISO27001 safety standards. EHDİS does not hold the data itself, but is the intermediary in the transmission of data. The EHDİS system ensures such important conditions such as data security, standardization, observability, traceability, and reliability. As part of the project the EHDİS technical, organizational and legal framework for the transfer of data between public authorities, citizens and businesses have been created. At the moment the Ministry of Communications and Information Technologies, the Ministry of Taxes, the State Customs Committee, the Ministry of Justice, the Ministry of Transport, the State Social Protection Fund, the General Prosecutor's Office, the Ministry of Labour and Social Protection, the Ministry of Education, the Ministry of Health are all participating in the pilot project[113].

Armenia. The exchange of data exchange takes place between different institutions and the automatic of data between databases exists. The most common form of data exchange is bilateral data exchange based on bilateral agreements. The decision to establish a data exchange layer is currently being prepared (EKENG).

Azerbaijan. The exchange of data between different institutions takes place and the automatic exchange of data between databases takes place. The most common form of data exchange is bilateral data exchange based on bilateral agreements. A modern and secure Data Exchange layer has been invisaged and is in the process of being developed (EHDİS).

Belarus. The automatic exchange between various registers and databases is still under construction. According to the list of registered information resources in Belarus[114] the integrated automated information system only provides interoperability for three agencies at the moment, but it is planned that 20 agencies will be able to use this system by 2015. The National Center for e-services has developed a set of standards for interoperability concerning data exchange[115].

Georgia. An infrastructure for data exchange is in place. There is an ongoing framework of cooperation within the Twinning project to make Georgian registries compatible with EU standards, including GIS. The automatic exchange of data between various registers and databases is also operational inside the country; and an interoperability framwork with the EU countries is being developed at the moment. The DEA is currently developing a standard catalogue of e-services for requests by the interested state agencies to implement the automated exchange of information.

Moldova. The Interoperability Framework Program approved by Government Decision no.656 of 05 September 2012 „describes the current situation in the given area, and defines the goals, objectives, required actions and measures establishing the implementation phases and the responsibilities of all the stakeholders involved in the efficient exchange of data, including the tools required at organizational, semantic, and technical level"[116].

Ukraine. A plan of measures for implementation of the Concept of creation and functioning of the information system of electronic interaction of state electronic information resources in Ukraine has been submitted to the Cabinet of Ministers of Ukraine[117].

E-identity

One of the prerequisites of the advancement of e-government is the adoption of digital identity. As digital identity as a concept entails questions of legal responsibility, the procedures of its establishment have to be reflected in laws. Having digital identity allows a user of an information system to establish him/herself unambiguously as a user of the system or an author of a digital document, an applicant or a recipient of a service or simply as a

113 The project was implemented in partnership with the Azerbaijani-Estonian company B.EST Solutions and with the participation of Azerbaijani and Estonian companies SayberNet, Cybernetica, Aktors. As a single information system for data exchange used by all government agencies - EHDİS can solve interaction not only among government agencies, but also with various companies and individuals. Thanks to EHDİS doing business in the old way with a physical visit to the government agencies and paperwork will remain in the past, and various services will be available over the Internet, just a few keystrokes away. Government employees in accordance with their duties and authority have access to the information from the information systems of various government agencies. For example, on request, data about property, vehicles, employment, insurance, credit, education and diplomas, etc. can be found. EHDİS can be compared to a living organism or a tree, which is constantly growing and evolving by connecting new services and databases. The introduction of this system in Azerbaijan in the near future will not only enhance the efficiency of the public authorities, but will also ensure the transparency of relations between citizens and public agencies and help to eliminate bureaucracy and corruption.

114 http://infores.mpt.gov.by/it/database_is/

115 http://nces.by/wp-content/uploads/smdo.pdf

116 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=344700

117 Проект Плана мероприятий подготовлен на выполнение Распоряжения Кабинета Министров Украины «Об утверждении Концепции формирования системы национальных электронных информационных ресурсов» от 5.05.2003 №259-р. http://zakon1.rada.gov.ua/laws/show/259-2003-%D1%80/print1331022139701229

person authorised to make changes, give orders or submit documents.

The main legal acts concerning e-identity are concerned with identity documents (ID-cards), digital signatures (regarding ID-card certificates) and the population (civil) register.

As a rule institution responsible for digital signature is also seen as responsible for electronic identity, however, it seems that realization of the importance of digital identity has not really occurred yet. In all the countries the most common method of authentication is still the use of the username and a password. It is clear that the level of data security is inadequate in these cases.

The coordinating institution is unambiguously designated only in Georgia: Public Services Development Agency (PSDA) (former Civil Registry Agency) – a semi-indepent Legal Entity of Public Law established under the Ministry of Justice. This agency is coordinating issuing eID and all related processes.

There are no general regulations concerning authentication or any legal acts which would define the hierarchy of the different authentication systems. The existing regulations are usually specific to a single application or define the approved authentication systems in a specific area.

The parallel development of Public Key Infrastructure (PKI)-based authentifiction methods is also taking place. In Armenia ID-cards issued from 2012 have certificates that enable a digital signature, EKENG is also the Certification Agency and the PKI will be launched in autumn 2013. In Azerbaijan cards enabling a digital signature are issued by the IT and Communication Ministry's subdivision EHDİS. In Georgia and Moldova ID-cards carrying certificates that enable authentication and a digital signature are issued. The PKI has been fully operational in Ukraine since 2005, and in Georgia since 2011, and also in Moldova. The launching of the PKI in Belarus has been postponed and it is now planned for December 2013.

Ukraine decided to renew the legal framework of its PKI and to establish conditions for recognizing the qualified certificates of foreign countries in April 2013.

There is one Certification Agency (CA) in Georgia, two in Moldova,and twenty one in Ukraine. Although the law in all these countries allows the private sector to establish CAs it in general has not shown any interest in doing so except in Ukraine.[118]

Although there has been an increasing use of these authentification systems in the government and the banking sectors, progress is slow in use of them in the other parts of these societies.

The use of Mobile-ID is common in Azerbaijan and Moldova and in other countries a plastic card is as a rule used as a token.

Biometry is used in in passports but that reflects adoption of international standards because of necessity of travel requirements.

An example of best practice with regard to this issue is found in Georgia. The most common online identification method is the use of the username and password. Commercial banks back it up with an automated SMS code sending service, and in some cases tokens. The use of e-IDs as an online identification tool has had a slow uptake, despite the fact that card-readers were subsidized for users as a result of several campaigns of the previous government. Currently PSDA offers a personal username and password for the e-government portal my.gov.ge. A citizen can receive it personally in the Public Service Hall after offering proof of their identity. Other methods of online identification include video link (Skype for notary services) and Georgian citizens living abroad often use a video link to remotely request public services.

Armenia. There is the Law on E-Identification Cards adopted by the Parliament on November 30, 2011[119]. The 1st article of this law defines the regulatory principles related to the identity card of the citizens, i.e its withdraw, converion and the invalidity of other processes.

In support of the Presidential Order of March 15, 2008, "On the Conception for the Migration System of the Republic of Armenia and for the Introduction of the System of Electronic Passports and Identification Cards with Biometric Parameters in the Republic of Armenia", the Government initiated a project for the introduction of electronic documents with biometric components which was coordinated by the Police and the EKENG CJSC[120].

As for all the other methods of identification, the most common method is in most cases the username and password and this also includes the e-banking sector.

In Armenia the ID-cards issued from 2012 have certificates that enable a digital signatuure. EKENG

118 http://czo.gov.ua/ca-registry?type=3

119 http://www.arlis.am/documentview.aspx?docID=73075

120 http://www.ekeng.am/?page_id=62

[121]is the only company in Armenia authorized to issue digital signatures to individuals and legal entities[122]. EKENG is also the Certification Authority and the Public Key Infrastructure (PKI) will be launched in late autumn 2013.

The Certification Agencies (CA) that have been creatied in Armenia are located in the Passport and Visa Departments of the Police. There is little information available on the Internet concerning these certification agencies and the e-identity registration process[123].

The token/carrier of e-identity is a plastic-card.

Azerbaijan. The coordinator is the Ministry of Communication and IT and the role of the Ministry is defined by specific regulations that have been approved by the President.

There are both username and password authentication, as well as authentication through the PIN number of an individual's passport. Also, there is the process of securing an e-signature, through the e-government portal through the Ministry of Communication and IT. The specific entitiy - EHDİS, which issues, stores and manages the e-signatures[124] is under the auspices of this ministry. EHDİS is a complete system consisting of a Certification Centre, central servers, a monitoring system, security servers, an adaptive server, and a support and official communications system.

Under the e-government initiative, there are a number of centers where a citizen can get the e-signature and/or a mobile-ID[125].

The tokens/carriers of e-identity are plastic-cards (Secure Signature Card)[126] and special SIM-cards.

Belarus. There are no acts regulating e-identity, also no appointed coordination unit for the creation or regulation of e-identity.

Publicly available web based services usually operate with the username/password access method. Some governmental and financial services use harder identification systems and encryption.

There is no established National Public Key infrastructure. The introduction of this infrastructure has been postponed since 2011- firstly to January 2013, and now to December 2013. A presidential Decree N 515 November 8 2011[127] designated the Operative Analytical Center as the regulator of the PKI. The National Center for E-Services was designated as an operator of the PKI. The Operative Analytical Center (OAC) issued an order on PKI 16.10.2012.[128]

The Order includes the Concept of State Public Key Infrastructure development[129]. The architecture of PKI is descried in articles 5 and 8 of the Concept. The organizational setup is described in Regulations on PKI.

There is no integrated list of certification agencies in Belarus. Some examples are presented below: 1) CA «Mailgov»[130]; 2) CA «БелГИЭ»[131]; 3) Ministry of Industry[132]; 4) State Customs Committee[133]; 5) Tax Ministry[134]; 6) State Border Committee of the Republic of Belarus[135]; 7) State Belarusian Railways[136]; 8) Ministry of Labour and Social Protection[137] ; 9) Ministry of Education[138]; 10) Ministry of transport[139]; 11) UIIP NAS Belarus[140]; 12) Belarusian Universal Commodity Exchange[141]; 13) National Center for Marketing and Price Study[142];

121 EKENG Closed Joint-Stock Company is a commercial legal entity, who provides services to governmental institutions and e-government services to other private entities and citizens.

122 http://www.ekeng.am/?page_id=18

123 http://passportvisa.am/

124 http://www.e-imza.az/index.php?lang=en

125 http://www.e-imza.az/regcenter.php?lang=en

126 The technology details can be found below: http://www.e-imza.az/e-signer.php?tp=certuse&ide=26&lang=en

127 http://www.pravo.by/main.aspx?guid=3871&p2=1/13064

128 N 79/ О некоторых вопросах функционирования Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь. http://www.pravo.by/main.aspx?guid=3871&p0=T61202222&p1=1

129 (Концепция развития государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь) and Regulation on PKI (Положение о государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь).

130 http://nces.by/service/ca-mailgov/documents/

131 http://edoc.by/about_ca

132 http://www.cniitu.by/cert

133 http://gtk.gov.by/ru/eldeclaration_new/udost_centr

134 http://www.pki.by/site/index.do?type=detail&view=article&hid=65, also see http://preview.tinyurl.com/lszlav7

135 http://infores.mpt.gov.by/ir/database/view_ir.php?id=5523

136 http://www.isc.by/isc/index.do?type=blog&view=article&hid=121&menuid=111

137 http://www.ssf.gov.by/priside/about/it/

138 http://www.giac.unibel.by/main.aspx?guid=16711

139 http://ca.mtk.by/

140 http://uiip.bas-net.by/structure/l_pzi/grid.php

141 http://www.butb.by/?page=195

142 http://ca.ncmps.by/

14) National Bank of the Republic of Belarus[143]; 15) Belarusian Finance and Stock Exchange[144].

In Operative Analytical Center (OAC) issued order on PKI 16.10.2012 No 79[145], where the following Certification Authorities are also mentioned: 1) CA of Council of Ministers; 2) CA of Ministry of foreign affairs; 3) CA of Ministry of Communication and Informatization; 4) CA of Commercial banks "and other commercial and state enterprises".

There is no standardized type of e-ID carrier and depending on the security solution, a variety of USB sticks, iButtons, and RFID cards are used.

Georgia. There is no separate legislation regarding e-identity. There is the law on the Public Service Development Agency the former the Civil Registry Agency (PSDA). The PSDA regulates the population registry, and the Ministry of Justice's internal regulations are adopted for all processes related to e-identity. The PSDA is a semi-indepent Legal Entity of Public Law established under the Ministry of Justice which coordinates the issuing of e-identity and all other related processes. It is also responsible for the maintenance of its databases, related to population registry data transfer, and part of various consular services. The PSDA has other functions that are not related to e-identity, but they make it possible to consult other state organizations in the development of similar projects and processes.

The most common online identification method is the username and password. Commercial banks back it up with automated SMS code sending service, and in some cases tokens. The Use of e-IDs as a method of online identification has has a slow uptake, despite the provision of subsidized card-readers for users as a result of several campaigns of the previous government. Currently the PSDA offers a personal username and password for the e-government portal my.gov.ge. A citizen can receive it personally in the Public Service Hall after offering proof of their identity. Other methods of online identification include video links (Skype for notary services) and Georgian citizens living abroad often use video links to request public services remotely.

PKI has been developed in parallel to the development of the eID project. It has been fully operational from 2011. Organizational setup: The PSDA provides the PKI which includes:

- A certificate authority (CA) that issues and verifies digital certificates. A certificate includes the public key or information about the public key;
- A registration authority (RA) that acts as the verifier for the certification authority before a digital certificate is issued to an individual;
- One or more directories where the certificates (with their public keys) are held;
- A certificate management system;

Online Services provided by CA in CRA are:

- E-ID Certificate generation services;
- Revocation status: OCSP & CRL;
- 24/7 certificate revocation of status service, which provide both CRL and OCSP certificate revocation status services;
- Time Stamp – TSA;
- Lightweight Directory Access Protocol-LDAP.

The only existing certification unit is operated by the Civil Registry Department of PSDA. No interest was expressed by any private organizations to establish CA according to the Electronic Document Law of 2008. To give boost to use of eID and electronic certification the government decided to assign this function directly to the CRD without the standard certification process.

The only current carrier of e-ID is a personal ID card but there are plans to introduce business e-ID for organizations.

Moldova: There is no legal act concerning e-identity and there is no coordination unit or ministry established by law with regard to e-identity.

The most common online identification method is the username and password within organizations and a two factor authentication method for systems accessed by outside organizations. As for the second one, the digital certificates are mostly used to identify and authenticate users and to authorize user actions[146]. Organisations that use digital certificates must have their own certification authorities (CA) within the respective organisations. There are also national CAs which issue qualified digital certificates[147].

According to the information provided on the http://pki.sis.md/md/catalog/[148], there are two CA: (1) – the Center for Certification of Public Keys at

143 http://www.nbrb.by/engl/, also see http://preview.tinyurl.com/ogvn2x8

144 http://www.bcse.by/,also see http://preview.tinyurl.com/ke34ox7

145 / О некоторых вопросах функционирования Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь, http://www.pravo.by/main.aspx?guid=3871&p0=T61202222&p1=1

146 http://cts.md/en/services/certification-authoritys-services.html

147 http://pki.sis.md

148 http://pki.sis.md/md/catalog/

the Superior Level[149] (the Security and Intelligence service of the Republic of Moldova is the holder of this registration certificate); (2) the Center for the Certification of the Public Keys of the Public Authorities[150] (the S.E. „Center of Special Telecommunications" is the holder of the registration certificate).

For qualified digital certificates ID-cards[151] and intelligent SIM-cards are used.

Ukraine. There are 3 laws in place: 1) State demographic Register Act (Population Register)[152]; 2) Digital Signature Act[153]; 3) Law of Ukraine "About electronic documents and electronic document management system"[154].

Responsible for Population Register are Migration Service, Ministry of Interior, Ministry of Foreign Affairs, Ministry of Justice and Data Protection Agency. Responsible for identification and usage of digital signature is Ministry of Justice and Administration of the State Service for Special Communication and Information Protection of Ukraine[155].

The most common online identification method is username and password. Also, there is the process of getting the e-signatures.

The development of Public Key Infrastructure was started in 2005 to provide digital signature services. The subjects of interrelations are signatories, users, certification authorities *(ЦСК)*, accredited certification authorities *(АЦСК)*, central certifying authority *(ЦОО)*, supervisory authority.

In April 2013 the decree of the Ministry of Justice "On the Approval of the Concept of reforming the legislation in the sphere of the use of the public key infrastructure and providing of electronic trust services" was past.

In addition, it is planned to create conditions in Ukraine for the recognition of foreign qualified sertificates in Ukraine. Although law in all the countries allows to establish sertification authorities freely, private sector has not shown any interest in that except in Ukraine[156].

There is more than 1.5 million users of electronic signature in Ukraine. Public key certificates are distributed through public telecommunication channels. Information on the valid certificates can be obtained from the official websites of certification authorities. The register of the certification authorities is located on the official website of the central certifying authority[157].

The token/carrier of e-identity is plastic-card.

About the personal identity code

An example of good practice with regard to this issue is found in **Armenia.** Initially there was a Social Security Card, which allocated a unique number to each individual. According to a Supreme Court's Decision an individual was not required to own this card. Therefore two numbers were created: (1) the social security number; (2) a number on a certificate recording an individual's refusal to accept a social security number. The Social Security Number was then converted into a Public Service Number and this is compulsory eventhough it is still possible to take a certificate of refusal. After the birth of an individual a number is allocated to them after their birth is recorded with the the registry service. The hospital does not give them numbers. The system works as follows: 1) a person goes to the registry service; 2) the service sends an inquiry to the police: 3) the police grants a number; 4) the register keeps the number and issues it to the person.

In **Azerbaijan** the Ministry of Justice provides e-services:all information about the personal identification numbers of citizens, as well as for foreigners and persons permanently residing in Azerbaijan.

In **Belarus** the requirement to include an identification number into a citizen's passport is stipulated by the Regulation on the Passport of the Citizen of Belarus based on a Presidential decree on the Documentation of Citizens. A more precise regulation has been implemented by the Ministry of Internal Affairs: Regulation of the Ministry of

149 http://pki.sis.md

150 http://www.pki.cts.md

151 "Electronic identity card - The Ministry of Information Technology and Communications launched the implementation of the electronic identity card, which provides the creation of an integrated information system foran individual's identification and the rendering of electronic services using digital signature. The electronic identity card promotes the use of ICT tools and allows the capitalization of the facilities offered by the information society for a citizen's security, comfort and well-being. http://www.mtic.gov.md/buletin_de_eid_eng/

152 Закон Украины «О Едином государственном демографическом реестре..." и документах, которые подтверждают гражданство Украины, свидетельствуют особу или ее специальный статус» от 20.11.2012 г. № 5492-VI , http://zakon4.rada.gov.ua/laws/show/5492-17

153 акон Украины «Об электронной цифровой подписи» от 22.05.2003 № 852-IV. http://zakon4.rada.gov.ua/laws/show/852-15

154 http://zakon4.rada.gov.ua/laws/show/851-15

155 Закон Украины «Об электронной цифровой подписи» от 22.05.2003 № 852-IV - http://zakon4.rada.gov.ua/laws/show/852-15

156 http://czo.gov.ua/ca-registry?type=3

157 http://czo.gov.ua

Internal Affairs On the Procedure of the Composition of Identification Numbers.

In **Georgi**a the personal identification number serves as the basis of all common identification needs. The Civil Registry Department of PSDA manages the identification system according to its internal regulations and the law on PSDA (formely the Civil Registry Agency).

Electronic services

Development of e-services has been the priority for Eastarn Partnership countries similarly to many other countries in the world. Quite often the plans for introducing electronic services have been put in place before the necessary conditions for their successful implementation have been developed. At the same time, modernisation of public services is clearly an issue where governments can demonstrate that they do something useful for their populations.

As a general observation, we can state that good examples of fully electronic services are hard to come by because of the shortcomings in the e-government infrastructure. However, the intermediate way of developing modern public service centers – the so called „one-stop-shop" approach is well underway in at least Georgia and in Azerbaijan.

Development of e-services seems to be a popular way of implementing development aid by variety of international donors and there are a number of good examples where modern services have been developed despite the shortcomings in overall e-infrastructure development.

In **Armenia** there is an Information Society Development Policy 2010-2012 which implies that all ministries ought to adopt this legislation, develop different e-services, create infrastructure, etc. Meanwhile, in order to provide the legal basis for specific e-services the Armenian parliament has approved changes in the corresponding laws, for example: changes and amendments to the law on taxes, etc.

In **Azerbaijan**, to speed up the implementation of plans for the State Program on the Development of Communications and Information Technologies of the Republic of Azerbaijan in 2010-2012 (Electronic Azerbaijan) the Decree of the President on the Provision of Electronic Services by State Bodies[158] was passed. On the basis of the President's decree on Nov 24th 2011 the Decree of the Cabinet of Ministers of Azerbaijan Republic[159] was legislated, which approved "The Rules for Providing of Electronic Services by Central executive bodies in Concrete Areas" and "List of Electronic Services". The Cabinet of Ministers decree determined that 285 e-services should be provided by 41 service providers in 29 spheres of e-services. The Cabinet of Ministers of Azerbaijan's 17.10.2012 decree No 235 modified The Cabinet of Ministers of Azerbaijan's 24.11.2011 decree No 191 and defined the already 417 e-services provided by 40 service providers.

There are no special legal acts regulating e-services in **Belarus.** The Information Society Strategy[160] contains a definition of e-service: an activity that provides search, retrieval, transfer, collection, processing, storage, distribution and (or) provision of information and the protection of information, carried out with the use of telecommunications and computer technology. Some regulations are included in the Law on administrative procedures[161] and the Law on citizen applications[162]. These legal acts state that citizens and judicial persons can apply to governmental agencies using both the traditional channels (paper and the mail) and the electronic forms or by sending an e-mail to the address of the authorized body or by using the official website of the authorized body in the global computer network - in cases stipulated by legislative acts and decrees of the Council of Ministers of the Republic of Belarus, as well as the decision of the authorized body, unless an individual wants a private meeting with the person concerned (Ch1, article 14 Law on administrative procedures). The same applies to the governmental agencies' answers and decisions (Ch.1, article 27 Law on administrative procedures). These options are supported by the Law on citizens' applications (Articles 3, 25).

158 Executive Order of the President of the Republic of Azerbaijan on the approval of the State Program on the Development of Communications and Information Technologies of the Republic of Azerbaijan in 2010-2012 (Electronic Azerbaijan). August 11, 2010.

159 "Mərkəzi icra hakimiyyəti orqanları tərəfindən konkret sahələr üzrə elektron xidmətlər göstərilməsi Qaydaları"nın və "Elektron xidmət növlərinin Siyahısı"nın təsdiq edilməsi haqqında. Cabinet of Ministers of Azerbaijan. Nov. 24, 2011.

160 http://www.pravo.by/main.aspx?guid=3871&p2=5/32317

161 Закон Республики Беларусь Об основах административных процедур. 28.10.2008 № 433-З. http://www.pravo.by/main.aspx?guid=3871&p2=2/1530

162 18. 07.2011 № 300-З / Закон Республики Беларусь Об обращениях граждан и юридических лиц http://www.pravo.by/main.aspx?guid=3871&p2=2/1852

The delivery of e-services are not regulated by a single law in **Georgia.** There is a general reference in the Law on Electronic Document and Electronic Signature. All other regulations related to the deployment and maintenace of e-services are internal acts of the service providers (Civil Registry Agency/PSDA, Revenue Service and others). It is planned to include the regulation of e-services in an e-government act that is currently under development.

E-services are regulated by a number of acts in **Moldova,** including the Government Decision no.330 of 28 May 2012 on the Creation and Administration of the Unique Governmental Public Services Portal[163], the Government Decision no.657 of 05 September 2012[164] on the approval of the Regulation on the administration of the content of the unique governmental portal for public services and the integration of electronic public services through this portal and the completion of another one that the governmeny has decided to create.

E-services are also regulated by a number of acts in **Ukraine**[165].

E-government portals

In all these countries the principle of the one-stop-shop has been implemented to provide information and e-services. Below there are some examples of this process which is mainly based on the use of government portals.

In **Armenia** the website www.e-gov.am[166] brings together the electronic governance tools and databases of the Armenian state agencies as well as providing a comfortable environment for their use. This is a platform that has links to all other services that are currently provided electronically.

In **Azerbaija**n the EHDIS portal mediates access to 152 e-services from 38 central state agencies, the main provider is the Ministry of Taxes. A success story is www.asan.gov.az , which unifies a number of services, provided by the different Government Bodies on a single platform and the number of services is still growing. In Azerbaijan an e-service register has also been formed by a presidential decree.

In **Belarus** e-services are drawn together through the national portal for e-services[167].

The my.gov.ge portal has been developed as a one-stop-shop, offering access to all state electronic services in **Georgia.** Although according to the law, until recently, its services were only available through theuse of an e-ID and the actual use of it was quite low (only 3 000 registered users). Users preferred to register on the e-services providers' websites using other identification tools and utilize the availiable services. An online electronic payment facility is integrated into the my.gov.ge and some sub-portals. There is a popular Justice Hall website psh.gov.ge established under the Ministry of Justice offering the e-services of various agencies. Another example is the Revenue Service tax administration and reporting portal that operates separately, but it is mandatory to use this for tax-reporting by all registered (and functional) organizations.

The Unique Governmental Portal of Public Services in **Moldova** is servicii.gov.md[168]. The e-payment gateway will be soon be availble through this portaal.

In **Ukraine** a common official e-service portal is in the process of being created[169].

Examples of best e-services

Armenia: From January 2010, an Electronic Tax Filing system was introduced which aims to simplify and automate the process of submitting tax reports. In addition to saving taxpayers' resources and time the system also minimizes the taxpayers and the assessors contact. This tool is especially useful for people living in distant and remote areas of Armenia. The e-business register and cadastre are also very new.

In **Belarus** the best example of e-service is the

163 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=343406

164 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=344701

165 Постановление Кабинета Министров Украины «О мероприятиях по созданию электронной информационной системы «Электронное правительство», Закон Украины «О платежных системах и переводе денег в Украине», Закон Украины «Об основних направлениях развития информационного общества в Украине на 2007-2015 года», Распоряжение Кабинета Министров Украины «Об одобрении Концепции развития электронного управления в Украине», Распоряжение Кабинета Министров Украины «Об утверждении плана мероприятий по реализации Концепции развития електронного управления в Украине», Постановление Кабинета Министров Украины «Об утверждении Порядка ведения Реестра административных услуг», Постановление Кабинета Министров Украины «Об утверждении Порядка ведения Единого государственного портала административных услуг», Распоряжение Кабинета Министров Украины «Об одобрении Стратегии развития информационного общества в Украине» etc.

166 https://www.e-gov.am/en/

167 Единый портал электронных услуг http://portal.gov.by/

168 https://servicii.gov.md/

169 http://poslugy.gov.ua/

State Real Estate Registry[170], which provides electronic documents from the State Real Estate Registry in real time and the public Cadaster maps.

The best example of e-service in **Georgia** which received a UN Public Service Award is the Georgian electronic procurement system[171],[172]. Another example is the provision of Notary services via skype video-link offered to Georgian citizens living abroad, making it possible for them to authorize the delivery of services remotely.

In **Ukraine** in 2013 the best e-services were evaluated[173],[174].

Open Government, e-Democracy and e-Participation

In recent years governments around the world have realized the importance of ICT for a more citizen centric form of governance. The Open Government Partnership[175] (OGP) initiative was launched in the international arena in September 2011 with the aim of encouraging governments to advance transparency, accountability and their citizens' engagement in public policy via the use of ICT. Since then, OGP has grown from 8 countries to the 62 participating countries coming from different continents of the Globe.

In order to join the OGP, countries must first meet pre-defined eligibility criteria. To reach this threshold each participating country is obliged to develop an OGP action plan in open dialogue with their Civil Society Organizations (CSOs). The action plan must contain concrete commitments to be implemented within a predetermined time contained in the plan.

Out of the six Eastern Partnership countries five of them - Armenia, Azerbaijan, Georgia, Moldova and Ukraine – have met the eligibility criteria and joined the OGP in 2012. In these countries there is a genuine interest in the advance towards an open form of governance but a lot of effort is needed to reshape their governmental processes and their administrative culture. As to the Belarus, the country is below the OGP eligibility threshold due to its opaque governmental processes and the lack of any real involvement of civil society organisations in their public affairs.

A recent study coordinated by the Ukrainian Institute for Public Policy (Kyiv) „The OGP Process in EaP Countries and Russia: Where are we now and where do we go further?"[176] presents a comprehensive overview of the state of affairs relating to the implementation of the OGP in these countries. The focus of our study is not specifically the OGP but it is instead an analysis of the existing preconditions for transparent and participatory governance and the extent to which e-democracy/e-participation are integrated into the strategic documents in the Eastern Partnership countries. Our main findings are summarized below.

Access to the public sector information

Wide access to the public sector's information is an important precondition of transparent and accountable government and an important tool in the fight against corruption. In many countries the right to have access to the information held by the public sector is provided for through the constitution and further elaborated through specific laws. Since access to information will be significantly broadened through the use of ICTs, it is important to harness the technology for the release of the public sector information.

Our review shows that all the Eastern Partnership countries have laws which regulate the legal regime concerned with public sector information. This has been put in place either through specific laws (Armenia, Azerbaijan, Moldova, Ukraine) or contained in the framework of a more general law (Belarus, Georgia). The level of elaboration of these laws differ considerably and may require further refinements in order to meet internationally recognized legal standards of freedom of information including the Council of Europe Convention on Access to Official Documents[177].

Through the questionnaire, we established that all Eastern-Partnership countries pay attention to the publication of information on the Web. The regulations in place demand from public bodies to have websites and to publish variety of information

170 http://gzk.nca.by; http://oz.nca.by; http://map.nca.by

171 http://procurement.gov.ge/index.php?lang_id=ENG&sec_id=10&info_id=800

172 http://transparency.ge/en/post/report/georgia-s-e-procurement

173 http://e-services.dp.gov.ua

174 http://www.ap.volyn.ua

175 http://www.opengovpartnership.org/

176 http://uipp.org.ua/uploads/news_message/at_file_en/0071/87.pdf

177 http://conventions.coe.int/Treaty/en/Treaties/Html/205.htm

online.

The implementation of a right to information is a complex process as it inevitably involves a large number of stakeholders. This process needs coordination and oversight. Our survey indicates that there are no specialized state level institutions dealing with freedom of information in the Eastern Partnership countries although the Human Rights Commissioners in Azerbaijan and Ukraine are empowered to exercise an oversight function in this area.

In conclusion, the legal ground for the implementation of a freedom of information has been established in all Eastern Partnership countries but the respective laws may need further refinement in order for them to meet the higher international standards. The coordination and oversight mechanisms should be the main target of activities to achieve the required tangible results for the respective societies.

Armenia. Access to public sector information is regulated by the Law on Freedom of Information[178] adopted by the Parliament in September 2003. The Law regulates the relations connected with freedom of information, defines the powers of persons holding (possessing) information, as well as the procedures, methods and conditions that must be met to secure information. The law applies to the activity of the state and local self-government bodies, state offices, organizations financed from the state budget, as well as private organizations of public importance. Organizations with public functions are those which either have a monopoly or have a dominant position in the market, as well as private organizations providing public services.

Every individual has the right to address an inquiry to an information holder to assess the information held about them and/or get the information sought by them as is laid out in the law. The inquiry may be either written or oral. The law stipulates that, as a rule, the information asked for should be provided within 5 days after the filing of the application. The cost to be paid for this information, if applicable according to the Law and Government Regulation, cannot exceed the costs of providing that information.

The person responsible for the implementation of the Law is the head of the information holder or an official appointed by the head. There is no state authority to monitor the implementation of the freedom of information by the information holders.

All governmental bodies are required to have an official website providing information about their activities. The maintenance and content of the websites is regulated by the Decision of the Government "The requirements of government organizations and local government authorities official websites" enacted in 2009[179]. This regulation also provides the list of the obligatory content which should be displayed on the website. This includes the governing body structure, objectives and functions of the separate units, the legal address, phone numbers and other requisites, the number of employees, the state government phone directory service, and information about state government employees and their supervisors etc.

As for the feedback features of the website, there is no specific requirements for that in the Government regulation. The main means of communication are email-addresses and phone numbers.

Azerbaijan. The right to obtain information from the public sector is regulated by the Law on access to the Information[180] adopted by the Parliament in 2005. The Law determines the terms, procedures and forms of information access, as well as the grounds for denial by the information owner from submitting such information; the limitations placed on access to public information and the procedures for disclosing and presenting the information that is not regulated by other laws and the procedures that organizethe process of acquiring the information. The law applies to state bodies and municipalities, other legal entities implementing public functions, as well as private legal entities and individuals engaged in the spheres of education, healthcare, the cultural and social sphere regulated by legal acts or contracts.

The submission of oral and written requests to the public body is the main method used by citizens to access information held by the public sector. The request for information has to be executed as soon as practicable but no later than 7 working days. If the requested information looses its worth and value in this period, the request ought to be processed immediately or, if that is impractical, no later than 24 hours after the request was made. Access to public information is free, but charges can be made for the service provided the charge does not exceed the actual expenses incurred in the preparation and presentation of the information.

178 http://www.foi.am/u_files/file/legislation/FOIeng.pdf

179 http://www.arlis.am/DocumentView.aspx?docID=52559 (in Armenian)

180 http://www.stat.gov.az/menu/3/Legislation/information_rules_en.pdf

The Law has a special chapter regulating proactive information disclosure in order to more easily and efficiently meet the public interests and lessen the number of multitudinous requests for information. The Law provides for a long list of information to be made available online and instructs the information owners to ensure the effective operation of the Internet information resources.

The head of the information owner has direct control over the implementation of the law. The Law also provides for a special institution with monitoring powers - Authorized Agent on Information Matters - but in reality no separate institution has yet been established, but a Presidential Decree from August 2011, gave the Commissioner for Human Rights[181] the power to exercise supervision over the implementation of the Law on Access to Information.

Belarus. There is no specific law on the freedom of information. General aspects of the legal regime of public sector information are regulated by the Law on Information, Informatization and Information protection[182] enacted in 2008. In this law public information is defined as information to which access and distribution is unlimited and it provides a list of information to which access cannot be restricted: information on the rights, freedoms and legitimate interests of individuals and legal persons and the order of realization of these rights, freedoms and legitimate interests; the activities of state bodies, public associations; the legal status of public bodies, except for information to which access is limited by legislative acts of the Republic of Belarus; emergencies, environmental, sanitary and epidemiological situations, hydro meteorological and other information, concerning the state of public safety; health, demography, education, culture, agriculture; crime, as well as violations of the rule of law; information about benefits and compensation provided by the state to individuals and legal entities; information about the size of the gold reserves; generalized indicators of external debt; health officials who hold positions that are included in the list of top government postsof the Republic of Belarus; Funds accumulated in open libraries and archives, information systems, government agencies, individuals and legal entities established (intended) for the information service of individuals.

The information for which access is restricted includes information about the private lives of individuals and their personal data; information constituting state secrets; information constituting commercial or professional secrets; information contained in cases of administrative offenses, materials related to the prosecution of criminal cases before the court before the case is adjudicated; and other information to which access is limited by legislative acts of the Republic of Belarus.

The Law also stipulates that state information systems should be created toensure that the public has access to the available information. The law also states that steps must be taken to ensure the objectivity, integrity and reliability of the available information. There must also be a high level of interoperability between the various government agencies and an improvement in the effectiveness of the asministrative functions of the state agencies (Charter IV).

The Law on Information, Informatization and Information is currently under revision in the Belarus Parliament[183].

All government organizations are required to have websites according to the Presidential Decree (01.02.2010) on measures on improvement of national segment of the Internet[184]. The regulation contains also the list of information government agencies should provide online including procedures concerning citizens' applications.

The requirements to official websites are further elaborated by the Council of Ministers Regulation (29.04.2010) on Requirements to the contents of the governmental websites[185]. Among other things the websites should be accessible free of charge, be user friendly and provide forms of feedback.

Georgia. Access to public information is regulated by the General Administrative Code[186]. Chapter 3 of the Code is entitled "Freedom of Information." It sets a general presumption that information that is kept, received or held by a public agency should be accessible regardless of the form that the information takes.

The main method of getting access to public information is through a written request to the public authority. The agency must respond immediately and there can only be a delay if the information that is being requested is either kept in another locality,

181 http://www.ombudsman.gov.az/view.php?lang=en

182 http://www.pravo.by/main.aspx?guid=3871&p2=2/1552

183 http://www.osce.org/fom/104711

184 http://www.pravo.by/main.aspx?guid=3871&p2=1/11368 (in Russian)

185 http://www.kasper.by/help/postanovlenie-soveta-ministrov-645/ (in Russian

186 http://unpan1.un.org/intradoc/groups/public/documents/untc/unpan004030.pdf

or consists of a large number of documents, or is kept at another agency. Fees can only be chargd for the costs of copying. The law also sets rules on the access and use of personal information.

Several attempts to introduce a Freedom of Information Act have failed until recently. Currently the Act is being drafted by various civil society organizations and several important steps have been taken with regard to increasing government transparency.

The government decree on Proactive Publication of Public Information and Electronic Requests (01.09.2013) for its Disclosure[187] has mandated that all government agencies must publish mandatory list of information and accept electronic requests for information. The public institutions also are responsible for the accuracy, authenticity and periodic updates of the electronically published information. However this decree is not applicable to President's Administration and local government institutions.

There are opportunities for requesting public information electronically on some of the state agencies websites, for example requests to the courts (court.ge) but the identification of the applicant is conducted through the scanning and the uploading of a signed pdf document.

There is no official authority at the state level to oversee access to public information. Overall policy development in the field is the responsibility of the Ministry of Justice. A special unit will be created to examine and redirect requests for public information disclosure to the responsible agencies. All the state organizations are obliged to nominate a person who is to be responsible for the provision of information to the public.

The new regulation that came into force from September 2013 obliges state organization to publish certain list of public information on their websites which in practice implies an official requirement to have a website. The mandatory information list is laid out in the regulation (Structure of Administrative Organization) that contains a description of the functions, laws and regulations governing the activities of Administrative Organization, annual reports, strategies, concepts and action plans, names, CVs, photographs of the Administrative Organization, full contact details of the Administrative Organ, job opportunities, along with the regulating acts, the number of employees according to categories, an annual plan of state purchases, with detailed information about actual purchases indicating the costs; advertising expenses and real estate property sales/acquisition budget, total salaries and bonuses for the management and for other staff, the expenditure on business trips, fuel, cars and their technical maintenance, communication costs; grants received and awarded. Information about the services offered by the Administrative Organization along with its respective fees should also be published online.

Moldova. Access to the information held by the public sector is regulated by the Law on Access to Information[188] enacted in May 2000. The Law aims to create and establish a general normative framework on the access to official information. According to the Law the official information holders are central and local public authorities and their subordinate institutions, non-profit organizations founded by public bodies at the state and local level and individuals and legal entities that are empowered to provide public services, including information services.

One of the main methods of securing access to public sector information is through either written or verbal requests. It is basically free of charge but the public entity may charge a fee only if a considerable amount of work was required to provide the requested information but it should not be higher than the reasonable cost for making the requested information available. The law also states that the information must be disclosed no later than 15 working days from the time the request was submitted.

The responsibility for ensuring free access to the official information lies with the information holder. The law requires all public entities to appoint and train information officers and to establish internal rules for the implementation of the law. When a person deems that his/her legitimate rights or interests have been violated by the information providers, he/she may contest these acts extra judicially or directly in court. At the state level, there is no special authority responsible for the oversight of the access to public sector information.

According to the Government Decision on Official Internet Pages of the Public Institutions[189] all administrative authorities are from April 2012 obliged to have websites. The document prescribes

187 http://www.right2info.org/resources/publications/laws-1/laws_georgia_electronic-request-and-proactive-publication-of-public-information-government-decree_2013_eng

188 http://ijc.md/Publicatii/mlu/legislatie/law_on_access_to_information.pdf

189 http://lex.justice.md/viewdoc.php?action=view&view=doc&id=342699&lang=2 (in Russian)

the requirements with regard to the content, style and designs of the web pages as well as the rules of administration. The mandatory information that public administrative authorities should publish on their web sites is quite extensive including declarations of income and property of the management of the public administration and information to ensure transparency in decision making.

In addition to their official websites, the authorities have started to release information on the Official Governmental Portal www.moldva.md and on the Open Data Portal www.date.gov.md. On the 26 December 2012 the Law on Re-use of Public Sector Information[190] was adopted with the aim to harmonize the Moldovan legal code with the respective European laws[191]. Recently the Government of Moldova approved methodological provisions for application of the Law [192].

Ukraine. The Law On Access to Public Information[193] was adopted by the Verkhovna Rada in 2011. The aim of this law is to ensure the transparency and openness of government agencies and to provide mechanisms for the realization of the right of every individual to secure access to public information. The Law establishes the proceduresfor the accessing information possessed by government agencies and other providers of public information. According to the Law the information providers are government agencies; legal entities financed by national or local budgets; legal entities with powers delegated to them by the government or local self-government for the provision of public services; commercial entities that have dominant positions in the market through special or exclusive rights, or are natural monopolies with regard to the supply and the provision of goods and services.

The Law defines two categories of information with different access modes: open information and restricted information and provides the grounds for the restrictions on access to certain information (secret or confidential information). Access to open information is secured by the publication of information through the public media, including official web-pages and by the provision of information on request. Information providers are responsible for appointing and organizing the work of information officials. The Human Rights Commissioner is empowered to exercise oversight over the implementation of the Law and information providers have to submit an annual report on their compliance with information requests to the Human Rights Commissioner.

All public agencies are required to have websites and obligatory content is defined by the Resolution of the Cabinet of Ministers of Ukraine "On the Procedure for publication on the Internet of information about the activities of the executive branch"[194] of 2002.

The state platform to submit electronic applications of citizens and requests for public information[195] was launched on 2012.

Involvement of non-governmental sector in policy making

Open government presupposes a close collaboration between the government and civil society. It requires that the Government as a political body and all the other public institutions are prepared to engage with citizens and listen to their concerns and advice. ICT provides new opportunities to enhance a government-citizens dialogue. However, the premise is based on the assumption that the country already has some enabling legal framework and administrative practices in place for the involvement of non-governmental partners in the decision making processes.

Te goal of the questionnaire was to come to some understanding of the overall situation of NGO involvement in law drafting since legislative openness is of fundamental importance for participatory policy making.

The survey indicates that the basic conditions for government-citizens interaction in the law making process are established in all Eastern Partnership countries except Belarus, where authoritarian rule prevents any open dialogue with civil society. Legal frameworks for legislative openness need to be further improved in order to create the appropriate mechanisms for public consultations and the engagement of the interest groups in the drafting of law. Moldova may be considered as a flagship country for legislative openness because the transparency in the decision making processes is enshrined in law.

190 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=347200 (in Rumenian)

191 http://ec.europa.eu/digital-agenda/en/legal-rules#summary-of-the-directive

192 http://lex.justice.md/viewdoc.php?action=view&view=doc&id=350277&lang=2

193 http://www.article19.org/data/files/pdfs/laws/ukraine-the-law-on-access-to-public-information.pdf

194 http://zakon4.rada.gov.ua/laws/show/3-2002-%D0%BF (In Ukrainian)

195 http://z.gov.ua/

Central consultative institutions that aim to facilitate government-citizen dialogue have been established in Azerbaijan, Georgia, Moldova and Ukraine. In the countries which joined the international OGP initiative, civil society groups have been given the impetus to better organize themselves in order to contribute to the OGP process. Currently the OGP platform presents a good mechanism to renew a government civil society partnership and cooperation for societal progress.

Online citizen engagement in policy making is still in the exploratory stage in the surveyed countries but Moldova and Ukraine are a step ahead of the other countries with the launching of an online platform for public consultations.

Armenia. According to the Law on Legal Acts[196] the drafting of legal acts is carried out with the participation of the non-governmental sector (businesses, NGOs, active citizens). The State or local government, state or local government agencies or entities may form a committee of employees and experts of the body to develop a legal draft and depending on the nature of the proposed law those who can be involved in this process can include individuals representating scientific organizations, and other interested bodies and organizations. The law-making body may also delegate the development of a normative legal act to businesses, NGOs or individuals and it may also delegate the preparation of alternative projects to multiple institutions, businesses, or individuals. The law-making body also has the right to declare a competition for the best project. Legal entities and individuals may on their own initiative develop and submit their proposals to the appropriate law-making bodies that draft regulations. Draft laws and resolutions designed by legal entities and individuals in accordance with the Constitution of the Republic of Armenia can be presented to individuals or bodies with the right to initiate legislation.

There is also the Government decision of March 2010 on the Procedure for the the organizing and managing of public discussions[197].

There is no central governmental portal to hold online public consultations.

Azerbaijan. The country has a legal framework that provides the basis for citizen participation in governance. From April 2008 there exists the presidential decree: State Council for the NGO support,[198] which brings together representatives of all the NGOs. The involvement of the nongovernmental sector in law drafting is mostly based on the roundtable meetings arranged by the Ministers where stakeholders can state their positions on different topics.

The Draft Law on Citizen Participation, which would create mechanisms for greater government cooperation with NGOs, is still pending in the Parliament[199].

There is no central governmental portal for online public consultations.

Belarus. The non-governmental sector has very few real opportunities to influence the law-drafting process. At present there is no regulation on the establishment and the operation of public councils, public discussions and there are no mechanisms for public participation in the development and implementation of national plans, programs, and regulations (see NGO Law Monitor: Belarus[200] and the analysis "Public Councils in Belarus"[201]).

There is no central governmental portal for online public consultations.

Georgia. Active NGOs and watchdog organizations are directly participating in law-drafting under the framework of the Anti-Corruption Council cooperation and through direct consultations with the Ministries and other Government agencies. There is an opportunity to leave comments on enacted legislation through the official web-page matsne.gov.ge[202] – Official Gazette of Ministry of Justice for publishing legislation.

Moldova. The Republic of Moldova is one of the few countries where the legislative process is regulated by law - The Law on Transparency in the Decision-making Process[203] adopted in November 2008. The Law sets out the framework to ensure transparency in the decision-making process within the central and local public administration authorities, and regulates their relations with citizens, organized nongovernmental partners with the aim of enabling participation in the decision-making process.

The Government–Civil Society dialogue is facilitated by the institutionalized cooperation platform

196 http://www.parliament.am/legislation.php?sel=show&ID=1280&lang=rus#3 (In Russian)

197 http://www.arlis.am/DocumentView.aspx?DocID=57300 (In Armenian)

198 http://cssn.gov.az/en/

199 http://www.icnl.org/research/monitor/azerbaijan.html

200 http://www.icnl.org/research/monitor/belarus.html

201 http://kamunikat.org/download.php?item=21247-1.pdf&pubref=21247 (in Russian)

202 https://matsne.gov.ge/index.php?lang=en

203 http://www.right2info.org/resources/publications/laws-1/Moldova-Law%20on%20transparency%20in%20the%20decision.doc/view

National Council for Participation[204] through various working groups including one working on the theme of egovernment.

The citizen participation portal www.particip.gov.md was launched in 2012. The platform was established through the joint efforts of the State Chancellery and National Council for Participation.

Ukraine. The Coordinating Council for the Development of Civil Society was established by President of the Republic in 2012. The Council has approved a public policy strategy to promote the development of civil society in Ukraine. The majority of local authorities have developed regional programs to promote the development of civil society.

The Cabinet of Ministers of Ukraine created in 2012 a consultative and advisory body - the Council of the Chairmen of public councils at the Government in order to strengthen their interaction with the representatives of civil society.

A separate mechanism has been established for online consultation with the public by government website "Civil Society and Power"[205].

E-Democracy/open government policy and best practices

E-democracy and open government are interrelated concepts aimed to promote democracy of 21st century. E-democracy means the support and enhancement of democracy by use of ICT. It is interlinked with traditional democratic processes, so as to widen the public access to the political and administrative processes. The open government approach has the same goal by stressing the transparency, accountability and citizen participation in governance.

In order to facilitate e-democracy deployment in the Member States the Council of Europe enacted the Recommendation on e-Democracy[206] in February 2009. This document stresses that „e-democracy is closely linked to good governance, which is the efficient, effective, participatory, transparent and accountable democratic exercise of power in electronic form, and includes informal politics and non-governmental players".

The Open Government Partnership initiative goes further from general principles and recommendations. The requirement is that the participating government elaborate concrete action plans to implement the principles. This kind of "tactical approach" is certainly more purposeful if government already has wider policy in place how to use ICT for better democracy. From this perspective the question was asked is e-democracy addressed in any of the policy documents in the countries under survey.

It appeared that presently the Open Government Partnership commitments and action plans are the main policy instruments related to the use of ICT for development of democracy. However, the recent Strategy of Information Society Development in Ukraine pays due attention to e-democracy thereby creating interlink with the government OGP commitments. It may be envisaged that participation of countries in the OGP process will have positive effect on the governments to prioritize use of ICT not only for service provision but also for e enhancement of democracy. It is unfortunate that Belarus is not part of this process.

Armenia. E-democracy is not directly mentioned in any government policies yet. Though there is an e-society development policy the e-participation and e-democracy development is not reflected in this document.

However, as Armenia joined the OGP initiative the government has adopted the OGP Action Plan[207], which may be considered as an important step towards the use ICT for strengthening democracy.

One of few examples of e-participation in Armenia is the iYerenan project[208] initiated and carried out by the Yerevan Municipality.The iYerevan website is a new platform to develop, discuss and implement projects aimed at the improvement of the city of Yerevan. It allows them to receive suggestions from the citizens and provides them with a way of getting to know their opinions. This initiative of the Yerevan Municipality is a new way for a dialogue with the citizens, which allowsthem to enter into direct communication with the municipality and to discuss suggestions for the improvement of the city in real-time. The website also gives information about the activities and projects that have already been carried out. The suggestions that were made with regard to the improvement of the city and received the highest levels of suport from the citizens, will be discussed in the respective depart-

204 http://www.cnp.md/en

205 http://civic.kmu.gov.ua/consult_mvc_kmu/news/article

206 http://www.coe.int/t/dgap/democracy/activities/ggis/cahde/2009/RecCM2009_1_and_Accomp_Docs/Recommendation%20CM_Rec_2009_1E_FINAL_PDF.pdf

207 http://www.opengovpartnership.org/country/armenia/action-plan

208 http://www.iyerevan.am/am/

ments of the Yerevan Municipality and will then be implemented if possible.

Azerbaijan. The main policy document is the Republic of Azerbaijan Open Government Initiative National Action Plan 2012-2015[209]. The aim of the country through its joining the OGP is the enhancement of transparency in its state institutions, the provision of accountability, the enlargement of public participation and the application of the new technologies. The Ministry of Communication and IT is tasked with developing and applying the specific activities required for e-democracy and e-participation in the country.

The responses to the Questionnaire do not provide any evidence of success with regard to these goals.

Belarus. E-democracy is not mentioned in the official policy documents. There are some non-governmental e-participation watch-dog initiatives: the monitoring of e-procurement;[210] the monitoring of the quality of the roads.[211] .

Georgia. The e-Georgia strategy and action plan 2014-2018[212] is presently in the process of approval by the Government. The document contains thematic chapters prioritizing Open Government and e-participation. The four main areas of e-participation are identified: feedback on e-services, the (co-) design of e-services, open data, transparency and open government and decision-taking and policy making.

Georgia's OGP Action Plan 2012 – 2013 aims to improve the public services and make them available online. A commitment has also been made to create new platforms for direct citizen engagement that will make public participation possible in the legislative, executive and judicial branches of the government.

In general e-participation initiatives are quite scarce. One of the best examples is the Fix My Street project[213], run by Transparency International. It allow users to electronically report the specific problems near their locations – on their streets and send requests to the local authorities to fix them. The project is being implemented in the 4 largest cities.

Moldova. The "Digital Moldova 2020" Strategy[214] was approved by the Government on September 19, 2013. The document does not directly address the use of ICT for the strengthening of democracy and the development of open government. The most important platform in this respect is the participation of Moldova in the international OGP initiative. The Moldova's OGP Action Plan 2012 -2013[215] set the objective of strengthening public integrity by increasing transparency in its governance through the creation of a participative decision-making process and citizen participation. At the moment the progress of the implementation of the Action Plan is being evaluated by the Independent Reporting Mechanism[216]. The assessment of the implementation of the Action Plan as a civil society initiative indicates that there has been som progress towards this goal but that the progress is slower than planned[217]. The e-Government Centre and the State Chancellery are the key actors responsible for the Open Government Agendas of the Moldovan Government. An OGP Action Plan for 2014 – 2015 is now under preparation.

Ukraine. Strategy of Information Society Development in Ukraine[218] law enacted on 15.05.2013 contains a special subdivision concerning "E-democracy". The main directions of the development of e-democracy are:

- The active use of new information and communication technologies for the participation of citizens and organizations in the formulation and implementation of public policy, including the support of pilot online projects;
- The forming of a network communication culture based on partnerships;
- The recognition of the important role of the media as a platform for public forums and debates, in which citizens are able to defend their social interests;
- The creation and implementation of an integrated data-processing system " e-Parliament of Ukraine", which will provide access to information on parliamentary activities and documents, and also stimulates the holistic development of an equitable information society from the use of modern

209 http://www.opengovpartnership.org/country/azerbaijan

210 http://editorfm.blog.tut.by/

211 http://belyama.by/

212 http://dea.gov.ge/uploads/20130706%20eGeorgia_%20final_DRAFT%20for%20public%20consultation.pdf

213 http://www.chemikucha.ge/ka/

214 http://www.mtic.gov.md/img/d2011/proiecte/md2012/Digital_Moldova_2020_draft_Strategy_Eng-01.04.2013.pdf

215 http://www.opengovpartnership.org/country/moldova/action-plan

216 http://www.opengovpartnership.org/about/about-irm

217 http://www.opengovpartnership.org/blog/olga-crivoliubic/2013/10/08/first-assessment-progress-and-problems-ogap-implementation-moldova

218 http://zakon2.rada.gov.ua/laws/show/386-2013-%D1%80

information and communication technologies and standards;

- The establishment of a National Centre for e-government system interactivity with citizens in the existing social network " We develop e-government";
- The promotion of cooperation between government and civil society institutions, experts and international partners in the drafting of regulations, standards and the implementation of pilot e-democracy, human rights, and the rule of law.

Ukraine's commitments under the OGP initiative are presented in their Government Action Plan[219] . It addresses the use of e-government technologies and the promotion of electronic democracy, among others suggestions. The monitoring report "Open Government Partnership Initiative: Civic Audit of the 1st Year of Implementation in Ukraine"[220] conducted by civil society organizations, shows that more attention should be paid to the mechanisms required for the implementation of the Action Plan.

Local governments of the Ukraine are also interested in the useof ICT for the provision of public services and the development of e-participation platforms. There exists a central portal „Your city"[221] - http://tvoemisto.org.ua/ where citizens can submit notices about the problems they want the authorities to resolve.

Conclusions, recommendations

There is a wide international consensus shared by the EU member nations that transparency and openness are good for both democratic developments and economic growth. Indeed, there are speculations that open data, i.e. machine accessible data in widely recognised formats might be as vital for information economies as oil was for the industrial economies.

The EU has one of the world's most advanced regulatory regimes for information society developments where both the regulations for the use of informatation technologies and the regulations for the protection of data are equally balanced. Since the internet does not recognise national borders and networks have become part of the everyday life both in the EU and in nations at our borders, it is imperative that we should promote these regulations not only in the narrowly defined area of questions concerning „data protection" but rather through the framework of the OGP process.

We would recommend that the Eastern Partnership countries be encouraged to take their commitments to the OGP seriously and that the EU should support this through their various programs. We also suggest that the EU regulations concerning the development of information societies should also be promoted and suggested for implementation in the EPC and that the EPC states should develop their national plans for the development of e-government and that the regulations should take into account the Digital Agenda of the EU and the basic principles and regulations concerning data protection and the re-use of public data.

Since the EPC are also member nations of the Council of Europe, the norms of the Council of Europe in these areas should be actively adopted by these countries.

Cyber Security and Data Protection

Cybersecurity

There are no real differences between countries with regard to their Cybersecurity arrangements. Whether it concerns National Cybersecurity, The security of government databases or personal data protection, every country is increasing its capabilities in these areas. Due to the fact that cybersecurity is a relatively new security area, countries are advancing step by step in this field. Some of the countries have developed some areas faster and the other areas, but all of them are following the same logical steps to improve cybersecurity.

It is also noticable that there is a clear relationship between the development of cybersecurity and the general development of an information sociey and e-governance. The implementation of new e-solutions in the country drives the improvement of cybersecurity and that there is often a timelag between these developments. The implementation of new e-services occurs and then some time later the cybersecurity arrangements follow. In many cases, but not always, these developments are tied to a significant security problem that has already taken place in the country. The global attention to Cybersecurity in recent years has been responsible for making the topic a major security concern.

219 http://www.opengovpartnership.org/country/ukraine/action-plan

220 http://ti-ukraine.org/system/files/docs/news/ogp_final_report_eng.pdf

221 http://tvoemisto.org.ua/

National cybersecurity

In the area of National Cybersecurity the countries were asked to answer to the following questions:

1. Is cybersecurity considered as an important security area and linked with other security areas and information society development process?
2. Are government leaders accountable for devising a national cybersecurity strategy and fostering local, national and global cross-sector cooperation?
3. Are there approved cybersecurity and data protection policies?
4. Have you developed a national cybersecurity framework that defines minimum or mandatory security requirements on issues as risk management and compliance?
5. Are there nominated government organizations that are responsible for cybersecurity and data protection in general?
6. Do you have a National Cybersecurity Focal Point – a multi-agency body that serves as a focal point for all activities dealing with the protection of the nation's cyberspace against all types of cyber threats?
7. Do you have a Cyber Incident Response Team (CIRT / CERT) available – an organization, which analyses cyber threat trends, coordinates responses and disseminates information to all the relevant stakeholders?
8. Has your country set up a separate unit to investigate cyber crimes?
9. Have you developed a national cyber security awareness and educational programme? Do you have programs available for ICT and cyber security professionals?
10. Do you have a meaningful public-private sector cyber security partnership format available?
11. Have you developed a national framework for international cooperation?

A general overview of the situation is given in a table on the next page.

Armenia. In the strategic policy documents the importance of cyber security is not mentioned. However, on the official website of the Armenian Permanent Mission in NATO it is stated:

"Armenia is developing policies and capabilities in the area of cyber security and is to shortly establish a State Cyber Security Committee. Armenia is keen to develop cooperation with NATO in this domain … A draft decision on the "creation and establishment of the Statute of the State Cyber Security Committee has been developed and submitted for discussion."[222]

Armenia has developed an Information Security Policy. The president of Armenia approved this document on 25th of July in 2009. The document defines national interests in information security, identifies the types and sources of threats, the main challenges and methods to provide information security[223]. Also, the Armenian e-Society Development Policy touches on the cyber security field. In Appendix 1 of the document it defines the scope of cyber security. The Armenian Government approved the policy on the 22nd of December in 2011.

With regard to the political attention being paid to cyber security, the answers in the study questionnaire do not specifically identify the role of the government leaders in the area of cyber security. However, processes have been initiated in order to ensure better coordination in the field of fighting cyber crime.

In Armenia, the National Security Council has the general responsibility for security and they are responsible for cyber security and information security among other areas of security. There is no specific organization in Armenia, whose main responsibility is for data protection and/or cyber security.[224]

The answers to the study questionnaire indicate that there is no specific national agency focused on cyber security and that there is no specific state agency that is responsible for cyber security. According to the available information, it is most logical to conclude that the National Security Council is operating as the focal point for cyber and data security. The Prosecutor-General's Office has a special department dealing with cyber crimes and it appears that this department is serving as the focal point for this specific issue.

Armenia has not yet developed a strategy for dealing with cybercrimes or even defined what should be the priority areas for cyber security. The particular approaches towards cybercrime security have been included in the document "The Concept on Telecommunication Security". This document defines the detection of new cybercrimes and the enhancement of the fight against cyber crimes as one of its objectives. The lack of a clearly defined action plan means that it is not yet clear what has

222 http://www.nato.mfa.am/en/defence

223 http://www.arlis.am/DocumentView.aspx?docID=52559

224 http://www.nsc.am/index.php?lang=eng

		ARMENIA	AZERBAIJAN	BELARUS	GEORGIA	MOLDOVA	UKRAINE
1	Importance of the area	Regular	Important, Ministry of ICT is responsible for the implementation of policy	Important, it is part of national ICT development program	Very important, it is part of national security	Important, it is one of the major concerns in ICT strategy	Its Importance is increasing
2	Political attention	In the area of cybercrime	Ministry of ICT, Ministry of Internal Affairs, Ministry of National Defence	Cybersecurity doesn't have any specific political attention	Through the National Security Council	The political attention is increasing	Cybersecurity gets regular political attention
3	Approved cyber security and data protection policy	Information Security Policy, e-Society Policy	Not available	Regulated in different policy documents	Law on Information Security, Cyber Security Strategy	Strategy on Personal Data Protection and combating cybercrime	Proposals to include cyber security in the national security
4	National cybersecurity framework	The Concept of Telecomm. Security	Under development	Covered by different documents	National Cyber Security Strategy	Under development	Draft document has been developed
5	Responsible organization	National Security Council	Ministry of ICT and Special State Protection Service	Government Operative Analytical Centre	National Security Council (+ Data Exchange Agency)	In the area of personal data protection – National Centre for Personal Data Protection	Shared responsibility between different institutions
6	National cybersecurity focal point	In the area of cybercime – Prosecutor-Genaral's Office	State Agency of Special Comm.	Not available	National Security Council's Office	Not available	CERT at the State Special Comm. Service
7	CIRT / CERT	Not available	Yes, under the Ministry of ICT	Government Operative Analytical Centre, not state-wide	Government CERT at Data Exchange Agency (under Ministry of Justice)	Government CERT at Centre of Special Telecomm. (under State Chancellary)	Shared responsibility between different oranizations
8	Cybercrime investigation unit	Hi-Tech Crimes Unit (2005), 4th Special Unit for counter-intelligence	Units under Ministry of ICT, Ministry of Internal Affairs and Ministry of National Security	Department of Hi-Tech Crimes (2001)	24/7 Cybercrime Unit under the Ministry of Internal Affairs	Units under Ministry of Internal Affairs (+ Ministry of ICT support), IT & Cybercrime Division (under General-Procecutor's Office), Security and Intelligence Service	State Special Comm. Service, Security Service, Ministry of Internal Affairs
9	Awareness and educational programme	Several professional training courses	Specific programs are not available	Several programs in universities	Awareness activities, no long-term programs	Different activities, no specific programs	Different activities, no specific programs
10	Meaningful public-private partnership	Not available	Project-based cooperation	Not available	Cybersecurity Forum is under development	Not available	Not available
11	Framework for international cooperation	In the area of combating cybercrimes	Cooperation with international organizations and countries	International and bilateral cooperation	Framework is part of cybersecurity strategy	In the area of Budapest Convention (cybercrime)	Several international formats

actually been done with regard to the fight against cybercrime let alone the implementation of any strategies for the protection of data.

Armenia has not yet established a National Cyber Incident Response Team. The absence of this specialized division and the lack of trained human resources in the regional police departments were discussed in the Prosecutor General's office. The investigation of digital crimes, especially when according to 2012 report the number of cyber crimes gradually increased and covered the whole

territory of Armenia,[225] was a major concern of this office.

In Armenia cyber crime investigations are carried out by the high-tech crimes unit at the organized crime division in the Armenian Police (since 2005) and in the 4th specialized unit of the National Security Service Counterintelligence department[226].

In 2012 the Prosecutor General's Office and the National Security Cyber crime Department prosecutors examined 199 cyber crime cases according to civilnet.am media agency (29/01/2013).

The high-tech crimes unit of the Organized Crime Division in the Armenian Police recorded about 40 cases in 2012 and 22 in 2013 according to tert.am media agency (15.04.2013)[227].

Since 2012 "World Vision Armenia" in cooperation with the high-tech crimes unit of Organized Crime Division is implementing a "Children's Online Security" program to raise awareness of parents and children concerning data protection, cyber crime dangers and security rules. In the framework of this program a computer game was created to enhance the reputation of the police officers, as well as to describe the dangers and threats that exist on the Internet[228].

There are no generally coordinated data protection and cyber security awareness and educational program available in Armenia. However, several professional training courses regarding the fight against cyber crimes have been organized for law enforcement agencies in the last 2 years (2011-2012) with funding coming from the OSCE Office in Yerevan and US Embassy in Armenia[229].

Public-private partnerships in the field of cyber security are at the moment very limited. This issue is mentioned in the Prosecutor-General's report "The Report on the Functioning of the Armenian Prosecutor-General's Office 2012": "Among other structural issues, the limited internal cooperation, which is also caused by the lack of resources is a major concern."[230].

The Republic of Armenia has put great deal of effort into the fight against cybercrimes, particularly in establishing international cooperation and implementing its international obligations. It lacks the necessary legislative and practical mechanisms to make this fight more effective. The provisions of the Armenian Criminal Code do not fully correspond to the European Convention on Cybercrimes which was ratified by Armenia in 2006. This discord continues to be a major concern.

Moreover, there are no legal mechanisms for the regulation of the activities of the electronic service providers or for their cooperation with the law enforcement agencies. The absence of any mechanisms for personal data protection and the insurance of the privacy and confidentiality is another serious problem in this area[231].

Azerbaijan. Cybersecurity is an important topic in Azerbaijan. Azerbaijan has established a specific ministry, the Ministry of Communications and Information Technology, which has the responsibility to coordinate the linking of cyber security with other security areas and the information society development process. The Ministry of Communications and Information Technology has the main responsibility for the area of cyber security, but law enforcement agencies, such as the Ministry of National Security, the Ministry of Internal Affairs along with others are also actively involved. There is a plan in Azerbaijan to establish a State Agency for Cyber Security, which will elevate consideration of this topic to a new level.

At the moment there are no strategic cyber security and data protection policy documents available in Azerbaijan. The Ministry of Communications and IT and the Special State Protection Service have the general responsibility for cyber security and data protection.

The Main Focal point for Cyber Security in Azerbaijan is The State Agency on Special Communication and the Information Security[232] which is responsible for the national cyber security framework. However, this is a new agency with and the official policy side is still coordinated with the Ministry of Communications and Information Technology. The CIRT / CERT organization is currently contained in the Ministry of Communication and Information Technology.

With regard to awareness and educational programs, at the moment there are no known publicity

225 The 2012 Report on the Functioning of the Armenian Prosecutor-General's office is available online: http://www.genproc.am/upload/File/Haxordum%202012.pdf

226 http://www.police.am/news/view

227 Arm_http://www.tert.am/am/news/2013/04/15/andrey-yashchyan/

228 Program web page: www.safeinternet.am

229 Information about the EU/EC 2012 regional seminar dedicated to the fight against cybercrime is available online: http://www.panarmenian.net/arm/news/105224/

230 The report is available online http://www.genproc.am/upload/File/Haxordum%202012.pdf

231 These problems are mentioned in the Prosecutor-General's report in 2012: http://www.genproc.am/upload/File/Haxordum%202012.pdf

232 http://www.dmx.gov.az/page/6.html

programmes organized in Azerbaijan.

Azerbaijan is in close cooperation with International agencies and also with other countries in the field of ICT and the development of Cyber Security. The main donors active in Azerbaijan are the World Bank, the United Nations Development Programme. In addition, big vendors like Cisco, have established a number of IT academies in the country. Also, the private companies, such as IT integrators, are closely cooperating with the Government with a number of projects, including those related to cyber security.

Belarus. In Belarus Cybersecurity is an important security concern. The national program for the accelerated development of services in the IT sphere (2011)[233] also includes the sub program the "ICT security and digital trust" (p. 32-34 of the National Program). The objective of the sub program is the development of information security, the provision of legal and safe use of ICT, the building of trust, and the provision of conditions for safe services in ICT sphere.

There is no single integrated policy document on cyber security and data protection in Belarus. The basic principles are provided in the following documents:

1. Concept of National Security 09.11.2010 № 575[234]
2. Law on information and informatization 10.11 2008. № 455[235]
3. The Law on state secrets 19.06. 2010 N 170-З[236]
4. Law on electronic document and on the electronic digital signature 28.12.2009 № 113-З[237]
5. Strategy for information society development 08.2010 Nr 1174[238]
6. National program for the accelerated development in the sphere of ICT for 2011-2015[239] Subprogram "ICT security and digital trust"
7. Presidential Decree 01.02. 2010 N 60 / O[240]
8. Operative Analytical Centre Decree on some issues for the implementation of the subprogram "ICT security and digital trust" 02.06.2011 N2/9 /O[241]
9. On regulations concerning the technical protection of state secrets 01.02.2011 N 115[242]

In Belarus the Presidential Decree N 60 of 01.02.2010[243] made the Operative Analytical Center[244] the state agency responsible for information protection. This centre is responsible for monitoring the critically important information objects. [245]he Council of Ministers have defined the critical information objects with a resolution on 30th of May, 2012[246] and ISO/IEC 27001 defines risk management and compliance.

In Belarus, there is no statewide Cyber Incident Response Team (CIRT/CERT). The Operative Analytical Centre manages these issues for the governmental sector. A special cybercrime unit in the Department of Hi-Tech Crime was created in 2001[247][248].

According to the Ministry of Internal affairs the number of cybercrimes is on the decline but some experts have noted that activities of ministry are mainly focused for instance on banking and payment cards while cases of the theft of personal data, are not recorded[249].

In Belarus, there are several institutions, which provide education in the information security area:

1. Belarusian State University[250]
2. Belarusian University of Informatics and Radio Electronics[251]
3. Belarusian National Technical University[252]
4. The Academy of Management under the President of the Republic of Belarus[253]
5. The Institute of advanced training and retraining of managers and specialists[254]

233 http://www.mpt.gov.by/File/Natpr/Natpr.pdf

234 http://www.pravo.by/main.aspx?guid=3871&p0=P31000575&p2={NRPA}

235 http://pravo.by/main.aspx?guid=3871&p2=2/1552

236 http://www.beltim.by/wiki/documents/zakon-respubliki-belarus-o-gosudarstvennykh-sekretakh/

237 http://pravo.by/main.aspx?guid=3871&p2=2/1665

238 http://pravo.by/main.aspx?guid=3871&p2=5/32317

239 http://www.pravo.by/main.aspx?guid=3871&p2=5/33546

240 http://pravo.by/main.aspx?guid=3871&p2=1/11368

241 http://preview.tinyurl.com/nxdt72u

242 http://pravo.levonevsky.org/bazaby11/republic03/text002.htm

243 http://pravo.by/main.aspx?guid=3871&p2=1/11368

244 http://oac.gov.by/info/history.html

245 http://base.spinform.ru/show_doc.fwx?rgn=51615

246 http://base.spinform.ru/show_doc.fwx?rgn=51098

247 http://mvd.gov.by/ru/main.aspx?guid=1881

248 Video of the interview with the head of the department http://www.tvr.by/download/video/63753.wmv

249 see http://www.profi-forex.org/novosti-mira/novosti-sng/belarus-/entry1008153168.html

250 http://www.bsu.by/en/main.aspx

251 http://www.bsuir.by/index.jsp?resID=100229&lang=en

252 http://en.bntu.by/

253 http://www.pac.by/en

254 http://ki.by/#

These universities provide programs on:

1. Technical safety
2. Computer security
3. Information protection in telecommunications
4. Electronic information protection
5. Electronic security system

Belarusian University of Informatics and radio electronics provides a PhD course on Methods and Systems for the Protection of Information Security. Several High Technology Parks together with four universities and their Indian partners have created an advanced IT training center, which provides specialised training in cyber security[255]. Since 2011 a national competition focused on cryptography and information protection has been conducted in Grodno for students of both universities and secondary schools[256]. Since 2002 Belarusian university of Informatics and Radio Electronics has conducted an annual Belarusian-Russian scientific and technical conference on the theme of "Technical means of information protection".

With regard to Public Private Partnerships, there are no initiatives in this area. As with Regard to international cooperation, the strategy for the development of information society[257] sets priorities for international cooperation:

1. Participation in the discussion of the problems of the formation of a global information society, the regulation of relations in the field of a global information infrastructure, the creation of monitoring systems and setting indicators of the development of information society;
2. Participation in the development and implementation of international standards in the field of ICT;
3. The fostering of the development of international and interstate information exchange;
4. Participation in the formation of the system of international security in the information sphere and combating the illegal use of ICT;
5. The integration of educational, scientific and cultural spheres of the country into the global scientific, educational and cultural space;
6. Participation in international projects to develop information society.

Belarus has joined the CIS agreement on information security[258] and they have signed the CIS Agreement on cybercrime prevention[259]. In 2012 Belarus announced that it had initiated the process for joining the Cybercrime Convention.

Following bilateral projects have taken place:

1. Belarusian and Lithuanian governments have signed an agreement on cooperation in the sphere of information society in 2013[260]
2. In 2012 an agreement on cooperation with Hi-TechParks and Nasscom (India) was signed
3. Some projects are being realized within the framework of Belarusian-Latvian Center of technology transfer[261]
4. Study visits to Institute of Applied programs – Lantmäteriet (Sweden)[262]
5. Masters programmes on e-government (Belarus – South Korea)
6. Study visits organized by PACT and the e-Governance Academy (Estonia)[263]
7. The President of Belarus Alexander Lukashenko has recently said that Belarus intends to expand its cooperation with China, significantly improving the protection of its national cyberspace[264].

Georgia. In Georgia the issue of cyber security is a very important component of National Security. Cyber Space is considered as an environment which must be protected along the same lines as the protection of their physical territory. Government leaders are not officially responsible for Cyber Security but the National Security Council and its head could be considered to have responsibility for it.

At the moment there is no national legislation concerning Cyber Security. The Law of Georgia on Information Security[265] (from June 2012) and Cybersecurity Strategy with 2013-2015 action plan (approved by the Presidential order in May 2013) currently regulate the policies in this field.

The National Security Council is the managing body and focal point with regard to cybersecurity. The responsibilities for this are distributed among several institutions – Ministry of the Interior, the Data Exchange Agency under the Ministry of Justice, and the Ministry of Defense. The Data

255 http://www.park.by/content/docs/Binder-small-ru.pdf

256 http://enigma.itready.org/

257 http://www.pravo.by/main.aspx?guid=3871&p2=5/32317

258 http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=INT;n=7785

259 http://www.cis.minsk.by/page.php?id=866

260 www.pravo.by/main.aspx?guid=3871&p0=C21300120&p1=1

261 http://www.blctt.metolit.by/ru/dir/index.php/297

262 http://vsbel.by/File/2011_4/ms.pdf; http://land-reform.com/upload/ecb6f44be2965de6f8bc8d41ff057a74.pdf

263 http://www.ega.ee/ru/node/1062

264 http://it.tut.by/355592

265 http://dea.gov.ge/uploads/InfoSec%20Law%20ENG.pdf

Exchange Agency is responsible for data protection and also for the cyber security of non-military institutions. The government CERT operates under the auspices of the Data Exchange Agency.

For combating cybercrimes, there is a separate 24/7 response Cyber Crime Unit/Contact point in the Ministry of Interior. Also, a 24/7 high-tech crime (cybercrime) international contact point was established as required by the CoE 2001 Convention against Cybercrime (The Budapest Convention).

There are no longterm educational and awareness programs available at the moment, but awareness-raising activities are regularly performed, including informing citizens about phishing and other threats. With regard to the cybersecurity professionals, the situation is the same - there are no programs for the ICT and cybersecurity professionals.

With regard to meaningful public-private partnerships, the Data Exchange Agency plans to organize a Cyber Security Forum, which will include all the leading IT specialists from public and private sector.

The national framewrok for international cooperation is a part of their Cyber Security Strategy. The Data Exchange Agency is a member of TF-CSIRT Trusted Introducer, FIRST and IMPACT. Also, a security cooperation agreement has been signed with Microsoft. In addition, the Georgian GOV-CERT cooperates and receives information from the following organizations and systems: Team Cymru, Shadow Server, Atlas Arbor Networks, N6 Arakis (CERT.pl) CleanMX, Inteco-CERT, Quarantainenent.

Moldova. Recent developments suggest that cybersecurity is a major concern of the Government. For e.g. the draft Information Society Development Strategy identifies cyberspece security as a major concern. Accoring to it:

„The more a society is computerized the more it is vulnerable and cyberspace security should be a major concern of all stakeholders, especially at the institutional level, which is responsible for coherent policy development and implementation in the field.“[266]

At the moment, Moldova does not have a national cyber security policy or strategy. The eGovernance Center in cooperation with the e-Governance Academy from Estonia has created a draft policy paper for Moldova. According to the Digital Agenda 2020, the Security and Inteligence Service of the Republic of Moldova, in cooperation with 4 other actors from the public sector, will develop a Program for cyber security in Moldova. In the area of data protection a draft strategy is being developed[267] and a draft action plan in the area of combating cybercrimes is also under development[268].

In July 2013, the Prosecutor General (PG) launched, for public consultation, a draft action plan for the prevention and combating of cybercrime and it urged civil society groups, individuals and businesses to submit their comments, views and proposals. A final plan is to be approved by an order of 11 inter-state institutions. According to a press release of the PG, the document provides an implementation period of three years and it is aimed at synchronizing their national legislation with the Council of Europe Convention on Cybercrime. Among the main objectives of the plan, are the improving of the legal framework and the enforcement provisions of the legislation, and insuring the functioning of an efficient mechanism for the reporting of cybercrimes. The final draft of the Plan can be viewed on the official website of the Prosecutor (www.procuratura.md), in the section “Information” subheading “Plans and programs of the Public Prosecutor of the Republic of Moldova”[269].

Last month, NATO expressed its willingness to share its cyber defense expertise with Moldova. In this regard, the Prime Minister said that all measures would be taken to ensure that the responsible institutions will apply these best practices as soon as possible to combat crimes.[270]

Currently, there is no National Cyber Security Focal Point available in Moldova. There is no public authority that is directly liable and responsible and empowered with the rights and duties concerning cybersecurity in Moldova. There are several institutions involved in this process but each of them is only concerned with the provision of security for their own information systems.

According to the draft Action plan for the implementation of the national strategy for information society development “Digital Moldova 2020”, the Security and Inteligence Service of the Republic of

266 http://www.mtic.gov.md/moldova_digitala_eng

267 http://datepersonale.md/ru/transp_consult/

268 http://www.procuratura.md/file/Planul%20comun%20TI%20(FINAL)2013%20proiect.pdf

269 http://www.trm.md/en/social/pg-elaboreaza-un-plan-de-combatere-a-crimelor-cibernetice

270 http://www.trm.md/en/social/asistenta-pentru-moldova-in-securitatea-cibernetica/

Moldova in cooperation with a number of other actors[271] are charged with the responsible authority to create the national programme on cyber security in Moldova.

The Computer Emergency Response Team (CERT) was created within the State Enterprise "Center for Special Telecommunications". However, according to the draft Information Society Development Strategy „Digital Moldova 2020":

„Although there are technical means, nowadays there are no legally binding provisions for reporting information to CERT-MD and this entity has no special liabilities or sufficient capacity to meet the new challenges at the national level."

There is no a specific unit established in Moldova for the combating of cybercrime but according to the law[272], there are 4 authorities, which have responsibilities in this regard:

- Ministry of Interior of the Republic of Moldova
- Ministry of Communications and Information Technology
- General Prosecutors Office (Informational Technologies and Cybercrime Investigation Division)
- Security and Intelligence Service

There are no national educational or awareness programs regarding cybersecurity. The e-Governance Center, in cooperation with the e-Governance Academy from Estonia, has organised a number of events for ICT professionals, lawyers, auditors, etc on the topic of information security.

Also, a framework for public-private partnership in the area of cybersecurity should be established. Internationally Moldova is cooperating mostly in the field of combating cybercrime, because they are a party to the Budapest Convention on Cybercrime.

Ukraine. The increasing dependency on communication technologies means that both national and international security will be affected by the further development of ICT. Ukraine is particularly vulnerable to cyber threats and this has led to an increase in the attention paid to this issue by the authorities. These issues are discussed at meetings of the National Security Council of Ukraine. The interdepartmental Working Group made several proposals:

- The establishment of an interagency commissioner authority to ensure information security in Ukraine;
- The Updating of the Interagency Committee on Information Policy and Information Security at the National Security Council of Ukraine;
- To analyse the feasibility of establishing units of information (cyber) security in government agencies and the executive branch;
- Amendments to the Information Security Doctrine of Ukraine;
- Drafting the concept and strategy of cybersecurity of Ukraine;
- The development of a state program creating a system of cyber security of Ukraine;
- Changes to the legislative and regulatory documents;
- The establishment of coordination bodies or working groups responsible for combating cyber terrorism and cooperation in the field of international information security.

In Ukraine there are more than 20 laws that regulate cyber security. The Cabinet of Ministers of Ukraine has drafted proposals for changes in the Law of Ukraine "On the Fundamentals of National Security of Ukraine", which outlines the terms "cyberspace", and "cyber security."

Today in Ukraine there is no single central authority overseeing cybersecurity. The functions are divided between the three key agencies: the State Special Communication Service, the Security Service of Ukraine (SSU) and the Ministry of Internal Affairs of Ukraine (MIA). The State Special Communication Service provides protection for the public communication systems. The SSU - investigates attacks on public authorities, and crimes in the sphere of information that threaten the national security of Ukraine. The MIA has the responsibility for the fight against economic crimes in cyberspace.

The following institutions are responsible for cyber security at the institutional level in Ukraine:

- The President of Ukraine;
- The Council of National Security and Defense Council;
- The Cabinet of Ministers of Ukraine;
- The Security Service of Ukraine;
- Ministry of Internal Affairs of Ukraine;
- The State Service of Special Communication and Information Protection;
- The Ministry of Defence;
- National Commission, which is responsible for state regulation in the field of communication and information;
- The National Bank of Ukraine;
- State Agency on Science, Innovations and Informatization of Ukraine

In order to protect the national information and

271 http://www.mtic.gov.md/moldova_digitala_eng

272 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=333508

communication systems the State Special Communication Service set up a team to respond to computer emergencies in Ukraine - CERT-UA. The group was accredited by the international organization FIRST. Other organizatins are also involved in the computer emergency response area:

- The State Service of Special Communication and Information Protection;
- The Security Service of Ukraine;
- Ministry of Internal Affairs of Ukraine;
- The Ministry of Defence (including the Defence Intelligence);
- The Foreign Intelligence Service.

There is a special office under the Ministry of Internal Affairs which is tasked with the fight against cyber crime. This office operates as an interdepartmental research centre for combating organized crime[273].

There are no awareness-raising and educational programs on cyber securityavailable at the moment but Ukraine has held forums, seminars and different conferences on the topic of cybersecurity.

A specific law regulates public private partnerships in this area[274] but it is very difficult to develop cybersecurity strategies in this manner. According to the National Institute for Strategic Studies the difficulties are following[275]:

- The lack of a transparent mechanism of cooperation in the framework of the PPP;
- A lack of motivation among civil servants to establish PPPs;
- Low level of awareness about the benefits, forms, institutions, partnerships;
- The ineffectiveness of incentives for PPPs;
- Insufficient availability of information.

International cooperation is organized through different cooperation formats with the European Union, the UN Security Council, NATO, the OSCE and the Council of Europe and Ukraine alsohas a special cooperation program with Great Britain.

Data security of government databases

In **Armenia** an Information security Concept was approved in 2012 in which its general goals, objectives and principles were defined. Special frameworks and measures for government databases do not exist and there is no common „best practice“practice. Central coordination is done by National Security Service but there is no information about nominated persons responsible for this in the various ministries.

In **Azerbaijan** their Internal Policy on Government Databases and Systems does defines some aspects of data security. Coordination is overseen by the State Special Protection Service of the Special Communication Department. The common practice in the ministries is that their IT staff and database administrators are fulfilling the role of information security officers. No standards and norms on databases security have yet been developed.

In **Belarus** the basic principles are outlined in the Strategy for Information Society, Concept of National Security and Law on State Secrets, and in the sub-program concerning ICT security and digital trust. Central coordination carried out by the Operative Analytic Centre. There are no special Information Security Officers at either the ministry or institutional level and a National standard, based on ISO 27001, for information security management has been adopted and a number of technical standards have also been defined. It seems that this field is very well regulatedbut there is no information about the actual implementation of these standards at the institutional level. Data protection measurements have been implemented at the ministry level and the management of it is provided by their IT staff. Each institution has its own „good practice“based on national standards and regulations.

In **Georgia**, the general cyber security policy also covers all government databases and information systems. Common information security standards have been defined but not implemented. Not all institutions have nominated persons for it but most of critical ones do have them. Common data protection requirements are mandatory but there is still no common understanding about the required concrete measures.

In **Moldova** the central focus in on personal data protection. There is no separate general policy paper available. Several institutions have nominated individuals to be responsible for data security but this has not happened in all the institutions. The ISO standard is used as an example but it has not been widely implemented in practice. There is an international project with the aim of developing a measurement framework and recommending standards for the protection of state databases and information systems. This project is connected to the government interoperability framework devel-

273 http://mvs.gov.ua/mvs/control/main/uk/publish/article/544754

274 http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2404-17

275 http://www.niss.gov.ua/articles/1059/

opment project which is to enablethe implementation of service frameworks throughout the government.

In **Ukraine** the general policy is fixed by Law on Basics of National Security of Ukraine (2003) and by the Presidental decree „Doctrine on Information security of Ukraine"(2009). There are no standards and regulations concerning the level of security for government databases and IT systems. Data protection at the institutional level is the responsibility of individuals nominated by the heads of these institutions. What counts as good practice is defined by government regulations but in reality there is no implementation of these standards.

Personal data protection

The following table shows, which Eastern Partnership countries have signed and ratified the Council of Europe's treaty 108 "Convention of the protection of Individuals with regard to Automatic Processing of Personal Data", and treaty 181 "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".

Information regarding Georgian ratification of the European Council's treaty 181[276] is based on the answer in the survey questionnaire.

Armenia. Armenia has signed and ratified both Council of Europe treaties (see the table in the beginning of the chapter). Also the Armenian Constitution regulates the privacy mattes of the citizens of Armenia. Fo example the acticle 23 says following:

"Everyone shall have the right to respect for his private and family life. The collection, maintenance, uses or dissemination of any information about the person other than that stipulated by the law without the person's consent shall be prohibited. The use and dissemination of information relating to the person for purposes contravening the aims of their collection or not provided for by the law shall be prohibited. Everyone shall have the right to become acquainted with the data concerning him/her available in the state and local self-government bodies. Everyone shall have the right to secrecy of correspondence, telephone conversations, mail, telegraph and other communications, which may be restricted only by court decision in cases and in conformity with the procedure prescribed by the law."[277].

Armenia has also a law on personal data, adopted on October 8, 2002. The article 1 states the subject of the law:

"This Law regulates relations connected with the processing of personal data by state and local self-governance bodies, state and community institutions, legal entities or natural persons. This Law does not

	Council of Europe treaty 108: Convention for the protection of Individuals with regard to Automatic Processing of Personal Data			**Council of Europe treaty 181: 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**		
	Signature	Ratification	Entry into force	Signature	Ratification	Entry into froce
Armenia	08.04.2011	09.05.2012	01.09.2012	08.04.2011	09.05.2012	01.09.2012
Azerbaijan	03.05.2010	03.05.2010	01.09.2010			
Belarus						
Georgia	21.11.2001	14.12.2005	01.04.2006	15.05.2013	27.07.2013	
Moldova	04.05.1998	28.02.2008	01.04.2009	29.04.2010	28.09.2011	01.01.2012
Ukraine	29.08.2005	30.09.2010	01.01.2011	29.08.2005	30.09.2010	01.01.2011

Sources:
http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=12/11/2013&CL=ENG
http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=181&CM=8&DF=12/11/2013&CL=ENG

276 http://parliament.ge/files/international-acts/conv_2013_spring.docx

277 http://www.parliament.am/parliament.php?id=constitution&lang=eng

regulate relations connected with the processing of personal data considered to be of state confidentiality, personal data published in public sources as well as the processing of personal data by individuals for their personal, family or other matters of the type."[278].

There is no single authority in Armenia, which is responsible for the oversight of the protection of personal data, although some appeals can be made to either the Human Rights Ombudsman[279] or to the courts.[280]

CARIM East - Consortium for Applied Research on International Migration[281] has drafted the new Armenian law on the Protection of Personal Data, which will replace the Armenian law on Personal Data that was previously enacted on October 8, 2002. According to Article 21 of the draft, there will be an authorized state body responsible for the protection of personal data[282].

There is no information available with regard to any public awareness activities. From the 19th -21st of November 2010 the Armenian-European Policy and Legal Advice Centre (AEPLAC) organized the seminar "Data Protection Principles in Armenia and the EU". The objective of the seminar was to raise the awareness of the Armenian officials involved in the processing and maintenance of personal data about the principles of data protection and EU standards[283].

Azerbaijan. Azerbaijan has signed and ratified the Council of Europe Convention 108 but it has not signed and ratified the additional protocol nr 181 covering supervisory authorities and cross-border information flows (see the table in the beginning of the chapter).

In Azerbaijan the Constitution provides the legal basis for privacy and personal data protection. In addition, Azerbaijan has a specific law „Personal Data"[284], which also deals with the protection of personal data protecton.

There is no specific institution that is specifically authorized to oversee data protection in Azerbaijan but the President and the Cabinet of Ministers are responsible for the oversight of the law on personal data[285].

Belarus. Belarus has neither signed nor ratified the Council of Europe Convention 108 and its additional protocol 181 (see the table in the beginning of the chapter) but the Constitutional guarantees on privacy do contain the basis for regulations concerning data protection. However, the the constitution does not prohibit the collection, use, storage and dissemination of information about the private life of a person without his or her consent. Article 28 states:

"Everyone shall have the right to protection against unlawful interference with his private life, including encroachments on the privacy of his correspondence and telephone and other communications, and on his honour and dignity."[286].

The following regulations cover the protection of personal data:

1. The Law on information, informatization and information protection (2008)[287],
2. The Law on the population register (2008, comes into force in July 2013)[288],
3. The Law on the population census (2006)[289],
4. The Law on individual (personified) registration in the social insurance system (1999)[290],
5. The law of the Republic of Belarus on credit histories (2008)[291],
6. Code of Laws of the Republic of Belarus (2002, current version 2012): Tax Code articles 67 , 249[292],
7. Code of Laws of the Republic of Belarus (2007, current version 2009): Customs Code article 300[293],
8. Code of Laws on Administrative violations of laws (2003) articles 22.6-22.7[294],

278 http://www.parliament.am/law_docs/071102HO422eng.pdf

279 http://www.ombuds.am/main/en/9/27/139/

280 Examples: http://www.foi.am/en/rcontent/14/

281 http://www.carim-east.eu

282 http://www.carim-east.eu/media/sociopol_module/File-4%20ARM%20Draft%20Law%20on%20Protection%20of%20Personal%20Data-Armenia%20English.pdf

283 http://www.ekeng.am/?p=613

284 http://archive.president.az/articles.php?item_id=20100606093305718&sec_id=67

285 www.president.az

286 http://www.president.gov.by/en/press19329.html#doc

287 http://www.pravo.by/main.aspx?guid=3871&p2=2/1552 Articles 17, 18, 23, 32

288 http://www.demoscope.ru/weekly/knigi/zakon/zakon093.html Articles 2, 7, 8, 10-17, 23-32

289 http://belstat.gov.by/homep/ru/perepic/2009/main2.php Artcles 1, 4, 7,9, 19, 22 – 27

290 http://pravo.levonevsky.org/bazaby09/sbor66/text66216.htm

291 http://www.pravo.by/main.aspx?guid=3871&p0=H10800441

292 http://etalonline.by/?type=text&regnum=Hk0200166#load_text_none_1

293 http://etalonline.by/?type=text&regnum=Hk0700204#load_text_none_1

294 http://etalonline.by/?type=text&regnum=Hk0300194#load_text_none_1_

9. Criminal Code (1999) articles 179, 212, 349, 352[295],
10. Presidential decree 04.12.2007 N 611 (version 11.04.2013) Chapter 3,article 9.9-1[296],
11. Council of Ministers Regulations on Basic e-Services 10.02.2012 N 138: Registration and licensing services (version 19.04.2013)[297],
12. Council of Ministers regulations on services provided by the National Center of e-Services 31.05.2012 N 509/[298],
13. Council of Ministers Regulation 10.09.2009 N 1178[299].

There is no special data protection authority has been established in Belarus and there is also no independent expert agency authorized to deal with personal data protection. There is also no information about any kind of activities concerned with raising awareness about data protection in the recent years.

Georgia. Georgia has signed and ratified both Council of Europe treaties (see the table in the beginning of the chapter) and the Constitution provides for basic personal data protection. Namely article 41 (2):

"Information existing in official papers connected with health, finances or other private matters of an individual are not available to other individuals without the prior consent of the affected individual, except in cases determined by law, when it is necessary for the state and public security, defense of health, rights and freedoms of others."

The Personal Data Protection Act[300] was adopted in December 2011, with different parts being implemented at different dates.

The Personal Data Protection Act continues to generate some concerns. Watchdog organizations, recalling previous experiences have the suspicion that the public organizations will be reluctant to disclose public information. They are fearful that they will interpret the Personal Data Protection Act in over-protective manner and they will, for example, refuse to publish the names and work contact information of the Heads of Departments on the grounds that it is personal information thereby avoiding fines for its disclosure.

The mechanisms of control to enforce the law and control Personal Data Protection with its very limited resources are not clearly detailed. The work to amend the law has been already started and in the new draft, the norms for the processing of sensitive information are tightened.

A Personal Data Protection Inspector was recently appointed. The position is fully independent one and the inspector does not report to anyone. In addition to the law – a special regulation was issued as a Government decree on 19.07.2013 to regulate the work of the Personal Data Inspector. It included rules concerning consultations, the inspections of data processing in both public and private organizations, and information campaigns on the topic.

Regarding public awareness on personal data protection the Data Exchange Agency (a state agency under the Ministry of Justice) has commissioned TV advertisements about personal data protection and cyber security. A special calendar was also published and distributed.

Moldova. Moldaova has signed and ratified both Council of Europe treaties (see the table in the beginning of the chapter) and according to the Constitution of the Republic of Moldova, the intimatedat concerning family and private life is protected. Article 28 states[301]:

"The state shall respect and protect the intimate, family and private life".

The Constitution of the Republic of Moldova does not include the „new generation" fundamental right such as data protection as is provided for in the EU Charter of Fundamental Rights.

On April 14th, 2012, the Law no.133 on personal data protection came into force.[302]

The Law no. 208 which amended and completed some legislative acts, which came into force on 16th of June 2012, seeks to ammend a number of specific acts, namely:

1. The Regulation of the national center for personal data protection approved by law no. 182-XVI as of 10 July 2008
2. The Law on access to information

295 http://etalonline.by/?type=text&regnum=HK9900275#load_text_none_1

296 http://pravo.levonevsky.org/bazaby11/republic17/text687.htm

297 http://pravo.by/main.aspx?guid=3871&p2=5/35264 Index, article 18

298 http://preview.tinyurl.com/lmn4dun

299 www.bankzakonov.com/republic_pravo_by_2010/blocke9/rtf-n5i2k6.htm

300 The full text of the law in English is available at: http://www.coe.int/t/dghl/standardsetting/dataprotection/National%20laws/Georgia%20%28Law%20of...%29%20on%20Personal%20Data%20Protection%20as%20amended%2014%2005%202013.pdf

301 http://www.constcourt.md/public/files/file/Baza%20legala/Constitution.en.pdf

302 http://lex.justice.md/viewdoc.php?action=view&view=doc&id=340495&lang=1 http://datepersonale.md/file/Data%20Protection%20Law%20133.pdf

3. The Law no.1260 of 19.07.2002
4. Law on the salarization system in the budgetary sector
5. The Contravention code (by establishing liability for violations of the legislation on personal data protection and empowering the center with the competences of a fact-finding authority).

The requirements for the assurance of personal data security were approved on December 14th, 2010 by the Government Decision no.1123, which entered into force a year later.[303] On May 15th, 2012 the Regulation on the Registry of evidence of the personal data controllers was approved by the Government, which made it possible to elaborate and officially launch the Automated Information System „Registry of evidence of the personal data controllers".

In Moldova the responsible authority for personal data protection is the National Center for Personal Data Protection (NCPDP).[304] The NCPDP in cooperation with a number of actors, have organised events to increase the people's awareness of personal data protection in general, and of its citizens, in particular.

According to Mr. Panis, the head of the NCPDCP:

„Due to the involvement of European officials and with the support of several non-governmental organizations, the NCPDP has been able to conduct training courses for health professionals and some awareness actions - advertising spots on radio and flash mobs. These actions, however, are not sufficient, as it is necessary to attract the permanent attention of population on the need to protect their personal data".

Furthermore, according to the NCPDP, the Center with the support of a few NGO and the Mayor's Office of the Chisinau Municipality inaugurated an exhibition of pictures/posters on the specifics of personal data protection in January 2012. The exhibition started with a flash mob entitled "Personal data protection – a positive obligation of the State" wherein promotional materials were disseminated (leaflets and calendars, specially designed for this occasion) to passers-by and answers were provided to the representatives of the mass media.

At the same time the representatives of the Center held courses on the concept of personal data, and discussed some aspects about the protection of personal data, particularly with regard to minors, and they also disseminated promotional materials in several high schools in the Chisinau municipality, which involved approximately 450 pupils and teachers.

In a parallel event the ‚representatives of civil society who are the subject of personal data, including representatives of the interested mass-media institutions, had the opportunity to ask questions and receive answers in the framework of the "Open Doors" Day, organized in the premises of the National Authority for Personal Data Protection. On this occasion interviews were conducted which were later broadcast on TV and radio.

For the first time the Moldcell Company was involved in the public awareness process, which, as a personal data controller, sent messages to 100 000 subscribers with the text "National Center for Personal Data Protection is warning you : protect your personal data and do not disclose it to third parties! www.datepersonale.md ".

The NCPDP placed instructions on its webpage[305] covering various aspects of children's interaction with the Internet. The "CHILDREN and the INTERNET "initiative was prepared in accordance with Directive 95/46/EC and Working Paper 2/2009 on the protection of the personal data of children and adopted by the Working Group "Article 29" on data protection. It was founded on the belief that education and responsibility are essential for the protection of personal data and it was specifically aimed at children. It was created to answer all questions about the rules for the protection of personal information such as:

- Name, password, address and home phone number, their parents' work place and phone number or phone number of the school where the minors are studying;
- On the appropriate behavior with images or photos of loved ones;
- Correspondence received or sent;
- Mail chat, forums, social networking, and so on;
- How to complete the registration forms on some sites, including the importance of the use of passwords and antivirus programmes."[306]

Data Protection Day is an event, which is organized annually by the NCPDP where representatives from the private and public sectors are present and

303 http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=337094 http://datepersonale.md/file/hotariri/cerinte_securitate%20eng_101228.pdf

304 www.datepersonale.md

305 http://www.datepersonale.md/md/newslst/1211/1/4343/

306 http://datepersonale.md/file/Raport/ReportEN_2012.pdf

his is another opportunity to speak about personal data protection and to raise awareness about the importance of this topic.

Although a number of events have been organised in the past, these actions, are not in themselves sufficient to attract the attention of population and the authourities on the need to protect personal data.

Ukraine. Ukraine has signed and ratified both Council of Europe treaties (see the table in the beginning of the chapter). Ukraine has a law: "Proterction of Personal Data" from 01.06.2010[307]. The law regulates the protection of personal data, fundamental rights and freedoms including the rights of privacy and personal data processing.

The authority for the overseeing of personal data protection in Ukraine is the State Service for the protection of personal data[308]. The specific functions for the protection of personal data are specified in the regulations of the Ministry of Justice.

The State Service for the protection of personal data is constantly organizing conferences, seminars, and round-tables to discuss and interpret the law. Ukraine also has the Association[309] for the protection of personal data, which deals with the raising of public awareness about this subject. The Internet Association of Ukraine also participates in these activities as well.

Findings and Recommendations

e-Governance Academy experts wished to highlight the following findings and provide some general recommendations on the development of e-governance and data security based of the study.

Overall, we were impressed with the developments that have taken place over the last 5 years or so. It seems that these topics have clearly been in focus for the policy makers in all these countries. We saw more readiness for e-governance and e-service delivery questions and less enthusiasm for e-democracy and e-participation. In cyber security area, there seemed to be political interest in the topic but general lack of know-how both in technical as well as organisational and legal questions.

We think that supporting the e-governance and cyber security developments in Eastern Partnership countries is a type of assistance that would benefit both countries under question and the EU as the cyber-space does not recognise national borders and in the real world improved governance by our neighbours improves also security and economies in the countries of the European Union.

While technology wise the developments have been impressive, there is still a lot of work to be done in order to change the mind-sets of both decision makers and populations at large. A good case in point is development of transparency and data protection regimes. We detected very little official awareness of the issues concerned, they were thought to be part of NGO topics and not serious governance questions, while in the European Union we recognized the value of the re-use of public data not only for the democracy but also for the economy already with Reuse of Public Data Directive (2003). And questions of data protection have been constantly debated on the highest EU levels, with major modifications forseen in the near future. We think that initiatives that would support the mind-set changes in these issues are more important for these countries than direct financial assistance to buy new technologies.

For cyber security, there is a clear need for coordinated confidence building measures across the borders for better and more secure IT systems would benefit not only them but us, too. We would recommend to have an annual EU/NATO sponsored cyber security regional conference covering all the Eastern Partnership countries.

e-governance developments in general need more systematic approach as the complexity of the developments increases. It is time to treat e-governance development as a whole and to fill in/develop the gaps that are missing from the overall picture. In all the countries information society developments have been based on enthusiasts work and therefore e-services are very unequally developed. To move forward, there is a need for nation-wide visions and action plans.

The management and coordination of e-governance development should be brought to a level with sufficient political power and competence. The countries where developing e-governance is directed by an authority under direct supervision of President with executive functions or Prime Ministers office have succeeded making largest improvements. Horizontal coordination is, in most cases, still lacking and can be considered as main risk when new large e-government projects would be launched. Today all considered countries are mak-

307 http://zakon4.rada.gov.ua/laws/show/2297-17/page

308 http://zpd.gov.ua

309 http://uapdp.org

ing efforts to set up strong horizontal frameworks but we did not come across any horisontal coordination success story.

Cooperation and coordination between government entities and private sector and non-profit sector should be strengthened. There is pleanty to do and these governments should trust businesses and third sector actors much more than they currently have.

The CIO's institution should be further developed in these countries. Usually, one can not find them in today's ministries. The role of IT management is given to some unit or person but in most cases these tasks are considered to be purely technical and not connected to the changes of processes and changes in ministerial level. It may be also one of the largest challengies to get support from political level to nominate CIO-s with concrete roles in management, in particular partnering in change management of ministries themselves.

It would be important to launch modern data exchange frameworks and to develop modern and strong e-identification solutions. In all countries access (citizens and officials) questions and digitalized information (information systems and databases) were already quite well developed. With reference to taking into use of digital ID-cards and e-passports there's also improvement in developing e-identity. Considering the fact that mobile penetration rate in all EP countries is already more than a 100%, the countries should consider developing mobile-ID systems along the lines what has been done in Moldova and Azerbajian.

Talking about developing e-governance as a whole, one should also pay attention to the following support systems for e-government development, such as: the register of registers, catalogue of services and the management system for the state information system; the layer of geoinformation systems; the layer of document management systems and document exchange centre; the system of classifications; the system of address details and the security system.

Although the purpose of the current survey was not to research and deal with public awareness, it is still important to point out the necessity to continuously promote the citizens' IT- and e-awareness. If people are not able to use the systems and will not embrace them, there is no benefit from e-services based on remarkable infrastructure. The focus that e-services are established mainly for people shouldn't for one moment be forgotton.

Main complications in ICT development in municipalities lie in their large numbers and lack of clear funding frameworks. Small municipalities are not able to run their own strategies and development projects. It means that some form of cooperation is needed whether it is done by central government associations of municipalities or by voluntary groups and agreements between separate municipalities. It would be good to encourage establishment of cooperation frameworks for joint developments and coordination in e-government on local level.

New challenges are connected with developing crossborder e-services. Parallel with national developments, international agreements and establishing crossborder infrastructure should be considered.

The development of the 6 countries so far shows that they all have technical preconditions and possibilities with political will to be a part of international e-infrastructure. On the basis of interoperability infrastructure, crossborder e-services can be developed, promoting the political and economical development in the region.

Annex. International rankings

UN e-Government Survey 2010

Country	E-Government Development Index 2012 (2010)	Rank/190
Armenia	0.4997 (0.4025)	94 (110)
Azerbaijan	0.4984 (0.4571)	96 (83)
Belarus	0.6090 (0.4900)	61 (64)
Georgia	0.5563 (0.4248)	72 (100)
Moldova	0.5626 (0.4611)	69 (80)
Ukraine	0.5653 (0.5181)	68 (54)
Finland	0.8505 (0.6967)	9 (19)
Estonia	0.7987 (0.6965)	20 (20)

Country	E-Participation Index 2012 (2010)	Rank/32
Armenia	0.0000 (0.0429)	32 (135)
Azerbaijan	0.1316 (0.1714)	27 (68)
Belarus	0.0789 (0.2429)	29 (51)
Georgia	0.2105 (0.0571)	24 (127)
Moldova	0.3947 (0.2000)	17 (58)
Ukraine	0.1579 (0.2571)	26 (48)
Finland	0.7368 (0.4143)	6 (30)
Estonia	0.7632 (0.6857)	5 (9)

World Economic Forum. The Global Information Technology Report 2012

Country	The Networked Readiness Index 2012 (2010-2011)	Rank/142
Armenia	3.49 (3.24)	94 (109)
Azerbaijan	3.95 (3.79)	61 (70)
Belarus	- (-)	- (-)
Georgia	3.60 (3.45)	88 (98)
Moldova	3.78 (3.45)	78 (97)
Ukraine	3.85 (3.53)	75 (90)
Finland	5.81 (5.43)	3 (3)
Estonia	5.09 (4.76)	24 (26)

World Economic Forum. The Global Competitiveness Report 2012–2013

Country	The Global Competitiveness Index 2012–2013 (2011-2012)	Rank/144 (142)
Armenia	4.02 (3.89)	82 (92)
Azerbaijan	4.41 (4.31)	46 (55)
Belarus	- (-)	-
Georgia	4.07 (3.95)	77 (88)
Moldova	3.94 (3.89)	87 (93)
Ukraine	4.14 (4.00)	73 (82)
Finland	5.55 (5.47)	3 (4)
Estonia	4.64 (4.62)	34 (33)

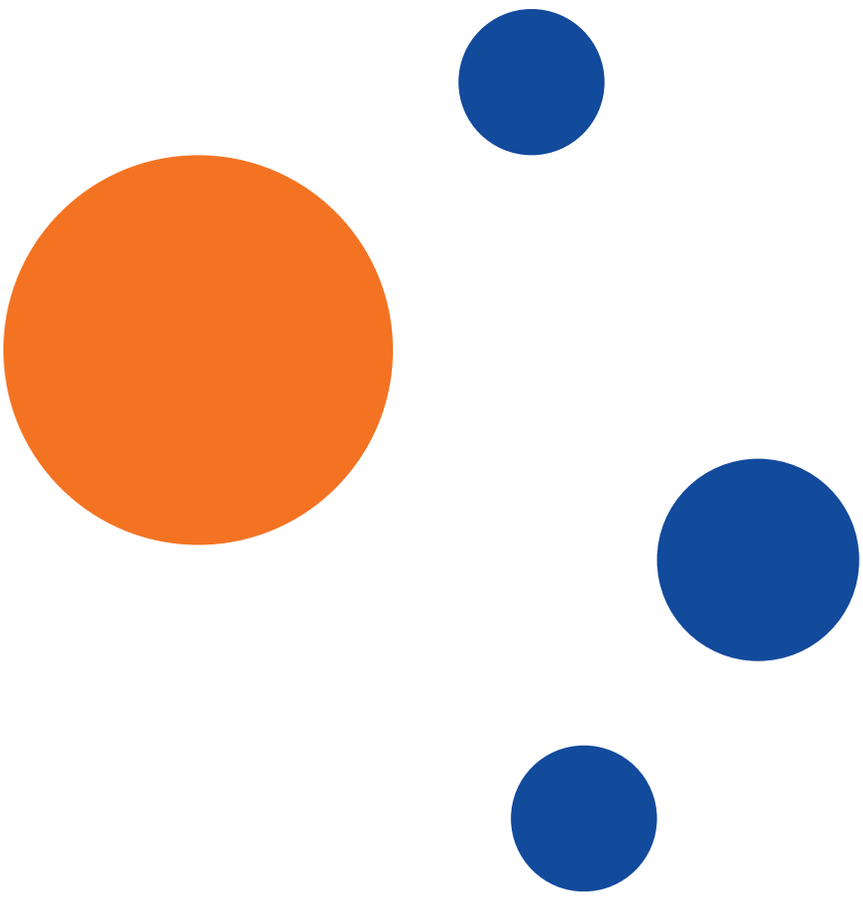
Corruption Perception Index 2012

Country	Corruption Perceptions Index 2012 (2011)	Rank/176 (182)
Armenia	34 (2.6)	105 (129)
Azerbaijan	27 (2.4)	139 (143)
Belarus	31 (2.4)	123 (143)
Georgia	52 (4.1)	51 (64)
Moldova	36 (2.9)	94 (112)
Ukraine	26 (2.3)	144 (152)
Finland	90 (9.4)	1 (2)
Estonia	64 (6.4)	32 (29)

ULKOASIAINMINISTERIÖ
UTRIKESMINISTERIET

ESTONIAN
DEVELOPMENT
COOPERATION

This document has been financed by the development cooperation funds of the Ministries of Foreign Affairs of Finland and Estonia. Finnish MFA and Estonian MFA do not necessarily share the views expressed in this material. Responsibility for its contents rests entirely with the authors.



Estonian Center of Eastern Partnership (ECEAP)
Tõnismägi 2
10122 Tallinn
Estonia
Tel. +372 631 7950
eceap@eceap.eu
www.eceap.eu