UiO : Faculty of Law
University of Oslo

Regulatory Framework for Personal Data Protection in Georgia and its accordance with EU regulations

COMPARATIVE ANALYSIS

Candidate number: 8010

Submission deadline: 01.12.2013

Number of words: 15100

Table of contents

PREFACE

The paper is an overview of the regulatory framework related to personal data protection in Georgia. It provides detailed analysis of the present legal instrument – Law of Georgia on Personal Data Protection and focuses on its main strengths and weaknesses. Also, it discusses basic differences and similarities between EU and Georgian regulatory instruments and presents their comparative analysis.

INTRODUCTION

For most of us our daily life is almost impossible without an Internet, where we create our own virtual world by sharing various kinds of personal data. On the internet we do almost the same activities as we do in the real world. Whenever we buy products on the Internet, book flight tickets, register ourselves on the social networking websites or use Internet banking we reveal most of our personal information such as our name, gender, age, bank card details and some other private data that have significant importance for our lives.

There is a legitimate question that should bother all of us: "What happens to this data? Could it fall into the wrong hands? What rights do you have regarding your personal information? "[1]

Personal information is an indivisible part of one's privacy and privacy itself is recognized as a fundamental human right by various legal instruments. "Our current understanding of informational privacy is based to some extent on how an individual relates to and controls access to information about themselves. Regulations and legislation have codified what Judge Samuel Warren and Louis Brandeis summarized in 1890 as the right of the individual to "be let alone"[2], and expanded the notion of data protection beyond the fundamental right to privacy."[3]

In order to protect our privacy we should be able to protect and control our personal information. Therefore various national and international normative instruments are based on a set of conditions or principles that include:

- Individuals should be informed when personal data is collected.
- Individuals should be told who is requesting the data and the reason for their request to help them decide whether to release control of all or part of such data.

---

[1] Protection of personal data, available here: http://ec.europa.eu/justice/data-protection/index_en.htm; Accessed 20.11.2013

[2] Warren, S.D and Brandeis, L.D. The Right to Privacy *Harvard Law Review* Boston Vol. IV No. 5 Dec 15; 1890

[3] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009

- Individuals should be told how they can access data about themselves in order to verify its accuracy and request changes.
- Individuals should be told how their data will be protected from misuse.

Implementing these conditions is not easy, particularly in today's world, where personal data is collected, processed and transferred in vast amounts, either on behalf of the individuals themselves (e.g. by the state to preserve security or improve public services) or for the benefit of commercial organizations. In such an environment, these principles must be observed in an effective way, guaranteeing the respect of the data subject's rights without overloading him with formal information in quantities that he cannot realistically be expected to process or comprehend.[4]

[4] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009

CHAPTER I – PERSONAL DATA PROTECTION IN EU

1.1 EU Directive

1.1.1 Introduction

"At the European level, the protection of privacy as an essential human right has been encased in a number of regulatory texts, most of which came into being after the Second World War. The tragedies and atrocities of this period, when large databases of personal data were used to segregate populations, target minority groups and facilitate genocide, made it abundantly clear how dangerous it could be to allow public intrusion into the private sphere.

The post-war period witnessed the arrival of the Universal Declaration of Human Rights (UN, 1948), the European Convention on Human Rights (Council of Europe, 1950), and the International Covenant on Civil and Political Rights (UN, 1966), all of which recognized privacy as a fundamental human right and focused principally on shielding the individual against abuse by protecting their personal data.

The private sector began to use personal data extensively following the arrival and broad uptake of Information, Communication Technology (ICT) in the 1970s. This increased the risk of personal data being abused and created concern that there would be a need for regulation to ensure that individuals remained adequately protected. Hence more specific regulations were introduced in the 1970s and 1980s to govern personal data processing, both at an international and a national level.

There was little harmonization between these rules at an EU level. Some Member States applied strict limitations and procedures, whereas other Member States had no rules at all. This diversity constituted a barrier to the development of the internal market (the "first pillar"), and it was in this context that the Directive was created: as an internal market instrument designed to improve cross-border trade by harmonizing data protection legislation."[5]

[5] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009. p. 6

The EU has adopted several Directives on data protection. The first and most important of these is Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data. This instrument is binding on E.U. member states, albeit with several qualifications, the most significant being that the Directive does not apply to activities relating to "public security, defence, State security ... and the activities of the State in areas of criminal law" (Article 3(2)). At the same time, though, member states are free to subject such activities to data protection regimes modelled on the Directive. Certain non-member states (Norway, Iceland and Liechtenstein) that are party to the 1992 Agreement on the European Economic Area (E.E.A.) are also bound to implement the Directive, with the same qualifications as just noted.[6]

One of the crucial characteristics of the Directive is that it is tied to the concept of personal data, and not to a notion of privacy. Indeed, the provisions of the Directive can apply to acts of data processing which are not considered to be privacy sensitive in their own right.

The Directive, therefore, serves a number of purposes, privacy protection being only one. Its rules fulfill a range of functions in practice, including encouraging freedom of expression, preventing discrimination and improving efficiency.[7]

While the Directive is primarily a European instrument for European states, it exercises considerable influence over other countries not least because it places a qualified prohibition on transfer of personal data to those countries unless they provide "adequate" levels of data protection (see Articles 25–26). As shown below, many non-European countries are passing legislation in order, at least partly, to meet this adequacy criterion. Furthermore, the Directive stipulates that the data protection law of an E.U. state may apply outside the E.U. in certain circumstances, most notably if a data controller, based outside the E.U., utilizes "equipment" located in the state to process personal data for purposes other than merely

[6] Lee A. Bygrave. *Privacy and Data Protection in an International Perspective*. 2010

[7] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009, p. 7

transmitting the data through that state (see Article 4(1)(c)). All of these provisions give an impression that the E.U., in effect, is legislating for the world.[8]

The influence of the Directive on data processing practices is undeniable: its principles have set the standard for the legal definition of personal data, regulatory responses to the use of personal data and other 'innovations in data protection policy'.[9] These include clarifying the scope of data protection rules, defining rights for data subjects, establishing the provisions regarding sensitive personal data and establishing supervisory authorities and transnational oversight arrangements in the form of the EU level Article 29 Working Party.

However, it is also important to realize that the Directive was written at a time when data processing involved filing systems and computer mainframes. The risks related to such a model could easily be managed by defining obligations and procedures linked to each role.

Its main objective was to harmonize existing regulations to safeguard the data subject's right to informational privacy and to create a common European market for the free movement of personal data, not to create a legal framework that could cope with future data processing and privacy challenges.[10]

The world has now moved on to a networked society where personal data is continuously collected, enriched, amended, exchanged and reused. It is clear that this new social environment needs well-adjusted data protection regulations to address the far greater risks of abuse. This leads to the question: is the current Directive, with its roots in a largely static and less globalised environment, still sufficiently flexible to handle the challenges of today?[11]

The Directive comprises 34 Articles and its provisions include data quality, special categories of processing, the rights of data subjects, confidentiality, security, liability and sanctions, codes of conduct and supervisory authorities. It shares a number of basic concepts

---

[8] Lee A. Bygrave. *Privacy and Data Protection in an International Perspective*. 2010

[9] Bennett C.J. and Raab, C. *The Governance of Privacy: policy instruments in a global perspective*; 2nd Edition, MIT Press, London 2006. p 97

[10] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009, p. 7

[11] Ibid

with other regulatory texts, such as the 1980 OECD Privacy Guidelines and the more recent Asia Pacific Economic Forum (APEC) Privacy Framework. While the Directive was not conceptually innovative, it has had a very powerful impact in the EU and can be credited with creating a binding and harmonized framework for data protection principles in all Member States.[12]

However, data protection in Europe is not solely dependent on state-initiated regulation. Self-regulatory approaches are increasingly common, and include sector specific codes of conduct at national and international levels, the conclusion of contracts implementing binding Model Clauses or Binding Corporate Rules (BCRs) to cover the exchange of personal data with a party outside of the European Union,[13] and identity management to deal with challenges such as data ownership, data stewardship and data broking at a non-regulatory level. The Directive acknowledges and encourages these practices.[14]

Finally, when examining the societal value of personal data, the fact that personal data protection has an inherent value to society in itself should not be overlooked. Exercising such freedoms as the freedom of speech, freedom of association and the freedom to practice religion in a meaningful way requires that the individual has a suitable personal sphere to develop his or her convictions and decide how to exercise these. Privacy rights thus can act as a vehicle to exercise other rights.[15] Privacy protection is therefore not only essential as a safeguard for personal wellbeing, but also to ensure the needed freedom and creativity that may benefit society as a whole. Thus, for the purposes of defining more or less stringent data protection rules, the debate cannot be posed purely in terms of trading personal free-

---

[12] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009, p. 7

[13] See e.g. Working Party document WP 108, « *Working Document establishing a model checklist application for approval of Binding Corporate Rules"*, adopted on 14 April 2005; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp108_en.pdf

[14] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009, p. 8

[15] Feinberg, J. *Freedom and Fulfillment: Philosophical Essays;* Princeton University Press. 1994, p248

dom for societal benefit. Privacy and data protection should not be characterized as a zero sum gain where an individual gain means a societal loss or vice versa.[16]

Circumstances have changed fundamentally since the European Data Protection Directive was created. The fluidity of personal data collections has increased as the scope, goals and ownership of such data continuously evolve. European citizens are becoming increasingly involved in managing their own data (e.g. by choosing permitted recipients or allowing preferred applications to re-use their data) through social networks, an interesting avenue of control that was not envisaged by the Directive.[17]

As was noted above, the Directive's scope is very closely tied to the notion of personal data, which is defined in the Directive in fairly strict terms, based on the linkability to individual data subjects. Using this notion as a building block, specific roles are defined in addition to that of the data subject, including those of the data controller and data processor, which are linked to specific acts of data processing (i.e. a controller in one act of data processing may become a processor in the next). Rights and obligations are defined in relation to these roles, including specific processes (information obligations, notifications, adequacy findings, etc.) to ensure that general data protection principles are observed.[18]

Generally, it is clear that there is a need for a flexible framework that allows data controllers to create and offer products and services at an international scale, while ensuring that data subjects retain their right to efficient data protection through effective enforcement and accountability mechanisms. This requires a legal framework that is sufficiently focused on real data protection impact and practical outcomes.[19]

---

[16] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009, p. 16

[17] Ibid, p. 18

[18] Ibid, p. 19

[19] Ibid

1.1.2 Main Strengths

Strength	**Evidence**
Serves as reference model for good practice	Legislation that permits practical exercise of fundamental rights derived from ECHR, and considered a leading international model. Other privacy legislations adopt elements from the Directive e.g. Hong Kong, Canada, parts of Latin America
Harmonizes data protection principles and to a certain extent enables an internal market for personal data	Implementation of legal rules across Europe for personal data processing that have greater compatibility than prior to the Directive's introduction
Flexible due to a principles-based framework	The Directive defines principles, without going into details for specific sectors/contexts. The exception to this rule is direct marketing
Technology neutral	No reference to specific technologies Security measures not specified Concept of personal data broad enough to be technologically neutral
Improves general awareness of privacy issues	Establishment and increasing numbers of privacy policies, privacy officers, etc. Consumer awareness regarding privacy[20]

The Directive as a reference model for good practice

One of the most frequently quoted positive aspects of the Directive was the impact it has had in structuring and organizing the debate surrounding data protection. While the OECD Guidelines were very influential in shaping this debate, the Directive can be credited with

[20] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009, p. 22

formulating legally binding rules that have become effective law across the Member States, following in the footsteps of the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data.[21]

As a result, the Directive is internationally respected, and its principles are often held up as a standard for good data protection practices even in contexts where it does not apply directly. Indeed, the APEC Privacy framework is one example where the provisions of the Directive have had a clear influence.[22]

A number of other jurisdictions are considering legislative reform based on the Directive. These include Hong Kong and several jurisdictions in Latin America, including Chile and Ecuador. The Directive was illustrative in inspiring Canada to develop its own Personal Information Protection and Electronic Documents Act (PIPEDA). Other examples of the Directive's influence can be found in the way that it has inspired the creation and recognition of the importance of supervisory authorities. The OECD refers to such bodies as Privacy Enforcement Authorities – reflecting a slightly different perspective of their role, emphasizing their enabling role as privacy enforcers especially in a cross border context – and has recently developed a framework to facilitate co-operation among them.[23]

Harmonizing data protection principles and enabling an internal market for personal data

One of the key goals of the Directive was to improve the harmonization of data protection rules across Member States, in order to ensure the right to privacy with respect to the processing of personal data and to permit the free flow of personal data between Member States (Article 1 of the Directive). The aim was to create a sufficiently harmonized European legal framework so that data controllers managed personal data in accordance with the

---

[21] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009, p. 22

[22] Ibid

[23] OECD, "Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy" (2007) available at: www.oecd.org/sti/privacycooperation

same principles in any Member State, and data subjects would have clear rights regardless of where they or the data controller were located.[24]

The Directive has ensured that broadly comparable legal rules for crucial aspects of personal data processing are in place throughout the EU. These include the concept of personal data, requirements for legitimacy, data quality and security, data subjects' rights and the possibility of enforcing these rules, as described by Korff.[25]

Flexibility due to a principles-based framework

Many of the Directive's obligations remain relatively high level. The framework approach based on principles allows Member States to implement the necessary measures while taking into account local traditions and sensitivities, and the needs of specific sectors.[26]

This flexibility can be seen in the case of direct marketing. It was observed during interviews with representatives from the direct marketing sector that Northern European countries are more open to direct marketing and legislate accordingly, while Southern European countries have more formal and stricter sets of rules. While the Directive itself contains certain restrictions with regard to personal data processing in the context of direct marketing – most notably the data subject's right to object to such data processing as foreseen in Article 14(b) – other aspects of direct marketing continue to diverge, and this national divergence (as a reflection of differing societal attitudes) was, perhaps surprisingly, characterized during these interviews as acceptable and even beneficial.[27]

---

[24] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009, p. 23

[25] Korff, D. *EC Study on the Implementation of the Data Protection Directive* - comparative summary of national laws; available at http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/univessexcomparativestudy_en.pdf

[26] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009, p. 24

[27] Ibid

Technology neutral

"The definition of personal data has been left deliberately abstract so that it can be applied in a number of technological contexts. The definition relies on considerations of 'content', 'purpose' and 'result', and can thus be applied to biometric data, behavioral data or characteristics that may be assigned by a data controller (e.g. passport number). The Opinions of the Article 29 Working Party on RFID and on the concept of personal data, and the responses to the 2002 Implementation Review concerning audio-visual information, attest to this flexibility.

The legal framework is therefore not limited to a specific societal and technological context, and so national data protection authorities can clarify how the Directive's provisions should be applied in each context, if needed. The Article 29 Working Party thus provides European level interpretations when required."[28]

Fostering a greater general awareness of privacy issues

"The inclusion of data protection considerations in bilateral trade negotiations between the EU and other countries (e.g. South Africa, Mexico and Thailand) indicates that awareness of data protection is improving. Agreements currently being negotiated between the European Commission and the Caribbean Community (CARICOM) and Central Africa are being amended to point to the Directive instead of OECD and UN principles.

The Directive raises awareness by stating high level goals and the way in which these goals should be achieved, and by promoting data protection tools that include notification, model contracts, standard contractual clauses, privacy policies and the appointment of Data Protection Officers. Notification, for instance, promotes the transparency goal by requiring that

[28] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009, p. 24

Data Controllers provide information about the data processing methods they intend to use and obliging them to make sure their data protection practices comply with the Directive. The transparency provisions have also helped individuals become more aware of privacy issues, especially regarding notice, consent, and choice. Interest and awareness[29] is demonstrated by responses from customers when notified about changes in privacy practices, and direct communications about uses of their personal data."[30]

1.1.3 Main Weaknesses

Weakness	**Evidence**
The link between the concept of personal data and real risks is unclear	The application scope of the Directive depends too strongly on whether or not the data processed can be defined as "personal" data. It is all or nothing: there is no room for "more or less personal" data (and accordingly "more or less protection"). Special categories of personal data processing are explicitly defined; but financial information and location data are not classified as sensitive. Strict application of the Directive's concepts sometimes leads to unpredictable or counterintuitive results.
Measures aimed at providing transparency of data processing through better information and notification are inconsistent and	Privacy policies not read in practice, as they are aimed at consumers yet written by/for lawyers Privacy policies do not play a role as a market differentiator Unclear purpose of notification Variety of 20 different notification processes, variety of exemption rules Uneven implementation of the process of registration

[29] See generally *Eurobarometer Report on Data Protection in the European Union: Citizens' perceptions*, published at http://ec.europa.eu/public_opinion/archives/flash_arch_en.htm

[30] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009, p. 24-25

ineffective	
The rules on data export and transfer to third countries are outmoded	Definition of 'third countries' is perceived as outmoded in the light of globalization Adequacy of countries is not relevant to business realities or to data protection Regulation in some other countries is stronger than the EU, but still not recognized as adequate
The tools providing for transfer of data to third countries are cumbersome	Length of time and effort required to get Standard Contractual Clauses, model contracts or Binding Corporate Rules approved is excessive Uneven practices of approval and authorization; too little coordination between the Member States
The role of DPAs in accountability and enforcement is inconsistent	Unclear rationale for enforcement Uneven implementation of enforcement across Member States either for punishment or to affect behaviors Differing criteria for imposing sanctions
The definition of entities involved in processing and managing personal data is simplistic and static	Globalization and increased re-use of personal data has outpaced the static definitions of controller and processor.[31]

The link between the concept of personal data and real privacy risks is unclear

"The scope of the Directive has been criticized because the relationship between privacy protection and data protection is vague: not all acts of personal data processing as covered by the Directive have a clear or noticeable privacy impact, and we must ask if this is a weakness in its focus. Should the impact on privacy be a relevant criterion for determining the applicability of data protection rules?

[31] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009, p. 26

The impact of the Directive is not defined in terms of situations with a privacy impact, but rather to acts of personal data processing. The Directive's approach is based strongly on a fundamental rights interpretation of data protection, where personal data is deemed inherently worthy of protection.

However, the notion of personal data is extremely broad and subject to much debate. Some argue that any data that could be linked to a specific individual should be considered as personal data. Under this absolute interpretation, Internet Protocol (IP) addresses are personal data, regardless of whether the entity processing them has a realistic possibility of linking them to a given individual. Freely chosen user names, even those that contain no semantic link to a user, and geographical information are also problematic. Data such as those in Google Street view may come under the Directive if they include images of individuals.

Anonymity in large datasets is also complicated. Healthcare research is one area that uses large sets of anonymized clinical data for statistical analysis, data mining etc. However, regardless of how rigorously the data is de-personalized, legally speaking under this absolute interpretation it remains personal data if there is a possibility of linking the data to an individual, however remote, difficult or complex that may be.

Determining what constitutes personal data becomes particularly acute in the context of mobile telecommunications, where a device with an IP address may easily be used by another entity. The problem is likely to get worse with IPv6, when IP addresses will become much more widely available and begin to be assigned to objects such as home appliances or cars.

While the relative interpretation is more flexible than the absolute one, the three criteria are still very broad. For instance, a website that uses IP addresses to determine the likely origin of a visitor for language customization purposes clearly uses information "to determine the treatment of a specific person" and "to have an impact on a specific person". Thus, data protection rules would apply, regardless of the apparent lack of privacy risk.

The Directive's rules on special categories of processing could also benefit from reconsideration. As it stands, the Directive acknowledges that certain types of personal data are more privacy sensitive and more likely to harm the data subject in cases of unauthorized

processing. These include personal data “revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life” (Article 8 paragraph 1 of the Directive). Based on this, more stringent conditions for the processing of such categories are imposed.
In addition, the special categories contain some surprising omissions, for instance financial and location data. The interpretation of location data (e.g. which locations are visited, suggesting which shops are frequented, and which products and services are bought), may in the future permit the identification of the health, social, sexual or religious characteristics of the data subject. Location based services provided via mobile devices are already seen as a growth market. This is an example of one aspect (protection of special categories of data processing) where the Directive appears to have favored a process oriented approach focused on linking specific obligations to formal criteria, rather than on an outcomes based approach that would consider the impact and the necessity of such obligations."[32]

Measures aimed at providing transparency through better information and notification are inconsistent and ineffective

"One of the goals of the Directive is to make data processing more transparent to data subjects. In order to achieve this goal, data controllers are required to provide certain information to the data subject, and in some cases to register a notification with the national data protection authority.
The information obligation is contained in Articles 10 and 11 of the Directive, which distinguish between situations where the data is directly (Article 10) or indirectly (Article 11) obtained from the data subject. In both cases, there is a list of information that must be provided to the data subject.

[32] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009, p. 27-28

The main way of providing this information is via a privacy notices, privacy policies or consent notices. While there is no strict definition of these types of documents, notices can be considered to be accessible texts aiming to inform the average data subject; policies contain specific legal information delineating data subjects' rights and data controller's obligations; and consent notices are aimed at obtaining the data subject's informed (in principle) consent for certain data processing activities, e.g. by ticking a box. Ultimately, these texts should provide consumers with the information needed to exercise their rights, and become a factor in how they value offerings.

More importantly, while privacy policies are considered to be the main way of obtaining consent from a data subject in the online world, consumers feel very strongly that current mechanisms do not help them to understand their rights.[33] The evidence suggests that their use is predominantly targeted to meet any applicable legal transparency requirement, rather than serving a real transparency benefit towards the consumer. Privacy policies are written by lawyers, for lawyers, and appear to serve little useful purpose for the data subject due to their length, complexity and extensive use of legal terminology.

Privacy policies may also differ significantly from one Member State to another. In some countries, for example, each privacy policy must state the relevant applicable decree, whereas in others the relevant law does not need to be referenced. Due to the pressures of efficiency and speed, service providers may opt to draft one privacy policy that is compatible with the most stringent legislative requirements in the hopes that this will cover the requirements of other Member States. Interviewees also mentioned that legal requirements for consent in certain countries were so restrictive that companies were dissuaded from investing in those countries.

Recent comments from the Article 29 Working Party on improving the accessibility of privacy policies by making them easier to understand were regarded as somewhat naive by those in the commercial sector, and contradictory. This is because some national laws re-

[33] E.g. see Scribbins, K., *Privacy@net – an International Comparative Study of consumer privacy on the internet* Consumers International - Programme for Developed Economies and Economies in Transition; 2001

quire full descriptions of data processing activities, and it is very difficult to describe them in a form the consumer can understand.

In addition, privacy policies have hidden costs. A recent experimental economic study of US privacy policies illustrates the potential economic damage that would result were consumers to read each policy. The cost to the US national economy just for reading each privacy policy was estimated to be $365bn, based on the length of time it takes to read a privacy policy and the monetary value of that time.

The end result is that privacy policies are not read. Companies have evidence indicating that few consumers access privacy policies. This does not necessarily demonstrate lack of interest – users notified about new privacy policies often ask questions. Surveys by Eurobarometer[34] and the social networking site Facebook[35] indicate that privacy awareness does exist, but that users do not view the privacy policy as a means of expressing their consent with its contents. An understanding that consent has already been implicitly given by accessing the service may help to explain this."[36]

The rules on data export and transfer to external third countries are outmoded

"One of the best known provisions of the Directive relates to the transfer of personal data to third countries. The Directive imposes restrictions on such data transfers to prevent personal data from being moved to countries where the data protection regime is less stringent.

Although the provision seeks to protect the data of European citizens, the sheer quantities of personal information transferred overseas may undermine this. It remains to be seen

---

[34] See the Eurobarometer *Reports on Data Protection in the European Union:* Data controllers' perceptions and Citizens' perceptions, both published at http://ec.europa.eu/public_opinion/archives/flash_arch_en.htm

[35] Thomson, M, presentation given at the *30th International Conference of Data Protection and Privacy Commissioners* "Protecting Privacy in a Borderless World" 15th – 17th October, Strasbourg 2008

[36] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009, p. 31-32

whether European citizens whose data is used and moved around by entities governed by legal frameworks outside the EU have the same level of protection.

The general rule presented by the Directive states that such transfers are only allowed if the third country ensures "an adequate level of protection", the adequacy rule. If this is not the case, certain alternative paths are available, such as the consent of the data subject, or the adoption of certain standard clauses or BCRs.

The system for assessing third counties was considered ineffective and too limited. After 13 years, only 5 non-EU countries have been found to have adequate legal frameworks: Switzerland, Canada, Argentina, Guernsey, Jersey and the Isle of Man.[37] Current and emerging trade powers such as China, India, Brazil, Japan and Russia, are not included, and the US is only covered through the 'Safe Harbor' Privacy Principles (and to a lesser extent the transfer of PNR data to the Bureau of Customs and Border Protection).

Interviewees considered that adequacy assessments as currently conducted were merely a review of paper and policy, rather than a serious investigation into how personal data is In addition, the adequacy rule was considered to be inappropriately focused. When determining whether the personal data of a specific subject is sufficiently protected in a third country, it is important to know that: (a) the data controller has taken sufficient measures to achieve this objective; and (b) the data controller can be held accountable for any incidents. The presence of an adequate legal framework that appears to match the provisions of the Directive in the third country does not address this problem fully. It was suggested by some interviewees that harmonization with third countries (those outside the EU) would automatically lead to a worse level of protection.

Assigning rights to data subjects was also seen as an issue. The example of a non-European company that wished to establish a data processing centre within Europe was cited. While this move is positive from an economic perspective, from a data controller's perspective it is confusing. Non-European citizens whose data is processed in Europe will be assigned

[37] DG Justice Freedom and Security ; *Decisions on Adequacy of Third Countries* available at : http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

rights that they do not ordinarily have, creating uncertainty as to which legal framework takes primacy."[38]

The tools providing for transfer of data to third countries are cumbersome

"Given the above, it is perhaps unsurprising that the alternative mechanisms, in particular BCRs and Standard Contractual Clauses (SCCs), were perceived as a much more positive approach to transfers to third countries. Essentially, these allow (or rather require) data controllers to assume direct responsibility for ensuring the security of the transfer and any other related data transfer.

However, even a contractual approach to data transfer leaves certain issues to be resolved. Most notably, data controllers commented that the processes for accepting standard clauses still varied from Member State to Member State, wasting considerable time for all involved. A clear call was made to: (a) harmonize the procedures for approving contractual clauses, and (b) make mutual acceptance mandatory, so that approval by the DPA in one Member State would make further steps in other Member States unnecessary. This would allow DPAs to make better use of their limited resources, instead of having to conduct an almost identical checking process across each Member State.

BCRs have come under some scrutiny due to the recent initiative whereby they are mutually accepted among a sub-group of sixteen Member States. Under this initiative, a BCR that is prepared, submitted and approved in one jurisdiction is considered as adequate in the other countries in the group. This 'passporting' of BCRs is regarded as counter-productive, since the regulators review them more stringently than SCCs because, if approved, they will be valid in several countries. However, one interviewee criticized the delay in mutually recognizing BCRs, arguing that this should have happened sooner. The lack of a clear framework under the Directive for facilitating this process was sometimes interpreted as a

[38] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009, p. 33-34

shortcoming within the Directive that placed too much importance on adequacy assessments over more pragmatic solutions.
BCRs were also criticized for being largely only useful for Human Resources data, which is structured sufficiently similarly across organizations so as to be internally consistent and hence suitable for transfer.
The practical application of BCRs has yet to be tested, since a very limited number of data controllers have attempted to implement them. Lack of harmonization was considered to be the major factor behind the uneven effectiveness of these tools."[39]

The role of DPAs in accountability and enforcement is inconsistent

"Enforcing the Directive can be difficult because the damages suffered are often intangible (or sometimes not evident in the short term), it is difficult to assign a value to any damages, and determining responsibilities is complex.
The provisions for remedies and liability in the Directive are quite broad, and in principle allow data subjects ample opportunity to obtain compensation for damages. However, this approach does not function in practice for a number of reasons, including:

- There may not be any immediate damages, such as when confidential data, e.g. credit card numbers, are leaked. As long as the data has not yet been abused, it may be difficult to obtain any compensation, even if negligence on the data controller's part has created a substantial security and privacy risk.
- The extent of damages may be difficult to quantify. To continue the example above: suppose a credit card is abused, but the bank rectifies the problem by refunding the injured party and by issuing a new card. The data subject must still obtain a new card, cancel any payments linked to the old number, notify service providers of changed

[39] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009, p. 34-35

payment info etc. Clearly, this loss of time and effort has a cost, but how can it be calculated fairly?

- Damages are typically too small to bother with on an individual scale. If 20,000 credit cards must be revoked because a data controller has been careless, 20,000 individuals will have to go through the aforementioned steps. The collective damage is clearly substantial, but it is quite unlikely that any of the individuals involved will undertake any action, since any compensation is likely to be dwarfed by the extra effort and expenditure required to obtain it. The risk of sanctions for the data controller responsible for such an incident therefore remains limited."[40]

The definition of entities involved in processing and managing personal data is simplistic and static

The relationship between processor and data controller envisaged in the Directive does not adequately cover all the entities involved in the processing of personal data in a modern networked economy. There is uncertainty about when a processor becomes a controller or vice versa, particularly in an online environment where the act of visiting a website might result in cookies being sent from a number of sources scattered around the globe.
Trends toward off-shoring, outsourcing, sub-processing and onward transfer have resulted in companies having to arrange contractual clauses with each and every sub-contractor involved in processing, in order to avoid being in breach of legislative requirements. The bureaucracy involved in reviewing each of the contracts which articulate these relationships (which may have to be re-authorized whenever there is even the slightest change) is clearly a burden for authorities and controllers.[41]

[40] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009, p. 35
[41] Ibid, p. 36

Other minor weaknesses

"Firstly, there is concern over a growing dichotomy between data protection in the first (internal market) and third pillar (law enforcement and judicial co-operation). While the Directive only covers the first pillar, the consensus seemed to be that a common vision on data protection was needed across pillars. The possible disappearance of the pillar distinction in the future is one reason behind this thinking. More importantly, the existence of special rules that substantially exempt third pillar activities from data protection principles undermines the status of these principles as an important part of the European interpretation of fundamental rights. While some concessions certainly need to be made in the light of third pillar efforts, the current approach to data protection in the third pillar is seen as being too ad hoc and lacking restrictions. While this criticism has been partially addressed through the recent Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation,[42] this does not resolve the continuing distinction between first and third pillar data protection rules and practices. The European Data Protection Supervisor (EDPS) recently raised these issues in an opinion on the Final Report of the High Level Contact Group on a transatlantic data sharing agreement.[43]

Secondly, the Directive expressly encourages codes of conduct that clarify how the provisions of the Directive apply in specific contexts and sectors at both the national and European levels. However, in practice codes of conduct are almost exclusively adopted at the national level, and their popularity varies greatly from country to country. Only two Codes of Conduct have been adopted at the EU level, one by IATA, the other by FEDMA. The

---

[42] Council Framework Decision 2008/977/JHA of 27 November 2008 *On the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*, Official Journal L 350, 30/12/2008 P. 0060 – 0071;
see http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:01:EN:HTML

[43] European Data Protection Supervisor: *Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection* Brussels, November 2008; see
http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-11-11_High_Level_Contact_Group_EN.pdf

Commission expressed its disappointment at the lack of EU level codes in its 2003 First Implementation Report.[44] The interviews for this study gave two main reasons for the lack of success with EU-wide codes of conduct. Firstly, DPAs seemed less interested in reaching a consensus on good data protection practices with the sector, and more interested in unilaterally imposing their own set of rules. Regardless of whether this is a fair statement or not, some data controllers believe that stakeholders and their legitimate interests are not adequately taken into account, and felt that their roles and interests were not adequately acknowledged in the Directive. Secondly, resources to promote and validate codes of conduct were considered insufficient, both within certain DPAs and at the European level. This may be due to a lack of resources or due to different priorities.

Finally, there is the question of the use of technology to achieve objectives. A positive aspect of the Directive was the fact that it does not specify particular technologies, but interviewees commented that technology could be used to help companies and individuals exercise the rights articulated in the Directive. It was felt that Privacy Enhancing Technologies (PETs) have not been widely taken up, for various reasons. Some respondents commented that use of PETs has been restricted because of the focus on anonymisation technologies rather than a broader definition encompassing pseudonymisation. A vicious circle appears to prevent PET uptake. Companies feel no need to deploy PETs because the regulator does not require their implementation. The regulator does not require PETs because they see no market for suppliers of such technology. Suppliers do not develop PET products because companies are not required to deploy them. The regulators thus know that a viable market for such technology to help compliance does not exist, so they may treat data controllers less harshly for not implementing such technology."[45]

---

[44] *Commission's First Report (2003) on the transposition of the Data Protection Directive*, see http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:EN:NOT

[45] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009, p. 36-37

CHAPTER II – PERSONAL DATA PROTECTION IN GEORGIA

2.1 Introduction

Until 2011 there was little specific privacy law in Georgia. As the country had not enacted the *lex specialis* legislation on data protection, the issue was mainly dealt in general manner. The Constitution of Georgia refers to the general right of privacy stating that private information of the person shall not be accessible without the consent of such person. Likewise, the Civil Code of Georgia makes no specific mention of privacy only referring to the general notion of non-materials rights of the person and establishing the general right of the person to have access to his/her private data. General regulation of data protection is also envisaged in General Administrative Code of Georgia. However, the latter is only applicable in vertical relationships and may be invoked only in relations of public law kind.

Sector-specific approach to data protection matter can be found in exceptional cases and in statutes such as the Tax Code of Georgia, Law of Georgia on Commercial Banks, Decree of National Commission of Communications of Georgia on Provision of Services and Protection of Consumers' Rights in the Sphere of Electronic Communications. However, the scope of application of these statutes is very narrow and covers the specific spheres for which these regulations have been enacted. As far as the definition of personal data is concerned, only two statutes provide the specification in this respect. According to General Administrative Code of Georgia personal data (information) means public in-formation allowing identification of a person.[46]

As mentioned above, until 2011 there was no particular law and complete legislative base on Personal Data Protection in Georgia. According to the European Neighborhood Policy Action Plan Georgia was responsible for implementation of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Therefore it was very necessary to adopt a specific law concerning this issue and make some important changes

[46] Irakli Sokolovski. *Bulletin DP@CIS, issue 1.* January, 2010

within the existing various laws in order to perform the processing, transferring, saving and protection of Personal Data according to the international standards.

2.2 Law of Georgia on Personal Data Protection

2.2.1 Overview

On December 28, 2011 the Parliament of Georgia adopted the Law on Personal Data Protection. The main part of the law was passed on May 1, 2012, while its Chapter 7 administrative liability for violation of the law was enacted since January 1, 2013. As far as the private sector is concerned, individual articles will enter into force from January 1, 2016.

The Law aims to protect fundamental human rights and freedoms, particularly the right to privacy in relation to processing personal data.

It is worth mentioning that this law is an important part of the on-going drive to open up public bodies to greater scrutiny, which would result in enhanced openness and transparency in public life. Equally important, an effective data protection law would also contribute to the regime of protection for the right to information by granting individuals the right to demand to be told what information is held on them by both public and private bodies.

The Law protects individuals' privacy in the processing of personal data by defining a number of "general principles of personal data processing", such as that personal data shall be processed lawfully and fairly, and that only relevant and accurate data shall be processed. The "data subject" is given a number of rights, including, in principle, a right to be informed that data about him/her is being processed and a right to access that data. The Law applies to data processing by any person, legal entity or administrative organ, subject to the operation of the Law on State Secrets, as well as to general exceptions for data held in relation to criminal investigations or prosecutions. Although the "data protection principles" outlined in the international treaties find some recognition in the Law, there are a number of important oversights. In particular, the exceptions relating to State secrets and

data processing in the context of criminal investigations and proceedings would limit significantly the operational scope of the law. At the same time, an exception should be added to ensure that the media are not unduly fettered in their work by the data access provisions.[47]

Article 3 of the Law provides that the law applies to "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 filing system or are processed to form part of a filing system." [48]

The same article (3) establishes some exceptions to this general principle:

1. "processing of data by a natural person for purely personal purposes, when the processing is not connected with his/her commercial or professional activities;
2. processing of data for case management purposes at the court;
3. processing of information which is considered state secret;
4. processing of data for the purposes of public and state security (including economic security), defense, operative-investigative activities and criminal investigation."[49]

The first exception, relating to data processing for personal purposes, is uncontroversial. Exceptions such as this are found in all data protection laws and have the aim of exempting people's personal address books, for example, from being subject to data protection law.

The other exceptions, however, are more problematic. They are framed as class exceptions, meaning that the Law will not apply to any data that falls in one of the relevant categories. No harm test is required and there is no provision for a public interest override.

With regard to the second and forth exception, protecting data processed in relation to criminal investigations, this would allow police or judicial authorities to shield serious wrong-doing within their departments. This is contrary not only to international standards, inasmuch as it fails to incorporate a harm test or public interest override. It also appears, on

---

[47] See Article 19. *Memorandum on the Draft Law of Georgia on Protection of Personal Data protection.* London, February 2004

[48] Law of Georgia on Personal Data Protection. Article 3, 2013

[49] Ibid

its face, to be contrary to the right to access personal information under Article 41 of the Constitution, which allows only for non-disclosure of "information containing state, professional or commercial secrets".[50]

The third exception effectively subjects the operation of the Law to the 1996 Law on State Secrets.[51] This Law defines as a "state secret", "a kind of information that includes data containing a state secret in the areas of defense, economy, external relations, intelligence service, state security and protection of law and order disclosure or loss of which may inflict harm on the sovereignty, constitutional framework or political and economic interests of Georgia."[52] An exception is provided that restricts the classification as "secret" of any information that "may prejudice or restrict basic human rights and freedoms or may cause harm to health and safety of population"[53] as well as information falling within one of the following categories:

a) information on natural disasters, catastrophes and other "extraordinary events" which have already occurred or may occur and which threaten the safety of citizens;
b) information on environmental conditions, health and living standards of the population, including information on medical services and social security, as well as social-demographic data and data on educational and cultural levels of the population.
c) information on corruption, unlawful action by officials and crime statistics;
d) information on privileges, compensations and benefits provided by the exception to citizens, officials, enterprises, institutions and organizations;
e) information on the exception monetary fund and national gold reserve; and
f) information relating to the health of "top officials of the state power".[54]

---

[50] Constitution of Georgia, Article 41(2)
[51] 1996 Law of Georgia on State Secrets, as amended by Law No. 1276 of 4 March 1998 and Law No. 1853 of 19 March 1999.
[52] Article 1
[53] Article 8
[54] Ibid

The regime established under the 1996 Law on State Secrets is problematic primarily because of the extremely broad range of material caught by the definition of "state secret". Despite the public interest exemptions provided in Article 8, the formulation as exception secret of any material relating to, for example, the economic situation of the country whose disclosure "may" cause harm would capture a wide range of materials, and is contrary to international standard according to which disclosure may be refused only where there is a serious likelihood of real harm and the overall public interest is served by non-disclosure. By subjecting the Law on Personal Data to the Law on State Secrets, an unnecessarily broad range of material has been withdrawn from the scope of the Law.[55]

2.2.3 Main Strengths

We currently enjoy de facto no protection of our private data in Georgia. Companies spam people with unsolicited advertising SMS and the Ministry of Interior continues to carry out systematic real-time surveillance of all electronic communication without sufficient court oversight. If you believe that your personal data is collected, stored and used in a way that is violating the law, there is a new authority that will soon be able to help you to address your privacy complaints and investigate your case – the Personal Data Protection Inspector's office.[56]

According to the Law of Georgia on Personal Data Protection, the new institute, Personal Data Protection Inspector shall be introduced. The Inspector shall carry out control on the lawfulness of data processing. Data Protection Inspector is appointed on the basis of an open competition. The Competition Commission is approved by the Prime Minister of

[55] Article 19. *Memorandum on the Draft Law of Georgia on Protection of Personal Data protection*. London, February 2004

[56] TI Georgia. *What you need to know about the new Personal Data Protection Inspector*. September 3, 2013; Available here http://transparency.ge/en/node/3335

Georgia. The Commission consists of representatives from the government of Georgia, the Parliament, Judiciary and Public Defender's Office, as well as NGO representatives. The Competition Commission shall select personal data protection inspector by the majority votes and submit him/her to the Prime Minister for approval. The Prime Minister appoints an inspector within 10 days term, or he announces a competition again.[57]

Personal Data Protection Inspector's office should obviously be considered as a positive novelty and main strengths of the Law of Georgia on Personal Data Protection of Georgia.

The Law on Personal Data Protection defines the Inspector's role in monitoring and enforcing of this law.

The job description of the Inspector includes:

- Providing instructions to the public and the private sector about how to ensure adequate protection of personal data;
- Reviewing data-related complaints and appeals;
- Inspecting public and private entities to ensure that the data processing is carried out in compliance with the law;
- Raising public awareness on the protection of personal data.

Among other powers, the Inspector will eventually be able to order

- that violations during the collection, processing and storage of data are corrected;
- that data that was collected or processed in violation of the law is secured, anonymized, removed or destroyed;
- a temporary or permanent stop on the processing of data if the handler of the data fails to comply with the law.

If the Inspector detects administrative offenses, she is empowered (from 2016 on) to impose sanctions on violators; the decisions are binding and can be appealed in court.

Every year, the Inspector has to issue a public annual report on the state of data protection that documents significant violations and issues recommendations for improvements. The

[57] GYLA. *Monitoring of Implementation of Personal Data Filing System in Georgian Ministries*. 2013

Inspector is entitled to submit proposals to Parliament and government institutions to improve the legal framework regarding data protection.

In line with conflict of interest rules, the Inspector cannot be an employee of another government body or carry out any other paid activity, with the exception of scientific, educational or artistic activities and must not be a member of a political party or engage in political activities.[58]

It is worth to mention that public knowledge about privacy and data protection is very low in Georgia. Most people are not fully aware that every time they go online, write an email, post a status or check-in on Facebook, Tweet their thoughts, use a chip card in a supermarket or simply send a SMS or go somewhere with their mobile phone turned on, they create a track of vast amount of information on who they are, where they are, what they purchase and where they are likely go. Analyzing all this data, which today is often referred as "new oil" and the "new currency of the digital world", gives governments, companies – anyone with access to it – the ability to analyze, understand and even predict humans' actions. This basic premise of personal data in the digital world makes it both an asset for positive developments as well as a potential object for misuse. The Inspector and her team will hopefully become a prominent and trusted institution that will not only promote an environment where both, state and private entities respect individuals' privacy rights, but also manage to increase citizens' awareness of this right.[59]

Personal data protection inspector plays a decisive role in implementation of the Law, especially when there is no experience of application of the Law and the inspector has to prepare number of different guiding recommendations. In spite of legislative obligations, the state has done nothing in that direction so far, and the inspector's position is vacant.[60]

---

[58] GYLA. *Monitoring of Implementation of Personal Data Filing System in Georgian Ministries*. 2013

[59] Ibid

[60] Ibid

2.2.3 Main Weaknesses

The regulation of personal data protection is indeed a requisite for democratic society, but the law fails to meet this objective and creates the danger of violating private life. Particularly, paragraph B of the Article 6, which envisages processing data of special category (the so-called sensitive data) without the consent of the data subject when the "public interest" is at stake. The data of special category is defined as follows: "personal data associated with the individual's racial or ethnic background, political views, religious or philosophical beliefs, membership of a professional organization, state of health, sex life, criminal history and biometrical data that can identify the above mentioned characteristics."

The corresponding provision does not fully comply with the Georgian Constitution. The Constitution already draws out the concrete public interests that can give rise to the dissemination of sensitive information. Specifically, paragraph II of the Article 41, states that in order to restrict a fundamental human right, one of the following goals must be met: "when it is necessary for ensuring the state security or public safety, for the protection of health, rights and freedoms of others."

Lasha Tordia (one of the initiators of the law) defined the idea of "public interest" in an interview with Netgazeti: "a kindergarten or a health unit must have information on whether its employee has AIDs or a kindergarten must know about the sexual orientation of its employee." "We are talking about protecting such information. This data must be used for concrete purposes and cannot be used dishonestly," – he added.

Yet the law creates a possibility of releasing sensitive information for the aim of undefined public interest thus a high risk for dishonest usage. Ucha Nanuashvili, the head of the Human Rights Center (Georgia) states: "Government creates additional mechanisms for exercising pressure on its citizens. In particular, the law envisages processing data of people's political and ideological views, ethnic and religious backgrounds and their sexual orientation. This has been the grounds for persecution of political opponents numerous times before and there is no guarantee that this data will not be used dishonestly. An employer

might not hire a person due to his illness, sexual orientation or political views and since this is not public an appeal cannot be made in any instance."[61]

After adopting the Law of Georgia on Personal Data Protection several non-governmental organizations submitted their critical reviews of the above-mentioned law. One of them was Georgian Young Lawyers' Association which presented their conclusion recognizing that adopting the specific law on Personal Data Protection is obviously a one step ahead relating to solving some legislative problems, but still it's not perfect enough to leave untouched. Even, some articles of the law should be evaluated as regressive. In particular:

- Georgian General Administrative Code establishes higher standards regarding personal data protection by public sector, than presented law. For example, according to the Article 9 of the law public institution is allowed to process and transfer the data regarding sex life, political opinions, religious or philosophical beliefs and state of health of the data subject without his/her consent. Whereas General Administrative Code fully prohibits the collection, saving, processing or transferring such kind of data which is related to racial or ethnic origin, political opinions, religious or philosophical beliefs, state of health, sex life or conviction of a person. We think the law should by no means allow the weakening of existing regulations and putting privacy in danger;
- The law establishes the price for giving out one and the same personal data to the person twice a year. But there is no definition of the price –it is the price for making a copy of the data or the data becomes requiring payment;
- Law foresees the data subject's right to appeal in case data processor refuses to rectify, update, add, block, erase and destroy the data. Data subject has the right to appeal the decision of the data processor to the higher administrative organ, personal data protection inspector or the court. The provided mechanism of appeal is quite vague. In particular, it is unclear whether it is established three-step mechanism of appeal or they are just alternatives. The law should be more specific regarding this issue.

[61] Nino Tsagareishvili. *Draft Law of Georgia on Personal Data Protection Fails to Ensure Inviolability of Private Life*. February 11, 2011

- It is also unclear what kind of final decision is made by personal data protection inspector and how strong is its legal power. In order to make personal data inspector's institution more effective it is necessary to give the obligatory character to his/her decisions.

All in all, we assume that provided version of the law is not strong enough and without making any serious changes it won't be able to fully protect people's privacy and ensure achieving its goals.[62]

2.3 Constitution and other laws

As we discussed above before 2011 there was no specific law regulating personal data processing and privacy in Georgia. Instead, there were and still are various kinds of laws thanks to which personal data protection and privacy issues were solved. In other words, before adopting the Law of Georgia on personal Data Protection all laws referring to the personal data protection were scattered and there was no complete and well-organized legislative base. In this paragraph we will name and discuss all these laws.

Constitution of Georgia

According to the Article 20 of Constitution of Georgia "everyone's private life, place of personal activity, personal records, correspondence, communication by telephone or other technical means, as well as messages received through technical means shall be inviolable." From this passage it is clear that people's privacy is protected by the supreme law, but the main problem is that it refers to the issue in a general manner. Although the Constitution foresees some exception from this general rule, in particular "restriction of the aforemen-

[62] Georgian Young Lawyers' Association. *Analysis of the Law of Georgia on Personal Data Protection.* Available here http://gyla.ge/geo/news?info=395

tioned rights shall be permissible by a court decision or also without such decision in the case of the urgent necessity provided for by law."

The most important part of the Constitution regarding privacy and personal data protection is Article 41 which explicitly states that all kind of personal data ("other private matters") is protected by law – "The information existing on official papers pertaining to individual's health, his/her finances or other private matters, shall not be accessible to anyone without the consent of the individual in question except in the cases determined by law, when it is necessary for ensuring the state security or public safety, for the protection of health, rights and freedoms of others."

Civil Code of Georgia

Civil Code of Georgia states that every person has the right to become familiar with the existing personal data about him/her which is related to his/her financial condition or other private matters and receive the copies of this data. Also, it is prohibited to refuse the transferring of the data which includes the information about him/her. It is worth to mention that the Civil Code of Georgia explicitly states that in order to process the personal data lawfully, written consent of that person is required.[63]

General Administrative Code of Georgia

The General Administrative Code of Georgia regulates personal data protection and privacy issues in relation to administrative agencies and ensures the lawfulness of their actions. The Code provides the definition of "Personal Data" according to which personal data is a public information, which allows the identification of the person. Also, it states that personal data can be considered as a private secret and it may be done so only by the person about whom this information exists. According to the Code the private secret is inviolable until the death of the person.[64]

[63] Civil Code of Georgia. Article 18^1

[64] General Administrative Code of Georgia. Article 27^1

According to the Article 43 (a) of the General Administrative Code of Georgia a public agency is allowed to "collect, process and store only those data that are expressly provided by law and are necessary for the proper functioning of the agency." Also, a public agency is not allowed to collect, process, save or transfer the personal data relating to person's religious, sexual or ethnical identity, political or philosophical beliefs. Except this, a public agency is supposed to notify immediately a concerned person at his current address of the claim of his personal data by a third person or a public agency.[65]
Article 43 also contains obligation of the public agency, in particular:

"Public agency shall

- before transferring personal data to another person/public agency take all reasonable measures for double-checking whether those data are accurate, relevant, updated and complete;
- during the collection, processing and storage of personal data inform a concerned person about the objectives and legal grounds for processing personal data, whether the person is required to provide personal information, the sources and composition of personal information and third persons who may gain access to it."[66]

As we have seen above Georgian legislation on personal data protection and privacy was consisted of above-mentioned declarative laws that made privacy related issues vague and difficult to solve.

[65] General Administrative Code of Georgia. Article 43
[66] Ibid

CHAPTER III – COMPARATIVE ANALYSIS

Protection of Personal Data is among EU top priorities and key paragraphs of the European Neighborhood Policy Georgia – EU action plan. The Law of Georgia "on Personal Data Protection" was based on the legislation of the European Union and its member states. Consequently, for determining and analyzing current standards we should review all the differences and similarities that are between EU Directive and Law of Georgia on Personal Data Protection.

3.1 Differences and Similarities

Principles of the processing of data

Article 4 of the Law of Georgia on Personal Data Protection and Article 6 of the EU Directive provide quite similar general principles for the processing of personal data:

- data should be processed fairly and lawfully;
- data should be collected only if there is a explicit and legitimate purposes;
- data should be adequate and not excessive in relation to those purposes;
- data should be valid and accurate;
- data should be kept only for as long as it is necessary for the processing of data purposes;

Grounds for the processing of data

According to the Article 5 of the Law of Georgia on Personal Data Protection and Article 7 of the EU Directive there are following criteria making data processing legitimate:

- data subject has given his/her consent;
- processing of data is envisaged by the law;
- processing of data is necessary for compliance with the obligations, compelled by the legislation, to which a data processor is subject;
- processing of data is necessary in order to protect the vital interests of a data subject;
- processing of data is necessary for the protection of legitimate interests of a data processor or a third party, except where such interests are overridden by the advanced interest of the protection of rights and freedoms of a data subject;
- processing of data is necessary for the protection of an important public interest, in accordance with the law;

As we see the grounds are exactly the same, only there are few differences. Article 5 of the Law of Georgia on Personal Data Protection states two more grounds that can make data processing legitimate. For example:

- according to the law, data are publicly accessible or a data subject has made them publicly accessible;
- processing of data is necessary for the consideration of an application of a data subject (for providing service to him/her).

Also it is worth to mention that the EU Directive is more specific and careful regarding the consent of the data subject and requires it (consent) to be "unambiguously given" while the Law of Georgia doesn't provide this kind of requirement. One can argue that this may cause misunderstanding while interpreting the law or make it difficult to know what kind of act can be considered as "consent".

When it comes to processing of special categories of data we should say that Georgian law fully corresponds with the EU Directive, stating that processing of special category of data should be prohibited. The definition of "special category of data" is provided in the Article 2(b) – data relating to racial or ethnic origin, political opinions, religious or philosophical

beliefs, trade-union membership, state of health, sex life or conviction of a person, as well as biometric data which allow for a person's identification through the above-mentioned factors;

The exceptions are also the same in both legislations. The prohibition doesn't apply if:

- data subject has given written consent to the processing of special category of data;
- processing of data is necessary for carrying out the employment obligations or enjoying the related rights by a data processor;
- processing of data is necessary for the protection of vital interests of a data subject or a third person and a data subject is physically or legally incapable of giving his/her consent to the processing of data;
- data are processed for the purposes of the protection of public health, for the protection of a natural person's health by a medical institution (employee), also if this is necessary for the management or functioning of healthcare system;

The difference is that the Article 6 of the Law of Georgia on Personal Data Protection provides one more ground for processing of special categories of data:

- data subject has made the data regarding him/her public, without explicit prohibition of their usage;

Post-Mortem Privacy

According to the EU Directive the issue of what happens to the deceased's data and individuals' privacy post-mortem is far from clear and settled from a legal and regulatory perspective. Currently, most of the data protection regimes do not include protection of decedents' personal data and they do not legally recognize this aspect of "post-mortem privacy".

Therefore, the question arises as to whether personal data should be protected both in life and upon death.[67]

In contrast to EU Directive the Law of Georgia on Personal Data Protection is quite clear about this issue. In particular, the Article 7 states:

- After the death of a data subject, the processing of data regarding him/her shall be allowed with the consent of a data subject's parent, child, grandchild or a spouse, or if 30 years have elapsed since the death of a data subject, except for the grounds envisaged by Articles 5 and 6 of this Law.
- After the death of a data subject, the processing of data regarding him/her shall also be allowed, if it is necessary for realization of the rights to inheritance.
- The processing of data on the grounds envisaged by Paragraphs 1 and 2 of this Article shall be prohibited, if a data subject has expressed in writing the will on the prohibition of the processing of data regarding him/her after death, except for the processing on the grounds envisaged by Articles 5 and 6 of this Law.
- For the processing of a deceased person's name, sex, dates of birth and death, presence of the ground for the processing of data envisaged by this Law shall be not required.
- The data on a deceased person can be disclosed for the historical, statistical and research purposes, except for the cases when a deceased person prohibited their disclosure in writing.

[67] Edina Harbinja. *Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be The Potential Alternatives?* April 15, 2013

Video surveillance

In contrast to Law of Georgia on Personal Data protection the EU Directive doesn't explicitly mention anything about video surveillance, but it doesn't mean that this issue isn't regulated. There are some general statements and requirements by which the aforementioned issue can be solved.

Directive is not applicable in matters of "public security" and if the data are not processed in files.

- So surveillance by the police cannot be judged by the Directive. On the other hand, technical surveillance by private bodies is completely regulated by the Directive, even if an enterprise is working in security.
- A simple conventional camera-monitor-system might not be a matter of the Directive, but the storage of digital pictures does.

Which are the regulations of the Directive that restrict Video surveillance?

Article 10 regulates the "notice". The affected person must be given information about:

- the identity of the person in charge for the processing;
- the identity of the processing body;
- the purpose of the processing;
- information on further recipients and
- the rights of the affected.

In addition Article 12 guarantees detailed information on the storage and the logical structure of the automatic processing.

There might be practical problems to realize the right to object (of Art. 14) in video surveillance, because the data collection happens automatically without any possibility of the affected to intervene in this process.

According to Article 15 nobody shall be subject to a considerably affecting decision made exclusively on the basis of automated data processing. This regulation is relevant, if biometrical methods of identification are used. The use of automated face recognition systems

in public areas, which can have an immense impact on the affected person, lies in conflict with this regulation.

Finally we have to mention Article 20 and 21 of the Directive: Undoubtedly video surveillance includes specific risks for rights and liberties. So this method has to be subject of a prior checking. Moreover the controller must make available (on demand) to everyone information about:

- the person in charge,
- the purpose,
- description of the categories of those affected,
- the data recipients,
- general description of the measures taken to guarantee the data security.[68]

The Law of Georgia on Personal Data Protection is more specific regarding this issue and contains several articles (Article 12, 13, 14) regulating the video surveillance of the streets and buildings (including residential ones). The Law provides some general principles which make video surveillance lawful, for example:

- Conducting video surveillance in the streets shall be allowed only for the purposes of crime prevention, as well as for the security of persons and protection of property, public order and the protection of minors from negative influence;
- In case of installing a video surveillance system, public and private institutions shall be obliged to post a relevant warning sign in a visible place. In this case a data subject shall be considered to be informed on the processing of data regarding him;
- Only outdoor perimeter and entrance of a building can be monitored by a video surveillance system;

[68] Dr. Thilo Weichert. Public Video Surveillance in View of the European Privacy Protection Directive and German Privacy Protection Law. February 22 to 24, 2000.
Available at: https://www.datenschutzzentrum.de/video/vidsur_e.htm

- Conducting video surveillance in dressing rooms and the places of hygiene shall be prohibited;
- Installation of a video surveillance system in a residential building shall require a written consent of more than a half of the owners of this building;
- Installation of a video surveillance system in a residential building shall be allowed only for the security purposes of persons and property;
- Only the entrance and common space can be monitored by a video surveillance system, installed in a residential building. Monitoring of the apartments of owners shall be prohibited;

Data security

The obligation of ensuring the adequate security and protection of the data while processing is provided in the Article 17 of the Law of Georgia on Personal Data Protection and in the Article 16-17 of the EU Directive. In particular, data processor is "obliged to apply the organizational and technical measures, which ensure the protection of data against accidental or unlawful destruction, alteration, disclosure, access, or any other form of unlawful use and accidental or unlawful loss."[69]

Also, the Article 17 of the Law of Georgia on Personal Data Protection contains some general principles according to which the data processing should be carried out:

- A data processor should ensure the registration of all actions performed on electronic data;
- The measures applied for data security shall be adequate to the risks related to the processing of data;
- The scope of power shouldn't be exceeded while processing of data;

[69] See the Law of Georgia on Personal Data Protection, Article 17

- The measures on the protection of data security shall be defined by the Georgian legislation.

Rights of a Data Subject

According to the Article 21 of the Law of Georgia on Personal Data Protection the rights of a data subject are exactly the same as they are according to the EU Directive. The law of Georgia foresees a data subject's right to request information from a data processor on the processing of data regarding him/her. A data processor should provide the following information to a data subject:

- which information regarding him/her is being processed;
- purpose of the processing of data;
- legitimate grounds for the processing of data;
- ways of collecting data;
- persons to whom the data regarding him/her ware issued, the grounds and purposes of issuance.

Also, every person have the right to check the personal data regarding him/her, stored in a public institution, and obtain the copies of these data free of charge, except for the data issuance of which requires fees in accordance with the Georgian legislation. [70]

The article 22 foresees the right of a data subject to request rectification, update, addition, blocking, erasure and destruction of data.

Like EU Directive the Law of Georgia on Personal Data Protection also provides some exemptions and restrictions from the abovementioned rights of a data subject. Exceptions are the same, in particular:

[70] See the Law of Georgia on Personal Data Protection, Article 21

- national security or defense interests of the country;
- public security interests;
- detection, investigation and prevention of crime;
- important financial or economic interests of the country (including monetary, budgetary and taxation matters);
- rights and freedoms of a data subject and of others.

Supervisory authority

The Article 28 of the EU Directive provides the obligation of appointing the supervisory authority on the protection of individuals with regard to the processing of personal data. According to this article: "Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. These authorities shall act with complete independence in exercising the functions entrusted to them."

The institution of Personal Data Protection Inspector can be considered as a direct implementation of the above-mentioned obligation in Georgian legislation. In the previous chapters we already discussed the main rights and responsibilities of the Personal Data Protection Inspector, so here we just briefly review some main characteristics of this institution.
According to the Article 27 of the Law of Georgia on Personal Data Protection there are following purposes of the activities of the personal data protection inspector:

- to provide consultations with public and private institutions (persons) on matters related to the data protection;
- to consider applications on the data protection;
- to examine (to inspect) the lawfulness of the processing of data in public and private institutions;

- to inform the public about the situation concerning the protection of data and important developments related thereto in Georgia;

The personal data protection inspector is appointed through the open competition procedure. The competition commission includes the representatives of the Government of Georgia, of the Parliament of Georgia, of the judicial authority, of the Office of the Public Defender of Georgia, as well as of the non-governmental sector, on the basis of the principle of proportionality. This ensures the objectivity and fairness of the procedure of the appointment.

The most important thing is the independence of the personal data protection inspector during fulfilling his/her responsibilities. The Article 31 of the Law of Georgia on Personal Data protection ensures the independence of the inspector by stating that:

- "In exercising his/her powers an inspector shall be independent and shall not be subordinated to any other public official or body. An inspector shall be guided by the Constitution of Georgia, international agreements, this Law, other normative acts and a statute. Any influence or interference with an inspector's activities shall be prohibited and punished by the law.
- For ensuring the independence of an inspector, the state shall be obliged to provide him/her with appropriate working conditions.
- An inspector shall have the right not to testify concerning the fact confided to him/her as to an inspector. This right shall be preserved to him/her even after the termination of the term of office."

The activities of the personal data protection inspector is financed from the state budget of Georgia and also he/she (inspector) is authorized to receive grants and contributions in accordance with the rules established by the Georgian legislation.

According to the Law of Georgia the inspector is "authorized to conduct an examination of any data processor and authorized person, based on his/her own initiative as well as on the statement of an interested person."

Examination conducted by an inspector implies:

- establishing of the protection of the principles on the processing of data and of the existence of the legitimate grounds for the processing of data;
- examining the compatibility of the applied procedures and organizational and technical measures in accordance with the requirements established by this Law;
- examining the compliance of the requirements established by this Law concerning a catalogue of filing system, register of the catalogues of filing systems and registration of data issuance;
- examining the lawfulness of the transmission of data to other states and international organizations;
- examining the compliance with the rules related to the protection of data, established by this Law and other normative acts.[71]

Transfer of personal data to third countries

The article 41 of the Law of Georgia on Personal Data Protection regulates the issue regarding the transferring of the personal data to third countries and organizations. The mentioned article states that the transfer of the personal data to third countries is allowed if:

- the grounds for the processing of data envisaged by this Law are present;
- adequate safeguards for the protection of data are ensured;
- transfer of data is envisaged by an international agreement of Georgia;
- 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.

[71] See the Law of Georgia on Personal Data Protection, Article 35

As we have seen above the Georgian legislation implemented all the grounds and general principles from the EU Directive that make the transferring of the personal data to third countries and organizations legitimate and fully corresponds with EU regulations.

CONCLUSION

The history of personal data protection in Georgia is not that long. As it was noted above, before 2011 Georgian legislation on personal data protection was consisted of the declarative laws only scattered in various kinds of codes. In 2011 Georgia made an important step forward by adopting the Law of Georgia on personal Data Protection which is the way more complete and organized legislation base on privacy issues.

As the review of the Law of Georgia on personal Data Protection showed Georgian legislation corresponds with EU Directive quite well. We also discussed the main strengths and weaknesses of the above-mentioned law and saw that it's not perfect enough and therefore needs further work. For recommendation purposes we will name some of the problematic aspects of the Law of Georgia on personal Data Protection which require more attention from the legislators. In particular:

- ✓ Public interest: According to the Law of Georgia on personal Data Protection the information (personal data) can be collected without an initial consent if the public interest is at stake (Article 6). The problem is that law doesn't provide any exact definition of "public interest", as a result of it very sensitive personal information can be collected and released easily for the aim of undefined public interest, which in its turn, creates the possibility of dishonest usage of special category of data. Legislators should be more specific and define what the term "public interest" exactly mean and this way reduce the bounds of the usage of this article.
- ✓ "Law enforcement: The government should establish a strong oversight mechanism for surveillance and communication data retention by law enforcement bodies. This oversight mechanism should have sufficient resources and enjoy a high level of independence from the executive branch of government. The mandate of the new personal data inspector and his office, which is currently established based on the Law on Personal Data Protection, could be extended to include cases related to criminal investigations, which are exempted from the mandate, as are issues related to national security.
- ✓ A team of legal experts located in the office of the personal data protection inspector could receive the mandate to scrutinize any applications, renewals and cancella-

tions of intrusive surveillance by law enforcement bodies and conduct sampling monitoring of how surveillance is implemented in practice.

✓ By law, the use of intercepts is subject to authorization by a judge. However, judges are typically not informed in depth about the subject matter of the investigation and are not told the results of the surveillance. In the past, judges have rubber-stamped prosecutors' applications for surveillance and communication interception. It is not clear to what extent this is still the practice.

✓ A lack of court oversight and a weak culture of accountability of law enforcement and intelligence bodies create a strong risk that direct access to communication data is abused and that journalists, civil society activists, politicians or members of the business community against have their movement and communication monitored.

✓ Intelligence: Parliament should establish appropriate oversight over the work of intelligence services and establish a new culture of accountability. A parliamentary commission could take on the role of monitoring of the general conduct of intelligence agencies, including their use of surveillance and wiretapping.

✓ Data collection: Ministry of Internal Affairs uses and maintains "Black Boxes" for systematic, electronic surveillance in the server infrastructure of all major telecommunication companies. These black boxes allow law enforcement bodies and security services to monitor all communication passing through the system, including text messages, internet traffic and phone calls. According to telecom insiders, the authorities have the technical capacity to monitor 21 000 mobile phone numbers at the same time. This real-time monitoring is done through a direct connection; no further assistance from telecom companies is needed. We believe the direct access to citizens' communication data has been systematically abused and that, in practice, there is no or insufficient court oversight over this surveillance.

✓ The Ministry of Internal Affairs should remove Black Boxes from the infrastructure of telecommunications companies. The existence of direct, unlimited access to peoples' communications data undermines the concept of independent court oversight over interception and creates an intrinsic risk for abuse. Law enforcement

should only be granted access to data after acquiring a court approval (w/exceptions as defined by law), and access should be limited to the persons, numbers, topics and time period covered by the court approval. Furthermore, any access to track potential abuse. The government should not outsource surveillance activities to mobile operators and internet service providers but develop a process for obtaining data in consultations with the judiciary, operators and the GNCC that is fully in line with the spirit of the law and that contains sufficient safeguards to prevent systematic, unchecked access to user data.

✓ Transparency: The Ministry of Internal Affairs should regularly and proactively release aggregate information about the number of cases in which surveillance is applied, the number of applications rejected by courts, the type of surveillance used, the duration of these efforts, the aggregate number of individuals affected and the articles of the criminal code under which this surveillance measures were approved. The Ministry of Internal Affairs should be open about the government's communications data retention. The public has a right to know if and what telecommunications data is collected, how it is collected and stored by the authorities and how long such data is retained."[72]

✓ Responsibility for individuals: Individuals should take more responsibility for their own personal data. Naive exhortations to conduct 'awareness raising campaigns' must be replaced by a more sophisticated approach, using the tools above, to alert individuals to the consequences of their actions, educate them on the risk levels and provide them with the tools to take responsibility. Those providing these tools must recognize the complex psychological and mental factors, especially concerning the perceptions and attitudes toward risk that individuals have, for example negative discounting, the perception that it will 'never happen to me' and other mental models used by individuals when deciding how to trade off their personal information for an expected social or economic benefit. Finally, individuals must have a better apprecia-

[72] Transparency International Georgia. *Secret surveillance and personal data protection: moving forward.* May 24, 2013

tion of the consequences of their behavior – however risky or not this might be. Whilst the right to privacy should be retained, there will invariably be consequences to exercising this right – and individuals must understand and be prepared to accept those consequences.[73]

✓ Responsibility for those collecting or using personal data: Greater responsibility should be placed on organizations using personal data to use that data in accordance with the General Principles outlined above. Organizations, public and private, would have to take the initiative in choosing the most appropriate tool for their particular circumstance in accordance with local requirements, and would be held responsible for their decision removing opportunity for "abdication of responsibility". The use of the tools will likely support the governance of the majority of the uses of personal data. There will always be a small minority that does not comply, either for reasons of error or more systematic failure. Enforcement should therefore be targeted at these organizations. More responsibility must rest with those using personal data, to take responsibility for their organizations and select which instruments are most relevant to their context and circumstance. In this way the market for personal data may become more self-managing, requiring less bureaucratic prior authorizations, checks and process orientated monitoring.[74]

The success or failure of privacy and data protection is not governed by the text of legislation, but rather by the actions of those called upon to enforce the law. It cannot be stressed enough that supervisory authorities must be given an appropriate level of responsibility for this arrangement to work. The stronger, results oriented approach aims to protect data subjects against personal harm resulting from the unlawful processing of any data, rather than making personal data the building block of data protection regulations. It would move away from a regulatory framework that measures the adequacy of data processing by measuring compliance with certain formalities, towards a framework that instead requires

[73] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009; p. 59
[74] Ibid

certain fundamental principles to be respected, and has the ability, legal authority and conviction to impose harsh sanctions when these principles are violated.[75]

The legislation of a country as regards the personal data protection, even identical with the one in the European Union or other western countries, can be only a first step in addressing the right to privacy and personal data protection. Maybe more important than the legislation itself is the political decision to create and support an independent authority for the personal data protection with a minimum of competent personnel. This authority has then the responsibility of creating the right strategy for its purpose that should include awareness campaigns for the citizen's rights related to personal data protection. These campaigns can be carried out even more efficiently in collaboration with the non-governmental organizations as well. The authority, in all its activities, must not forget the purpose of its creation: to safeguard the privacy and provide personal data protection for its citizens.[76]

[75] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009; p. 60

[76] Bogdan Manolea. *Institutional Framework for Personal Data Protection in Romania*

Table of reference

1. Article 19. *Memorandum on the Draft Law of Georgia on Protection of Personal Data protection*. London, February 2004;
2. Bennett C.J. and Raab, C. *The Governance of Privacy: policy instruments in a global perspective*; 2nd Edition, MIT Press, London 2006;
3. Bogdan Manolea. *Institutional Framework for Personal Data Protection in Romania*
4. Civil Code of Georgia, Act No. 786, adopted on 26 June 1997, in force since 25 November 1997;
5. *Commission's First Report (2003) on the transposition of the Data Protection Directive*;
6. Constitution of Georgia, Adopted on 24 August 1995;
7. Council Framework Decision 2008/977/JHA of 27 November 2008 *On the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*, Official Journal L 350, 30/12/2008;
8. DG Justice Freedom and Security ; *Decisions on Adequacy of Third Countries*;
9. Dr. Thilo Weichert. Public Video Surveillance in View of the European Privacy Protection Directive and German Privacy Protection Law. February 22 to 24, 2000;
10. Edina Harbinja. *Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be The Potential Alternatives?* April 15, 2013;
11. EU Directive 95/46/EC;
12. *Eurobarometer Report on Data Protection in the European Union: Citizens' perceptions*, published at http://ec.europa.eu/public_opinion/archives/flash_arch_en.htm;
13. European Data Protection Supervisor: *Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection* Brussels, November 2008;
14. Feinberg, J. *Freedom and Fulfillment: Philosophical Essays;* Princeton University Press. 1994;
15. General Administrative Code of Georgia;
16. Georgian Young Lawyers' Association. *Analysis of the Law of Georgia on Personal Data Protection*. Available here http://gyla.ge/geo/news?info=395;

17. GYLA. *Monitoring of Implementation of Personal Data Filing System in Georgian Ministries*. 2013;

18. Irakli Sokolovski. *Bulletin DP@CIS, issue 1*. January, 2010;

19. Korff, D. *EC Study on the Implementation of the Data Protection Directive* - comparative summary of national laws; available at

20. Law of Georgia on Personal Data Protection, December 28, 2011 #5669-RS, in force since 1 May 2012;

21. Law of Georgia on State Secrets, as amended by Law No. 1276 of 4 March 1998 and Law No. 1853of 19 March 1999;

22. Lee A. Bygrave. *Privacy and Data Protection in an International Perspective*. 2010

23. Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. *Review of the European Data Protection Directive*. May 2009;

24. Nino Tsagareishvili. *Draft Law of Georgia on Personal Data Protection Fails to Ensure Inviolability of Private Life*. February 11, 2011;

25. OECD, "Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy". (2007) available at: www.oecd.org/sti/privacycooperation;

26. Protection of personal data, available here: http://ec.europa.eu/justice/data-protection/index_en.htm;

27. Scribbins, K., *Privacy@net – an International Comparative Study of consumer privacy on the internet* Consumers International - Programme for Developed Economies and Economies in Transition. 2001;

28. Thomson, M, presentation given at the *30th International Conference of Data Protection and Privacy Commissioners* "Protecting Privacy in a Borderless World" 15th – 17th October, Strasbourg 2008;

29. TI Georgia. *What you need to know about the new Personal Data Protection Inspector*. September 3, 2013; Available here http://transparency.ge/en/node/3335;

30. Transparency International Georgia. *Secret surveillance and personal data protection: moving forward*. May 24, 2013

31. Warren, S.D and Brandeis, L.D. The Right to Privacy *Harvard Law Review* Boston Vol. IV No. 5 Dec 15;

32. Working Party document WP 108, *"Working Document establishing a model checklist application for approval of Binding Corporate Rules"*, adopted on 14 April 2005;