

Data Protection in Eurasian Countries

Choice of Policy Approaches and Instruments

Candidate number: 8005

Submission deadline: 01.12.2014

Number of words: 15 756



ACKNOWLEDGEMENTS

This thesis paper would not have been possible without the guidance and the help of several individuals who in one way or another contributed and extended their valuable assistance in its preparation and completion.

First and foremost, my utmost gratitude to Olga Enerstvedt, my supervisor at the NRCCL (University of Oslo) for her support and advice.

I would like to thank all my friends and peers, who have provided valuable feedback and useful guidance on the drafts.

It is also my pleasure to thank Library staff, those who made this thesis possible by being helpful in finding the necessary sources.

Lastly, I offer my regards and blessings to all of those who supported me in any respect during the completion of the research.

Table of contents

INTRODUCTION.....	1
0.1. Background to thesis	1
0.2. Research questions and methodology.....	4
0.3. Challenges and impact.....	5
CHAPTER 1. POLICY INSTRUMENTS	7
1.1 Introduction	7
1.2 Transnational instruments.....	7
1.2.1 Council of Europe’s Convention 108.....	8
1.2.2 Guidelines of the Organisation for Economic Cooperation and Development	9
1.2.3 The European Union Directive	10
1.2.4 Commonwealth of Independent States Model Law	12
1.3 Regulatory instruments	12
1.4 Self-Regulatory instruments	17
1.5 Technological instruments.....	19
1.6 Findings	21
2 CHAPTER 2. CONCEPT OF PERSONAL DATA	22
2.1 Introduction	22
2.2 Identifiability	24
2.3 Data in medium	27

2.4	Findings	29
3	CHAPTER 3. TRANSBORDER DATAFLOW REGULATION	30
3.1	Introduction	30
3.2	Definition.....	32
3.3	Grounds for transfer.....	35
3.3.1	Adequacy approach (geographical targeting)	41
3.3.2	Accountability approach (organizational targeting).....	44
3.4	Findings	45
4	CHAPTER 4. NATIONAL REGULATORY AUTHORITIES	47
5	CONCLUSIONS.....	51
	BIBLIOGRAPHY	56
	ANNEX A. DEFINITION OF PERSONAL DATA	1
	ANNEX B. GROUNDS FOR CROSS-BORDER DATA TRANSFERS	4

Introduction

0.1. Background to thesis

As the title hints, this paper analyses the data protection law in Eurasia. As an introduction, we explain the choice of topic.

This paper focuses on personal data protection, which is relatively young and evolving branch of the law. In short, data protection is a part of privacy laws, and we use the term ‘personal data’ in the meaning of Convention 108, which defines it as ‘any information relating to an identified or identifiable individual’¹. Accordingly, data protection policy refers to choice of regulatory instruments to address the issues of data protection. We use Eurasia to refer to non-Baltic former Soviet countries. To sum up, the focus is on the choice of regulatory instruments available in global arsenal employed by selective countries to fashion their data protection frameworks. Now, we explain the topic choice in more detail.

There are a number of reasons behind the choice of the topic. To start with, for the last forty years, states all over the world have been attempting to regulate the collection, use, storage, and dissemination of individually identifiable personal data in recognition of the power of new information and communication technologies in the hands of large public and private persons. My genuine interest in ‘informational self-determination’ of human-beings is the driving force of the research and this research offers me a stimulating ‘brain exercise’.

¹ Article 2, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

Secondly, the data protection laws are analysed for specific range of countries (ie Eurasia). The term 'Eurasia', in geographic sense, refers to Europe and Asia taken together. However, in this paper we use it as a short and easy grouping of the non-Baltic former Soviet countries²:

1. Azerbaijan;
2. Armenia;
3. Belorussia;
4. Georgia;
5. Kazakhstan;
6. Kyrgyzstan;
7. Moldova;
8. Russia;
9. Tajikistan;
10. Turkmenistan;
11. Ukraine;
12. Uzbekistan.

Now, we turn to explain why these countries have been selected. There are a number of reasons:

- a. Common legal tradition. For almost 70 years or more, these countries had the same legal system and legislation, sharing unified legal tradition. The traces of history can still be observed on laws of these countries which somewhat resemble each oth-

² In its sense, 'Eurasia' in this paper corresponds to geopolitical meaning accorded to the word by Russia. The 'Russian' Eurasia consists of the territory between Europe and Russia, reflecting Russia's interests that underpins foreign policy in that part of the world. See Finn A., 'The Concept of Eurasia - Part I' <<http://commentandoutlook.blogspot.fr/2014/04/the-concept-of-eurasia-part-i.html>> accessed 30 Oct 2014.

er. To that extent, we analyse the data protection laws of these countries in order to spot common approaches (if any). It is worth to note, additionally, that three Baltic states were also in the Soviet Union, yet they are not listed above. The reason is simply their EU membership: having them included, this paper would engage in writing about EU data protection regime on which a large number of scholarship is already available;

- b. Little comparative research on this group of countries. While a large number of privacy studies have been carried out in advanced economies of the world, few scholarship exist for the given group (both comparatively and individually (for certain countries)). As such, this study is contribution to scholarly discussion in the area for the specified group of countries;
- c. Limited availability of research in English. Apart from the common legal tradition, these countries also share common language - Russian (use of which varies from country to country). This paper is a result of research in two languages, namely English and Russian (which comparatively has more research for Eurasian countries than the former);
- d. Relative advantages of the author. The author has two advantages in relation to the selected countries: knowledge of Russian and home jurisdiction is Uzbekistan. They are expected to contribute to the accuracy of the analysis in the paper.
 - i. During the research, original texts of legislation have been studied (as these countries (except Georgia) make laws in both local and Russian languages). This helps to avoid the pitfalls of translated texts, and allows more depth analysis of the legislative texts;

- ii. The author's home jurisdiction is Uzbekistan and he is familiar with common legal tradition (which is shared to different extents by the Eurasian countries).

0.2. Research questions and methodology

The main research question that directs the analysis in this paper is: which regulatory instruments do Eurasian countries employ to design their data protection policy? This question consists of the following subquestions:

1. What regulatory instruments are used? We consider the role of transnational, domestic legal, self-regulatory and technological instruments.
2. To what extent Eurasian countries have common approaches in data protection laws? We have mentioned that the countries shared common legal tradition for a long period of time (see 0.1. Background to thesis above).
3. Is the data protection policy a 'race to the top' or a 'race to the bottom'? This question reflects the two broad global trends: 'race to the top' where countries progressively increase the standard of protection and 'race to the bottom' where countries deregulate in order to gain competitive advantage over the former countries.

The structure of the thesis is built based on these research questions. Chapter 1 addresses the first research question. The second and third research questions are directly answered in conclusions part, based on the findings of the analysis in chapters 2-4. In chapters 2, 3 and 4, we analyse the concept of personal data, transborder data flow regulation and national regulatory authorities (respectively) in Eurasia. We compare these three items among Eurasian countries, as well as against transnational instruments. This comparison will allow us to establish the extent to which Eurasian countries have common approach in data protection area (i.e. research question 2). Furthermore, in Conclusion, we will sum up the find-

ings of the whole paper and attempt to answer to the last research question, based on those findings. Finally that leads us to the thesis statement that Eurasian countries mostly regulate the information privacy through general (framework) data protection acts, which they develop independently from each other yet they have commonly followed the European model of data protection. In other words, data protection is regulated by *lex specialis* act of parliament, and there is no such thing as post-Soviet approach (given the historical common statehood of the Eurasian countries) to data protection issues.

To answer the research questions, we involve mostly qualitative methods. The major part of the research is carried out using inductive approach. Once the necessary body of information and opinions has been accumulated, we will attempt to anticipate the future trends in the region with regard to data protection legislation.

The study will essentially follow a theoretical research methodology, by text analysis of primary legal sources (data protection legislation of the countries), and other relevant legal literature. As the paper studies a group of countries, we follow comparative analysis approach, in particular in chapters 2-4 and conclusion.

0.3. Challenges and impact

The major challenges encountered while writing this thesis was the scarce literature in English on the topic. Legal scholarship mainly reviews by comparison the European or American privacy policies, or studies the data protection regime in the Eurasian countries country by country.

The impact of this study would be to contribute to a further discussion on the privacy policies in the Eurasia. This analysis can be useful, in particular, for the following purposes:

1. To understand the policy choices made in the data protection area in the region;

2. To determine the level of protection for personal data available in the given countries. Although this paper does not seek to analyse the national data protection laws with scrutiny, yet comparison of the definition of personal data, of provisions on transborder data flows and of national regulatory authorities can prove helpful in assessing the level of protection, in particular for the purposes of establishing EU 'adequacy' level (see chapter 3 on transborder data flows);
3. To identify possible future trends in the selected countries. This is possible if we find out which policy approach the countries follow (ie 'race to the top' or 'race to the bottom').

Chapter 1. Policy instruments

1.1 Introduction

In this part we analyse the various policy instruments that now occupy the data protection landscape. We subgroup the inventory of instruments into obvious, but imperfect categories of transnational, legislative, self-regulatory, and technological ones. This grouping is based on the assumption that data protection is international and global issue with social, organizational, political and technological dimensions. We discuss the various instruments in order to assess their features and to identify their use by Eurasian countries.

1.2 Transnational instruments

By transnational we mean the instruments whose rules apply to more than one country. Here we do not address if transnational dimension is generally necessary for data protection. We stem from the assumption that the information society that we live in creates a regulatory interdependence as ‘the ability of any one jurisdiction is inescapably linked with the actions of organizations that operate outside its borders’³.

A large number of international organizations have been involved with the privacy issue⁴. Results of their activities vary from legally binding conventions and down to declaration of principles, to formal guidelines. Transnational instruments were a reflection of conventional wisdom and legal activity in several countries in the 1970s, and they powerfully influenced policy and legislation from the 1980s to the present⁵. In a transnational dimension,

³ Bennett C.J. and Raab Ch.D., *The Governance of Privacy: Policy Instruments in Global Perspective*, (MIT Press 2006), p.xvi

⁴ Bygrave L., ‘Privacy protection in a global context: a comparative overview’ in Wahlgren P. (eds) *IT Law* (Stockholm Institute for Scandinavian Law 2014).

⁵ Note 3, p.121.

three arenas are important to note⁶: Council of Europe, the Organisation for Economic Co-operation and Development (OECD) and the European Union (EU).

1.2.1 Council of Europe's Convention 108

The organization was founded in 1949 to strengthen democracy, human rights, and the rule of law throughout its member states. Since 1989, it expanded to Central and Eastern Europe and as of 2014 it has 47 member states. From the Eurasian countries, Armenia, Azerbaijan, Georgia, Moldova, Russia and Ukraine are its members⁷.

In 1980, *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data*⁸ (Convention 108) was adopted and opened for ratification in January 1981. In short, Convention 108 is a treaty as defined by the 1969 Vienna Convention on the Law of Treaties.

Although we do not pursue to analyse the Convention in detail, its short account is nevertheless useful for our discussion. The Convention is the first international text to set out basic privacy principles (Article 5), but applies only to 'automatically processed' data. It also requires appropriate security measures (Article 7), and empowers data subjects with certain rights (Article 8). The Convention seeks to establish an equivalent level of protection among its contracting parties to assure the free data flow. It leaves the question of data transfers from contracting states to non-contracting ones up to national law. This gap undermines the mutual confidence of its members in one another as safe destinations for personal data. Therefore, as an instrument to regulate the international flow of personal data, the Convention is limited, and has since been overshadowed by the EU Directive (see 1.2.2 below).

⁶ Recently, two more arenas started gaining important role in data protection policy. One with the standard-setting and certification, and the other with wider process of international trade negotiation. Policy role and identity of these arenas are out of scope of this paper.

⁷ See <http://www.coe.int/en/web/portal/country-profiles>.

⁸ Strasbourg, 28.I.1981.

The Convention has acted as a template for those countries without data protection legislation⁹, rather than as a binding instrument of international law. The Council of Europe does not have institutional framework in place to enforce the Convention. Hence, one cannot assume that the Convention actually implemented a common minimum standard of data protection¹⁰.

Nevertheless, the Convention has had influence on the data protection policy in Eurasia. All 6 Eurasian countries named above, that are members of the Council of Europe, have ratified the Convention¹¹. In practice, they incorporated the Convention into their domestic laws. In Chapters 2-3 we see, in the examples of the concept of personal data and the data transfer provisions, how the Convention influenced the national data protection legislation.

1.2.2 Guidelines of the Organisation for Economic Cooperation and Development

Organisation for Economic Cooperation and Development (OECD) comprises of countries with big influence in the world and focuses primarily on trade and economic cooperation. It ‘provides a setting where governments compare policy experiences, seek answers to common problems, identify good practice and coordinate domestic and international policies’¹². Given that none of the Eurasian countries are members of the OECD, we contain ourselves to a short account of OECD activity relevant for our discussion¹³. In particular, three documents worth mentioning:

1. Guidelines on the Protection of Personal Privacy and Trans border Flows of Personal Data (1981). In short, the Guidelines have been an influential instrument. Greenleaf notes that Turkey is the only OECD member country, other than the USA in re-

⁹ Note 3, p.85-87.

¹⁰ Bainbridge, D., *The EC Data Protection Directive*, (Butterworths 1996), p.9.

¹¹ See the Chart of signatures and ratifications at

<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=28/10/2014&CL=ENG>.

¹² OECD, ‘The OECD’, (2008) <<http://www.oecd.org/newsroom/34011915.pdf>> accessed 3 Nov 2014, p.7

¹³ Even though none of the studied countries are OECD members, this mere fact does not mean lack of influence. Therefore, we analyse in Chapters 2-3 if OECD Privacy Guidelines has had any influence on the Eurasian data protection policy. As to the Guidelines in points 2 and 3, our study has not found their influence in Eurasian policy, and we shall not discuss them further in the text. Yet, they can serve as a good starting point in addressing relevant issues under national laws.

lation to the private sector, which does not have a data privacy law implementing the Guidelines. Its influence might further increase if its enlargement plans are realized (through adoption of data protection laws by joining countries). In 2013, the Guidelines were updated;

2. A set of guidelines on Security of Information Systems (1992 and 2002). These guidelines addressed the availability, integrity, and confidentiality of information systems. They advise a range of policies, laws, codes of conduct, technical measures, management and user practices, and public education and awareness activities at both national and international levels;
3. Guidelines for Cryptography Policy (1997) concern the export of cryptographic products for civilian use. This voluntary agreement seeks to identify the basic issues that countries should consider in designing cryptographic policies at national and international level.

Despite the influence that OECD exerted on data protection policies, its activity was serving to justify self-regulatory approaches as opposed to promoting good data protection practices. The situation changed with the EU Directive, as we discuss below.

1.2.3 The European Union Directive

In 1995, the Directive on the Protection of Personal Data with Regard to the Processing of Personal Data and on the Free Movement of Such Data (EU Directive) was adopted¹⁴. It is referred to as ‘by far the most influential international policy instrument’ so far¹⁵. It was driven by the underlying assumption that data protection and free flow of data complement each other rather than conflict. It recognized that the free flow of data is as important as other flows on which European single market is based: freedom of movement of capital, goods, labour and services.

¹⁴ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

¹⁵ Note 3, p93.

In comparison to preceding the Directive Convention 108 and OECD 1981 Guidelines, it makes a number of innovations. Firstly, it updates the concepts used, for example it abolishes some artificial differences, by covering both public and private sector, and applying to both automated and non-automated (i.e. filing systems) processing. It simply unifies data collection, use and disclosure under 'data processing' term. Secondly, the Directive provides for the creation of independent supervisory authority (Article 28(1)), which is meant to achieve better levels of compliance. Thirdly, the Directive sets up an advisory Working Party to give to European Commission advice on divergences among national laws, on the level of protection in third countries, on codes of conduct, and on proposed amendments to the Directive (Articles 29-30). In addition, by far the most extraterritorial effect of the Directive was the prohibition to transfer personal data outside the EU, if the recipient country did not have an adequate level of protection¹⁶.

As we will see in Chapters 2-4, EU Directive has had an influence on the data protection legislation of some Eurasian countries. In particular, its strong influence can be seen on those countries which are in the Eastern partnership agreement¹⁷ (namely, Armenia, Azerbaijan, Georgia, Moldova and Ukraine (European Commission 2014)). In some countries, EU Directive is explicitly recognized as the standard to achieve¹⁸. This influence is expected to increase in those countries who are signing Association agreements with the EU (Georgia, Moldova and Ukraine¹⁹). And obviously, in case if they join the EU, the EU data protection regime will apply in them.

¹⁶ Currently, the EU data protection framework is being reformed. However, in this paper we do not discuss the proposed changes.

¹⁷ For more information see http://eeas.europa.eu/eastern/index_en.htm.

¹⁸ See Georgian DPA (Personal Data Protection Inspector), Report on the State of Personal Data Protection in Georgia, (2014) <personaldata.ge/res/docs/annual_report%28eng%29%284%29.pdf> accessed 30 Oct 2014, p21, recommending the Government of Georgia to bring domestic legislation 'in full compliance with European standards'.

¹⁹ EU External Action, 2014, EU forges closer ties with Ukraine, Georgia and Moldova, [accessed on Oct 13 2014], available at: http://eeas.europa.eu/top_stories/2014/270614_association_agreement_en.htm.

1.2.4 Commonwealth of Independent States Model Law

The Commonwealth of Independent States (CIS)²⁰ is a regional organisation whose participants are ex-Soviet countries (except Baltic states and Georgia)²¹. As an organization, it has only few supranational powers.

CIS does not legislate or work on data protection direction among its participants. It develops model laws which are meant to serve as templates for legislators and also has the model law ‘On Personal Data’²². The common statehood that its participants shared over the twentieth century has an impact on their legal systems in the post-Soviet era. In Soviet era, they had the same laws and now the traces of the soviet legal tradition can be found in their legislative thinking.

The Model Law on Personal Data was approved by the CIS Inter-Parliamentary Assembly. Chronologically, it precedes all the general data protection laws in Eurasian countries, and as such we wonder if it has had any influence on the legislative drafting in Eurasia. We do this in this Chapters 2-4, where we discuss the concept of personal data and cross-border data transfer provisions, as well as the national regulatory authorities in the data protection field.

1.3 Regulatory instruments

As we talk of ‘regulatory’ instruments, we need to clarify what is meant by that. We use it in a broad sense to embrace a variety of instruments that aim to control the processing of personal data and its consequences. Here we refer to ‘regulation’ broadly as Baldwin and Cave do: it is not only Selznick’s idea of regulation as ‘sustained and focused control exercised by a public agency over activities that are valued by a community’, but also a specific set of commands (when a specific agency imposes binding rules), deliberate state influence

²⁰ In Russian: Содружество Независимых Государств, СНГ.

²¹ http://en.wikipedia.org/wiki/Commonwealth_of_Independent_States

²² Adopted at the fourteenth plenary meeting of the Interparliamentary Assembly of the CIS Member-States (decree 14-19 dated 16.10.1999)

(actions that go beyond commands and influence industry or society), and all forms of social control or influence (whether by the state or the market)²³.

Data protection can be taken as an example of regulation by the state. Baldwin and Cave (1999, p.2) note that regulation may be seen as both an enabling and facilitating activity, as well as one that constrains actions; it can empower as well as prevent²⁴. There are a variety of legal routes that are available for regulating data protection. They can be general or sector specific laws, constitutional provisions (the Fourth Amendment in the US), privacy torts, contractual remedies and privacy protective restrictions in other laws (e.g. control of wiretapping)²⁵.

Since the 1970s, comprehensive and general data protection laws have been regarded as essential tools for regulating the use of personal data through the law²⁶. Greenleaf provides short survey of the data protection laws history²⁷. Until 1980s data privacy laws were a European phenomenon (Sweden, Germany, Austria, Denmark, France, Norway and Luxembourg, UK, Ireland, Iceland, Finland, San Marino and the Netherlands, and three UK territories had data protection laws), other than the US which regulated only the public sector. In 1981 Israel was the first non-European state to enact, with Australia, Japan and Canada providing 'public sector only' legislation. Most remaining western European countries (EU and EEA) enacted laws (Portugal, Belgium, Spain, Switzerland, Monaco, Italy and Greece) in 1990s. They were joined by former 'eastern bloc' following the collapse of the Soviet Union (Slovenia, Czech Republic, Hungary, Slovakia, Poland and Albania), and the first ex-Soviet-republics (Lithuania and Azerbaijan) did likewise. In this way, the trend spread outside Europe to other parts of the world.

²³ Baldwin, R., and Cave, M., *Understanding Regulation: Theory, Strategy, and Practice*, (OUP 1999), p.2

²⁴ Ibid.

²⁵ Gellman, R., 'Conflict and Overlap in Privacy Regulation: National, International, and Private' in B.Kahin and C.Nesson (eds), *Borders in Cyberspace* (The MIT Press 1997).

²⁶ Note 3, p.125.

²⁷ Greenleaf G., 'Global data privacy laws: 89 countries, and accelerating', [2012] Privacy Laws & Business International Report, Issue 115 Special Supplement, February 2012.

Bennett attempts to explain the spread of data protection that started from the 70s of the last century (yet he does not examine the changes in the content of the laws)²⁸. As prerequisite factors, he mentions the growth of big governments and consequent public perceptions of the decline of accountability and the increase of state intrusiveness in private lives. He shows that these factors are insufficient to explain the passage of legislation, and mark other factors as important, such as patterns of diffusion and policy-learning through the interactions of a policy community or ‘network or policy experts that enjoyed constant communication through informal personal meetings, international organizations, conferences, articles, and books’²⁹. He further refers to effects of penetration into domestic policy agenda by external sources and obligations (such as, Convention 108 or EU Directive).

In Eurasia, all but four countries have general data protection laws in place. The Table 1 summarizes their regulatory instruments³⁰:

Table 1. Legislative Instruments

<i>Country</i>	<i>Act</i>	<i>Year</i>	<i>Sector</i>	<i>Convention 108</i> ³¹
Armenia	Law on Personal Data	2002	Both	RC; RP;
Azerbaijan	Law on Personal Data	2010	Both	RC
<i>Belarus</i>	<i>No specific law</i>			
Georgia*	Law on Personal Data Protection	2012	Both	RC; SP
Kazakhstan	Law on Personal Data and its Protection	2013	Both	
Kyrgyzstan	Law on Personal Data	2008	Both	
Moldova	Law on Personal Data Protection	2007	Both	RC; RP

²⁸ Bennett, C., ‘Understanding Ripple Effects: The Cross-National Adoption of Policy Instruments for Bureaucratic Accountability’ (1997) 10 Governance: An International Journal of Policy and Administration 213.

²⁹ Ibid., p.227.

³⁰ The data is taken from Greenleaf, 2013.

³¹ RC = Member and has ratified the Convention;

RP = has also ratified the optional protocol;

SP = Member and has signed but not ratified Additional Protocol;

Russia	Federal Law on Personal Data	2006	Both	RC; SP
<i>Tajikistan</i>	<i>No specific law</i>			
<i>Turkmenistan</i>	<i>No specific law</i>			
Ukraine	Law on Personal Data Protection	2012	Both	RC; RP
<i>Uzbekistan</i>	<i>No specific law</i>			

We can make several observations from the information on the table. First, half of the countries are members to the Convention 108 and within the Convention's framework are obliged to incorporate its rules into their domestic laws. Accordingly, we can see with a degree of certainty that the Convention 108 was also affluent, at the least in motivating the countries that have ratified it to adopt general data protection laws (we will question whether Convention 108 had any effect on its content in Chapters 2-4).

Second, most of the countries (eight out of twelve) have chosen to address the data protection issues in a general law. These countries are six Convention 108 ratifiers plus Kazakhstan and Kyrgyzstan.

Thirdly, four countries do not have general data protection laws, namely, Belarus, Tajikistan, Turkmenistan and Uzbekistan. However, this paper anticipates that these countries will also adopt general data protection laws. In particular, Uzbekistan is believed to have already ready draft of comprehensive law, but not adopted³².

Fourthly, all of the countries have enacted their laws after 2000. The chronology allows us to wonder whether transnational instruments discussed above could have had an impact on the legislation in Eurasian territory.

Furthermore, the post-2000 adoption also allows us to assume that Eurasian countries have mostly designed their frameworks *ab initio*: a relatively blank slate has allowed comprehensive legislation to be introduced in both public and private sectors.

³² Russian DPA (Federal Service for Supervision of Communications, Information Technology and Mass Media), 'Information on Authorized Bodies of Other Countries' (2010) <<http://pd.rkn.gov.ru/authority/p119/>> accessed 3 Nov 2014.

A number of Eurasian countries regulate specific sectors with separate legislation, along having a general data protection law. The limits of this thesis do not allow to comprehensively embrace all sectoral legislation of each Eurasian country. Therefore, we only summarize here the main purposes of sector specific regulation as well as examples of areas regulated sectorally in global practice.

Sectoral laws may be employed for various reasons such as³³:

1. to deal with special problems and to grant specific individual rights;
2. to empower public agencies or to legalize certain functions for which personal data are processed with privacy safeguards;
3. to clarify rights and responsibilities;
4. to restrict the application of privacy principles in order to accommodate policies that are considered more important (for example, internal security, organized crime and antidrug activities in Switzerland).

A number of countries with general data protection laws also regulate specific industries and technologies sectorally. Examples of such countries are Netherlands, Germany, Austria, Finland, Norway, Sweden, and Denmark and the laws cover diverse set of issues, such as the census, public service ‘one-stop-shops’, public order, telecommunications, video surveillance, sensitive data registers, credit cards, public archives, the media, data matching in the field of taxation, and the collection of personal data for payroll wage-deduction³⁴.

In the following subsections, we consider the instruments that are not purely legal.

³³ Note 3, pp.131-132.

³⁴ Ibid., pp.131-132.

1.4 Self-Regulatory instruments

Legal instruments have been the dominant way of data protection regulation since the 1970s. Now we turn to analyse the instruments without statutory force. They can be in the forms of codes, guidelines, standards and other titles. Generally, they are made to “influence, shape, or set benchmarks for behaviour in the marketplace”³⁵, with range of incentives and sanctions for compliance.

Data protection laws of Eurasian countries do not provide for self-regulatory instruments³⁶. Therefore, the purpose of this section is to offer policy-makers the pros and cons of self-regulatory instruments. We believe that self-regulatory instruments should be encouraged as a complimentary tool to laws. In the EU, for instance, Article 27 of the EU Directive explicitly requires the European Commission and Member States to ‘encourage the drawing up of codes of conduct intended to contribute to the proper implementation of...national provisions...taking account of the specific features of various sectors.’

Self-regulatory instruments can be useful in a number of ways. Netherlands Data Protection Authority suggests (in the example of privacy codes of practice) that self-regulatory instruments are developed with four motivations: to avoid legislation, to anticipate legislation, to implement legislation, and to supplement legislation (Hustinx 1991). Given the condition that self-regulation should be complementary to a general data protection law, we can slightly rephrase them. First, self-regulatory instruments can help organizations to avoid further legislation for sector-specific issues. For instance, financial institutions in country A might agree on a code of practice, which is based on a general data protection law that would deal with data protection in data sharing area. This might help them avoid

³⁵ Ibid..

³⁶ During the course of this research, we have found only self-regulation example in Ukraine. Article 27(2) of Ukrainian Data Protection Act allows associations and legal entities are allowed to draw-up codes of conduct, which are subject to approval of the data protection authority. Such codes are used in Ukraine by mobile companies, payment data exchange companies, by members of the American and European Chambers of Commerce in Ukraine (Kozak V., Personal data protection in Ukraine: Practice and problems, (2013) 60 Journal of Personal Data 7).

statutory regulation provided that the code of practice effectively operates. Second, they can be used to anticipate the legislation. Most of the Eurasian countries, even those that have general data protection laws, do not specifically regulate use of cookies. Popular online businesses might work out a solution that can strike the balance between the need to protect privacy of web-site users and their own commercial interests. There is a good chance that businesses, being market insiders might come up with a viable solution as opposed to those sitting in public offices. Such solution could be taken up by policy makers and spread to the whole sector. Third and fourth, self-regulation might assist implementing and supplementing the legislation, by filling in the gaps.

It is worth to note that data protection authorities could act as negotiators with data controllers in drawing up, for example, codes of practice. Furthermore, they could themselves publish template instruments ready for use by data controllers. UK Information Commissioner's Office, as an example, has published codes of practice for anonymisation, big data, CCTV, employment, privacy notices and other issues³⁷.

Unlike laws, self-regulatory instruments are not subject to statutory enforcement. For that reason, it is important to have the necessary mechanisms in place to ensure their efficacy. Bennet&Raab, in particular, identify the four items³⁸:

- a) there should be an agreement and commitment to an organizational policy;
- b) that policy should be codified throughout the organization or sector;
- c) some external and independent conformity assessment process should be set up to verify the practices; and
- d) a 'seal of good house-keeping' (i. e. compliance) can be assigned based on the findings of the assessment process.

More often than not, however, self-regulatory instruments lack the second and third elements. Moreover, there is often a presumption that self-regulatory instruments are more symbolic than real as those who are interested in data processing carry the responsibility to

³⁷ UK DPA (Information Commissioner's Office), Topic Guides for Organisations, (2014) <http://ico.org.uk/for_organisations/data_protection/topic_guides> accessed 4 Nov 2014.

³⁸ Note 20, pp151-176.

implement the instruments. Likewise, some scholars have argued that capitalists enterprises³⁹ or, generally, bureaucratic organizations⁴⁰ might inherently have, in their logic, the urge to collect and process bigger number and more refined types of personal data. This and other criticisms drive us to disfavour self-regulation as self-sufficient alternative to legal regulation. As we have mentioned above, Eurasian countries' data protection laws do not provide for self-regulatory instruments. Yet we believe that self-regulatory instruments should be encouraged as a complimentary tool to laws, and above discussed advantages and shortcomings of self-regulatory instruments should taken into consideration.

1.5 Technological instruments

Today's war on privacy is intimately related to the dramatic advances in technology. Bennett&Raab shortly analyses this truism, by questioning the extent to which technology operates as an autonomous or deterministic force. For the purposes of this paper, we avoid this heavy debates and content ourselves with the view that if one accepts that at least part of the privacy problem is caused by the properties inherent in the design of certain information technologies, then it follows that the same tool can be employed to protect privacy, rather than invade it. We, furthermore, do not address the technologies itself available in Eurasian countries, but rather focus on how they can be used as policy instruments.

Likewise to self-regulatory instruments, the present study has not found practical examples of technological instruments that are used to address data protection problems in Eurasian countries. Therefore, this subsection recommends Eurasian policymakers to consider the use of technological instruments and is meant to serve as a starting analysis point.

To begin with, in the area of data protection, it is usually referred to PETs - privacy-enhancing technologies, which need to be differentiated from data security technologies. Data security refers to making data processing safe regardless of the legitimacy of processing (eg with passwords). By contrast, PETs "seek to eliminate the use of personal data altogether or to give direct control over revelation of personal information to the person

³⁹ Gandy, O.H., *The panoptic sort: A political economy of personal information* (1993 Westview Press).

⁴⁰ Rule et al, *The Politics of Privacy*, (New American Library 1980).

concerned⁴¹. To illustrate, a company can store personal data of highly sensitive nature extremely secure. This is an example of data security, but not a PET, which would question, rather, if such data should be collected in the first place (or undergo other types of processing). As such, data security is an important element, and many legislative instruments require data processors to put in place the necessary data security measures. Yet, data protection is definitely broader than data security, and looks at the legitimacy of data processing in the first place.

Having clarified the difference from data security, we can move on to their use as policy instruments. Policy-makers can consider the following uses⁴²:

- i. As systemic instruments - those that are created as a result of decisions made by engineers (both hardware and software). This group corresponds to Lessig's (1999) Code⁴³ and Reidenberg's (1998) Lex Informatica⁴⁴. A privacy-friendly example is the Internet Protocol (IP) address, which is designed to identify the machines exchanging data packets, but not the users⁴⁵. A privacy-unfriendly example are the cookies that allow organizations to maintain and profile data on users of a website;
- ii. As collective instruments - those that are created as a result of government policy which envisages building privacy into services and goods. A good example is the development of public-key infrastructures (PKI);
- iii. As instruments of individual empowerment - those that require end-users to make the choice. Examples are encryption, anonymity and pseudonymity, filtering and other tools.

It is possible to reach three conclusions:

⁴¹ Burkert, H., 'Privacy-enhancing technologies: typology, critique, vision' in Agre P.E. & Rotenberg M. (eds), *Technology and Privacy* (The MIT Press 1997), p125.

⁴² Bennett&Raab 1997, pp177-202.

⁴³ Lessig L., *Code: Version 2.0*, (2006)

⁴⁴ Reidenberg, J: "Lex Informatica: The Formulation of Information Policy Rules Through Technology", *Texas Law Review*, 1998, volume 76, pp. 553-593.

⁴⁵ Note 44, pp32-33.

1. PETs complement, rather than replace, regulatory and self-regulatory approaches. On a policy level, Eurasian governments can encourage the development of PETs (through research funding, procurement, legislation etc.) or discourage (e.g. Levy 2001 notes the attempts by US law enforcement and security agencies to restrict the availability of free encryption);
2. PETs can serve as a standard or a condition in service delivery systems. Eurasian regulators might, for instance, require advanced encryption technologies in biometric data processing.

1.6 Findings

We broadly reach three conclusions. First, European data protection instruments have been the most affluent in Eurasian countries. A number of them (Armenia, Azerbaijan, Georgia, Moldova, Russia and Ukraine) are ratifiers of the Convention 108 and as a result have incorporated its rules into their domestic legislation. Furthermore, some countries are in the pursuit of closer integration with the EU, including in legislative framework, and have enacted laws resembling the EU Directive. This resemblance can especially be seen in Georgia, Moldova and Ukraine, which also have institutional framework (ie data protection authorities) alike to European Union model.

Second, like in most parts of the world, Eurasian countries recognize data protection values (through the notion of privacy, in general) on a constitutional ('the right to privacy') and a statutory level. Most of the countries in region have data protection laws in place. Other countries are either drafting their general data protection laws, or addressing the issues through sector-specific laws. Furthermore, those countries with general laws also regulate certain area/types of data processing sectorally (in particular, in law enforcement area).

Third, there is currently no studies conducted to assess the level of use in these countries of self-regulation and technology as policy instruments. Similarly, there is a lack of studies in practical implementation of data protection laws, in other words, the extent to which they provide protection to data subjects in reality. These three issues require further research and are not within the scope of this paper.

2 Chapter 2. Concept of personal data

In this part, we analyse the scope of data protection regulation in Eurasian countries in the example of ‘personal data’ definition. We look at the concept of personal data - the central concept in data protection laws which directly affect their scope of application. In particular, we identify the core elements, as well as discuss certain ambiguities in the used terms.

2.1 Introduction

The data protection regulation aims to protect *personal data*. As such, all types of data but personal fall outside the regulatory scope. The central question is, thus, what data is personal? During our study, we analyse eight Eurasian countries (see Table 4 and Annex A) which have general data protection laws, as well as three transnational instruments discussed in Part I, as these instruments have had considerable influence in global data protection policies.

To start with, Eurasian law, like most of the laws in the world do not define ‘data’ and its exact meaning, together with the term ‘information’ is usually “taken for granted in the regulatory discourse”⁴⁶. The laws usually stress on the link between data and persons, as we discuss in the next section.

As we can see from the Table 4, which provides the statutory definitions, the core of the ‘personal data’ definition is information/data that relates to an identified or identifiable natural person. This basic definition is also contained in Convention 108 (Article 2(a)) and OECD Guidelines (para 1(b)), and the EU Directive (Article 2(a)). Georgia and Moldova offer more clarification by defining further who an ‘identifiable person’ is. According to their laws, the person is identifiable if they can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors (eg physical, physiological, mental, economic, cultural or social). This definition matches with the text of the EU Directive (Article 2(a)) and demonstrates that these countries adopted the European approach.

⁴⁶ Bygrave L., Data Privacy Law (OUP 2014), p126.

Based on these definitions, it is possible to identify two requirements for finding of personal data. First, the data must be about or linked to a natural person. As such legal persons' data is not afforded protection under data protection legislation. Similarly, all eight Eurasian countries that have general data protection laws recognize only natural persons as subjects of personal data (See Table 2 and Annex A). Second, the personal data allows identification of a natural person. We discuss this condition separately, as identifiability has a number of issues that needs broader analysis.

*Table 2. Definition of Personal Data*⁴⁷

Country	Definition
Armenia	any data fixed in writing or other otherwise on tangible medium containing facts, events and circumstances a natural person, in a form that allows or may allow to identify the individual
Azerbaijan	any information that allows directly or indirectly to identify a person
Georgia	any information relating to an identified or identifiable natural person. An identifiable person is the one who can be identified directly or indirectly, in particular by reference to an identification number or to the factors specific to his/her physical, physiological, mental, economic, cultural or social identity
Kazakhstan	information relating to an identified or identifiable thereof data subject recorded in electronic, paper and (or) any other tangible medium
Kyrgyzstan	information recorded in tangible form about a specific person, matched with a specific person or that can be matched with a specific person, allowing to identify this person directly or indirectly by referring to one or several factors specific for his/her biological, economic, cultural, civil or social identity. Personal data include biographic and identifying data, personal characteristics, information on the marital status, financial position, state of health, etc.
Moldova	any information relating to an identified or identifiable natural person ('personal data subject').

⁴⁷ For full text of concerned articles, see Annex A.

	An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity
Russia	any information related directly or indirectly to an identified or identifiable natural person
Ukraine	information or aggregate information about a natural person who is identified or may be identified
Convention 108	any information relating to an identified or identifiable individual
OECD Guidelines	any information relating to an identified or identifiable individual (data subject).
EU Directive	any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity
CIS Model Law	information (recorded in a tangible medium) about a particular person, that is related or can be related to him. Biographical and identifying data, personal characteristics, information on family, social status, education, profession, business and financial situation, health and others are considered to be personal data.

2.2 Identifiability

In general, identification means the ability to distinguish a person from others by linking them to collected data. In this sub-section, we discuss some of the issues related to the identifiability criterion.

The starting point is that personal data is generally given broad interpretation. The confirmation can be found in the language used in Eurasian laws which refer to *any data* (see

Table 4).⁴⁸ In the EU, for instance, data is usually presumed to be ‘personal’, unless it can be clearly shown that it would be impossible to tie the data to an identifiable person (ie the data is truly anonymous)⁴⁹. Bearing this broad interpretation approach in mind, we analyse some of the characteristics of identifiability that affect the application scope of data protection laws.

First, a natural person can be distinguished from others directly or indirectly. Name is an obvious example of direct identification, while indirectly it is possible to identify a person with one piece of data, such as via identification numbers (eg passport number, car registration number, social security number) or a set of data ‘which allows ... to be recognized by narrowing down the group to which [the person] belongs (age, occupation, place of residence etc)’⁵⁰. An example of the data set would be when we look at ‘all males over 50 living in city X who are physicians, have two daughters, listen to Verdi operas and have vacation houses in the south of France’⁵¹. In this example, if we consider each fact separately from others, it will not be possible to identify, however, taken together there is a possibility to link this description with a specific person or persons. The EU Directive expressly covers both direct and indirect forms of identification (Article 2(a)). Similarly, Azerbaijan⁵², Georgia⁵³, Kyrgyzstan⁵⁴, Moldova⁵⁵, and Russia⁵⁶ expressly mention in their laws both types of identification. The rest of the Eurasian countries (Armenia, Kazakhstan, Ukraine) are silent and do not offer clarification on the issue.

Second issue is the level of identification, i.e. how easily a person must be identified from data in order for it to be regarded as ‘personal’. Eurasian countries do not set the level of identification applicable under their legal frameworks. The level of identification is im-

⁴⁸ This paper has not studied any public report or case law confirming or denying broad interpretation approach in the Eurasian countries.

⁴⁹ Kuner Ch., *European Data Protection Law: Corporate Compliance and Regulation* (2nd edn, OUP 2007), para 2.76.

⁵⁰ European Commission (COM(92) 422 final - SYN 287) 9.

⁵¹ Note 50, para 2.75.

⁵² Article 2.1.1, Azerbaijani Data Protection Act.

⁵³ Article 2(a), Georgian Data Protection Act.

⁵⁴ Article 3, Kyrgyz Data Protection Act.

⁵⁵ Article 3, Moldovan Data Protection Act.

⁵⁶ Article 3(1), Russian Data Protection Act.

portant as data protection laws safeguard individuals against potential of identification, as opposed to actual achievement of identification. In other words, it is irrelevant whether data controllers do/did identify the natural person, mere capability of identification bring the laws into operation. Two international instruments offer some guidance on this question. Explanatory Report for Convention 108 (para28) refers to ‘easy’ identification and provides that identification by means of ‘very sophisticated methods’ is not covered under the term ‘identifiable person’. Bygrave⁵⁷ criticizes this approach as it is based on the false assumption that as sophistication level increases, ease of identification decreases⁵⁸. In practice, advanced sophistication often allows to identify a data subject easily. By contrast to Convention 108, the EU Directive takes account of ‘all the means likely reasonably to be used’ for identification purposes (Recital 26). As such, the Directive sets two interlinked criteria: likelihood (or probability) and reasonableness (or difficulty) of identification. In general, it seems that the main focus should be on the reasonable means available for identification, and such ‘reasonableness’ might change over time, in particular with advancement of technologies.

Third related issue to the previous identification level question is whose capability the laws consider for the purposes of identifiability criteria. In other words, should do we assess only the abilities of the data controllers/processors who are processing the data or should we take into account the possibility of identification by any person? Unlike most laws that are silent on this issue⁵⁹ (including Eurasian laws), the EU Directive specifies that any person can be the legally relevant agent. Nevertheless, the standard of ‘any person’ should be weighed against the ‘reasonable’ likelihood, which excludes use of illegal means (eg hacking) for identification.

Fourth, most of the data protection laws assume individuation of data - that is, that the data is linked to one person as opposed to a number of them (eg family, social group)⁶⁰. The

⁵⁷ Note 47, p131.

⁵⁸ Subsequent recommendations of Council of Europe instead refer to factors of reasonableness, time, resources, and cost of identification. See note 47, p131 where he refers to a number of such recommendations.

⁵⁹ Note 47, p132.

⁶⁰ *ibid.* p135.

definitions contained in Eurasian laws also use individuation language and do not grant protection to collective personal data. By contrast, some countries also protect data that can be linked to ‘family’ or ‘household’ (Finland), yet such provisions are rare⁶¹.

Finally, it is worth to note that the above discussed identifiability issues are not simply academic exercises, and carry practical weight. They affect the extent to which data can be classified as personal, and consequently determine the scope of application of data protection laws.

2.3 Data in medium

A number of Eurasian laws also include a requirement that the personal data need to be recorded in a tangible medium. Such requirement can be found in Armenia⁶², Kazakhstan⁶³, Kyrgyzstan⁶⁴, and the CIS Model Law⁶⁵. However, these laws do not provide clarification as to what tangible medium is. Some guidance is available as to the forms such medium can take. Two of the laws give examples of tangible mediums, such ‘in writing or otherwise’ (Armenia), and ‘in electronic, paper and (or) other tangible medium’ (Kazakhstan). These examples suggest that any medium fulfils the requirement as long as it is tangible (phrases ‘otherwise’ and ‘other’). As such, the reason behind the requirement of ‘tangible medium’ seems to be the intention of the legislator to exclude data in purely oral form. If the oral personal data is recorded in audio or video format for example, electronically, such data might become subject to data protection rules.

Georgia, Moldova, and Ukraine, by contrast, do not use ‘tangible medium’ requirements. Similarly to the European approach, they instead apply ‘automated’ and ‘non-automated’ data classifications and do not refer to ‘tangible medium’. Statutory provisions defining the scope of application cover ‘the processing of data wholly or partly by automatic means, as well as to the processing otherwise than by automatic means of data which form part of a

⁶¹ *ibid.*

⁶² Article 3, Armenian Data Protection Act.

⁶³ Article 1(2), Kazakh Data Protection Act.

⁶⁴ Article 3, Kyrgyz Data Protection Act.

⁶⁵ Article 2, CIS Model Law.

filing system or are processed to form part of a filing system’⁶⁶. The filing system means that non-automated data is covered only when it is structured according to a specific criteria, thereby excluding unstructured records (e.g. manual records). As such, they specify two types of data: any data processed automatically and non-automated data in a filing system. These provisions resemble those under the EU Directive⁶⁷, and demonstrates the adoption of the Directive’s approach by Georgia, Moldova, and Ukraine with regard to the concept of personal data.

There are several implications that follow depending on whether a legislator adopts ‘tangible medium’ requirement or ‘automated/non-automated’ data classification. First, ‘tangible medium’ requirement covers both the automated and non-automated structured data, as well unstructured non-automated data (i.e. any data). This means, on the one hand, that data subjects are granted comparatively wider protection than under the latter approach. On the other hand, it places relatively greater burden on data controllers, for example, if data subjects request to disclose their personal data that data controllers hold, the controllers might have to check all their files, both automated and non-automated and non-structured. In other words, they will have to ‘leaf through files, possibly at great length and cost, and fruitlessly, to see whether it or they contain information relating to the person requesting information and whether that information is data’⁶⁸ subject to data protection laws.

Perhaps these are the reasons why Russian law uses both criteria. Its law applies to ‘activities related to the processing of personal data ... both automatically ... and manually, provided that manual data processing is by its nature similar to automatic data processing, i.e. allows users to search personal data recorded in tangible medium or contained in filing systems or other systematized collections of personal data in accordance with the specified algorithm...’⁶⁹. In this way, the Russian law excludes oral forms of data and also addresses

⁶⁶ Article 3 of Georgian, Article 2 of Moldovan, and Article 1 of Ukrainian Data Protection Acts.

⁶⁷ Article 3(1).

⁶⁸ *Durant vs Financial Services Authority* [2003], EWCA Civ 1746, Court of Appeal (Civil Division) paras 47-48.

⁶⁹ Article 1(1), Russian Data Protection Act.

the shortcomings of not differentiating structured non-automated data from the unstructured one.

2.4 Findings

In this chapter, we have analysed the concept of personal data under Eurasian data protection laws.

First, all Eurasian countries apply the same basic standard to categorisation of data as personal (see 2.1. above). The origin of this approach lies in Convention 108, and we can conclude, in the example of the ‘personal data’ concept, that Convention 108 has had an important influence in Eurasian data protection framework. Moreover, clear adoption of the European data protection model (specifically, the EU Directive) can be found in the laws of Georgia and Moldova. In particular, we have observed this when we discussed who an ‘identifiable person’ is, and in classification of personal data to automated and non-automated ones.

Second, most of the Eurasian laws do not offer guidance on deeper issues surrounding the key criterion of the concept, namely identifiability (see 2.2 above).

Thirdly, unlike European data protection laws, some Eurasian countries also require personal data to be in a tangible medium (Armenia, Kazakhstan, Kyrgyzstan, and Russia) (see 2.3 above). These countries (except Russia), furthermore, do not differentiate between ‘automated’ and ‘non-automated’ data.

3 Chapter 3. Transborder dataflow regulation

3.1 Introduction

We have mentioned earlier that development of data protection laws have been continuing since the 1970s, as a response to privacy risks posed by new technologies. The invention of Internet has increased these risks, expanding the problem transnationally, allowing data to flow through jurisdictional barriers. We particularly choose to compare the laws of Eurasian countries in relation to transborder dataflow regulation for the following reasons:

- A) Economic globalization. Advanced technology, as well as communications, services, transport, industry, economic and institutional innovations (such as World Bank) have increased the pace of world integration. The result was the increased flows of data, amongst other things (such as capital, goods, services, labour). Eurasian countries are obviously also part of economic globalization and are experiencing higher levels of data transfers than they did before;
- B) Economic importance. It was estimated in 2010, as an illustration, that data analytics industry alone was worth more than 100 billion USD, with annual growth rate of almost 10%⁷⁰. Given the economic importance, it is assumed that Eurasian states would also be keen to develop and benefit from industries connected with data processing;
- C) Social and cultural importance of online activity. People, irrespective of their geolocation, experience online social and cultural exchange with each other. Online activity might also have political implications, as it was in ‘Arab Spring’ in 2011⁷¹. Eurasian states, as any other, might be interested in facilitating and/or controlling this process;

⁷⁰ The Economist, ‘Data, data everywhere—A special report on managing information’, (2010) <<http://www.economist.com/node/15557443>> accessed 5 Nov 2014.

⁷¹ Journalist’s Resource, ‘*The Arab Spring and the Internet: Research roundup*’, (2013) <<http://journalistsresource.org/studies/international/global-tech/research-arab-spring-internet-key-studies>> accessed 5 Nov 2014.

- D) Ubiquity of data flows. Data packets do not flow according to jurisdictional division rules. They are devised to find the optimal route through network. Such flow happens naturally, without the awareness of its senders and recipients, not mentioning the law enforcement agencies. Regulation of data transfers is an example of how domestic laws are dealing with global phenomena;
- E) EU adequacy test. Article 29 Working Party explicitly acknowledges the relevance of data transfer provisions for ‘adequacy’ assessment⁷². As such, the comparative analysis here could be useful for the purposes of ‘adequacy’ studies of Eurasian states, at least in relation to data transfer provisions.

In this chapter, we analyse the regulation of transborder data flows in Eurasian countries under data protection laws (see Annex B). Apart from data protection law, it can be a subject of regulation under telecommunications, import-export regulations and other laws, which we do not cover due to the focus of this paper on privacy law. The followings are the key aspects of the transborder dataflow regulation:

- 1) definition. The definition of ‘transborder data flow’ directly affects the extent to which the law applies. The challenge is to strike the balance between covering too little and extending to everything;
- 2) grounds. Data controllers should have the grounds broad enough to facilitate free flow of data (which brings economic, social and cultural benefits), and narrow enough to protect privacy rights of data subjects;

This chapter will be organised accordingly under two respective headings.

⁷² Article 29 Working Party (Working Party on the Protection of Individuals with regard to the Processing of Personal Data), *Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive* (1998).

3.2 Definition

In general, there is a lack of clarity as to its meaning as a term⁷³. To illustrate, the EU Directive refers to ‘transfer to a third country of personal data’ without addressing what ‘data transfer’ is (Article 25(1)). Convention 108 refers to ‘transborder flows of personal data’, defining the term as ‘the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed (Article 12(1)). OECD Guidelines refer to ‘transborder data flows’, defining the term as ‘movements of personal data across national borders’ (§1(c)).

Furthermore, there are different approaches in wording of the phrase. To illustrate, in most of the Eurasian data protection laws (five out of eight) we see ‘transborder transfer’⁷⁴. This can be compared with the EU Directive which refers to ‘transfer to a third country’ (Article 25) and Armenian (Article 13), Georgian (Article 41), and Ukrainian (Article 29) laws - ‘transfer to foreign states/organizations/persons’, the Convention 108 - ‘transborder flows’ (Article 12), and OECD Guidelines referring to - ‘transborder data flows’ (para 17). Other instruments might use different phrases, for example ‘international transfer’, ‘information flows across borders’, ‘cross-border information flow’, and ‘cross-border data transfer’ (used interchangeably in APEC Privacy Framework), or ‘data transfer’ (Canadian PIPEDA). For the purposes of this paper, we use the terms interchangeably.

The various wording and lack of clarity reflects the difficulty of defining it. As a starting point, ‘data transfer’ can take active form (organization A sending data to Organization B in third country) and passive form (data being made available to recipients in other countries, for example on a web-site). Kuner claims that current laws see transborder data flows only in active form, where it is initiated by a person (public or private)⁷⁵. It is not entirely clear if this is the explicit choice of law-makers.

⁷³ Kuner Ch., *Transborder Data Flows and Data Privacy Law* (OUP 2013), pp11-14

⁷⁴ Azerbaijan (Article 14), Kazakhstan (Article 16), Kyrgyzstan (Article 25), Moldova (Article 32), Russia (Article 12), CIS Model Law (Article 10).

⁷⁵ Note 74, p11.

On the other hand, if passive data transfers are also covered by the term ‘transborder data flows’, then its regulation would apply to the whole Internet (for example, data on a web-site can be accessed from any place in the world with Internet access). This view was acknowledged in the EU by the European Court of Justice in *Bodil Lindqvist* case⁷⁶. The Court found that there is no data transfer to a third country within the meaning of Article 25 of the EU Directive where a person in the EU loads personal data onto a web-page hosted by a natural/legal person established in the EU. The Court based on the fact that the information was not being sent automatically from the server to other Internet users (‘targeting’).

In Eurasian context, ‘targeting’ seem to take primary role, or at the least more explicit one. While most of the laws do not define ‘data transfer’, four instruments that have the definition use the phrase ‘provision’. It supposes that data controller provides or makes the data accessible for processing to third persons (or ‘targets’ them), thereby referring to the active form of transfer. Three of these (Azerbaijan⁷⁷, Kyrgyzstan⁷⁸ and CIS Model Law⁷⁹) refer to provision of ‘data’ and Kazakhstan⁸⁰ refers to provision of ‘access to data’, although this difference in word choice is insignificant, as provision of ‘data’ unavoidably involves provision of ‘access’ to it and the vice versa. Although other Eurasian countries’ data protection laws do not clarify what ‘data transfer’ is, we assume that they understand the term in its active form whereby the transfer would be targeted at specific recipients.

Yet it should be kept in mind that technological developments in the future could blur the distinction between active and passive transfers up to a ‘point where it can no longer be maintained’⁸¹. As such, it is not possible to rely solely on ‘targeting’. Kuner notes that establishing ‘data transfer’ may depend on the facts of the particular case⁸². In particular, he mentions three circumstances, namely establishment, targeting, and degree of control,

⁷⁶ C-101/01 [2003] ECR I-12971.

⁷⁷ Article 2.1.13, Azerbaijani Data Protection Act.

⁷⁸ Article 3, Kyrgyz Data Protection Act.

⁷⁹ Article 2, CIS Model Law.

⁸⁰ Article 1(15), Kazakh Data Protection Act (the definition of the term ‘data dissemination’).

⁸¹ Note 74, p13.

⁸² *Ibid.*, p14.

which can be used to determine if ‘data transfer’ took place and if, as a result, transfer provisions apply. He contrasts, for instance, the occasion where the data controller has an establishment⁸³ in the country where the data subject resides with the situation when the controller does not have any operations in the country. Similarly, the ‘data transfer’ is more likely to be found when the controller in some way targets the individual, rather than when the individual initiates the contact with the controller without being targeted. The probability of finding ‘data transfer’ is also high when the controller has some degree of control over the means used by the individual to process the data, but less likely when the controller does not exercise control over the purpose or means which the individual uses to process the data.

Furthermore, it is necessary to differentiate between data transfers and ‘mere transits’. An example of such transit is where data is routed on the Internet according to technical parameters, based on the best path for a data packet to travel, irrespective of geographic places it crosses. Transborder data flow regulations usually do not apply to situations where data only transits through territories. For instance, as we read this paper, huge number of data packets could be crossing the country of our location, without our awareness. Neither are regulators nor do they need to be aware (as the ‘transit’ does not create legal implications in the country it crosses). As a matter of clarity, however, interpretation of ‘transit’ is usually construed narrowly⁸⁴, and the extent of the distinction between transfer and transit remains uncertain. Only two Eurasian countries (Georgia⁸⁵ and Moldova⁸⁶) explicitly exclude ‘mere transit’ from the scope of their data protection laws, with very similar wording to the text of the EU Directive. Similarly to the EU Directive text, they do not draw clear line between data transfer and transit⁸⁷.

⁸³ For a recent example, see Google Spain case (C-131/12 (2014) not yet published), para 45-60.

⁸⁴ Article 29 Working Party 2010, p23.

⁸⁵ Article 3(2)(b), Georgian Data Protection Act.

⁸⁶ Article 2(2)(c), Moldovan Data Protection Act.

⁸⁷ *ibid.* Acts apply ‘to the processing of personal data carried out by controllers that are not established on [their] territory ..., making use of equipment situated on [their] territory ..., unless such equipment is used only for purposes of transit through the territory...’.

Finally, most of the Eurasian countries refer to ‘territorial’ or, in other words, physical crossing of borders in their transborder data flow provisions. This is the case in the laws of Armenia⁸⁸, Azerbaijan⁸⁹, Kazakhstan⁹⁰, Georgia⁹¹, Moldova⁹², and Russia⁹³. Kyrgyzstan⁹⁴, CIS Model Law⁹⁵ and Ukraine do not use ‘territorial’ division, instead the first two refer to ‘foreign jurisdictions’ whereas Ukraine⁹⁶ takes the foreign recipient as the criterion for application. Perhaps, the majority preference for ‘territorially’ based application reflects the challenges that regulators with traditional legal tools face in the environment of modern technologies.

To sum up, transborder dataflow rules apply to cases where the data is transferred actively across borders, save for ‘mere transits’. However, the regulators envisage the circumstances where the data should or should not flow, as we see further.

3.3 Grounds for transfer

Data transfer regulations might target broadly recipients based on two criteria: their geographic location or the organizations themselves. Table 3 summarises the grounds for cross-border transfer available under Eurasian countries legislation. We use the information on the table to analyse their regulatory approaches in comparison with each other, as well as with transnational instruments discussed in 1.2. above (i.e. Convention 108 (as well as Additional Protocol to it), the EU Directive, OECD Guidelines, and CIS Model Law). We use the information in the table in order to determine whether the Eurasian countries have adopted adequacy approach, or accountability approach, or a combination of them (see 3.3.1-3.3.2 below).

⁸⁸ Article 13, Armenian Data Protection Act.

⁸⁹ Article 2.1.16, Azerbaijani Data Protection Act.

⁹⁰ Article 16(1), Kazakh Data Protection Act.

⁹¹ Article 41, Georgian Data Protection Act.

⁹² Article 32(1), Moldovan Data Protection Act.

⁹³ Article 3(11), Russian Data Protection Act.

⁹⁴ Article 3, Kyrgyz Data Protection Act.

⁹⁵ Article, CIS Model Law.

⁹⁶ Article 29(3), Ukrainian Data Protection Act.

Table 3. Grounds for cross-border data transfers (simplified)⁹⁷

Country	Grounds
Armenia	1. international treaties.
Azerbaijan	1. absence of threat to national security; 2. equivalent level of legal protection in the recipient country; 3. irrespective of the level: a. with the consent of the data subject; b. to protect the life and health of the data subject.
Georgia	1. adequate safeguards provided in a recipient state or international organization; 2. international agreement; 3. agreement with adequate safeguards.
Kazakhstan	1. protection of personal data in foreign country; 2. without such protection: a. based on the consent of the data subject; b. without such protection, based on international treaties; c. in order to protect the constitutional order, public order, the rights and freedoms of human and citizens, health and morality of population; d. in order to protect the constitutional rights and freedoms of humans and citizens, if the consent cannot be obtained.
Kyrgyzstan	1. an international treaty between the parties by virtue of which the re-

⁹⁷ Full texts of concerned articles in Annex B.

	<p>recipient ensures an adequate level of protection;</p> <ol style="list-style-type: none"> 2. irrespective of the level of protection: <ol style="list-style-type: none"> a. with the consent of the data subject; b. for the protection of vital interests of the data subject's; c. in relation to data stored in a public databases.
Moldova	<ol style="list-style-type: none"> 1. Pursuant to special law or international treaty; <p>OR</p> <ol style="list-style-type: none"> 2. DPA authorization; AND 3. adequate level of protection in the recipient country; OR 4. without protection, but with contractual safeguards; <p>AND</p> <ol style="list-style-type: none"> 5. without protection in one these cases: <ol style="list-style-type: none"> a. data subject's consent; b. for the conclusion or performance of an agreement or contract concluded between the personal data subject and the controller or between the controller and a third party in the interest of the data subject; c. in order to protect the life, physical integrity or health of the data subject; d. if transfer is made from a public register; e. public interest (eg national defense, public order or national security), carrying out in good order a criminal trial or ascertaining, exercising or defending a right in court.
Russia	<ol style="list-style-type: none"> 1. if no threat to the constitutional system, to morality, health, rights and lawful interests of citizens, to national defense and state security; <p>AND</p>

	<ol style="list-style-type: none"> 2. adequate protection in foreign countries: <ol style="list-style-type: none"> a. Convention 108 countries; b. other countries 'approved' by DPA; OR 3. without protection: <ol style="list-style-type: none"> a. data subject's written consent; b. pursuant to international treaties; c. pursuant to federal laws, provided that it is necessary in order to protect the constitutional system, national defense and state security, as well as the security of sustainable and safe functioning of the transport system to protect the interests of individuals, society and the state in the sphere of transport complex of acts of unlawful interference; d. for the performance of a contract, to which a data subject is a party; e. in order to protect vital interests (eg life, health) of the data subject or other persons when it is impossible to obtain the written consent of the data subject.
Ukraine	<ol style="list-style-type: none"> 1. pursuant to international treaties; OR 2. pursuant to the law or international treaties; AND 3. adequate level of protection in the recipient countries: <ol style="list-style-type: none"> a. EEA countries; b. Convention 108 countries; c. countries 'approved' by the Government (Ukrainian Cabinet of Ministers); 4. without protection: <ol style="list-style-type: none"> a. data subject's explicit consent; b. for the conclusion or performance of an agreement concluded be-

	<p>tween the personal data subject and the controller or between the controller and a third party in the interest of the data subject;</p> <ul style="list-style-type: none"> c. to protect the vital interests of the data subject; d. to protect the public interest, the establishment, implementation and enforcement of legal requirements; e. where the data controller provides appropriate safeguards regarding non-interference in private and family life of the data subject.
Convention 108	<ul style="list-style-type: none"> 1. to Convention 108 countries, except: <ul style="list-style-type: none"> a. special categories of data; b. if Convention 108 country is a 'transit' country to third countries.
Additional Protocol to Convention 108	<ul style="list-style-type: none"> 1. Convention 108 country; 2. non-Convention 108 country or organisation with adequate protection; 3. without adequate protection: <ul style="list-style-type: none"> a. specific interests of the data subject; b. legitimate prevailing interests, especially important public interests; c. safeguards provided by data controller which are authorized by a regulator.
EU Directive	<ul style="list-style-type: none"> 1. EU/EEA country; 2. other countries with adequate level of protection; 3. without protection: <ul style="list-style-type: none"> a. unambiguous consent of the data subject; b. for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

	<ul style="list-style-type: none"> c. for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or d. the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or e. to protect the vital interests of the data subject; or f. the transfer is made from a public register.
OECD Guidelines	<ul style="list-style-type: none"> 1. country which: <ul style="list-style-type: none"> a. substantially observes Guidelines; or b. sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines.
CIS Model Law	<ul style="list-style-type: none"> 1. no threat to national security; and 2. adequate level of protection: <ul style="list-style-type: none"> a. international treaty; b. domestic legislation. 3. without protection: <ul style="list-style-type: none"> a. explicit consent of the data subject; b. for the conclusion and/or performance of a contract between data subject and data controller or controller and third person in the interests of the data subject; c. to protect the vital interests of the data subject; d. data from public register.

3.3.1 Adequacy approach (geographical targeting)

The first approach regulates data transfers based on the standard of data protection in the country of import. Out of eight Eurasian countries that have general data protection laws (all included in the Table 3), seven (i.e. all except Armenia) require certain level of protection as a basis of cross-border data transfer. This approach can also be found in Convention 108, the EU Directive, a number of European, Latin American, African and Asian countries⁹⁸. The required standard of data protection varies from country to country, some of the examples are the followings:

- ‘an adequate level of protection’ (EU Directive⁹⁹, Additional Protocol to Convention 108¹⁰⁰);
- ‘an equivalent protection’ (Convention 108¹⁰¹);
- ‘the same principles of data protection’ (Bosnia and Herzegovina¹⁰²);
- ‘a sufficient level of protection for privacy rights, rights and freedoms of data subjects in relation to the processing of personal data’ (Senegal¹⁰³).

Similarly, there is no consistency in the standard of protection required by the Eurasian laws. While most refer to ‘adequate level of protection’ (Kyrgyzstan¹⁰⁴, Moldova¹⁰⁵, Ukraine¹⁰⁶, also CIS Model law¹⁰⁷) or ‘adequate protection’ (Russia¹⁰⁸) or ‘adequate safe-

⁹⁸ Kuner (note 74, p64) names all EU member states, as well as Albania, Andorra, Bosnia and Herzegovina and Russia (from Europe), Argentina (from Latin America), Benin, Morocco, Senegal (from Africa) and Macau (from Asia).

⁹⁹ Article 25(1).

¹⁰⁰ Article 2(1).

¹⁰¹ Article 12(3)(a).

¹⁰² Law on the Protection of Personal Data, Article 8.

¹⁰³ Law No. 2008–12 of January 25, 2008, on the Protection of Personal Data, Article 49.

¹⁰⁴ Article 25(1) of Kyrgyz Data Protection Act.

¹⁰⁵ Article 32(3) of Moldovan Data Protection Act.

¹⁰⁶ Article 29(3) of Ukrainian Data Protection Act.

¹⁰⁷ Article 10(3) of CIS Modal Law.

¹⁰⁸ Article 12(1) of Russian Data Protection Act.

guards' (Georgia¹⁰⁹), others require equivalency (Azerbaijan¹¹⁰) or merely 'protection of personal data' (Kazakhstan¹¹¹).

'Adequacy' can be understood differently by different regulation. None of the Eurasian laws clarify how the adequacy will be established or what level of protection constitutes 'adequate' (except Russia, who refers to the Convention 108 protection standard¹¹²). Half of the countries named in the Table 3 do not appoint the actors who decide on 'adequacy' finding, except for Georgia, Moldova, Russia, Ukraine. Among these four countries, three appoint their special data protection authorities as the 'adequacy' finding bodies, except for Ukraine which saves this power with its Cabinet of Ministers (note that Ukraine has a special data protection authority). As to the 'adequacy' finding mechanism, the two (Russia and Ukraine) put into operation 'white-listing' method whereby the authority determines the list of countries deemed to provide the required protection level. The other two prefer 'case by case' approach, where their data protection authorities review each data transfer and determine whether the recipient country ensures the required level of protection. The rest of the countries who require certain level of protection (Azerbaijan, Kazakhstan and Kyrgyzstan) do not specify the body responsible for confirming the protection level. Neither do they determine the criteria or procedure. Finally, all the laws except Georgian, target the level of protection existing in the recipient country. This shows the preference of the countries in favour of 'territorial' jurisdiction in the matters of data transfer which more often is carried out electronically. This reflects the challenges to the traditional jurisdiction schools posed by new technologies.

By contrast, the situation in the EU is clearer. The EU 'adequacy' approach requires not only existence of a certain level of data protection under the laws of the recipient country ('content' requirements), but also the actual compliance with content requirements ('proce-

¹⁰⁹ Article 41(1) of Georgian Data Protection Act.

¹¹⁰ Article 14.2.2 of Azerbaijani Data Protection Act.

¹¹¹ Article 16(2) of Kazakh Data Protection Act. See Loskutov (2011), who mentions that earlier drafts of the Act required 'adequate' protection.

¹¹² Article 12(2) of Russian Data Protection Act.

dural/enforcement' requirements)¹¹³. 'Content' requirements include adherence of the legal system to six basic data processing requirements (i.e. principles of purpose limitation, data quality and proportionality, transparency, security, rights of access, rectification and opposition, and restrictions on onward transfers), as well as to other 'additional' principles (e.g. restrictions on processing sensitive data, on direct marketing, on automated individual decisions)¹¹⁴. The second part of analysis checks the procedural/enforcement mechanisms (vaguely termed as 'good level of compliance, support and help to individual data subject, and appropriate redress')¹¹⁵. As it can be seen, a finding of adequacy is a complex and time-consuming process. Furthermore, it is politically sensitive, as delays (in the example of Israel) or non-finding (in the example of Australia) of adequacy might cause tensions between involved states¹¹⁶.

There can be a number of aims that a regulator pursues by choosing an adequacy approach. Firstly, the regulator intends to ensure that its privacy protections cannot be avoided simply by engagement of third countries that do not provide data protection. Secondly, the regulator might be motivated to encourage such states to adopt data protection rules. This was the case in the EU Directive, and States interested in attracting data exports from the EU and support thus their data processing industry were motivated to legislate in data protection area¹¹⁷.

There are a number of things that a regulator should consider in implementing the adequacy approach¹¹⁸. First, it is necessary to define what constitutes an 'adequate level of protection, in particular the standards and procedures used to determine it. Secondly, the regulator should consider what exemptions should apply to transfers to countries without 'adequate' protection. Third, the regulator should determine how it will deal with onward transfers from a country with 'adequate' protection. These third issues are challenging, as the mech-

¹¹³ Article 29 Working Party (Working Party on the Protection of Individuals with regard to the Processing of Personal Data), *Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive* (1998), p5.

¹¹⁴ *ibid.*, pp6-7.

¹¹⁵ *ibid.*, p7.

¹¹⁶ Note 74, p66.

¹¹⁷ *ibid.*

¹¹⁸ *ibid.* p70.

anism chosen might weaken protection or, by contrast, make data transfers stringent (eg thus business unfriendly).

3.3.2 Accountability approach (organizational targeting)

The second approach focuses on data exporters and importers, making them accountable for ensuring protection of transferred data irrespective of geographic direction. The ‘original’ data controllers are expected to comply with the ‘original privacy framework that applied when and where the data was collected’¹¹⁹, irrespective of its onward transfers (to different countries or organizations). This approach operates, for example, under OECD Guidelines¹²⁰, in Canada and Mexico, while Colombia allows both first and second approaches¹²¹.

As such, this approach does not restrict transborder data flows as in the adequacy approach, which prohibits transfers unless adequacy is in place. By contrast, accountability approach imposes compliance responsibilities on those who transfer data. In practice, it means that organizations need to take steps to comply with their responsibilities, such as implementing internal privacy policies; conducting trainings for its employees; putting in place internal oversight and external verification mechanisms; ensuring transparency to individuals (as to policies and their implementation); and adopting appropriate enforcement mechanisms¹²². EU Directive also indirectly recognizes the principle of accountability in the example of standard contractual clauses¹²³ and binding corporate rules. The uptake of adequate safeguards is not popular in Eurasia, with only three countries (Georgia, Moldova and Ukraine)

¹¹⁹ Crompton M., Cowper Ch. and Jefferis Ch., ‘The Australian Dodo Case: An Insight for Data Protection Regulation’, (2009) 9 Bloomberg BNA Privacy & Security Law Report 5, p181.

¹²⁰ Para. 14 and 16. The latter states: “A data controller remains accountable for personal data under its control without regard to the location of the data”

¹²¹ Note 74, p64, also see Moerel L., *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*, (OUP 2012), pp177-227.

¹²² Centre for Information Policy Leadership, ‘Data Protection Accountability: The Essential Elements, A Document for Discussion’, (2009) <http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf> accessed 8 Nov 2014, pp11-14.

¹²³ Wojtan B., ‘The new EU Model Clauses: One step forward, two steps back?’ (2011) 1 International Data Privacy Law, 1, p80.

explicitly providing contractual clauses as a ground for data transfer to non-adequate countries.

Kuner suggests that the widespread use of accountability can replace more bureaucratic mechanisms of data protection, such as registration/authorization by data protection authorities¹²⁴. Importantly, adequacy and accountability are not opposing approaches, they can function in parallel and often overlap. However, Kuner notes that the former may mean different things to data controllers and regulators: the former may see it as a way to relieve them from bureaucratic requirements, whereas for regulators it is an extra layer of protection¹²⁵. Regulators should consider using both approaches in order to cope with complex data transfer issues, which can be increased with new technological developments.

3.4 Findings

In this chapter, we have analysed the understanding of ‘transborder data transfers’ and the legal bases for cross-border flows. The definition of ‘transborder data transfer’ under Eurasian laws, similar to global data protection regulations, covers the active form of transfers. None of the laws explicitly or impliedly regulate passive transfers.

Regulatory approach towards transborder transfers under Eurasian laws clearly demonstrate the preference of European ‘adequacy’ approach. Accountability approach is less common, and furthermore, those countries that explicitly mention them resemble the relevant provisions of the EU Directive on ‘adequate safeguards’.

Thirdly, it is possible to spot the influence of traditional ‘territorial’ jurisdiction theory in Eurasian legislation. As we have mentioned earlier, Internet is structured to transit data based on optimal technical parameters. As such, Internet, unless restructured, transfers data irrespective of jurisdictional borders, and chooses the most optimal route available from all possible options. So it can be assumed that the route to be taken for a data transit is practically unpredictable. This led Kuner to suggest that ‘it may no longer be feasible to differen-

¹²⁴ Note 74, pp75-76.

¹²⁵ Ibid.

tiate between transborder data flows and those that do not cross national borders¹²⁶. Thus, the regulatory framework for transborder data flows is in effect the same as that for data transfers on the Internet, and for the Internet itself.” Eurasian rules favouring traditional ‘territoriality’ principle of jurisdiction will continue to struggle with modern challenges brought by technologies, as is the case in other legal systems of the globe.

¹²⁶ Note 74, p6.

4 Chapter 4. National regulatory authorities

This chapter briefly analyses an element of institutional data protection framework of Eurasian countries, namely national regulatory authorities for protection of personal data.

To start with, data protection laws are enforced mainly through three types of agencies: specialized agencies (e. g. data protection authorities, privacy commissioners), central coordinating agencies (e. g. law enforcement) and courts or specialized tribunals. As we have mentioned above, on a transnational level, the EU Directive innovated with introduction of specialized supervisory bodies for data protection (see 1.2.3 above). These bodies do not only ensure implementation, but also work to establish the culture of privacy. We have also mentioned that the data protection laws in Eurasia were adopted post-2000 (see 1.3 above). These two facts allow us to assume that if Eurasian countries have provided for creation of such independent supervisory authority, then they have followed the European model.

Functionally, data protection authorities may perform different roles that the law-maker assigns to them. Flaherty lists ‘oversight, auditing, monitoring, evaluation, expert knowledge, mediation, dispute resolution, and the balancing of competing interests’¹²⁷. Bennet&Raab name seven different roles: of ombudsmen, auditors, consultants, educators, negotiators, policy advisers, and enforcers¹²⁸.

The Table 2 summarizes the supervisory authorities in Eurasian countries.

*Table 2. Regulatory Authorities*¹²⁹

<i>Country</i>	<i>Data Protection Authority</i>	<i>Central Coordinating Agencies</i>
Armenia		Ministry of Transport and Communications ¹³⁰ ; Police

¹²⁷ Flaherty, D., ‘Controlling Surveillance: Can Privacy Protection Be Made Effective?’ in P.Agre and M.Rotenberg (eds), *Technology and Privacy: The New Landscape* (MIT Press 1997), p175.

¹²⁸ Note 3, pp133-143.

¹²⁹ Based on the information from Russian DPA (Federal Service for Supervision of Communications, Information Technology and Mass Media), ‘Information on Authorized Bodies of Other Countries’ (*in Russian*) (2010) <<http://pd.rkn.gov.ru/authority/p119/>> accessed 3 Nov 2014.

Azerbaijan	Ministry of Communications and Information Technology ¹³¹	Ministry of Justice
Belarus		Operative and Analytical Center under the President ¹³² (authorized body on data security)
Georgia	Office of the Personal Data Protection Inspector ¹³³	
Kazakhstan		Ministry of Transport and Communications ¹³⁴ ; Ministry of Justice
Kyrgyzstan	State Registration Service under the Government ¹³⁵	
Moldova	National Center for Personal Data Protection ¹³⁶	
Russia	Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) ¹³⁷	
Tajikistan	<i>information not available</i>	<i>information not available</i>
Turkmenistan		Ministry of Communications
Ukraine	State Service of Ukraine on Personal Data Protection ¹³⁸ ;	

¹³⁰ http://www.mtc.am/main.php?lang=1&page_id=595.

¹³¹ <http://www.mincom.gov.az/activity/information-technologies/personal-data/>.

¹³² <http://oac.gov.by/>.

¹³³ <http://personaldata.ge/en/home>.

¹³⁴ <http://mtc.gov.kz/index.php/en/>.

¹³⁵ <http://grs.gov.kg/ru/>.

¹³⁶ <http://datepersonale.md/en/start/>.

¹³⁷ <http://eng.pd.rkn.gov.ru/>.

¹³⁸ <http://zpd.gov.ua/dszpd/en/index>.

	Ombudsman ¹³⁹	
Uzbekistan		National Security Service

A number of observations can be made based on the table. First, half out of twelve countries have data protection authorities. Four of them (Azerbaijan, Georgia, Moldova and Ukraine) are in EU Eastern Partnership Agreement and three of them (Georgia, Moldova and Ukraine) have signed Association Agreements with the EU. These agreements show that the named countries are seeking closer integration with the EU. It is possible that these countries might join the EU in the future (in particular the latter), in which case the EU data protection regime will apply in them.

Secondly, countries assign different levels of functions to data protection authorities. While Azerbaijan¹⁴⁰ and Kyrgyzstan¹⁴¹ tasks their DPAs as registries of databases, and assigns some enforcement rights, others grant broader powers. In Georgia¹⁴², the DPA fulfils consultative, educative, auditing, ombudsman, advisory, enforcement (in particular registration) and reporting roles. Moldova prefers notification system, and assigns auditing, ombudsman, and enforcement roles to its DPA¹⁴³. Russian DPA assumes ombudsman, auditing, enforcement, policy advisory, and educative roles¹⁴⁴. Ukrainian DPA is tasked with ombudsman, auditing, enforcement, policy advisor educative, consultative roles.

Based on this short analysis, it is difficult to state that the EU Directive had significant role in creation of data protection policy in Eurasian countries. Nevertheless, it is plausible to conclude that the EU Directive has clearly influenced data protection legislation in Georgia, Moldova, Russia and Ukraine.

As to CIS Model Law on Data Protection, it simply offers the possibility of establishing data protection authorities (Article 16). The Model Law itself was drafted after the EU Di-

¹³⁹ http://www.ombudsman.gov.ua/en/index.php?option=com_content&view=article&id=1105.

¹⁴⁰ Azerbaijan Data Protection Act, Chapter V.

¹⁴¹ Kyrgyz Data Protection Act, Chapter V.

¹⁴² Georgian Data Protection Act, Chapter V.

¹⁴³ Moldovan Data Protection Act, Chapter V.

¹⁴⁴ Russian Data Protection Act, Chapter V.

rective, and as such one can assume that the Article 16 of the Model Law is inspired by the Article 28 of the EU Directive. This assumption is further confirmed by the resemblance of rights and responsibilities incorporated into the Model Law with those under EU Directive. In general, the countries without data protection authorities might introduce them in the future. For instance, it has been recommended in Armenia establish an independent, national data protection authority¹⁴⁵.

¹⁴⁵ EU Advisory Group to the Republic of Armenia, 'Analysis of EU legislation on Personal Data Protection and Recommendations for Approximating the Armenian Legal and Institutional Framework', (2012), <<http://www.euadvisorygroup.eu/sites/default/files/Policy%20Paper%20on%20Analysis%20of%20the%20EU%20legislation%20on%20Personal%20Data%20Protection.pdf>> accessed 10 Oct 2014, p20

5 Conclusions

This paper has been driven by one central question: which regulatory instruments do Eurasian countries employ to design their data protection policy? For the purposes of analysis, we have broken it down to three subquestions.

Question 1. What regulatory instruments are used?

In chapter 1, we analysed the various policy instruments that now occupy the data protection landscape. In particular, we scrutinized transnational, legislative, self-regulatory, and technological instruments. This grouping is based on the assumption that data protection is international and global issue with social, organizational, political and technological dimensions. We attempted to assess these instruments' features and to identify their use by Eurasian countries and broadly reached three conclusions.

First, European data protection instruments have been the most affluent in Eurasian countries. In particular, we see its strong influence on those countries which are in the Eastern partnership agreement (namely, Armenia, Azerbaijan, Georgia, Moldova and Ukraine). In Georgia, the EU Directive is explicitly recognized as the standard to achieve. Furthermore, some countries are in the pursuit of closer integration with the EU, including in legislative framework, and have enacted laws resembling the EU Directive. This resemblance can especially be seen in Georgia, Moldova and Ukraine, which also have institutional framework (ie data protection authorities) alike to European Union model. This influence is expected to increase in those countries who are signing Association agreements with the EU (Georgia, Moldova and Ukraine). And obviously, in case if they join the EU, the EU data protection regime will apply in them.

Second, like in most parts of the world, Eurasian countries recognize data protection values (through the notion of privacy, in general) on a constitutional ('the right to privacy') and a statutory level. Most of the countries in region have data protection laws in place (except four). Based on our study we have established a number of findings.

Firstly, half of the countries with general data protection laws are members to the Convention 108 and within the Convention's framework are obliged to incorporate its rules into their domestic laws. Accordingly, we can see with a degree of certainty that the Convention 108 was also affluent, at the least in motivating the countries that have ratified it to adopt general data protection laws (we will question whether Convention 108 had any effect on its content in Chapters 2-4).

Secondly, most of the countries (eight out of twelve) have chosen to address the data protection issues in a general law. These countries are six Convention 108 ratifiers in Eurasia plus Kazakhstan and Kyrgyzstan.

Thirdly, four countries do not have general data protection laws, namely, Belarus, Tajikistan, Turkmenistan and Uzbekistan. However, this paper anticipates that these countries will also adopt general data protection laws. In particular, Uzbekistan is believed to have already ready draft of comprehensive law, but not adopted.

Fourthly, all of the eight countries, that have general data protection acts, have enacted their laws after 2000. The chronology allows us to wonder whether transnational instruments discussed above could have had an impact on the legislation in Eurasian territory. Furthermore, the post-2000 adoption also allows us to assume that Eurasian countries have mostly designed their frameworks *ab initio*: that is, a relatively blank state has allowed comprehensive legislation to be introduced in both public and private sectors.

Finally, a number of Eurasian countries regulate specific sectors with separate legislation, along having a general data protection law. The limits of this thesis do not allow to comprehensively embrace all sectoral legislation of each Eurasian country. Therefore, we only summarized the main purposes of sector specific regulation as well as examples of areas regulated sectorally in global practice.

Third, we could not find any literature/studies assessing the level of use of self-regulation and technology as policy instruments in Eurasia. Similarly, there is a lack of studies in practical implementation of data protection laws, in other words, the extent to which they provide protection to data subjects in reality (as opposed to provisions on paper). These three issues require further research and are not within the scope of this paper.

Question 2. To what extent Eurasian countries have common approaches in data protection laws?

In the introduction, we have mentioned that the countries shared common legal tradition during former Soviet Union. Having analysed the choice of policy instruments employed by Eurasian countries, we moved on, in the subsequent chapters, to determine whether there are any common approaches in data protection frameworks of the studied countries. We attempted to answer this question by examining selective issues of data protection framework: a) the concept of personal data, which is key to the scope of application of the laws; b) transborder dataflow regulations, as data protection laws need to strike the balance between the protection of personal privacy and facilitating the free flow of data; and c) national regulatory authorities, the design of which directly impacts the enforcement and compliance levels. Each of the issues were dealt individually with in chapters 2, 3, and 4 (respectively).

Chapter 2 inquired into the concept of ‘personal data’ and produced three main findings. They lead to somewhat mixed result: Eurasian laws apply a requirement of ‘tangible medium’ which cannot be spotted in the European approach, yet the basic criteria for ‘personal data’ is adopted from the European instruments.

First, all Eurasian countries apply the same basic standard to categorisation of data as personal (see 2.1. above). They all accept ‘personal data’ as any data/information that relates to identified/identifiable person. The origin of this approach lies in Convention 108, and we can conclude, in the example of the ‘personal data’ concept, that Convention 108 has had an important influence in Eurasian data protection framework. Moreover, clear adoption of the European data protection model (specifically, the EU Directive) can be found in the laws of Georgia and Moldova. In particular, we have observed this when we discussed who an ‘identifiable person’ is, and in classification of personal data to automated and non-automated ones (see 2.2. above).

Second, most of the Eurasian laws do not offer guidance on deeper issues surrounding the key criterion of the concept, namely identifiability (see 2.2 above).

Third, unlike European data protection laws, some Eurasian countries also require personal data to be in a tangible medium (Armenia, Kazakhstan, Kyrgyzstan, and Russia) (see 2.3 above). These countries (except Russia), furthermore, do not differentiate between ‘automated’ and ‘non-automated’ data. We have also analysed a number of implication flowing from these requirements (see 2.3 above).

In chapter 3, we have compared the transborder dataflow regulation in Eurasian countries under their data protection laws. We focused on two key aspects, namely (a) definition of ‘transborder data flow’ and (b) grounds for data transfer. The former is essential for the purposes of delimiting the scope of application for transborder dataflow regulations. The latter is important in the context of balancing ‘personal privacy’ interests against the principle of ‘free flow of data’. In relation to both issues, we have found the influence of European approach in Eurasia.

First, the definition of ‘transborder data transfer’ under Eurasian laws, similar to global data protection regulations, covers the active form of transfers. None of the laws explicitly or impliedly regulate passive transfers.

Second, the analysis of the grounds revealed that regulatory approach towards transborder transfers under Eurasian laws clearly demonstrate the preference of European ‘adequacy’ approach. Accountability approach is less common, and furthermore, those countries that explicitly mention them resemble the relevant provisions of the EU Directive on ‘adequate safeguards’.

Chapter 4 contains a short analysis of national regulatory authorities for protection of personal data in Eurasian countries. On a transnational level, the EU Directive innovated with introduction of specialized supervisory bodies for data protection (see 1.2.3 above). Also, the data protection laws in Eurasia were adopted post-2000 (see 1.3 above). Based on these two facts, we assumed that if Eurasian countries provided for creation of such independent supervisory authorities, then they followed the European model.

Our analysis resulted in two findings. First, six Eurasian countries have specialized data protection authorities. Four of them (Azerbaijan, Georgia, Moldova and Ukraine) are in the EU Eastern Partnership Agreement and three of them (Georgia, Moldova and Ukraine) have signed Association Agreements with the EU. These agreements show that the named

countries are seeking closer integration with the EU. It is possible that these countries (especially the latter) might join the EU in the future, in which case the EU data protection regime will apply in them.

Secondly, Eurasian countries assign different levels of functions to data protection authorities. While few of them grant limited roles (e.g. registries of databases, some enforcement rights), others grant broader powers (e.g. consultative, educative, auditing, ombudsman, policy advisory, enforcement (in particular registration), reporting roles). Based on this short analysis, it is difficult to state that the EU Directive had significant role in creation of data protection policy in Eurasian countries with regard to national regulatory authorities (only six countries have special institutions for data protection purposes and two of these six have limited functions). Nevertheless, it is plausible to conclude that the EU Directive has clearly influenced Georgia, Moldova, Russia and Ukraine (which assign broad powers).

Question 3. Is the data protection policy a ‘race to the top’ or a ‘race to the bottom’?

This question reflects the two broad global trends: ‘race to the top’ where countries progressively increase the standard of protection and ‘race to the bottom’ where countries de-regulate in order to gain competitive advantage over the former countries.

To sum up, Eurasian countries show clear preference of domestic legislation as a tool of regulating protection of personal data. Initially, they started designing their data protection frameworks from relatively blank state. Eurasian states (except for Belarus, Tajikistan, Turkmenistan, and Uzbekistan who do not have any general law) have enacted their general data protection laws after the year 2000. Among global data protection models, clear influence of the European model (ie Convention 108 and the EU Directive) can be observed in the Eurasian laws. In particular, this paper has established such influence in relation to the concept of personal data, transborder dataflow regulation, and national data protection authorities. Likewise to European model, Eurasian countries are expected to progressively increase the standard of data protection.

Bibliography

Legislation

Transnational

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 CETS No.: 181

Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, [2004] OJ L385/74

Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, [2010] OJ L39/5

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28.I.1981

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

National

Law on Personal Data dated 07.11.2002 No 3P-422 Armenia)

Law on Personal Data dated 11.05.2010 No998-IIQ (Azerbaijan)

Law on Personal Data Protection dated 28.12. 2011 #5669-RS (Georgia)

Law on Personal Data and Its Protection dated 21.05.2013 No 94-V (Kazakhstan)

Law on Information of Personal Nature dated 14.04.2008 No58 (Kyrgyzstan)

Law on Personal Data Protection dated 08.07.2011 No 133 (Moldova)

Federal Law on Personal Data (No. 152-FZ, dated 27 July 2006) (Russia)

Law on Personal Data Protection dated 01.06.2010 No 2297-VI (Ukraine)

Law on Principles and Guarantees of Freedom of Information dated 12.12.2002 No 439-II (Uzbekistan)

Privacy (Cross-border Information) Amendment Bill 221-2 (2008) (New Zealand)

Cases

Bodil Lindqvist case C-101/01 [2003] ECR I-12971 (EU)

Google Spain case C-131/12 (2014) (EU)

Durant vs Financial Services Authority [2003], EWCA Civ 1746, Court of Appeal (Civil Division) (UK)

Other

APEC Privacy Framework (2005), accessed Nov 5 2014],
<http://www.apec.org/Groups/Committee-on-Trade-andInvestment/~media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

Article 29 Working Party (Working Party on the Protection of Individuals with regard to the Processing of Personal Data) Opinion 3/99 on Public Sector Information and the Protection of Personal Data (WP 20, 3 May 1999)

Article 29 Working Party (Working Party on the Protection of Individuals with regard to the Processing of Personal Data), Opinion 4/2007 on the concept of personal data (2007)

Article 29 Working Party (Working Party on the Protection of Individuals with regard to the Processing of Personal Data), *Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive* (1998)

Article 29 Working Party (Working Party on the Protection of Individuals with regard to the Processing of Personal Data), *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 Oct 1995* (2005)

Article 29 Working Party (Working Party on the Protection of Individuals with regard to the Processing of Personal Data), *Opinion 8/2010 on applicable law* (2010)

Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (OECD 2013)

Model Law on Personal Data (Commonwealth of Independent States 1999)

Books

Bainbridge, D., *The EC Data Protection Directive*, (Butterworths 1996)

Baldwin, R., and Cave, M., *Understanding Regulation: Theory, Strategy, and Practice*, (OUP 1999)

Bennett C.J. and Raab Ch.D., *The Governance of Privacy: Policy Instruments in Global Perspective*, (MIT Press 2006)

Burkert, H., 'Privacy-enhancing technologies: typology, critique, vision' in Agre P.E. & Rotenberg M. (eds), *Technology and Privacy* (The MIT Press 1997)

Bygrave L., 'Privacy protection in a global context: a comparative overview' in Wahlgren P. (eds) *IT Law* (Stockholm Institute for Scandinavian Law 2014)

Bygrave L., *Data Privacy Law* (OUP 2014)

Flaherty, D., 'Controlling Surveillance: Can Privacy Protection Be Made Effective?' in P.Agre and M.Rotenberg (eds), *Technology and Privacy: The New Landscape* (MIT Press 1997)

Gandy, O.H., *The panoptic sort: A political economy of personal information* (1993 Westview Press)

Gellman, R., 'Conflict and Overlap in Privacy Regulation: National, International, and Private' in B.Kahin and C.Nesson (eds), *Borders in Cyberspace* (The MIT Press 1997)

Lessig L., *Code: Version 2.0*, (2006)

Liu N., *Bio-Privacy: Privacy Regulations and the Challenge of Biometrics*, (Routledge 2011)

Kuner Ch., *European Data Protection Law: Corporate Compliance and Regulation* (2nd edn, OUP 2007)

Kuner Ch., *Transborder Data Flows and Data Privacy Law* (OUP 2013)

Moerel L., *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*, (OUP 2012)

Rule et al, *The Politics of Privacy*, (New American Library 1980)

Tridimas T., *The General Principles of EU Law*, (2nd ed, OUP 2009)

Reports

EU Advisory Group to the Republic of Armenia, 'Analysis of EU legislation on Personal Data Protection and Recommendations for Approximating the Armenian Legal and Institutional Framework', (2012),
<[http://www.euadvisorygroup.eu/sites/default/files/Policy%20Paper%20on%20Analysis%](http://www.euadvisorygroup.eu/sites/default/files/Policy%20Paper%20on%20Analysis%20of%20EU%20Legislation%20on%20Personal%20Data%20Protection.pdf)

[20of%20the%20EU%20legislation%20on%20Personal%20Data%20Protection.pdf>](#) accessed 10 Oct 2014

Council of Europe, Explanatory Report on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CoE 1981)

Georgian DPA (Personal Data Protection Inspector), Report on the State of Personal Data Protection in Georgia, (2014) <[personaldata.ge/res/docs/annual_report%28eng%29%284%29.pdf](#)> accessed 30 Oct 2014

UK DPA (Information Commissioner's Office), 'Data Protection Act 1998: The eighth data protection principle and international data transfers', (2010), <[http://ico.org.uk/for_organisations/data_protection/the_guide/~media/documents/library/Da-ta_Protection/Detailed_specialist_guides/international_transfers_ico_recommended_approach.ashx](#)> accessed Nov 6 2014

Journal Articles

Bennett, C., 'Understanding Ripple Effects: The Cross-National Adoption of Policy Instruments for Bureaucratic Accountability' (1997) 10 *Governance: An International Journal of Policy and Administration* 213

Bygrave L., 'The Body as Data? Biobank Regulation via the "Back Door" of Data Protection Law' (2010) 2 *Law, Innovation and Technology* 1

Crompton M., Cowper Ch. and Jefferis Ch., 'The Australian Dodo Case: An Insight for Data Protection Regulation', (2009) 9 *Bloomberg BNA Privacy & Security Law Report* 5

Evseev S. et.al., 'Comparative analysis of the international legal framework in protection of personal data' (*in Russian*), (2014) 1050 *Bulletin of NTU 'KhPI'* 7, 56

Greenleaf G., 'Global data privacy laws: 89 countries, and accelerating', [2012] Privacy Laws & Business International Report, Issue 115 Special Supplement, February 2012

Greenleaf G., 'The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108', (2012) 2 International Data Privacy Law 1

Kozak V., Personal data protection in Ukraine: Practice and problems, (2013) 60 Journal of Personal Data 7

Makarenko, E., 'Transborder Transfer of Personal Data: Problems and Solutions' (*in Russian*), (4 Journal of Information Security 2013), <<http://www.itsec.ru/articles2/pravo/transgranichnaya-peredacha-pdn-problemy-i-puti-resheniya/>> accessed 14 Oct 2014

Margulis, 'On the Status and Contribution of Westin's and Altman's Theories of Privacy', (2003) 59 Journal of Social Issues 2, 411

Margulis, 'Privacy as a Social Issue and Behavioral Concept', (2003) 59 Journal of Social Issues 2, 243

Reidenberg, J. "Lex Informatica: The Formulation of Information Policy Rules Through Technology", Texas Law Review, 1998, volume 76, pp. 553–593

Westin A.F., 'Social and Political Dimensions of Privacy', (2003) 59 Journal of Social Issues 2, 1

Wojtan B., 'The new EU Model Clauses: One step forward, two steps back?' (2011) 1 International Data Privacy Law, 1

Other resources

Abdalimova D., 'Legal Regulation Questions of Personal Data Protection', (2008) <http://online.zakon.kz/Document/?doc_id=30531354> accessed 20 Oct 2014

Baker & McKenzie, 'The Global Employer. Data Privacy and Protection in the Workplace', (2010 Volume XV, No. 3), <http://www.bakermckenzie.com/files/Publication/b5c887f7-d96e-4bdc-afbf-04b354ce2a87/Presentation/PublicationAttachment/eb81001c-071a-4011-9aa7-08e2d0c14167/bk_employment_globalemployer_sep10.pdf> accessed 11 Sept 2014

Baker&McKenzie, 'On 1 January 2015, companies will most likely be required to store and process personal data of Russian citizens on Russian Territory' (2014) <<http://www.lexology.com/library/document.ashx?g=1216900c-a0c4-4842-9bab-6b3d9220362c>> accessed 14 Oct 2014

BaltInfo, 'Ministry of Justice of the RF approved the list of countries that provide adequate protection of personal data' (in Russian), (2013) <<http://www.baltinfo.ru/2013/04/24/Minyust-RF-utverdil-perechen-stran-obespechivayuschikh-adekvatnuyu-zaschitu-personalnykh-dannykh-350614>> accessed 14 Oct 2014

Canadian DPA (Office of the Privacy Commissioner of Canada), 'Guidelines for Processing Personal Data Across Borders', (2009) <http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.pdf>

Centre for Information Policy Leadership, 'Data Protection Accountability: The Essential Elements, A Document for Discussion', (2009) <http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf> accessed 8 Nov 2014

Clarke R., 'What's 'Privacy'?', (2006) <<http://www.rogerclarke.com/DV/Privacy.html>> accessed 28 Oct 2014

Debevoise&Plimpton LLP, 'News from the BRICS: bringing money and data back to Russia', (2014, 5 FCPA Update 12, 6-8) <<http://www.debevoise.com/files/Publication/be3e5482-134e-477a-a4d8->

f7a19386d0ff/Presentation/PublicationAttachment/4b552d98-d2be-4628-bc3c-11c6ff3a61f9/FCPA_Update_July2014.pdf> accessed 14 Oct 2014

Deloitte, 'Legal Alert for May 2013' (2013) <http://www.deloitte.com/assets/Dcom-Kazakhstan/Local%20Assets/Documents/T&L/En/Legislative%20tracking_%D0%92%D0%B5%D1%81%D1%82%D0%BD%D0%B8%D0%BA%20%D0%B8%D0%B7%D0%BC%D0%B5%D0%BD%D0%B5%D0%BD%D0%B8%D0%B9%20%D0%B2%20%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD%D0%BE%D0%B4%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D1%81%D1%82%D0%B2%D0%BE/2013/Legal%20Alert_May%202013_en.pdf> accessed 18 Aug 2014

DLA Piper (Arievich P.), 'Data protection in Russian Federation: overview', (2012) <<http://uk.practicallaw.com/2-502-2227>> accessed 14 Oct 2014

DLA Piper (Malloy M., & Arievich, P.), 'Important changes to Russian data protection rules' (2014, Legal Alert), <<http://www.dlapiper.com/en/us/insights/publications/2014/08/important-changes-to-russian-data-protection-rules/>> accessed 14 Oct 2014

EMPP – Russian Law Firm, 'Russian Federation: Personal Data Protection (Privacy) Laws In Russia', (2014) <<http://www.mondaq.com/x/307162/data+protection/Personal+Data+Protection+Privacy+Laws+In+Russia>> accessed 14 Oct 2014

European Commission, 'Commission decisions on the adequacy of the protection of personal data in third countries', (2014) <http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm> accessed 6 Nov 2014

European Commission, 'Eastern Partnership' (2014) <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/international-affairs/eastern-partnership/index_en.htm> accessed 3 Nov 2014

Finn A., 'The Concept of Eurasia - Part I' <<http://commentandoutlook.blogspot.fr/2014/04/the-concept-of-eurasia-part-i.html>> accessed 30 Oct 2014

Grata law firm, 'Data Protection Law in Uzbekistan', (2006) <www.gratanet.com/up_files/data%20protection.pdf> accessed 20 Oct 2014

Ibraeva A, 'Opinion on the draft law "On personal data" and "On amendments and additions to some legislative acts of the Republic of Kazakhstan on issues of personal data"', (Kazakhstan International Bureau for human rights and rule of law, 2012) <http://www.bureau.kz/data.php?n_id=30&l=ru> accessed 10 Nov 2014

ISO 2382-1, 'Information Technology - Vocabulary - Part 1: Fundamental Terms' (1993)

Jalagania B., 'Regulatory Framework for Personal Data Protection in Georgia and its accordance with EU regulations', LLM Thesis, (University of Oslo, 2013) accessed Oct 30 2014], <<http://urn.nb.no/URN:NBN:no-43277>>

Jones Day (Paez M.F., Volfson S., Fridman V., Dr. von Diemar U. & Leung A.), 'Russia adopts restrictive changes to its data privacy law', (2014) <<http://www.lexology.com/library/detail.aspx?g=1030f5f9-4dff-4d7b-8e43-f5f17bd1df3c>> accessed 14 Oct 2014

Journalist's Resource, '*The Arab Spring and the Internet: Research roundup*', (2013) <<http://journalistsresource.org/studies/international/global-tech/research-arab-spring-internet-key-studies>> accessed 5 Nov 2014

Linklaters, 'Data Protected. Russia', (2014) <<https://clientsites.linklaters.com/Clients/dataprotected/Pages/Russia.aspx>> accessed 14 Oct 2014

Loskutov I.Y., 'Expert opinion on the draft of the law 'On Personal Data'' (*in Russian*), (2011) <<http://pravo.zakon.kz/4454747-jekspertnoe-zakljuchenie-po-proektu.html>> accessed 10 Oct 2014

OECD, 'OECD work on privacy' (2013) <<http://www.oecd.org/sti/ieconomy/privacy.htm>> accessed 6 Nov 2014

OECD, 'The OECD', (2008) <<http://www.oecd.org/newsroom/34011915.pdf>> accessed 3 Nov 2014

Reed Smith, 'Kazakhstan: Kazakhstan Introduces New Privacy Law', (2013) <<http://www.mondaq.com/x/283254/Data+Protection+Privacy/Kazakhstan+Introduces+New+Privacy+Law>> accessed 12 Oct 2014

Russian DPA (Federal Service for Supervision of Communications, Information Technology and Mass Media), 'Information on Authorized Bodies of Other Countries' (*in Russian*) (2010) <<http://pd.rkn.gov.ru/authority/p119/>> accessed 3 Nov 2014

Russian DPA (Federal Service for Supervision of Communications, Information Technology and Mass Media), 'Judicial Practice (2008-2009)', (2011) <<http://pd.rkn.gov.ru/law/p139/>> accessed 14 Oct 2014

Schwartz P.M. and Solove D., 'Privacy Law Fundamentals' (International Association of Privacy Professionals 2011)

Shyngyssov A, Zhamalova B & Shuster V, 'Kazakhstan Adopts Personal Data Protection Law', (2013) <http://www.morganlewis.com/pubs/IP_LF_KazakhstanAdoptsPersonalDataProtectionLaw_03july13> accessed 18 Aug 2014

The Economist, 'Data, data everywhere—A special report on managing information', (2010) <<http://www.economist.com/node/15557443>> accessed 5 Nov 2014

UK DPA (Information Commissioner's Office), Topic Guides for Organisations, (2014) <http://ico.org.uk/for_organisations/data_protection/topic_guides> accessed 4 Nov 2014

White & Case (Puzrakova M.), 'Recent amendments to the procedure of personal data processing in Russia', (2014) <<http://www.whitecase.com/articles/092014/recent-amendments-to-the-procedure-of-personal-data-processing-in-russia/#.VD1OBI7qGuY>> accessed 14 Oct 2014

White&Case, 'New Personal Data Protection Law', (2014)
<<http://www.whitecase.com/files/Publication/dab330b2-e75d-42d2-91a6-ad001c456e12/Presentation/PublicationAttachment/c02a6fd4-43a9-44ae-aea7-b8d60358159c/alert-New-Personal-Data-Protection-Law-012014.pdf>> accessed 12 Oct 2014

Wikipedia, 'IP address' <https://en.wikipedia.org/wiki/IP_address>

Annex A. Definition of personal data

Country	Definition	
	<i>Russian</i>	<i>English (unofficial translations)</i>
Armenia	Статья 3. Основные понятия, используемые в Законе персональные данные – любые данные о фактах, случаях, обстоятельствах, относящиеся к физическому лицу, закрепленные на материальном носителе письменно или иным образом, в таком виде, который дает или может дать возможность идентифицировать личность индивидуума;	Article 3. Main definitions used in the law a) Personal data: any data fixed in writing or other otherwise on tangible medium containing facts, events and circumstances a natural person, in a form that allows or may allow to identify the individual
Azerbaijan	Статья 2. Основные понятия, используемые в Законе 2.1.1. персональные данные — любая информация, позволяющая прямо или косвенно определить лицо;	Article 2. The basic concepts used in the Act 2.1.1. personal data - any information that allows to directly or indirectly identify a person;
Georgia		Article 2. Definition of terms a) personal data (hereinafter – data) – any information relating to an identified or identifiable natural person. An identifiable person is the one who can be identified directly or indirectly, in particular by reference to an identification number or to the factors specific to his/her physical, physiological, mental, economic, cultural or social identity;
Kazakhstan	Статья 1. Основные понятия, используемые в настоящем Законе 2) персональные данные - сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе;	Article 1. The basic concepts used in this Act 2) personal data - information that is related to identified or identifiable thereof data subject, recorded in electronic, paper, or other tangible medium;
Kyrgyzstan	Статья 3. Термины и определения Информация персонального характера (персональные данные) - зафиксированная информация на материальном носителе о конкретном человеке, отождествленная с конкретным человеком или которая может быть отождествлена с конкретным человеком, позволяющая идентифицировать этого человека прямо или косвенно, посредством ссылки на один или несколько факторов, специфичных для его био-	Article 3. Terms and definitions Information of a personal nature (personal data) – information recorded in tangible form about a specific person, matched with a specific person or that can be matched with a specific person, allowing to identify this person directly or indirectly by referring to one or several factors specific for his/her biological, economic, cultural, civil or social identity.

	логической, экономической, культурной, гражданской или социальной идентичности. К персональным данным относятся биографические и опознавательные данные, личные характеристики, сведения о семейном положении, финансовом положении, состоянии здоровья и прочее.	Personal data include biographic and identifying data, personal characteristics, information on the marital status, financial position, state of health, etc.
Moldova	Статья 3. Основные понятия персональные данные – любая информация, связанная с идентифицированным или идентифицируемым физическим лицом (субъектом персональных данных). Идентифицируемым лицом является лицо, которое может быть идентифицировано прямо или косвенно, в частности, посредством ссылки на идентификационный номер либо на один или несколько факторов, специфичных для его физической, физиологической, психической, экономической, культурной или социальной идентичности;	Article 3. Definitions personal data - any information relating to an identified or identifiable natural person ('personal data subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;
Russia	Статья 3. Основные понятия, используемые в настоящем Федеральном законе 1) персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);	Article 3. The basic concepts used in the Federal Law 1) personal data is any information relating to, directly or indirectly, identified or identifiable natural person (data subject);
Ukraine	Статья 2. Определение терминов персональные данные — сведения или совокупность сведений о физическом лице, которое идентифицировано или может быть конкретно идентифицировано;	Article 2. Term Definitions Personal data shall mean information or aggregate information about a natural person who is identified or may be identified;
Convention 108	Статья 2 – Определения а) «персональные данные» означают любую информацию об определенном или поддающемся определению физическом лице (субъект данных);	Article 2 – Definitions "personal data" means any information relating to an identified or identifiable individual ("data subject");
OECD Guidelines		Definitions 1. For the purposes of these Guidelines: b) “Personal data” means any information relating to an identified or identifiable individual (data subject).
EU Directive	Статья 2(а) любую информацию, относящуюся к определенному или определяемому физическому лицу ("субъекту данных"); определяемым является лицо, которое может быть определено, прямо или кос-	Article 2(a) any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in

	венно, в частности, через идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности;	particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity
CIS Model Law	<p>Статья 2. Основные термины и определения</p> <p>Персональные данные - информация (зафиксированная на материальном носителе) о конкретном человеке, которая отождествлена или может быть отождествлена с ним.</p> <p>К персональным данным относятся биографические и опознавательные данные, личные характеристики, сведения о семейном, социальном положении, образовании, профессии, служебном и финансовом положении, состоянии здоровья и прочие.</p>	<p>Article 2. Basic terms and definitions</p> <p>Personal data - information (recorded in a tangible medium) about a particular person, that is related or can be related to him.</p> <p>Biographical and identifying data, personal characteristics, information on family, social status, education, profession, business and financial situation, health and others are considered to personal data.</p>

Annex B. Grounds for cross-border data transfers

Country	Grounds	
	<i>Russian</i>	<i>English</i>
Armenia	Статья 13. Передача персональных данных в иностранные государства Персональные данные передаются в иностранные государства в соответствии с международными договорами Республики Армения или по основаниям, предусмотренным статьей 6 настоящего Закона.	Art 13. Transfer of personal data to the foreign countries Personal data are transferred to foreign countries according to international treaties of Armenia and on the basis stipulated under Articles 6 of this Law.
Azerbaijan	Статья 14. Трансграничная передача персональных данных 14.1. Трансграничная передача персональных данных осуществляется при соблюдении установленных настоящим Законом требований и с учетом установленных настоящей статьей особенностей. 14.2. Трансграничная передача персональных данных запрещается в следующих случаях: 14.2.1. при наличии угрозы для национальной безопасности Азербайджанской Республики; 14.2.2. если законодательство страны, в которую передаются персональные данные, не обеспечивает правовую защиту этих данных <i>на уровне, установленном законодательством</i> Азербайджанской Республики. 14.3. Трансграничная передача персональных данных может осуществляться независимо от уровня их правовой защиты в случаях, когда субъект дал согласие на трансграничную передачу персональных данных, а также если передача персональных данных необходима для охраны жизни и здоровья субъекта.	Article 14. Cross-border transfer of personal data 14.1. Cross-border transfer of personal data is carried out in compliance with the requirements established by the Law and taking into account established in this article special provisions. 14.2. Cross-border transfer of personal data is prohibited in the following cases: 14.2.1. If there is a threat to the national security of the Azerbaijan Republic; 14.2.2. If the legislation of the country, to which the personal data is transferred, does not provided legal protection of these data at the level established by the legislation of Azerbaijan Republic. 14.3. Cross-border transfer of personal data may take place irrespective of the level of legal protection in cases when the subject has given consent to transborder transfers of personal data, as well as if the transmission of personal data is necessary for the protection of life and health of the data subject.
Georgia		Article 41. Transfer of data to another state and international organization 1. Transfer of data to another state and international organization shall be allowed, if the grounds for the processing of data envisaged by this Law are present and if <i>adequate</i> safeguards for the protection of data are ensured in a respective state or international organization. 2. Transfer of data to another state and international organization, except for Paragraph 1 of this Article, shall also be allowed, if: a) transfer of data is envisaged by an international agreement of Georgia;

		<p>b) data processor provides adequate safeguards for the protection of data and the protection of the fundamental rights of a data subject on the basis of an agreement concluded between a data processor and a respective state, a natural or legal person of that state or an international organization.</p> <p>3. Transfer of data on the basis of Subparagraph “b” of Paragraph 2 of this Article shall be allowed only after the permission of an inspector.</p> <p>Article 42. Establishing adequate safeguards for the protection of data Presence of adequate safeguards for the protection of data in a foreign state and/or in an international organization shall be assessed and decided upon by an inspector, on the basis of an analysis of the processing of data legislation and practice.</p>
Kazakhstan	<p>Статья 16. Трансграничная передача персональных данных</p> <p>1. Трансграничная передача персональных данных - передача персональных данных на территорию иностранных государств.</p> <p>2. В соответствии с настоящим Законом трансграничная передача персональных данных на территорию иностранных государств осуществляется только в случае <i>обеспечения этими государствами защиты</i> персональных данных.</p> <p>3. Трансграничная передача персональных данных на территорию иностранных государств, не обеспечивающих защиту персональных данных, может осуществляться в случаях:</p> <p>1) наличия согласия субъекта или его законного представителя на трансграничную передачу его персональных данных;</p> <p>2) предусмотренных международными договорами, ратифицированными Республикой Казахстан;</p> <p>3) предусмотренных законами Республики Казахстан, если это необходимо в целях защиты конституционного строя, охраны общественного порядка, прав и свобод человека и гражданина, здоровья и нравственности населения;</p> <p>4) защиты конституционных прав и свобод человека и гражданина, если получение согласия субъекта или его законного представителя невозможно.</p> <p>4. Трансграничная передача персональных данных на территорию иностранных государств может быть запрещена или ограничена законами Республики Казахстан.</p>	<p>Article 16. Cross-border transfer of personal data</p> <p>1. Cross-border transfer of personal data – is a transmission of personal data to foreign States.</p> <p>2. In accordance with this Law, cross-border transfer of personal data to foreign States shall be carried out only in the case of the protection by these States of personal data.</p> <p>3. Cross-border transfer of personal data to foreign States, without ensuring the protection of personal data, can be carried out in the following cases:</p> <p>1) with the consent of the subject or his or her legal representative on transborder transfers of personal data;</p> <p>2) where stipulated by international treaties ratified by the Republic of Kazakhstan;</p> <p>3) under the laws of the Republic of Kazakhstan, if this is necessary for protection of the constitutional system, the protection of public order, the rights and freedoms of man and citizen, public health or morals;</p> <p>4) for the protection of constitutional rights and freedoms of man and citizen, if obtaining the consent of the subject or his or her legal representative is impossible.</p> <p>4. Cross-border transfer of personal data to foreign States may be prohibited or restricted by laws of the Republic of Kazakhstan.</p>

Kyrgyzstan	<p>Статья 25. Трансграничная передача персональных данных</p> <p>1. При трансграничной передаче персональных данных держатель (владелец) массива персональных данных, находящийся под юрисдикцией Кыргызской Республики, передающий данные, исходит из наличия международного договора между сторонами, согласно которому получающая сторона обеспечивает <i>адекватный уровень защиты</i> прав и свобод субъектов персональных данных и охраны персональных данных, установленный в Кыргызской Республике.</p> <p>2. Кыргызская Республика обеспечивает законные меры охраны находящихся на ее территории или передаваемых через ее территорию персональных данных, исключаяющие их искажение и несанкционированное использование.</p> <p>3. Передача персональных данных в страны, не обеспечивающие адекватный уровень защиты прав и свобод субъектов персональных данных, может иметь место при условии:</p> <ul style="list-style-type: none"> - согласия субъекта персональных данных на эту передачу; - если передача необходима для защиты жизненно важных интересов субъекта персональных данных; - если персональные данные содержатся в общедоступном массиве персональных данных. 	<p>Article 25. Cross-border transfer of personal data</p> <p>1. In cases of cross-border transfer of personal data, the holder (owner) of the personal data, who is under the jurisdiction of the Kyrgyz Republic, which transmits data, shall be guided by the existence of an international agreement between the parties, pursuant to which the receiving party provides an adequate level of protection of the rights and freedoms of data subjects and the protection of personal data established in the Kyrgyz Republic.</p> <p>2. Kyrgyz Republic provides legal protection for personal data in its territory or across its territory transmitted, to exclude their distortion and unauthorized use.</p> <p>3. Transfer of personal data to countries that do not provide an adequate level of protection of the rights and freedoms of data subjects may take place if:</p> <ul style="list-style-type: none"> - the consent of the subject of personal data to that transfer is obtained; - the transfer is necessary to protect the vital interests of the subject of personal data of; - if the personal data is contained in publicly available database of personal data.
Moldova	<p>Статья 32. Трансграничная передача персональных данных</p> <p>(1) Настоящая статья применяется в случае передачи в другое государство – независимо от используемых носителей или средств – персональных данных, которые составляют предмет обработки или собираются с целью подвергнуть их обработке.</p> <p>(2) Персональные данные, предназначенные для передачи другому государству, защищаются в соответствии с настоящим законом.</p> <p>(3) Трансграничная передача персональных данных, которые являются предметом обработки или подлежат обработке после передачи, может осуществляться с разрешения Центра в установленном законом порядке, лишь если государство назначения обеспечивает <i>адекватный уровень защиты</i> прав субъектов персональных данных и данных, предназначенных для передачи.</p> <p>(4) Уровень защиты определяется Центром с учетом условий, в которых осуществляется передача персональных данных, в частности, природы персональных данных, цели и продолжительности предполагаемых обработки или обработок, государства назначения, его законодательства, а также профессиональных норм и мер безопасности, соблюдаемых в государстве назначения.</p>	<p>Article 32. Transborder transfer of personal data</p> <p>(1) This article shall apply to the transfer to another state, regardless of used medium or means, of personal data undergoing processing or are intended for processing.</p> <p>(2) Personal data intended for transfer to another state shall be protected in accordance with this law.</p> <p>(3) Transborder transmission of personal data undergoing processing or are intended for processing after transfer may take place only with the authorization of the Centre, as provided for by law, and only if the country in question ensures an <i>adequate level of protection</i> of personal data subjects' rights and of data intended for transfer.</p> <p>(4) The level of protection shall be established by the Centre taking into account the conditions in which personal data transmission takes place, especially the nature of data, the purpose and duration of proposed processing operations, the country of destination, the legislation in force in the country in question and the professional rules and security measures which are complied with in that country.</p>

	<p>(5) Если Центр установит, что уровень защиты, обеспечиваемый государством назначения, неудовлетворителен, он запрещает передачу данных.</p> <p>(6) Центр может разрешить в установленном законом порядке передачу персональных данных в государство, законодательство которого не предусматривает уровня защиты, по меньшей мере равнозначного предоставляемому законодательством Республики Молдова, если контролер представляет достаточные гарантии защиты и осуществления прав субъектов персональных данных, установленные в заключенных между контролерами и физическими или юридическими лицами договорах, на основании которых производится передача.</p> <p>(7) Положения частей (3)–(6) не применяются, если передача персональных данных производится на основе положений специального закона или международного договора, ратифицированного Республикой Молдова, в частности если передача осуществляется в целях предотвращения или расследования преступлений. Специальный закон или международный договор должны предусматривать гарантии защиты прав субъектов персональных данных.</p> <p>(8) Положения частей (1)–(6) не применяются в случае обработки персональных данных, осуществляемой исключительно в целях журналистики или в целях художественного или литературного творчества, если обрабатываются данные, добровольно и явно сделанные общедоступными субъектом персональных данных либо тесно связанные со статусом публичной фигуры субъекта персональных данных или публичным характером действий, в которые он вовлечен.</p> <p>(9) Передача персональных данных в государства, не обеспечивающие адекватный уровень защиты, может иметь место только в случаях:</p> <ul style="list-style-type: none"> a) наличия согласия субъекта персональных данных; b) необходимости заключения или исполнения соглашения или договора между субъектом персональных данных и контролером либо между контролером и третьей стороной в интересах субъекта персональных данных; c) если это необходимо для защиты жизни, физической целостности или здоровья субъекта персональных данных; d) если передача производится из регистра, который предназначен для информирования общественности и который открыт для ознакомления либо общественности в целом, либо любому лицу, проявляющему законный интерес, в той мере, в какой условия, предусмотренные законом для ознакомления, выполняются в конкретном случае; e) если это необходимо для удовлетворения важного общественного интереса, такого как национальная оборона, государственная безопасность или обще- 	<p>(5) Where the Centre considers that the country of destination does not ensure an adequate level of protection, it shall prevent any transfer of data.</p> <p>(6) The Centre may authorise, as provided for by law, the transfer of personal data to another state, which legislation does not ensure at least the same level of protection as the one offered by the law of the Republic of Moldova, where the controller provides sufficient guarantees regarding the protection and the exercise of the personal data subjects' rights, that are laid down by contracts concluded between controllers and natural or legal persons, on which provision the transfer is carried out.</p> <p>(7) The provisions referred to in paragraphs (3)-(6) shall not apply where the transfer of personal data takes place in terms of the provisions of a special law or of an international treaty ratified by the Republic of Moldova, in particular if the transfer is necessary for the purpose of preventing and investigating crimes. The special law or international treaty must contain guarantees regarding the protection of personal data subject's rights.</p> <p>(8) The provisions referred to in paragraphs (1)-(6) shall not apply where the processing of personal data is carried out solely for journalistic, literary or 20artistic purposes, if such data are voluntarily and manifestly made public by the personal data subject or if they are closely related to the personal data subject's status of a public person or to the public nature of the acts in which he is involved.</p> <p>(9) Transmission of personal data to states that do not ensure an adequate level of protection may take place only:</p> <ul style="list-style-type: none"> a) with the personal data subject's consent; b) if the transfer is necessary for the conclusion or performance of an agreement or contract concluded between the personal data subject and the controller or between the controller and a third party in the interest of the personal data subject; c) if the transfer is necessary in order to protect the life, physical integrity or health of the personal data subject; d) if transfer is made from a register which according to the law is intended to provide information to the public and which is open to consultation either by the public or by any person who demonstrates a legitimate interest, to the extent that the conditions for consultation in particular cases laid down in law are fulfilled; e) the transfer is necessary for the accomplishment of an important public
--	--	---

	<p>ственный порядок, для нормального осуществления уголовного судопроизводства либо определения, осуществления или защиты права в суде, при условии, что персональные данные обрабатываются в связи с этими целями и только в течение срока, необходимого для достижения этих целей.</p>	<p>interest, such as national defense, public order or national security, carrying out in good order a criminal trial or ascertaining, exercising or defending a right in court, on the condition that the personal data is processed solely in relation to this purpose and only for longer period is necessary to achieve it.</p>
Russia	<p>Статья 12. Трансграничная передача персональных данных</p> <p>1. Трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих <i>адекватную защиту</i> прав субъектов персональных данных, осуществляется в соответствии с настоящим Федеральным законом и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.</p> <p>2. Уполномоченный орган по защите прав субъектов персональных данных утверждает перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных. Государство, не являющееся стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, может быть включено в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, при условии соответствия положениям указанной Конвенции действующих в соответствующем государстве норм права и применяемых мер безопасности персональных данных.</p> <p>3. Оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных.</p> <p>4. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:</p> <ol style="list-style-type: none"> 1) наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных; 2) предусмотренных международными договорами Российской Федерации; 	<p>Article 12. Cross-border transfer of personal data</p> <p>1. Cross-border transfer of personal data to the territory of foreign States that are parties to the Council of Europe Convention on the protection of individuals with regard to automatic processing of personal data, as well as to other foreign States that ensure adequate protection of the rights of subjects of personal data is carried out in accordance with this Federal Law and may be prohibited or restricted in order to protect the foundations of the constitutional system of the Russian Federation, morality, health, rights and legitimate interests of its citizens, ensuring the defence of the country and the security of the State.</p> <p>2. The authorized body for the protection of the rights of subjects of personal data approves list of foreign States that are not parties to the Council of Europe Convention on the protection of individuals with regard to automatic processing of personal data and that ensure adequate protection of the rights of subjects of personal data. State who are not party to the Council of Europe Convention on the protection of individuals with regard to automatic processing of personal data may be included in the list of foreign States that ensure adequate protection of the rights of subjects of personal data, subject to compliance with the provisions of the said Convention established under that State's legislation and measures of personal data security.</p> <p>3. The operator must ensure that the foreign State to the territory of which the transfer of personal data is made adequately protects personal data subjects rights, prior to the implementation of the cross-border transfer of personal data.</p> <p>4. Cross-border transfer of personal data to foreign States not providing adequate protection for the rights of subjects of personal data can be carried out in the following cases:</p> <ol style="list-style-type: none"> 1) with the written consent of the subject of personal data to transborder transfers of his personal data; 2) pursuant to international treaties of the Russian Federation;

	<p>3) предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;</p> <p>4) исполнения договора, стороной которого является субъект персональных данных;</p> <p>5) защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.</p>	<p>3) pursuant to a federal law, if this is necessary to protect the foundations of the constitutional system of the Russian Federation, the national defense and security of the State, as well as the security and sustainable functioning of the transport system, the protection of the interests of the individual, society and the State in the transport industry against acts of unlawful interference;</p> <p>4) for the performance of the contract to which the subject of the personal data is a party;</p> <p>5) for the protection of life, health, and other vital interests of the subject of personal data or other persons if it is not possible to obtain written consent of the subject of personal data.</p>
Ukraine	<p>Статья 29. Международное сотрудничество и передача персональных данных</p> <p>1. Сотрудничество с иностранными субъектами отношений, связанных с персональными данными, регулируется Конституцией Украины, настоящим Законом, другими нормативно-правовыми актами и международными договорами Украины.</p> <p>2. Если международным договором Украины, согласие на обязательность которого дано Верховной Радой Украины, установлены другие правила, нежели те, которые предусмотрены законодательством Украины, то применяются правила международного договора Украины.</p> <p>3. Передача персональных данных иностранным субъектам отношений, связанных с персональными данными, осуществляется только при условии обеспечения соответствующим государством <i>надлежащей защиты</i> персональных данных в случаях, установленных законом или международным договором Украины. Государства — участники Европейского экономического пространства, а также государства, подписавшие Конвенцию Совета Европы о защите лиц в связи с автоматизированной обработкой персональных данных, признаются обеспечивающими надлежащий уровень защиты персональных данных. Кабинет Министров Украины определяет перечень государств, которые обеспечивают надежную защиту персональных данных. Персональные данные не могут распространяться с другой целью, нежели та, с которой они были собраны.</p> <p>4. Персональные данные могут передаваться иностранным субъектам отношений, связанных с персональными данными, также в случае:</p> <p>1) предоставления субъектом персональных данных однозначного согласия на такую передачу;</p>	<p>Article 29. International Cooperation and Transfer of Personal Data</p> <p>1.Cooperation with foreign subjects of relations related to personal data shall be regulated by the Constitution of Ukraine, this Law, other normative and legal acts and international treaties of Ukraine.</p> <p>2.If the international treaty of Ukraine which was made binding by the Verkhovna Rada of Ukraine establishes other regulations than those stipulated by legislation of Ukraine, the regulations of the international treaty shall apply.</p> <p>3. Personal data may be transferred to foreign parties having relation to personal data in the cases stipulated by law or an international treaty of Ukraine only on condition that an <i>adequate level</i> of personal data protection is ensured by the relevant foreign state. Member states of the European Economic Area as well as states signatory to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data., shall be assumed to ensure an adequate level of personal data protection. The Cabinet of Ministers of Ukraine shall compile a list of the states that ensure an adequate level of personal data protection. Personal data may not be distributed for the purpose other than the one for which they have been collected.</p> <p>4. Personal data may also be transferred to foreign parties having relation to personal data in case of the following:</p> <p>1) a personal data subject's explicit consent to the transfer;</p> <p>2) the need to conclude and perform a legal agreement between a personal data controller and a third party who is a personal data subject for the benefit of the personal data subject;</p>

	<p>2) необходимости заключения или выполнения сделки между владельцем персональных данных и третьим лицом — субъектом персональных данных в пользу субъекта персональных данных;</p> <p>3) необходимости защиты жизненно важных интересов субъектов персональных данных;</p> <p>4) необходимости защиты общественного интереса, установления, выполнения и обеспечения правового требования;</p> <p>5) предоставления владельцем персональных данных соответствующих гарантий относительно невмешательства в личную и семейную жизнь субъекта персональных данных.</p>	<p>3) the need to protect vital interests of personal data subjects;</p> <p>4) the need to protect public interests, or establish, pursue and enforce a legal claim;</p> <p>5) a personal data controller has provided the required guarantees of non-intrusion into the private and family life of the personal data subject.</p>
Convention 108	<p>Статья 12 – Трансграничные потоки персональных данных и внутреннее законодательство</p> <p>1. В отношении передачи через национальные границы с помощью каких бы то ни было средств персональных данных, подвергающихся автоматизированной обработке или собранных с целью их автоматизированной обработки, применяются нижеследующие положения.</p> <p>2. Сторона не должна запрещать или обуславливать специальным разрешением трансграничные потоки персональных данных, идущие на территорию другой Стороны, с единственной целью защиты частной жизни.</p> <p>3. Тем не менее каждая Сторона вправе отступать от положений пункта 2:</p> <p>а) в той степени, в какой ее внутреннее законодательство включает специальные правила в отношении определенных категорий персональных данных или автоматизированных баз персональных данных в силу характера этих данных или этих файлов, за исключением случаев, когда нормы другой Стороны предусматривают такую же защиту;</p> <p>б) когда передача осуществляется с ее территории на территорию Государства, не являющегося Стороной настоящей Конвенции, через территорию другой стороны, в целях недопущения такой передачи, которая позволит обойти законодательство Стороны, упомянутой в начале данного пункта.</p>	<p>Article 12 – Transborder flows of personal data and domestic law</p> <p>1. The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.</p> <p>2. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.</p> <p>3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:</p> <p>a. insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;</p> <p>b. when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.</p>
Additional Protocol to Convention 108	<p>Статья 2 – Трансграничные потоки данных личного характера получателю, который не является субъектом юрисдикции Стороны в Конвенции</p> <p>1. Каждая Сторона будет обеспечивать передачу данных личного характера получателю, который не является субъектом юрисдикции государства или организации, которая не является Стороной в Конвенции, только в том случае, если государство или организация обеспечат соответствующий уровень защи-</p>	<p>Article 2 – Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention</p> <p>1. Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer.</p>

	<p>ты при такой передаче данных.</p> <p>2. В качестве исключения из пункта 1 Статьи 2 к настоящему Протоколу каждая Сторона может разрешить передачу данных личного характера:</p> <p>a. если это разрешено национальным правом, с учетом</p> <ul style="list-style-type: none"> – конкретных интересов, связанных с предметом данных, или – законных преобладающих интересов, особо важных общественных интересов, или <p>b. если контролером, ответственным за передачу данных, обеспечиваются гарантии, которые, в частности, могут вытекать из договорных условий, и которые рассматриваются компетентными органами как соответствующие, в соответствии с внутренним правом.</p>	<p>2. By way of derogation from paragraph 1 of Article 2 of this Protocol, each Party may allow for the transfer of personal data :</p> <p>a. if domestic law provides for it because of :</p> <ul style="list-style-type: none"> – specific interests of the data subject, or – legitimate prevailing interests, especially important public interests, or <p>b. if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law.</p>
EU Directive	<p>Глава IV Передача персональных данных в третьи страны</p> <p>Статья 25 Принципы</p> <p>1. Государства-члены ЕС предусматривают, что передача в третью страну персональных данных, которые подвергаются обработке или предназначены для обработки после передачи, может осуществляться только если, без ущерба для соблюдения национальных норм, принятых в соответствии с иными нормами настоящей Директивы, соответствующая третья страна обеспечивает достаточный уровень защиты.</p> <p>2. Достаточность уровня защиты, предоставляемого третьей страной, оценивается в свете всех обстоятельств, связанных с операцией по передаче или с последовательностью операций по передаче данных; особое внимание уделяется характеру данных, цели и продолжительности предлагаемой операции или операций по обработке, стране происхождения и стране конечного назначения, законодательным правилам, как общим, так и отраслевым, действующим в соответствующей третьей стране, а также профессиональным правилам и мерам безопасности, соблюдаемым в этой стране.</p> <p>3. Государства-члены ЕС и Европейская Комиссия информируют друг друга о случаях, когда они считают, что третья страна не обеспечивает достаточный уровень защиты по смыслу параграфа 2.</p> <p>4. Если Европейская Комиссия установит, в соответствии с процедурой, предусмотрено в Статье 31 (2), что третья страна не обеспечивает достаточный уровень защиты по смыслу параграфа 2 настоящей Статьи, Государства-члены ЕС принимают необходимые меры, чтобы предотвратить любую передачу данных того же типа в соответствующую третью страну.</p> <p>5. В подходящий момент Европейская Комиссия вступает в переговоры с це-</p>	<p>Chapter IV Transfer of personal data to third countries</p> <p>Article 25 Principles</p> <p>1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.</p> <p>2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.</p> <p>3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.</p> <p>4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.</p> <p>5. At the appropriate time, the Commission shall enter into negotiations</p>

	<p>люю исправления ситуации, обусловленной заключением, сделанным согласно параграфу 4.</p> <p>6. Европейская Комиссия может установить, в соответствии с процедурой, упомянутой в Статье 31 (2), что третья страна обеспечивает достаточный уровень защиты по смыслу параграфа 2 настоящей Статьи, в силу ее внутреннего законодательства или международных обязательств, которые она дала, особенно после завершения переговоров, упомянутых в параграфе 5, по защите частной жизни, основных свобод и прав физических лиц. Государства-члены ЕС принимают меры, необходимые для исполнения решения Европейской Комиссии.</p> <p>Статья 26 Ограничения</p> <p>1. В порядке отступления от положений Статьи 25, и если иное не предусмотрено внутренним законодательством, регулирующим конкретные случаи, Государства-члены ЕС предусматривают, что передача или последовательность передач персональных данных в третью страну, которая не обеспечивает достаточный уровень защиты по смыслу Статьи 25 (2), может совершаться при условии, что:</p> <ul style="list-style-type: none"> (a) субъект данных однозначно дал свое согласие на предполагаемую передачу данных; или (b) передача необходима для исполнения договора между субъектом данных и оператором или осуществления преддоговорных мер, принимаемых по просьбе субъекта данных; или (c) передача необходима для заключения или исполнения договора, заключенного в интересе субъекта данных между оператором и третьим лицом; или (d) передача необходима или требуется на основании закона по соображениям важного общественного интереса, либо для установления, осуществления или защиты правовых требований; или (e) передача необходима в целях защиты жизненно важных интересов субъекта данных; или (f) передача осуществляется из реестра, который, в соответствии с законами или подзаконными актами, предназначен для предоставления информации общественности и который открыт для доступа как общественности в целом, так и любого лица, могущего продемонстрировать законный интерес, в той мере, в какой в конкретном случае выполняются условия, установленные законодательством о доступе. <p>2. Без ущерба для положений параграфа 1, Государство-член ЕС может разре-</p>	<p>with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.</p> <p>6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals. Member States shall take the measures necessary to comply with the Commission's decision.</p> <p>Article 26 Derogations</p> <p>1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:</p> <ul style="list-style-type: none"> (a) the data subject has given his consent unambiguously to the proposed transfer; or (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or (e) the transfer is necessary in order to protect the vital interests of the data subject; or (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case. <p>2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article</p>
--	--	---

	<p>шить передачу или последовательность передач персональных данных в третью страну, которая не обеспечивает достаточный уровень защиты по смыслу Статьи 25 (2), когда оператор представляет достаточные гарантии в отношении защиты частной жизни и основных прав и свобод физических лиц и относительно осуществления соответствующих прав; такие гарантии могут, в частности, следовать из соответствующих условий договора.</p> <p>3. Государство-член ЕС информирует Европейскую Комиссию и другие Государства-члены ЕС о разрешениях, которые оно выдает в соответствии с параграфом 2.</p> <p>Если Государство-член ЕС или Европейская Комиссия возражает по обоснованным причинам, связанным с защитой частной жизни и основных прав и свобод физических лиц, Европейская Комиссия принимает надлежащие меры в соответствии с процедурой, установленной в Статье 31 (2).</p> <p>Государства-члены ЕС принимают необходимые меры для исполнения решения Европейской Комиссии.</p> <p>4. Когда Европейская Комиссия решает, в соответствии с процедурой, установленной в Статье 31 (2), что отдельные стандартные договорные условия предлагают достаточные гарантии, предусмотренные параграфом 2, Государства-члены ЕС принимают необходимые меры для исполнения решения Европейской Комиссии.</p>	<p>25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.</p> <p>3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2. If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2). Member States shall take the necessary measures to comply with the Commission's decision.</p> <p>4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.</p>
OECD Guidelines		<p>16. A data controller remains accountable for personal data under its control without regard to the location of the data.</p> <p>17. A Member country should refrain from restricting transborder flows of personal data between itself and another country where</p> <p>(a) the other country substantially observes these Guidelines or</p> <p>(b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines.</p> <p>18. Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.</p>
CIS Model Law	<p>Статья 10. Трансграничная передача персональных данных</p> <p>1. Не может запрещаться или ставиться под специальный контроль трансграничная передача персональных данных, за исключением случаев, создающих угрозу национальной безопасности, и при необеспечении адекватного уровня</p>	<p>Article 10. Cross-border transfer of personal data</p> <p>1. Cross-border transfer of personal data cannot be banned or be placed under special control, except in cases of threat to national security, and the failure to provide an adequate level of protection of personal data.</p>

	<p>защиты персональных данных.</p> <p>2. Государство обеспечивает законные меры защиты находящихся на его территории или передаваемых через его территорию персональных данных, исключающие их искажение и несанкционированное использование.</p> <p>3. При трансграничной передаче персональных данных передающая сторона исходит из того, что в соответствии с межгосударственными соглашениями либо национальным законодательством другая сторона обеспечивает <i>адекватный</i> уровень защиты прав субъектов персональных данных и охраны этих данных.</p> <p>4. Передача персональных данных в страны, не обеспечивающие адекватный уровень защиты этих данных, может иметь место при условии:</p> <ul style="list-style-type: none"> - явно выраженного согласия субъекта персональных данных на эту передачу; - необходимости передачи персональных данных для заключения и (или) исполнения договора между субъектом и держателем персональных данных либо между держателем и третьей стороной в интересах субъекта персональных данных; - если передача необходима для защиты жизненно важных интересов субъекта персональных данных; - если персональные данные содержатся в общедоступной базе персональных данных. 	<p>2. The State shall guarantee the legal protection of the personal data on its territory or passing through its territory, in order to exclude their distortion and unauthorized use.</p> <p>3. In a cross-border transfer of personal data, transferring party shall be guided that, in accordance with international agreements or national law, the other party ensures an adequate level of protection of personal data and the protection of these data.</p> <p>4. Transfer of personal data to countries that do not provide an adequate level of protection of such data, may be carried out if:</p> <ul style="list-style-type: none"> - the express consent of the subject of personal data to that transfer is obtained; - the transfer of personal data is necessary to conclude and/or perform an agreement between the subject and the holder of the personal data, or between a holder and a third party in the interests of the subject of personal data; - the transfer is necessary to protect the vital interests of the data subject; - the personal data are contained in a publicly available database of personal data.
--	---	---