universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master‘s Thesis

„COMPARATIVE ANALYSIS OF DATA PROTECTION SYSTEMS AND REGULATORY APPROACHES IN AZERBAIJAN AND EU “

verfasst von / submitted by

Araz Poladov

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2017 / Vienna 2017

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	A 992 548
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Europäisches und Internationales Wirtschaftsrecht / European and International Business Law
Betreut von / Supervisor:	Univ.Prof. Dr. Dr. hc. Peter Fischer

TABLE OF CONTENT

LIST OF ABBREVIATIONS

AR	Azerbaijan Republic
CC	Criminal Code of AR
Charter	Charter of Fundamental Rights of the European Union
CIS	Customs Information Systems
CJEU	Court of Justice of European Union
CoE	Council of Europe
Constitution	Constitution of Azerbaijan Republic
DPD	Data Protection Directive
DPO	Data Protection Officer
EC	European Communities
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EU	European Union
Europol	European Police
GDPR	General Data Protection Regulation
ICCPR	International Covenant on Civil and Political Rights
JSB	Joint Supervisory Body
OECD	Organization for Economic Cooperation and Development
SIS	Schengen Information System
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights
UN	United Nations
UN GA	United Nations General Assembly
USA	United States of America
VIS	Visa Information System

INTRODUCTION

XXI century can surely be called as an "Information century". Information technologies have deeply penetrated almost every sphere of human life. Such development of information technologies is a contemporary phenomenon of modern society. The information today is one of the most important strategic resources of state or any individual can possess. Every institution and organization, whether private and public, uses information. Millions of organizations and individual persons are in a need to or are required to process personal information for some purpose. For instance, health care institutions need to retain information about their patients, employers need to process the data of the employees in order to perform their activity properly, financial organizations on the other hand need to exchange information for providing these financial services.

The current phenomenon of globalization is mainly due to the close integration of borderless communications with our everyday lives. As a result of rapid expansion of information technologies nowadays, their penetration in all spheres of life, collection and processing of personal data through the use of new technologies makes inevitable to ensure the protection of personal data on the international and regional level.

With the emergence of information technology in the 1960s, a growing need developed for more specific rules to safeguard individuals by protecting their data. There is actual and substantial threat related to processing of personal data. Protection of personal data is interconnected with a right to privacy and right to private life. One can be negatively affected due to inaccurate data about him. Inappropriate use or abuse of personal data can have an adverse impact on the person. In order to protect individuals against abuses in regard to collection, storage, processing and flow of personal data, and lay down the fair and lawful principles of procession of such data, the creation of international and national legal instruments was vital. The new branch of law was referred to as Data Protection law, which was comprised of legal rules and instruments designed to protect the rights, freedoms and interests of individuals whose personal data are stored, processed and disseminated by computers against unlawful intrusions, unauthorized alteration, loss, destruction or disclosure.[1] Privacy laws and in particular the data

[1] Frits W Hondius, *Emerging Data Protection In Europe* (North-Holland Pub Co 1975) 1.

protection laws are being created and used to shield persons from the detrimental effects of this development.[2] All this makes the data protection laws as a vital part of protection of privacy. Not surprisingly, personal data protection is a fundamental right in the European Union; it is part of the European DNA and deserves the highest protection standards.[3]

Unlike national legal systems which are within the boundary of one state, the information crosses the borders of different states and legal systems by means of modern Technologies. Such an international and global character of data protection policy makes the international-legal cooperation in this sphere inevitable and requires the adoption of international legal instruments and their implementation in national law.

The emergence of data protection laws is recent. The first pieces of legislation were enacted in early 1970s. These pieces of legislation intend on regulating the general principles and rules for processing, use, storage and dissemination of personal data, granting the data subject proper legal safeguards. To this end, on January 28, 1981 the European Council adopted a Convention for the "Protection of Individuals with regard to automatic processing of personal data", the first and until now the only internationally binding legal document in this. The typical aim of these instruments is safeguarding of individual's right to private. As set out in article 1 of CoE Convention, the main object is to secure for every individual, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him.

This study seeks to analyze the protection of personal data in EU and Azerbaijan, as well as to undertake a comparative analysis of regulatory approaches of those jurisdictions. The principal objective of this thesis is to systematically review the protection of personal data in Azerbaijan, and to assess the adequacy of the protection of personal data in Azerbaijan in regard and relation to EU, as well as to contribute to the field of data protection in Azerbaijan.

The main part of the thesis is composed of Introduction, four chapters and Conclusion. The first chapter provides insights to the right to privacy in general, and role

[2] Lee A Bygrave, *Data Protection Law* (Kluwer Law International 2002) 4.
[3] European Commission, Taking data protection into a digital and globalized era: Joint Statement by Vice-President Ansip and Commissioner Jourová ahead of the 2017 Data Protection day Brussels, 27 January 2017, STATEMENT/17/154, available at: http://europa.eu/rapid/press release_STATEMENT-17-154_en.htm [accessed 25 June 2017] 1.

of internationals organizations and instruments for facilitation of protection of this right. The second chapter is set to carry out prospective study of DPD and other EU legislation on protection of personal data. The third chapter is aimed to investigate the legislation of AR and detailly evaluate the legislation vis-à-vis EU. The last chapter assesses the adequacy of data protection of AR in the light of all relevant circumstances and in regard to EU. The Conclusion sums ups all the findings and analysis undertaken by the thesis.

CHAPTER I. RIGHT TO PRIVATE LIFE AS A FUNDAMENTAL RIGHT

1.1. What is right to private life?

The right to privacy or the right to respect for private and family life, home and correspondence is a fundamental human right. This right was first laid down in an international legal instrument in Article 12 of the Universal Declaration of Human Rights which proclaims that no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Almost all the international and regional instruments, such as European Convention for Human Rights, International Covenant on Civil and Political Rights, European Charter of Fundamental Rights provide the right a to respect for one's "private and family life, his home and his correspondence". Over 160 national constitutions mention this right.[4]

Private life is a broad term not susceptible to exhaustive definition.[5] The concept of private life is clearly wider than the right to privacy.[6] The European Court of Human Rights has interpreted, on a case-by-case basis, the concept of 'private life' and the situations falling within this dimension. including bearing a name, the protection of one's image or reputation, awareness of family origins, physical and moral integrity, sexual and social identity, sexual life and orientation, a healthy environment, self-determination and personal autonomy, protection from search and seizure and privacy of telephone conversations.[7] Privacy protection is frequently seen as a way of drawing the line at how far society can intrude into a person's affairs. It can be divided into the following facets :

- **Bodily privacy**, which concerns the protection of people's physical selves against invasive procedures such as drug testing and cavity searches;

[4] 'Read About "Right To Privacy" On Constitute' (*Constituteproject.org*, 2017) <https://www.constituteproject.org/search?lang=en&key=privacy> accessed 23 June 2017.
[5] P.G. and J.H. v UK App no 44787/98 (ECHR, 25 September 2001), para 56.
[6] Ursula Kilkelly, *The Right To Respect For Private And Family Life* (Directorate General of Human Rights, Council of Europe 2001) 11.
[7] Ivana Roagna, *Protecting The Right To Respect For Private And Family Life Under The European Convention On Human Rights* (Council of Europe 2012) 12.

- **Privacy of communications,** which covers the security and privacy of mail, telephones, email and other forms of communication; and
- **Territorial privacy**, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space.
- **Information Privacy**, which involves the establishment of rules governing the collection and handling of personal data such as credit information and medical records.[8]

This right is however, not an absolute right and must be balanced against other rights.[9] As the CJEU held, this right must be considered in relation to its function in society.[10] The right most probably to come to conflict with the right to privacy is freedom of expression. The ECHR and CJEU have had to deal with reconciliation of the right to privacy with the freedom of expression[11][12][13], freedom of art and sciences[14] and right to property[15].

Thus, in order to reconcile the right to privacy and other rights, as well as to regulate the collection, processing and protection of personal data, new instruments called "Data Protection Laws" were introduced.

1.2.Data Protection Laws

Data processors, who are the main and physical controllers of personal data, can use the personal data in a manner incompatible with the normal and traditional business activities: they view the personal data as a commodity with a commercial value. There are different ways of inappropriate use of data: the data of the customers may be sold to other businesses offering the goods and services. The data can also be "warehoused"[16],

[8] 'Privacy And Human Rights - Overview' (*Gilc.org*, 2017) <http://gilc.org/privacy/survey/intro.html> accessed 25 June 2017.
[9] Case C-92/09 and C-93/09 Volker and Markus Schecke Gbr and Hartmut Eifert v. Land Hessen [2010] ECR 2010 I-11063, para 48.
[10] Ibid.
[11] Axel Springer AG v. Germany App no 39954/08 (ECHR, 7 February 2012).
[12] Von Hannover v. Germany App no 40660/08 (ECHR, 7 February 2012).
[13] Mosley v. the UK App no 48009/08 (ECHR, 10 May 2011)
[14] Vereinigung bildender Kunstler v. Austria App no 68345/01, (ECHR, 25 January 2007).
[15] Case C-275/06 Productores de Musica de Espana v. Telefonica de Espana Sau [2008] ECR 2008 I-00271
[16] David I Bainbridge and Nick Platten, *European Dataqqq Protection Directive* (Butterworths 1996) 5.

where bulks amount of personal data is collected and retained. Information relating to a particular individual an also come from different sources and be combined, which is known as data matching.[17]

Although the international and regional instruments, such as UDHR, ECHR, ICCPR prescribed the right to private life of individuals, the new data processing power of computer technology raised the problem which could not be dealt with a general right to privacy.[18] Therefore, a new class of laws commonly referred to as Data Protection Laws emerged. The term Data Protection is most commonly used in European jurisdictions. In jurisdictions like USA, Canada and Australia, the term "privacy protection" is preferred instead.[19] These laws can be briefly described as rules regulating the processing of personal data.

Data protection is a legal response to a potential and real problem of all human beings: threat to privacy by the mass processing of data. Its main aim is to stimulate the creation of adequate national data protection laws and regimes, in order to prevent the divergence between them. This is not only to strengthen the data protection and protection of right to private life, but also to ensure the free flow of personal information across the borders and thereby ensure the freedom of expression, which covers the right to receive and impart information and ideas regardless of frontiers.[20] Similar concerns are also evident in OECD and UN Guidelines.[21]

1.3.International organizations and legal instruments

International organizations have been playing a vital role with regard to the development of data protection instruments on international plain. In the United Nations at the international level and in the Council of Europe at regional level, a series of studies on computers and human rights were conducted.

A major aim of international data protection instruments is the creation of adequate data protection regimes and prevention of divergence. This approximation of

[17] Ibid 6.
[18] Ibid 14.
[19] Bygrave, (n 2) 1.
[20] Bygrave, (n 2) 40.
[21] Ibid.

laws carries out 2 main tasks: the strengthening the data protection and the right to private life in general and ensuring the free flow of personal data between the states. This concern is due to existence of data protection norms in many countries which provide for restriction of trans-border data flows without equivalent or adequate level of protection.[22]

United Nations

One of the most important international instrument regulating the right to privacy is Universal Declaration on Human Rights which was proclaimed by the UN General Assembly in 1948[23]. Article 12 prescribes that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." Article 17 of International Covenant on Civil and Political Rights[24], opened for signature by the UN General Assembly in 1966, is also similar and states that Everyone has the right to protection from arbitrary or unlawful interference with his privacy, family, home or correspondence, and against to unlawful attacks on his honor and reputation.

Some account has to be given to United Nations Guidelines Concerning Computerized Personal Data Files, adopted by the UN General Assembly in 1990. The Guidelines called upon the UN Member States to take steps and enact the legislation based on these Guidelines. However, these Guidelines had little practical importance because of its non-binding and recommendatory nature.

Council of Europe

In Europe, the first organization to address the emerging problem was the Council of Europe. By virtue of the Council of Europe, the most important instrument for protection of right to privacy and in general the human rights and freedoms – the European Convention on Human Rights and Fundamental Freedoms had been created. The particular significance of this Convention was a legal mechanism of implementation. Unlike the subsequent legal instruments, an individual court bring the case to the court if

[22] Ibid.
[23] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR)
[24] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR)

his rights under the Convention were violated. The article 8 of this convention consists of 2 parts: the scope of the right and limitation thereto:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Nevertheless, the general right to private life under article of ECHR could not properly address the issues related to processing of personal data. Therefore, The subsequent attempt was made by Council of Europe in 1981 and "The Convention for Protection of Individuals with regard to automatic processing of personal data" was opened to signature in 1981. Despite of its binding legal force, it lacked the implementation mechanism. Unlike ECHR, it did not address individuals. The individuals could not invoke the provisions of the Conventions before a court. It was rather addressed to Member States, which were to "take necessary measures in their domestic law to give effect to basic principles of data protection.[25]

OECD.

Another attempt at international plain was made by Organization for Economic Co-operation and Development, which adopted a recommendation on principles of the protection of privacy, namely, the OECD Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data. However, these Guidelines ultimately failed to address the potential issues because of its recommendatory character.[26] Nonetheless, these Guidelines had a great impact on enactment of Data Protection legislation in Non-European Jurisdictions.[27]

Other International Organizations and instruments.

[25] Council of Europe Convention for the Protection of Individuals with regard to automatic processing of personal data (opened for signature 28 January 1981, entered into force 1 October 1985) (Convention 108) art 4(1).
[26] Bainbridge and Platten, (n 16) 16.
[27] Bygrave (n 2) 32.

Some other international organizations, such as The International Telegraph and Telephone Consultative Committee, the Intergovernmental Bureau for Informatics, The World Intellectual Property Organization and the Nordic Council carried out studies on privacy and secrecy in international data networks. During their operation, they elaborated certain safeguards and stressed the importance of appropriate forms of legal protection of computer programs. The secrecy and confidentiality of data and processing was of a primary concern.[28]

[28] Hondius (n 1) 73-74.

CHAPTER II. DATA PROTECTION IN EU

2.1.General background

EU law is composed of the treaties and secondary EU Laws. The treaties, namely Treaty on European Union(TEU), the Treaty on the Functioning of the European Union(TFEU) and Charter of Fundamental Rights of European Union are referred to as "Primary EU Law". On EU level, none of the original treaties of the European Communities(TEU and TFEU) made any reference to human rights and freedoms in general. Therefore, ECJ brought the fundamental rights in so called general principles of European Law. In 2000, EU adopted the Charter of Fundamental Rights of the European Union. The Charter contains full range of civil, political, economic and social rights of the European Citizens. The Charter is legally binding both on Member States and EU Institutions when implementing EU Law. The binding legal nature of the Charter was established with the coming into force of Lisbon Treaty in December 2009.[29]

The Charter contains both the right to private and family life(Article 7) and right to data protection(Article 8). Accordingly, the right to data protection has gained the force of fundamental human right on EU level.

The principal secondary EU legal instruments on data protection are Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data[30], Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[31], Regulation on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[32] and

[29] *Charter of Fundamental Rights of the European Union*, [2012] OJ C 326/02, art 51 (Charter of Fundamental Rights).
[30] Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (Data Protection Directive).
[31] 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 [2008] OJ L350/60 (Council Framework Decision).
[32] Council Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L8/1 (Community Institutions Regulation).

Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector.[33]

There are also some other sectoral data protection instruments available, such as Prüm Decision which regulates the processing of special data, such as fingerprints, DNA, Europol, Eurojust decisions which contain provisions regulating the processing of personal data by specialized agencies, Schengen II Decision, VIS Regulation, Eurodac Regulation and CIS Decision, which deal with special joint information systems, Directive on markets in financial instruments which contains provisions in regard to protection of financial data.

The European Commission put forward its EU Data Protection Reform in January 2012 to make Europe fit for the digital age.[34] They include a policy Communication setting out the Commission's objectives and two legislative proposals: a **Regulation** setting out a general EU framework for data protection and a **Directive** on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities. As a result, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data[35] and Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data,[36] were adopted on of 27 April 2016. However the Regulation and Directive shall apply after a two-year transition period, from 25 may 2018[37] and 6 may 2018[38] respectively. Therefore, it is beyond of the scope of this thesis to examine General Data Protection Regulation and Council Directive on the protection of natural persons with regard to the processing of personal data by

[33] Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in electronic communications sector [2002] OJ L201/37 (E-privacy Directive)
[34] 'Reform Of EU Data Protection Rules - European Commission' (*Ec.europa.eu*, 2017) <http://ec.europa.eu/justice/data-protection/reform/> accessed 28 June 2017.
[35] Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (General Data Protection Regulation).
[36] Council Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89 (Police and Criminal Authorities Directive).
[37] General Data Protection Regulation, art 94.1.
[38] Police and Criminal Authorities Directive , art 59.1

competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

2.2.Data Protection Directive

2.2.1. Aims of the directive

One of the primary objectives of the European Union is the ensuring of economic and social progress by eliminating all the barriers and creating a Common Internal Market.[39] The economic and social integration resulting from the establishment and functioning of the internal market inevitably leads to a substantial increase in cross-border flows of personal data between Member States.[40] The divergence between the legislation and the difference in levels of protection of personal data in Member States could prevent the free flow of personal data. Therefore, the principal task of the Directive is to remove the obstacles to flows of personal data and approximate the national laws of the Member States.

The Data Protection Directive has two main objectives, which are stated in Article 1: protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data; and ensuring the free flow of personal data between Member States.

Throughout, the Directive tries to achieve a difficult balance between the data subjects rights and conflicting rights. Although the interests of data subjects and data controllers are often irreconcilable and contradicting, the Directive does strike a fair balance.[41]

2.2.2. Scope of the directive

Scope in regard to type of data

[39] Data Protection Directive, recital 1.
[40] Data Protection Directive, recital 5.
[41] Bainbridge and Platten (n 16) 42.

The regulatory focus of Data Protection Directive is centered upon personal data or information[42]. The personal data means any information relating to identified or identifiable person.[43] 2 criteria are important: the data has to relate to a person and the data has to facilitate the identification of such person. In other words, the information has to potentially enable to identify the person by reasonable means.[44]

Information relating to dead individuals is in principle not to be considered as personal data subject to the rules of the Directive, as the dead are no longer natural persons in civil law.[45]

Scope in regard to type of processing

Data Protection Directive regulates all stages of data-processing. The type of processing is not important, the Directive covers the processing by automated, semi-automated and manual means. Pursuant to the Directive, purely manual data processing is to be regulated insofar as the data forms or is intended to form a part of filing system within the meaning of Art 3(1) of Directive. The rationale behind this approach is to limit the application of data protection laws to data that can be linked to a particular individual without great difficulty.[46] It is also partly based on the fact that manual processing of data can have significant impact on the privacy and integrity of data subjects, as the most sensitive personal data could be found in manual record systems.[47]

Scope in regard to purpose of processing

As mentioned before, the Directive was adopted to remove the barriers of free flow of personal data in order to facilitate the Internal Market. Therefore, the Directive does not apply to activities which are outside the Community law, namely, the processing operations concerning public security, defense, State Security(including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.[48] This approach is reinforced in

[42] Data Protection Directive, art 1.
[43] Data Protection Directive, 2(a).
[44] Data Protection Directive, Recital 26.
[45] Article 29 Working Party Opinion 4/2007 of 20 June 2007 on the concept of personal data 01248/07/EN WP 136. 22.
[46] Bygrave (n 2) 52.
[47] Ibid 53.
[48] Data Protection Directive, art 3.

Art 13(1) of the Directive, which allows the Member States to derogate from some rights and obligations under the Directive for the purposes of national security, defence, public security and prevention, investigation, detection and prosecution of criminal offences.

The second principal exception is the so called "household" exception. The Directive shall not apply to the processing of personal data by a natural person in the course of a purely personal or household activity. Recital 12 refers to activities which are exclusively personal or household, and clarifies that activities such as correspondence and the holding of records of addresses are excluded from the Directive. Keeping an address book of friends and acquaintances on a home PC, having files relating to their own commercial affairs – e.g. bank statements, mortgage payments or insurance documents, holding records relating to family members' health checks, school reports and so forth, having a list containing individuals' contact details, keeping a personal diary containing references to friends and workmate would normally fall under household exemption and be excluded from the scope of the Directive. However, this exemption has to be interpreted narrowly, especially in context of disclosing of data. Publication of personal data to unlimited number of people in internet would not be covered under household exemption.[49]

The third exemption from the Directive is prescribed in Art 9 of it, where it requires the Member States to lay down exemptions from the central provisions of the Directive with respect to processing "carried out solely for journalistic purposes or the purpose of artistic or literary expression", where it is necessary to reconcile the right to privacy with the rules governing freedom of expression.

Subjective and territorial scope of Directive

The Directive is addressed to Member States which are obliged to bring their data protection laws in conformity with the Directive. The Directive also applied to the processing of personal data by the Community Institutions until the adoption of Regulation 45/2001 of the Parliament and the Council on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data.

[49] Case C-101/01 Bodil Lindqvist [2003] ECR 2003 I-12971, para 31.

Moreover, the Directive was incorporated into the 1992 Agreement on the European Economic Area, so that non-EU states Norway, Iceland, Liechtenstein were legally bound to bring their laws in conformity with the Directive.[50] The Directive also has some indirect political and legal influence over third countries as it prohibits the transfer of data to the countries if they have no adequate level of protection.[51]

2.2.3. Main legal issues of the Directive.

2.2.3.1. Main definitions

Personal Data. Under EU law, personal data is defined as any information relating to an identified or an identifiable natural person[52]. However, EU Law does not specify when a person is considered to be identified. The person is identified if his identity is sufficiently clear and evident. The person is identifiable if additional information for identification can be obtained without unreasonable effort. Identification means a person is described in such a way that he or she is distinguishable from all other persons and recognizable as an individual. [53]According to recital 26 of Directive, the benchmark is whether there are reasonable means for identification available. For information to be 'personal data', it is not necessary that it be true or proven.[54] The protection afforded by the rules of the Directive applies to natural persons, that is, to human beings. Member States' legislation, usually in the field of Civil Law, outlines more precisely the concept of personality of human beings, understood as the capacity to be the subject of legal relations, starting with the birth of the individual and ending with his death. As the definition of personal data refers to individuals, i.e. natural persons, information relating to legal persons is in principle not covered by the Directive, and the protection granted by it does not apply.[55]

Special categories of personal data. Under the Directive, there are special categories of personal data, which, by their nature, may pose a risk to the data subjects.

[50] Bygrave (n 2) 31.
[51] Ibid.
[52] Data Protection Directive, art 2(a)
[53] *Handbook on European data protection law* (Publications Office of the European Union 2014) 39.
[54] Ibid (n 45) 6.
[55] Data Protection Directive , recital 24.

These categories of data are called sensitive data and are subject to more strict safeguards and enhanced protection. Pursuant to Article 8 of Directive, the categories are:

- Personal data revealing racial or ethnic origin
- Personal data revealing political opinions, religious or philisophical beliefs, trade-union memberships
- Personal data concerning health or sexual life.

The users of personal data. Pursuant to the Data Protection Directive, the main users of personal data are controller, processor, and third-party recipient. The most important legal consequence of being a controller or processor is the obligation for compliance with legal obligations stemming from the directive. The **controller** is any natural or legal person, public authority or agency which determines the purposes and means of processing of personal data. The controller is the de-facto controller, irrespective of legal entitlement to process the data. In other words, the controller is considered as such even if he had unlawfully decided that the data should be processed.[56]

The **processor** is a natural or legal person, public authority, agency or any other body which processes the data on behalf of the controller. Even if the power to determine the means of processing is delegated to the processor, the controller must have the power to interfere with the decisions of the processor. The relationship between controller and the processor should be governed by a contract or legal act.[57] The processor and the controller are jointly liable for damages, if the processor breaches the mandate of controller.[58]

A third party is any natural or legal person other than the data subject, the controller and the processor who is authorized to process the data. The persons working for an organization which is legally distinct from the controller, even if it belongs to the same group or holding company- will be a third party.[59] Disclosing data to a third party therefore needs a specific legal basis.

The recipient is any natural or legal person to whom the data is disclosed. It is a broader term that the third party within the meaning of art. 2(g) of Directive, as the

[56] Article 29 Working Party Opinion 1/2010 of 16 February 2010 on the concepts of "controller" and "processor" 00264/10/EN WP 169. 9.
[57] Data Protection Directive , art 17(3).
[58] Ibid (54) 25.
[59] *Handbook on European data protection law* (n 53) 54.

recipient can either be a third party or a person inside the controller or processor, to whom the data is disclosed.

The consent pursuant to art. 2(g) of the Directive shall mean freely given specific and informed indication of wishes of data subject which signifies his agreement to processing of his personal data. The data subject's consent has always been a key notion in data protection, but it is not always clear where consent is needed, and what conditions have to be fulfilled for consent to be valid. Moreover, in the online environment - given the opacity of privacy policies - it is often more difficult for individuals to be aware of their rights and give informed consent.[60]

Consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent. If the consequences of consenting undermine individuals' freedom of choice, consent would not be free. [61] To be valid, consent must be specific. In other words, blanket consent without specification of the exact purpose of the processing is not sufficient.[62] To be specific, consent must be intelligible: it should refer clearly and precisely to the scope and the consequences of the data processing. It cannot apply to an open-ended set of processing activities. This means in other words that the context in which consent applies is limited. [63]

2.2.3.2. Main principles of data processing

Data Protection Directive sets out the fundamental principles of processing of data. Where the controller cannot satisfy the Data Protection Principles (and if no exemption or derogation applies) then such processing will be unlawful. As a result, it is important for controllers and processors to understand and respect those principles.

Principle of lawful processing

[60] Article 29 Working Party Opinion 15/2011 of 13 July 2011 on the definition of consent 01197/11/EN WP187. 3
[61] Ibid 12
[62] Ibid 17
[63] Ibid

Member States shall provide that personal date is processed lawfully.[64] In a bid to understand the principle of lawful processing, the conditions for lawful limitations of right to private life or right to data protection have to be analyzed. Pursuant to art. 8(2) of ECHR, the limitations are justified if it is in accordance with law, pursues a legitimate aim and is necessary in a democratic society. The jurisprudence of European Court on Human Rights stressed that the interference with right to privacy has to be based on law which is accessible and has foreseeable consequences.[65] The legitimate aim of processing is either a public or private interest. As the Court held, absence of sufficient or relevant reasons for processing of personal data would constitute a violation of Article 8 of ECHR.[66] ECtHR has reiterated that the necessity in democratic society implies that the interference corresponds to a pressing social need and is proportionate to the legitimate aim pursued.[67]

According to Article 52(1) of EU Charter on Fundamental Rights, the limitations on the exercise of fundamental rights are justified if they are provided by law, respect the essence of the right in question, are necessary and proportionate and meet the objectives of general interest recognized by the Union. In spite of different wording, conditions for lawful limitation in Article 52(1) of the Charter are complementary of Article 8(2) of the ECHR. Insofar as the rights contained in the Charter corresponding to rights under ECHR, the meaning and the scope of those rights shall be the same.[68]

So, any processing of data within the meaning of art. 2(b) of Directive, shall be lawful if it is based on domestic provisions of law, pursues a legitimate aim and if the fair balance is struck between the right of data subject and the rights of the others.

Principle of fair processing of data

The principle of fair processing implies the transparency of processing of personal data. In other words, the data subject must be in a position to know about the existence of the processing operations.[69] Controllers have to inform the data subjects before the processing operations commence, at least about the identity of controller, the purposes of

[64] Data Protection Directive, art 6(1)
[65] Amann v Switzerland App no 27798/95 (ECHR, 16 February 2000), para 50.
[66] Peck v the United Kingdom App no 44647/98 (ECHR, 22 October 2002).
[67] Leander v Sweden App no 9248/81 (ECHR, 26 March 1987), para 58.
[68] Charter of Fundamental Rights, art 51
[69] Data Protection Directive, recital 38.

the processing, the recipients of the data and rights of the data subjects.[70] Except the circumstances envisaged by law, the processing operations should not be covert and secret.

The principle of purpose specification and limitation.

Member States shall provide that personal data is collected for specified, explicit and legitimate purpose and not further processed in a way incompatible with those purposes. In essence, this principle is a prerequisite of lawfulness of data processing.

First, any purpose must be specified, that is, sufficiently certain to enable the implementation of any necessary data protection safeguards, and to limit the scope of the processing operation.[71] This means that the purpose has to be specified by the controller before the collection or processing of data starts. Second, to be explicit, the purpose must be sufficiently unambiguous and clearly expressed. The ultimate objective of this requirement is to ensure that the purposes are specified without vagueness or ambiguity as to their meaning or intent. What is meant must be clear and should leave no doubt or difficulty in understanding.[72] Third, purposes must also be legitimate. In order for the purposes to be legitimate, the processing must - at all different stages and at all times - be based on at least one of the legal grounds provided for in Article 7.

Article 6(1)(b) of the Directive also requires that further processing must not be incompatible with the purposes for which personal data were collected. In particular, Article 6(1)(b) requires that personal data should not be 'further processed in a way incompatible' with those purposes originally specified. Further processing for historical, statistical or scientific purposes shall not be considered incompatible. In incompatibility test, due account has to be taken from the relationship between the initial and further purposes, the context in which the data have been collected and the reasonable expectations of the data subjects, the nature of the data and the impact of the further processing on the data subjects.[73]

The principle of data quality

[70] Data Protection Directive , art 10.
[71] Article 29 Working Party Opinion 03/2013 of 2 April 2013 on purpose limitation 00569/13/EN WP 203. 40.
[72] Ibid (n 60) 19.
[73] Ibid (n 71) 40.

The data quality principles requires that the data must be adequate, relevant, not excessive and accurate.[74] This principle implies that the categories of data chosen for processing must be suitable to achieve the overall purpose of processing. In other words, the controller has to ensure that the personal data is relevant for the specific purpose of the processing.

The data accuracy principle infers that the personal data has to be accurate and kept up to date and the controller has to take reasonable steps to ensure this. Inaccurate and incomplete data are to be erased or rectified.[75] Data controllers must ensure that data subjects can rectify, remove or block incorrect data about themselves;

The principle of limited retention of data

Article 6(1)(e) of the Data Protection Directive requires the Member States to provide that the personal data are kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes the data was initially collected or for which they are further processed. This principle implies that the data must be either deleted, anonymized or pseudonymized after the purposes of processing have been achieved. The exception to this principle is storage of personal data for historical, scientific and statistical purposes subject to appropriate legal safeguards.

2.2.3.3 Rules on processing of data

The data protection Directive established a layer of detailed rules which must be implemented in national law. These rules are aimed to harmonize the level of protection of the personal data in Member States in order to ensure the free flow of personal data between them.

The directive establishes the rules on lawful processing, rules on secure processing, rules on transparency of processing and rules on promoting compliance. The Directive envisages two different set of rules for lawful processing: rules for processing of non-sensitive personal data(art 7) and rules for processing of sensitive data(art 8).

[74] Data Protection Directive, art 6(1), paras (c),(d).
[75] Data Protection Directive, art 12(b).

Rules on lawful processing of non-sensitive data.

Data Protection Directive provides that non-sensitive personal data may only be processed on 6 legal grounds enumerated in Article 7. This list is exhaustive.[76]

Consent. Under EU law, the consent is a first basis for legitimate processing of data. **The consent** pursuant to art. 2(g) of the Directive shall mean freely given specific and informed indication of wishes of data subject which signifies his agreement to processing of his personal data.[77]

Second legitimate basis for the processing is a **contractual relationship** between the controller and data subject. This provision also applies to pre-contractual relationships, where the data subject intends to enter into a contract, but some formalities are to be complied with.

The 3rd criterion for legitimate processing is the **compliance with the legal obligation** to which the controller is subject. The provision refers to controllers in private sphere, whereas the legal obligations of controllers in public sphere falls under Article 7(e) of the Directive. A notable example of compliance with the legal obligation by the controller is the processing of personal data of the employees by the employers due to legal obligations in sphere of social security and taxation.

EU Law explicitly mentions another criterion for legitimate processing of data, namely, if the processing is necessary in order to protect the **vital interests of the data subjects.** Such interests are mainly relating to the well-being of a data subject in a physical sense. Such interests could be a legitimate legal basis for processing of health data if the data subject is not able to give his consent.

Article 7(e) of the Directive provides that the data may be lawfully processed if it "is necessary fir the **performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller or in a party to whom the data are discloses". An example of the processing on this ground can be the processing of personal data by Migration and Refugee offices, processing of data by tax authorities and etc.

The last ground for processing of personal data is **legitimate interests of the controller or of the third party**. Data subject is not the only person with legitimate

[76] Cases C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado [2011] ECR 2011 I-12181.
[77] See Chapter 2.2.3.1.

interests. However, his data can be processed only if his interests for fundamental rights and freedoms are overridden by the legitimate interests of controller or third parties. Therefore, the balancing of clashing interests is to be conducted.

Rules on lawful processing of sensitive data.

Article 8 of the Data Protection Directive lays down the detailed regime for processing the data which reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships and data related to health and sex life of a person. In principle, the processing of such data is prohibited, unless there is an exemption enumerated in para. 2 of the Article. In contrast to processing of non-sensitive data, a contractual relationship is not a basis for processing of sensitive data.

The first exemption for lawful processing of sensitive data is **explicit consent** of the data subject. Unlike the consent required for processing of non-sensitive data, this consent cannot be implied from the circumstances. Therefore, the explicit consent of the data subject is essential.

As in the case of non-sensitive data, **vital interests** of the data subject or of another person can be a ground for lawful processing. This infers the cases where the data subjects are legally or physically incapable of giving consent.

Legal obligations of the controller in field of employment law could be a legal ground for processing the sensitive data, where for instance, the employer is legally obliged to specify the number of disabled persons working for him.

The processing could also be carried out in course of its legitimate activities by foundations, associations or any other body with a **political, philosophical, religious or trade-union aims.**

Legitimate interests of others could also serve as a ground for processing of sensitive data. This could be the case there sensitive data are used in the context of legal proceedings before a court or administrative authority for the establishment, exercise or defence of a legal claim.

Further exceptions allowing the processing of sensitive data are contained in the remainder of Article 8 para. 3, which allows the processing of personal data for the purposes of preventive medicine, diagnosis, the provision of care or treatment or the management of health care services. Member States could lay down additional

exemptions from the prohibition, on grounds of substantial public interest. These grounds could be scientific research and government statistics.[78] Article 8(5) permits processing of personal data relating offences, criminal convictions or security measures under the control of the official authority. However, this category is not mentioned in the definition of sensitive data pursuant to Article 8 para. 1 of the Directive.

Security of the data processing.

The principle of security of processing implies the legal obligation of the controller and the processor in regard to implementation of appropriate technical and organizational measures to protect personal data against unlawful acts of processing and abuse. A similar provision could also be found in CoE 108.[79] The due regard has to be given to the state of art and security features available in the market, the costs of implementation and nature of the data in question. The security of the processing could be achieved by utilization of industrial, national or international standards, for instance, The European Privacy Seal, for safe processing of data. Data security also requires adequate internal organizational rules, which would provide the employees under the authority of the controller and processor with proper information about the security of processing, confidentiality and their respective obligations.

Under EU law, the secure processing of data is guaranteed by the obligation of processor, controller and any person acting under the authority of aforementioned, to keep the data confidential.[80]

Transparency of the processing.

The transparency of processing is closely related with principle of fair processing of data, which implies that the data subject has to be informed about the processing before it commences. This obligation must be complied with proactively by the controller, regardless of the interest of the data subject.[81] Such information includes the identity of the controller, the purposes of the processing, the recipients of data and rights of the data subject. In cases where the data is not obtained from the data subject, the controller has

[78] Data Protection Directive, recital 34.
[79] Convention 108, art 7.
[80] Data Protection Directive, art 16.
[81] *Handbook on European data protection law* (n 53) 96.

to provide the information about the categories of the data and right to access and rectify the data concerning data subject. In regard to time of providing information, in case where the data is collected from data subject, information has to be provided, at the latest, at the time of collection. Where the data is collected from third parties, the information has to be provided at the latest, before the data are disclosed to a third party.

The controller is exempted from the obligation to inform a data subject, where the processing of data carries out historical, scientific or statistical purpose. Such an obligation would prove impossible or involve a disproportionate effort.

Nevertheless, exemptions and restrictions from the transparency obligation of the controller can be laid down, where such exemption or restriction constitutes a necessary measure to safeguard certain public interests(national security, defence, public security) or private interests(rights of the data subject freedom of others) on the condition that these restrictions are proportionate.

Rules on promoting compliance.

Notification.

National law can oblige the controllers to notify the competent supervisory authority about their processing operations before carrying out those operations. The notification shall include at least the information about the controller, the purpose of processing, the categories of data, recipients, intended third country transfers and general description of security measures. The competent supervisory authority registers all the processing operations and holds a register in accordance with article 21 of the Directive, unless the Member States lay down an exemption on one of the grounds of article 13.

Member States may provide for simplification or exemption from notification where the processing operations are unlikely to adversely affect the rights and freedoms of the data subject which are stated in article 18(2) of the Directive or where the controller appoints a data protection official.

Prior checking

According to Article 20 of the Directive, the supervisory authority must check processing operations which are likely to present specific risks to the rights and freedoms

of the data subjects- before they begin. It is for national to determine which operations qualify for prior checking. For instance, if a company intends to conduct processing operations, which are subject to prior checking, this company cannot start processing before receiving a positive response from the supervisory authority.

Data Protection Official

Data Protection Directive creates the possibility of appointing an official who acts as a data protection official. The rationale behind the appointment is the simplification of the notification obligation of the controllers and minimizing the risks of adversely affecting the rights and freedoms of data subjects.[82] In order to achieve this aim, the independency of the data protection officer has to be ensured.

Codes of Conduct

To encourage compliance, business and other sectors may draw up codes of conduct, which contain the best practices- detailed rules of processing data. These codes of conduct are intended to contribute to the proper implementation of laws of Member States, which are adopted pursuant to the Directive. In accordance with article 27 of DPD, Member States may establish a procedure of evaluation of these codes, where trade associations or other bodies representing other categories of controllers are able to submit their opinion. Such codes are also subject for evaluation by Working Party referred in Article 29. After the approval of Working Party, such codes of conduct can be published.

2.2.3.4 The data subject's right and their enforcement

Under the Data Protection Directive, the data subjects are granted several rights in regard to processing of their data.

The first right under Article 12 of the Directive is the **right to access**, which implies the right to obtain from processor information regarding processing. Such information should at least include: the confirmation about the processing of his data, the categories of the data concerned, the purposes of processing and recipients of the data.

[82] Data Protection Directive, art 18(2)

Data subject has a right to get the data undergoing the processing operations in an intelligible form. This is an essential right, as the data subject is able to determine whether the data undergoing processing is accurate and complete. In case the data are incomplete or inaccurate, they shall also have their data **rectified**. The controller may demand the proof of alleged inaccuracy. However, this demand may not place an unreasonable burden on the data subject. Where automated evaluations referred in Article 15 are performed, the general logic and algorithm of the evaluation have to be explained to the data subject.

The data subject has a right to request to delete or erase the information about him, where there is no legitimate basis for the processing of data, or where he has withdrawn his consent. The burden of proof of legitimacy lies within the controller, who is responsible to show the legitimacy of the processing at any time. Additionally, the data subject is legally empowered to obtain from the controller the notification to third parties of any blocking, erasure or rectification, where the data was received prior to processing operations.

However, the right of access of the data subject can be restricted as a result of overriding public interest or interest of a 3rd party.[83] Subject to adequate legal safeguards, this right can be restricted if the data is processed solely for the purpose of scientific research or statistics.

There is no general right of the data subject to object to the processing of their data. [84]Data subject shall have the **right to object** to the processing of his data, only in limited circumstances: where the processing is necessary for the performance of the task carried out in the public interest, or where processing is necessary for purposes of legitimate interests of controllers or third parties; right to object to processing of his data for the purposes of direct marketing and to object to the disclosure of their data to 3rd parties; and right to object to automated individual decision-making. Where the objection of the data subject is justified, the processing or transfer of the data has to be stopped.

Automated decisions are decisions which are taken solely by automated means. These decisions have a considerable impact on the data subjects and can relate to his performance at the workplace, reliability, creditworthiness. Therefore, this decisions need a careful legal protection and safeguards. Data Protection Directive provides that no

[83] Data Protection Directive, art 13.
[84] *Handbook on European data protection law* (n 53) 113.

individual shall be subject to such decisions, where those decisions significantly affect him.

2.2.3.5.Transfer of personal data to 3rd countries

The principal aim and objective of the Directive is the freedom of movement of personal data throughout the Community. The area of free flow of data is also extended to the European Economic Area, which covers Norway, Liechtenstein and Iceland. However, transfer of personal data to a recipient who is outside the Community and subject to a foreign jurisdiction may pose serious threats to the right to privacy, where those states do not have adequate level of protection of data. Another problem encountered is that some data users store and process the data outside the Community to take the advantage of lax data protection laws.[85] Therefore, the legal regulation of trans-border flaws of data is essential.

Article 25(1) states the main principle of transfer of data to third countries: the adequacy of protection. The directive uses the term adequacy rather than equivalency. In other words, the transfer of personal data which are undergoing processing or are intended to be processed after the transfer, shall be allowed if the third country in question offers adequate level of protection. Factors to be taken into account in the evaluation of adequacy are the circumstances of data transfer, the nature of the data, the purpose and duration of processing, the general and sectoral rules in place in third country and etc. This provision is nevertheless not absolute and can be derogated from. Pursuant to article 26, the transfer may take place if :

a. The data subject has given its consent
b. It is necessary for the performance of the contract or pre-contractual measures
c. It is legally required on the ground of public interest
d. It is necessary for establishment, exercise or defence of a legal claim
e. It is necessary to protect vital interests of the data subject
f. The information is already available in the public or public registry

The controller implements adequate safeguards with respect to protection of privacy and fundamental rights of individuals. Such safeguards may result from adducing

[85] Bainbridge and Platten (n 16) 70.

additional contractual clauses. In accordance with the procedure laid down in Article 31(2), the Commission developed the standard contractual clauses which offer adequate safeguards. These clauses were officially certified by a Commission decision as a proof of adequate protection.

The Commission issues adequacy decisions pursuant to Article 31, where it considers that a third country does ensure an adequate level of protection, by reason of its domestic law or of the international commitments it entered to. The decision of the Commission is binding and all Member States and states of EEA have to follow the decision, meaning that the data can be transferred to those states without any checking procedure by the national authorities. If the Commission finds out that a third country does not offer an adequate level of protection, it shall inform the Member State and the latter in turn, has to take measures necessary to prevent any transfer of data to the third country in question. However, this is not an absolute prohibition. In any case, the derogations in Article 26 are available.

2.2.3.6.Enforcement, legal remedies and sanctions.

Enforcement.

The effectiveness of any legal rule is dependent on the existence of effective mechanism for implementation and realization. Under DPD, data subjects are legally empowered to protect their rights.

The first facet of effective data protection is the establishment of independent supervisory authorities under national law, which are responsible for monitoring and promoting the compliance with data protection laws, handling the complaints of data subjects, supervising controllers and processors and intervening if is necessary. The authority has to be completely independent, which lies within its specific organizational structure. The CJEU referring to them as "guardians" of rights relating to data processing, stressed that these authorities have to remain free from any external influence and do not have to seek or take instructions from anybody".[86] Acting objectively and impartially, the authorities have the power to investigate processing authorities, order the rectification,

[86] Case C-518/07 European Commission v Federal Republic of Germany [2010] ECR 2010 I-01885, para 27.

blocking, erasure or destruction of the data and impose a temporary ban on processing of data.

Legal remedies.

For effective enforcement, the right to an **effective remedy**, which is guaranteed under the ECHR, has to be available to every person. This right requires that judicial remedies against infringements of data protection rights are available under national law. Before turning to the court, the data subjects have to approach the controller. The entity which was addressed as a controller has to respond without excessive delay. It is for the Member States to prescribe the period for response.

Where a person doesn't get a satisfactory answer from the data controller, he can lodge a claim with the supervisory authority. The data subject must be informed by the supervisory authority about the outcome of the proceeding.

Against the decisions of the national supervisory authority, the data subjects have the right to appeal. It is left for the Member States to regulate whether it is mandatory to approach the national supervisory authority before turning to the court.[87] The data subjects may bring their cases to CJEU if a regulatory act of EU directly infringes upon the right to data protection of individual[88] or through the procedure of preliminary ruling under article 267 of TFEU, where they ask the national court to refer the questions for clarification by CJEU.

Sanctions.

Under EU Law, Member States shall lay down the sanctions for the infringement of the provisions of the Directive.[89] The Directive however does not specify the specific sanctions and therefore leaves a margin of appreciation for Member States. CJEU has repeatedly stressed out that the Member States are not completely free to determine sanctions: In order to achieve the true and effective protection, legal remedies must trigger penal and/or compensatory procedures leading to sanctions with a deterrent effect.[90]

[87] Data Protection Directive, art 22.
[88] Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C326/47 (TFEU), art 263(4).
[89] Data Protection Directive, art. 24
[90] *Handbook on European data protection law* (n 53) 127.

2.3. Processing of data by Community institutions

Community institutions are obliged to apply the data protection acts with regard to processing of data.[91] In order to ensure effective compliance with the rules governing the protection of fundamental rights and freedoms of individuals and the free flow of personal between Member States and the Community Institutions or between Community bodies,[92] the adoption of Regulation No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data(Community institutions Regulation) was necessary. Community institutions shall mean institutions and bodies set up by, or on the basis of, the Treaties Establishing European Communities.[93]

The Regulation shall apply to the processing of personal data by all Community institutions and bodies, where the processing is carried out within the scope of Community Law. Similar to DPD, the processing operations which fall under Titles V and VI of TEU, shall be governed by rules adopted on the basis of article 255 of TEU.[94]

The Regulation envisages the creation of independent supervisory authority referred to as the European Data Protection Supervisor, who is responsible for monitoring and ensuring the application of the Regulation and other acts relating to data protection.[95] As in DPD, the operations which are likely to pose a specific risk to data subjects shall be subject to prior checking by the EDPS.[96] EDPS shall be endowed with effective investigative and intervention powers: he shall hear and investigate the complaints, conduct inquiries, monitor the application and compliance, where necessary, advise the Community institutions.[97] The interventive powers of EDPS shall include the power to warn and admonish the controller, order the rectification, blocking and erasure of data, imposing a temporary or definitive ban on processing and refer the matter to CJEU.[98]

[91] Consolidated Version of the Treaty on European Union [2008] OJ C115/13 (TEU), art 286
[92] Community Institutions Regulation , recital 13.
[93] Community Institutions Regulation , art 1(1)
[94] Community Institutions Regulation , recital 15
[95] Community Institutions Regulation art 41(2).
[96] Community Institutions Regulation, art 27.
[97] Community Institutions Regulation, art 46.
[98] Community Institutions Regulation, art 67.

The definitions, principles and rules of processing of personal data are mainly the same with those of DPD. The principles such as lawful and fair processing, principle of purpose specification and limitation, principle of data relevancy and adequacy, principle of data quality and principle of limited retention of data are reiterated in the Regulation. The grounds for lawful processing of data which are listed in article 5 of the Regulation are same to those of DPD. The Regulation imposes obligations on controller to ensure the confidentiality and security of processing. Unlike DPD, the appointment of Data Protection Officer is obligatory for each Community institution. As in DPD, the DPO shall be responsible for keeping a register of processing operations. Before any processing operation commences, the controller shall a give a prior notice to the DPO.

The rules for transfer of data are dealt with in article 9 of the Regulation. The main approach here is the adequacy approach, where the data could be transferred to recipients other than the Community institutions and bodies which provide an adequate level of protection of personal data. However, derogations are available in article 9 para. 6 and 7.

The scope of the rights of the data subjects are similar to those provided under DPD. The data subject has the right of access, rectification, blocking, erasure and object, the scope of which are the same as of DPD. Nevertheless, the Regulation provides for some exceptions and derogations. For instance, the data could be processed for other purpose where the change is permitted by the internal rules of Community institution or for purpose of prevention, investigation, detection and prosecution of serious criminal offences.[99] In addition, the Community institutions and bodies may restrict some rights and derogate from obligations, for example, from right to access or the obligation to provide information where it is a necessary measure to fight the criminal offences, to protect the data subject or rights and freedoms of others.[100]

The full and comprehensive protection of personal data requires not only the endowment with specific rights and freedoms, but also adequate remedies for breaches of those rights. The data subject could file a complaint with the EDPS if his rights have been infringed as a result of processing operations. This would however, be without prejudice to the right to apply to the CJEU, whenever their rights under the regulation are deemed to be violated. The decisions of EDPS shall also be brought before CJEU.[101]

[99] Community Institutions Regulation, art 6.
[100] Community Institutions Regulation, art 20.
[101] Community Institutions Regulation, art 32.

2.4. Other data protection instruments.

One of the fundamental objectives of the EU is maintaining and developing the Union as an area of freedom, justice and security. Common action in the field of police cooperation and judicial matters cooperation under Article 30(1) of the TFEU imply the processing of information, which also contains personal data. Since neither DPD, not Community Institutions Regulation apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, as those provided by Title VI of the TEU, clear and precise rules creating mutual trust between the national competent authorities, as well protection of personal data in regard processing of data in police and judicial cooperation has to be ensured. At EU Level, the cross-border police and judicial cooperation in criminal matters is regulated by Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters(Framework Decision). In addition, there are also specific data protection regimes for Europol, Eurojust, as well as EU-level cross-border information exchange systems between the competent authorities, such as Schengen II, the Visa Information System, Eurodac, Eurosur.

2.4.1. Data Protection Framework decision

The main purpose of this Framework Decision is to ensure the protection of fundamental rights and freedoms of natural persons, in particular their right to privacy, with regard to the processing of personal data in the framework of police and judicial cooperation in criminal matters, while guaranteeing a high level of public safety.[102]

Scope.

This Directive concerns the protection of personal data in the framework of police and judicial cooperation in criminal matters, where personal data are made available between the competent authorities within the meaning of article 2(h) of the Framework Decision. These competent authorities are Competent authorities of Member States and EU working in the area of police and criminal justice. The scope in regard to type of data

[102] Council Framework Decision, recital 3.

and processing is same with DPD: the Framework Decision shall apply to processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means, of personal data intended to form a filing system. However, the scope of the Framework Decision is limited to cross-border cooperation between the competent authorities and is without prejudice to matters of national security.[103]

Main rules and principles of processing.

The Framework Decision relies largely on the rules, principles and definitions which are enshrined in the DPD. Similar to DPD, article 3 of the Framework decision provides that personal data may be collected by the competent authorities for specified, explicit and legitimate purposes. The data could only be processed for the same purpose for which it was collected, or for the further purpose which is not incompatible with the previous one. However, unlike DPD, data could be further processed for other purpose where the processing is necessary and proportionate to the other purpose. Nonetheless, these purposes have to relate to prevention, investigation, detection or prosecution of criminal offences, or execution of criminal penalties other than those for which they were transmitted, other judicial and administrative proceedings directly related to prevention investigation, detection or prosecution of criminal offences or the execution of criminal offences, the prevention of an immediate and serious threat to public security.[104]

Similar to DPD, the Framework Decision contains fundamental principles of data protection such as principle of data quality, where the personal data has to be kept accurate, complete and up-to date[105] and the principle of limited retention of data, where personal data has to erased when it is no longer necessary.[106] Principle of fair processing also requires Member States to inform the data subject about the collection or processing of his personal data, although this rule is subject to exceptions.[107]

Several safeguards were introduced in order to enhance the protection of right to privacy of data subjects, in particular, the specific duty of the competent authorities to log and document all the transmissions of the data,[108] the obligation to take necessary security

[103] Council Framework Decision, art 1(4).
[104] Council Framework Decision, art 11.
[105] Council Framework Decision, art 4.
[106] Council Framework Decision, art 5.
[107] Council Framework Decision, art 16.
[108] Council Framework Decision, art 10.

measures against unlawful forms of processing[109], the obligation of confidentiality in processing,[110] processing of special categories of data only when it is strictly necessary with due regard to adequate safeguards[111], the obligation of receiving authority to comply with the restrictions provided under national law of transmitting authority[112]. Member States shall also ensure that the national supervisory authorities are consulted prior to the processing of personal data, where the processing involves special categories of data or poses specific risks to the rights and freedoms of the data subject.[113] One of the most important safeguards for protection of rights of data subject is the establishment of national supervisory authorities with complete independence. These authorities shall be endowed with investigative, intervention powers and the right to bring the infringements to the court. The authority shall act as an administrative remedy and hear the claims lodged by any person whose rights and freedoms are concerned.[114]

Onward transfer of data to third States or to international body is possible only if it necessary for prevention, investigation, detection or prosecution of criminal offences, where the receiving authority is responsible for those tasks, on a condition that the Member State from which the data originated has given its consent and where the third state or international body ensures adequate level of protection for the processing.[115] Nonetheless, some exemptions are available in urgent cases, where it is necessary for prevention of an immediate and serious threat to public security, or where the transfer is necessary for legitimate interest of data subject or on important public grounds. [116]

The data subject is entitled to several rights under the Framework Decision, such as right to obtain information about the processing of his personal data, right to rectification, erasure or blocking of his data.[117] However, these rights can be limited on compelling grounds. Yet, the data subject has a right to appeal to competent national supervisory authority or judicial bodies, for any breach of his rights under the Framework

[109] Council Framework Decision, art 22.
[110] Council Framework Decision, art 21.
[111] Council Framework Decision, art 6.
[112] Council Framework Decision, art 12.
[113] Council Framework Decision, art 23.
[114] Council Framework Decision, art 25.
[115] Council Framework Decision, art 13.
[116] Council Framework Decision, art 13(2),(3).
[117] Council Framework Decision, art 17.

Decision.[118] The data subjects are entitled to compensation as a result of unlawful processing operations or any other act.[119]

2.4.2. The Prüm Decision.

The Prüm Convention is a treaty which was signed on 27 May 2005 by Austria, Belgium, France, Germany, Luxembourg, the Netherlands and Spain in the town of Prüm in Germany, and which is open to all members of the European Union, 14 of which are currently parties. Core elements of the convention were picked up by EU Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, which incorporated the Prüm decision in EU Law[120]. The main objective of the Prüm decision is to improve information sharing for the purpose of preventing and combating crime in fields of terrorism, cross-border crime and illegal immigration.[121] To this end, the Prüm decision envisages the automated access and exchange of information between member states in regard to DNA profiles, fingerprint data and certain national vehicle registration data, the supply of data in relation to major events with cross-border dimension, the supply of information to prevent terrorist offences and other measures for stepping-up cross-border cooperation.[122] Such a supply of personal data in context of exchange of information in framework of preventing and combating crimes shall be subject to a legal protection at least equal to the CoE 108 Convention. Prüm Decision also contains some safeguards and principles common to data protection laws, such as principle of purpose limitation[123], principle of quality of data, principle of limited retention of a data[124], the security and protection of personal data,[125] the obligation of logging and recording of supply by the relevant authorities[126] and etc.

---

[118] Council Framework Decision, art 17(3).
[119] Council Framework Decision, art 19.
[120] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime [2008] OJ L210/1 (Prüm Decision).
[121] Prüm Decision, recital 1
[122] Prüm Decision, art 1.
[123] Prüm Decision, art 26.
[124] Prüm Decision, art 28.
[125] Prüm Decision, art 29.
[126] Prüm Decision, art 30.

2.4.3. Europol.

The present status of Europol as an EU institution is regulated by the Council Decision of 6 April 2009 establishing the European Police(Europol Decision). Pursuant to Annex of the Europol Decision, the objective of Europol is to deal with serious crimes. In so far as it is necessary for the achievement of its objectives, Europol shall process information and intelligence, including personal data. Europol shall establish and maintain the Europol Information System, which is a database for Member States to exchange information. The Data may be retrieved by Europol where that is necessary for the performance of its tasks in a particular case.[127] Similar to Prüm Decision, the Europol Decision also contains safeguards and established the general principles, such as principle of purpose limitation[128], principle of limited retention of data[129],principle of data quality[130] general rules for transfer of data to third States[131], security measures[132] and etc. In general, article 27 states that Europol shall take account of the principles of the Convention 108 and shall observe those principles in the processing of personal data, inter alia, in respect of automated and non-automated data. In order to promote compliance with the data protection norms, the independent supervisory authority called Europol Joint Supervisory body is established.[133] The data subjects are also endowed with rights like right to access, right to his data to be rectified or erased, right to complain to JSB and competent court of the Member State.

2.4.4. Eurojust.

Eurojust is an EU body promoting the judicial cooperation in investigations and prosecution of serious crimes concerning at least two Member States. It shall enhance the coordination and cooperation in investigations and prosecution between the competent authorities of Member States. The processing of personal data within the context of

[127] Council Decision of 6 April 2009 establishing the European Police [2009] OJ 2009/371/JHA (Europol Decision), art 13.
[128] Europol Decision, art 19(1).
[129] Europol Decision, art 20.
[130] Europol Decision, art 31.
[131] Europol Decision, art 23.
[132] Europol Decision, ch 5.
[133] Europol Decision, art 34.

activities of Eurojust is governed by Rules of procedure on the processing and protection of personal data at Eurojust approved by the Council on 24 February 2005. The Rules lay down safeguards for processing of personal data. Eurojust can only process personal data in so far as it is necessary to achieve the legitimate objectives. Such information is limited to personal data of persons who are suspected of committing a crime, witnesses or victims of crimes. Where the data are relevant to investigation, Eurojust may also process more extensive personal data relating to the circumstances of crime. Like Europol, Eurojust has to also ensure a level of protection at least equivalent to Coe Convention 108. The Rules also provide specific rules in regard data flows to third States and organizations.[134]

2.4.5. Joint Information Systems

In addition to Europol and Eurojust, some other joint information platforms were established. These joint information systems pursue legitimate objectives like immigration, asylum and customs law. These systems are Schengen information system, Visa Information System, Eurodac, Eurosur and Customs Information System. The Schengen Information system which came into operation on 9 April 2013 has incorporated the CoE 108 Convention, where the personal data has to be processed in accordance with the Council of Europe Convention 108.[135] **The Visa Information System** was created to support the implementation of common EU visa policy. The system contains data on applicants, his photographs, dactiloscopic data, and application files of person accompanying him.[136] The system envisages the exchange of data between Member States. Access to the data is limited solely for the visa authorities of Member States for immigration purposes. The data can nevertheless be transmitted to national competent authorities and Europol for the purpose of preventing, detecting and investigating terrorist and other criminal offences.[137]

[134] Rules of Procedure No 2005/C 68/01 of 24 February 2005 on the Processing and Protection of Personal Data at Eurojust approved by the Council, OJ [2005] C 68/01 (Eurojust rules).
[135] Council Decision No 2007/533/JHA of 22 June 2007 on the establishment, use and operation of second generation Schengen Information System(SIS) [2007] OJ L205 (Schengen II Decision), art 57.
[136] Council Decision No 2007/533/JHA of 8 June 2004 establishing the Visa Information System(SIS) [2004] OJ L213 (Visa Decision), art 5.
[137] Council Decision No 2008/633/JHA of June 23 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of

Eurodac is a centralized database containing the fingerprints of third-state nationals applying for asylum in one of EU Member States. The Council Regulation (EC) No. 343/2003, also referred as Dublin II Regulation establishes the requirements for examining asylum application of third-state nationals. The personal data contained in Eurodac may be used only in order to enhance the application of abovementioned regulation. The protection of data in Eurodac is regulated by Council Regulation (EC) concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention.[138] The Eurodac Regulation contains some safeguards for the protection of personal data, such as rules regarding storage, transmission and erasure of data, the general security measures, the pseudonymizing of data when it is stored. The data can be stored up to 10 years after they are collected, unless the data subject obtains citizenship, residence permit or leaves EU, where the data has to be immediately erased.

One of the joint information platforms at EU level is the **Customs Information System.** The system contains personal data with regard to goods, means of transport, business and cash. The Customs Information System Decision provides that the data can only be used for facilitating of customs policy and carrying out measures for finding the persons who violated the customs provisions.[139] The processing has to comply with CIS Regulation, as well as DPD, EU Institutions Data Protection Regulation, CoE Convention 108 and Police Recommendation.

---

the prevention, detection and investigation of terrorist offences and of other serious criminal offences, [2008] OJ L218.

[138] Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention [2000] OJ L316 (Eurodac regulation).

[139] Council Decision No 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes [2009] OJ L323 (CIS Decision).

CHAPTER III. DATA PROTECTION IN AZERBAIJAN

3.1. General background

Human rights are one of the most important values in Azerbaijan. The legal value of a person is based on human rights. The Constitution of Azerbaijan Republic defines human rights as the "ultimate value" and proclaims the protection of human rights and fundamental freedoms as the core purpose of the State. In accordance with article 12 of Constitution, the protection of human rights and fundamental freedoms, as well as ensuring the proper living conditions of its citizens is the ultimate goal of the state.[140]. The rights and freedoms conferred within the Constitution are applied in a manner consistent with the international instruments which Azerbaijan is a party to.

The regulation of human rights and freedoms is one of the important political-legal policies in a modern secular state. No provision of Constitution can be interpreted in a manner which would prejudice the realization of human rights and freedoms, nor would be construed to abolish those rights.[141] The rights and freedoms are protected and guaranteed as core of a legal system.[142] .

The right to private or family life is protected on the level of constitutional right in Azerbaijan. Pursuant to article 32 of Constitution, everyone has the right to personal inviolability. It involves the right to keep their family life, their correspondence, telephone conversations and information transmitted by mail, telegraph or other means of communication secret or private. Everyone has a right to protection against unlawful interference with his or her private or family life. Except in cases specified by law, interference with a person's private or family life is prohibited. It is prohibited to gather, store, use or disseminate information about a person's private life without his or her consent. No one shall be followed, filmed, photographed, recorded, or subjected to any other similar actions without his or her knowledge or despite his or her disapproval, except when such actions are prescribed by law. Everyone may become familiar with the materials collected in regards to him or her save in cases prescribed by law. Everyone has a right to demand rectification or deletion of the information collected in regards to him

[140] Azərbaycan Respublikasının Konstitusiyası. Bakı: Biznes xəbərləri, 2012.
[141] Cəfərov İM. Azərbaycan Respublikası Konstitusiyasının Şərhi. Bakı: Hüquq ədəbiyyatı, 2003, s180.
[142] Əsgərov ZA. Konstitusiya hüququ: Dərslik. Bakı: Bakı Universiteti nəşriyyatı, 2006, s102.

or her, which does not correspond to the truth or is incomplete or collected through violation of the provisions of law.

Azerbaijan Republic signed and ratified the Convention 108 of the Council of Europe on 03.05.2010. The Convention entered into force in Azerbaijan on 01.09.2010.[143] As an implementation of Convention 108 into national law of AR, the Law on Personal Data of Azerbaijan Republic was signed on 11.05.2010 and entered into force on 06.06.2010 as of publication. The Convention 108 covers all fields of processing of personal data, including the processing operations in fields of police and criminal justice. However, by Declaration contained in the instrument of ratification deposited on 3 May 2010, AR declared that provisions of the Convention will not be applied to the categories of personal data files, which are subject to State secret.[144] International agreements, to which Azerbaijan is a party to, are parts of legislative system of AR.[145] If there is a contradiction between the Laws of AR and international agreements which are parts of legislative system of AR, the international agreements shall apply.[146] This implies that the international agreements to which AR is a party to, in particular Convention 108 shall have a superior force in comparison to Law of AR on Personal Data and shall apply whenever there is a contradiction.

Azerbaijan Republic is also a party to The CoE Convention on Cybercrime, which is also known as Budapest Convention on Cybercrime. Azerbaijan has ratified this Convention on 15.03.2010. The Convention is the most influential international treaty dealing with breaches of law over the internet or other information networks.[147] In principle, the Convention is not an instrument for data protection, but rather criminalizes some acts in internet network which often come to a collision with a right to private and family life. In accordance with article 15.1 of the Convention, the Contracting Parties have to foresee adequate protection of human rights and liberties, in particular the right to data protection.

As the Constitution stipulates, there shall be no interference with right to privacy except the cases specified by law. One of the examples of interference of right to privacy

[143] Full list, 'Full List' (*Treaty Office*, 2017) <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=B7TntMsT> accessed 23 June 2017.
[144] Ibid.
[145] Azərbaycan Respublikasının Konstitusiyası, m 148.3.
[146] Azərbaycan Respublikasının Konstitusiyası, m 151.
[147] *Handbook on European data protection law* (n 53) 148.

is the medical secrecy. The information constituting the medical secrecy is regulated by law of AR on "Protection of health of population". Pursuant to article 53 of that law, the application of a person for medical help, his diagnosis, his treatment and the information disclosed during his treatment constitute the medical secrecy. The information constituting medical secrecy can be handed to 3rd parties in cases the citizen or his/her legal representative give their consent thereto, whereas this information is essential for the purpose of treatment of the patient, for conducting researches and study or pedagogic purposes. The information constituting medical secrecy can be handed to 3rd party without the consent of the patient in cases:

- The patient is not able to give his consent; whereas it is essential for the treatment and diagnosis of the patient;
- If there is threat of dissemination of infectious diseases;
- By the request of investigative, inquiry or prosecution organs or by request of the court;
- The information relating to a person who has not reached the aged of puberty can be handed to his parents or his legal representatives.

The persons possessing the information which is under medical secrecy, are responsible for the damages suffered by the patient as a result of dissemination of such information.

In the commercial sphere, the derogations from protection of personal information are also envisaged in law. The protection of such information is foreseen in Civil Code of AR, in Taxation Code of AR, on Law of AR on Banks and banking activity and etc. In accordance with article 967 para.2 of the Civil Code, the personal data of the customers can be transmitted to other state bodies and organs in cases explicitly stipulated by law. Pursuant to article 76 para 3. of the Taxation Code, the data regarding bank accounts and transactions can be transmitted to other relevant executive organs where it is envisaged by a legal act. Otherwise, the transmission of information to other state organs or citizens is prohibited.

One of the reasons of limitation of right to private and family life is the state security. The limitation of those rights are regulated by the law on State Secret, law on Fighting the Terrorism, law on Operational-Search Activity and etc. The states have large

margin of appreciation in limiting the right to privacy for the purpose of public and state security. [148]

Summing above mentioned, it could be said that the limitation of the right to private and family life in Azerbaijan is based on the same criteria held by CJEU and ECHR:

- The limitation has to be based on law;
- The limitation has to pursue a legitimate aim;
- The limitation has to be necessary and proportionate in a democratic society.

These criteria are to be read in cumulation. The absence of one of the criteria would subsequently be evaluated as a violation of right to private and family life prescribed in Article 32 of the Constitution.[149]

3.2.Law on personal data.

3.2.1. Aim of the Law

Law on Personal data("Law" hereinafter) regulates the collection, processing and protection of personal data, the trans-border flows of data, as well as the rights and obligation of state bodies, legal entities and natural persons in this sphere. The main objective of this Law is reflected in article 1, where it is stated that the main aim of this Law is the establishment of general principles and legitimate basis for the collection, processing and protection of personal data, the regulation of transfer of data, the legal obligations and rights of physical and legal entities in this sphere. The law explicitly mentions the protection of main rights and freedoms of people, in particular, the right to private and family life.

3.2.2. Scope of the Law

[148] Əsgərov ZA. Konstitusiya hüququ: Dərslik. Bakı: Bakı Universiteti nəşriyyatı, 2006, s34.
[149] Ibid .

The Law regulates the collection, processing and protection of personal data within the meaning of article 2.1.1. of the Law. Accordingly, the personal data is any kind of information which enables the direct and indirect identification of a natural person. Article 2.1.2. defines the data subject is a natural person to whom the personal data is related. Apparently, the law does not concern the data of legal entities and its regulatory scope is limited to natural persons. The question arising here is whether a dead person is considered as a data subject. The definition does not mention whether the data related to a dead person is covered under the definition of personal data. Nevertheless, Article 8.3 stipulates that in case the data subject has died, is missing or declared dead by the decision of a court, the consent for processing of his data shall be given by his heirs, parents or legal representatives. Based on the fact that a dead person was referred to as a data subject and his/her personal data could be processed on the same grounds applicable to other personal data, it could be concluded that the notion of personal data also covers the data related to a dead person.

In regards to scope of processing, the processing and accumulation of personal data in sphere of intelligence, operational-search activity, the processing of data classified as state secret and data accumulated in National Archive of Azerbaijan Republic is explicitly excluded from the scope of the Law and is regulated by relevant legislation of AR.[150]

Similar to DPD and GDPR, the Law also excludes the processing of personal data by natural persons purely for household purposes[151], which is known as household exception.

The Law is totally silent on issue of type of processing. It does not mention to what kind of processing it relates, whether the processing is performed by automatic or manual means. The definition referred to processing of personal data in article 2.1.8 of the Law merely enumerates the operations covered under the term of processing and does not specify whether those operations are performed by automated or manual means. However, declaration contained in the instrument of ratification of Convention 108

[150] Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanunu. Bakı şəhəri, 11 may 2010-cu il № 998-IIIQ, m 3.2

[151] Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanunu, m 3.3.

deposited on 3 May 2010 declares that provisions of the Convention will be applied to personal data files which are not processed automatically.[152]

3.2.3. Main legal issues

3.2.3.1 Main definitions

Personal Data. Under the law, the personal data is any kind of information which enables the direct and indirect identification of a natural person. Pursuant to article 2.2 of the Law, the notion of information is to be understood within the meaning of relevant Laws of the AR. In accordance with article 2 of the Law on Information of AR, information means any fact, opinion, knowledge, news or data of other character, regardless of the data of creation, classification and form of presentation. From this definition, it could be understood that information could be both objective(fact) and subjective(opinion). The law does not define what does direct or indirect identification of a person mean. The law affords protection only to natural persons, therefore the information related to legal entities is in principle not covered by the Law.

Special categories of personal data. The article 2.1.6. of the Law, enumerates the special categories of personal data. The processing of these categories of data are subject to more stricter rules. The categories are:

- Personal data relating to racial or ethnic origin,
- Personal data relating to religion and beliefs,
- Personal data concerning family life,
- Personal data relating to health,
- Personal data relating to criminal convictions.

EU and Azerbaijan have established different legal scopes of special categories of data. The legislation of Azerbaijan does not afford special protection to categories of data relating to political opinions and trade-union memberships. The Law does not explicitly mention the data relating to sex life in contrast to EU. However, the family life covers, inter alia, the information concerning sex life, about civil status(marriage, divorce),

[152] (2017) <http://www.coe.int/en/web/conventions/full-list/ /conventions/treaty/108/declarations?p_auth=B7TntMsT> accessed 23 June 2017.

information regarding adoption of a child.[153] EU law does not afford a special protection to data relating to family life as a whole, but rather treats it as a normal category of personal data. Therefore, the Law of AR grants a specific protection to personal data relating to family life.

The users of personal data. Pursuant to the Law, the main users of personal data are controller, processor, and user. The **controller** is any natural or legal person, public authority or agency which determines the purposes and means of processing of personal data in accordance with law and having the full ownership, enjoyment and disposal rights on the data.[154] The entity is considered a controller within the meaning of this law only in cases the processing is legitimate and lawful. In other words, the controller is not considered as such in case if he had illegally decided that the data should be processed. The main obligations of the controller is the ensuring of legality and security of processing of personal data.[155]

The **processor** is a natural or legal person, public authority, agency or any other body which processes, collects and protects the data entrusted to him. The responsibilities and legal obligations of the controller shall be governed by a contract between the controller and processor.[156] The main legal obligation of the processor is ensuring the legality of the collection and processing of personal data, as well as carrying out obligations deriving from a contract concluded with the controller.[157]

A user is any natural or legal person, state organ who is authorized to use the data in a scope and extent legally defined by the controller for the its own purpose.[158] Transfer of data to the data users shall be based on legitimate grounds.[159] According to the defined scope, a user is any entity to whom the data is legally transferred.

The consent. The Law of establishes the consent of the data subject as one of the grounds for processing of personal data. Article 8.1. of the Law stipulates that the consent has to be in either in written form or an electronic form with an electronic signature. It means that the oral consent given by the data subject is not to be treated as a valid consent.

---

[153] İnformasiya əldə etmək haqqında Azərbaycan Respublikasinin Qanunu. Bakı, 30 sentyabr 2005-ci il № 1024-IIQ, m 38.3
[154] Fərdi məlumatlar haqqında qanun, m 2.1.9.
[155] Fərdi məlumatlar haqqında qanun, m 10.1.
[156] Fərdi məlumatlar haqqında qanun, m 10.3.
[157] Fərdi məlumatlar haqqında qanun, m 10.4.
[158] Fərdi məlumatlar haqqında qanun, 2.1.11.
[159] Fərdi məlumatlar haqqında qanun, m 2.1.13.

The written consent has to indicate the identity of processor and controller, the purposes of processing and collection of data, the categories of data undergoing processing as well as the rules for erasure and archiving such data[160]. Although the definition does not clearly indicate the main features of a valid consent, article 8.2 clearly illustrates that the consent has to be specific and informed. In other words, the data subject has to be know the purpose of processing as well as the categories of data undergoing processing. The consent to process the personal data could also be given by the heirs, parents, legal representatives of the data subject if the data subject has died, is missing, is declared dead by the court decision, did not reach the age of puberty(18 years old[161]) or is legally incapable of giving a consent. So, it implies that the legal age of a valid consent is 18 years old.

3.2.3.2.Main principles of processing of data.

The general principles of processing of personal data are enshrined in article 4 of the Law. Accordingly, the collection and processing of data has to be conducted on the basis of principles of legality, confidentiality taking into account the respect to rights and fundamental freedoms reflected by the Constitution. The violation of right to honor and dignity of a person in a course of processing, collecting and protecting of personal data shall be prohibited by law.

Legality of processing

The principles for processing of personal data are similar to those of EU. The first principle of processing of data is the **legality of processing**. Although it is not explicitly mentioned as a principle, it could be found out in different provisions of the Law. The legality of processing means that the processing has to be based on law, the criteria which could be found in article 8.1 of the Law. Accordingly, the data can only be processed either on the mandatory grounds which are stated in law or based on the consent of the data subject.

[160] Fərdi məlumatlar haqqında qanun, m 8.2.
[161] Azərbaycan Respublikasının Mülki Məcəlləsi. Bakı şəhəri, 28 dekabr 1999-cu il, № 779-IQ, m 28.2

The principle of purpose specification and limitation.

In accordance with article 9 of the Law, which describes the main conditions for processing of data, the personal data has to collected for specified, explicit and legitimate purpose. The law explicitly mentions that the purpose of processing has to be declared before the processing takes place. The data has to be processed only for the specified purposes which would suffice to conclude that further processing of data for any other purpose shall be deemed illegal.

The legislator establishes that the purpose has to be explicit, which is referred to as "dəqiq". This word implies the meaning of being sufficiently clear and unambiguous. [162]The ultimate objective of this requirement is to ensure that the purposes are specified without vagueness or ambiguity as to their meaning or intent. Third, purposes must also be legitimate. In order for the purposes to be legitimate, the purpose of the processing has to be legal, i.e. has to be based on provisions of law.

The principle of data quality

The data quality principles is enshrined in article 9.3 of the Law, which requires that the data must be accurate, full, and kept up-to date when necessary. The data subject is endowed with the right to access and rectification, which implies that whenever the data about the subject is inaccurate or incomplete, the data subject shall be empowered to demand the rectification of the inaccurate data, or where it is impossible, demand the erasure. However, unlike EU, the Law does not impose obligation on controllers to notify third parties and recipients about the rectification of inaccurate data.

The principle of limited retention of data

Article 9.4 of the Law requires the deletion of the data as soon as the purposes for which it was collected and processed are fulfilled and there is no further need for retaining the data. Article 15.6 of the Law provides that, whenever the state registration of Personal Information System is terminated, the data contained in that system shall be immediately erased in accordance with the rules specified by relevant executive authority.

[162] Azərbaycan dilinin izahlı lüğəti. Dörd cilddə. I cild. Bakı: Şərq-Qərb, 2006, s 251.

3.2.3.3. Rules on processing of data

The Law establishes a detailed layer of rules regarding lawful processing, rules on secure processing, rules on transparency of processing and rules on promoting compliance. Similar to DPD , the Law sets two different sets of legal basis for processing:: rules for processing of non-sensitive personal data(art 9.6) and rules for processing of sensitive data(art 9.7).

Lawful processing of data

Rules on lawful processing of non-sensitive data.

The Law provides four grounds for lawful processing of non-sensitive personal data. The list is exhaustive.

Consent. Under the Law, the consent is a first basis for legitimate processing of data. The consent of the data subject shall mean a written indication of a will of data subject in regard to processing of his data.[163]

The second basis for legitimate processing of personal data is the **processing based on relevant legislative acts** which specifies the means and purposes of processing. The law does not explicitly mention the processing of personal data in context of performance of a contract, employment relationship, for the purpose of legitimate interest of a third party as a ground for processing in contrast to DPD. However, these grounds are enshrined in the relevant legislative acts which specify the means and purposes of processing. For instance, the Civil Code of AR provides that the natural person is obliged to inform all his creditors about changing his name[164], the legal representatives and guardians are legally obliged to inform the relevant executive body when they change the place of residence. Such legal grounds could also be found in Labor Code of Azerbaijan Republic, which states that the employer can process the personal data of the employees in a context of employment relationship. Pursuant to Law of Azerbaijan Republic on Trade Unions, the trade unions can process the data of the members in the context of membership, as long as it is necessary for performance of the tasks set forth in this Law.

[163] Fərdi məlumatlar haqqında qanun, m 8.1. See Chapter 3.2.3.1.
[164] Azərbaycan Respublikasının Mülki Məcəlləsi, m 26.4.

The processing of personal data for **statistical and scientific research purposes** shall be considered as a legitimate ground for processing, only if the personal data is anonymized. Anonymization shall mean sanitization of a data, so that the identification of the data subject is no longer possible.[165]

The last legal ground for processing is the processing of personal data for protection of life and health of the data subject. The Law prefers to use the notion of health and life, rather than "vital interest" notion used in DPD.

Rules on lawful processing of special categories of personal data.

Article 9.7 of the Law lays down the detailed regime for processing the data which reveal racial or ethnic origin, , religious or philosophical beliefs, and data related to health and family life of a person. The Law takes a similar "prohibition" approach which is also prescribed in DPD. The processing of such data is prohibited in general, unless there is an exemption falling under the article 9.7. Article 9.8 of the Law provides that the special categories of personal data shall be immediately deleted as soon as the purpose of processing if fulfilled and the data subject does not give his consent for retaining of the data.

Unlike EU law, the Law does not explicitly mention consent as a legitimate ground for processing of special categories of personal data. However, it is unclear whether the paragraph 1 of article 8, which regulates the processing of personal data on the basis of consent of data subject also covers the special categories of data. Special categories of data are personal data within the meaning of article 2.1.6 of the Law. Therefore, it could be assumed that the consent of the data subject established under article 8.1 in principle, also covers the special categories of personal data. Moreover, article 9.7.3 of the Law stipulates that the special categories of data can be processed for protection of health and life of the data subject, where it is impossible to get the consent of the latter. Therefore, it could be concluded that the consent could also be a basis for processing of sensitive data.

The second exemption from the general prohibition of processing special categories of personal data is where the collection and processing of data are based on mandatory provisions of law. This could be the case of processing of data related to

[165] Fərdi məlumatlar haqqında qanun, m 2.1.15.

criminal convictions of a data subject by the investigative, inquiry, prosecution bodies and the court,[166] or where the employer is obliged to inform the relevant executive body about the number of disabled persons working for him.[167]

As mentioned above, the processing of special categories of data is also permitted in order to protect the life and health of data subject, third party of group of people.[168] Pursuant to article 53 of the law on "Protection of health of population, the information constituting medical secrecy can be handed to 3rd parties in cases the citizen or his/her legal representative give their consent thereto, whereas this information is essential for the purpose of treatment of the patient, and where the patient is not able to give his consent.

The special categories of personal data could also be legally processed when they are already available to the public within the meaning of article 5.3 of the Law. Accordingly, publicly available data shall be considered the personal data which is anonymized, made available to the public or included to the public information systems with the consent of the data subject. The name, surname and the patronymic of a person shall be considered publicly available data. With the consent of the data subject, the personal data as the date of birth, sex, nationality, phone number and email, address and place of residence, the place of work, occupation, employment, family status, photo and other personal information could be entered to public information systems.

Security and confidentiality of processing

One of the principle objectives of the Law is the ensuring of security of data processing.[169] [170] This could also be proven by the definition of both controller and processor within the meaning of article 2.1.9 and 2.1.10 respectively, which define them as entities responsible, among others, for security of processing. Article 5.8 of the Law defines the security of processing as imposition of organizational and technical measures against unlawful alteration, loss, access, erasure or other acts. In a broad sense, security could be understood as appropriate organizational and technical measure for protection

[166] Azərbaycan Respublikasinin Cinayət-prosessual Məcəlləsi. Bakı şəhəri, 14 iyul 2000-ci il № 907-IQ, m 222.1.
[167] Azərbaycan Respublikasinin Əmək Məcəlləsi. Bakı şəhəri, 1 fevral 1999-cu il № 618-IQ, m 28.2.
[168] Fərdi məlumatlar haqqında qanun, m 9.7.3.
[169] Fərdi məlumatlar haqqında qanun, m 1.
[170] Fərdi məlumatlar haqqında qanun, m 4.

of personal data. Several provisions of the Law reiterate the obligation of controller and processor in regard to security and confidentiality of processing.[171] Pursuant to article 10.1 of the Law, the controller is liable for the damages caused by the absence or inappropriateness of the security measures. Nonetheless, no definition of appropriate security measures is found in the law.

The confidentiality of the processing refers to protection of personal data from unauthorized people, as well as the obligation of the controller and processor on non-disclosure.[172] Obligation on confidentiality also applies to the employees and other natural persons under the control of the controller and processor, even after the dismissal or end of the employment relationships.[173] Confidentiality does not cover the publicly available data.[174]

The obligation of confidentiality covers not only the controllers and processors, but also the relevant executive body for promoting the compliance within the meaning of article 17. The relevant executive body shall also ensure the confidentiality of the personal data while carrying out its activity.[175]

Transparency of the processing

The transparency of processing implies that the data subject has to be informed about the processing before it commences.[176] The information has to at least include: the identity of the controller and the processor, the purposes and the means of the processing, the security measures available, the categories of the data concerned, the approximate time frame within which the processing takes place, and the rules regarding deletion or archivisation of data after the processing, as well as the rights of the data subject.[177] [178] This obligation has to be fulfilled proactively, before the processing takes place, namely, at the time of collection of information from the data subject.[179]

[171] Fərdi məlumatlar haqqında qanun, m 10.1.
[172] Fərdi məlumatlar haqqında qanun, m 5.2.
[173] Fərdi məlumatlar haqqında qanun, m 5.5.
[174] Fərdi məlumatlar haqqında qanun, m 5.3.
[175] Fərdi məlumatlar haqqında qanun, m 17.3.
[176] Fərdi məlumatlar haqqında qanun, m 9.1.
[177] Fərdi məlumatlar haqqında qanun, m 8.2.
[178] Fərdi məlumatlar haqqında qanun, m 11.
[179] Fərdi məlumatlar haqqında qanun, m 11.2.

The law does not lay down any exemption to this rule. Therefore, in principle, the data subject has to be given the information specified above, whenever the data is collected from him. In some cases, this would involve a disproportionate effort of the controller, where, for instance, the data is processed for statistical purposes.

Transfer of data to 3rd parties.

The Law lays down the detailed rules and norms of transferring of data to 3rd . Generally, the data could be transferred to a third party only with a written consent of the data subject. This rule is however, subject to certain exceptions:

1. Where the data is already publicly available;
2. Where the transfer of data is essential for the life and health of the data subject, and where the data subject is incapable of giving his consent;
3. Where the envisaged transfer is related to carrying out of obligations of state and municipal bodies, in a condition that adequate safeguards are available.

The consent of the data subject can be withdrawn at any time. Upon such a withdrawal, the controller or processor shall immediately stop the transfer of the data.

Rules on promoting compliance.

Registration of personal information systems.

The Law provides for registration of Personal Information Systems in accordance with the decision of relevant executive authority. Pursuant to art. 2.1.3 of the Law, Personal Information systems shall mean information systems providing the collection, processing and protection of personal data. The rules for registration are defined by the decision of Cabinet of Ministers on Registration of Personal Information Systems. Personal data cannot be processed without the registration of Personal Information Systems.[180] However, the 3rd paragraph of the Law provides for exemptions from registration:

1. The personal information systems regarding the information classified as state secret;
2. The personal information systems containing personal data of subjects who are in employment relationships with the controller or processor

[180] Fərdi məlumatlar haqqında qanun, m 15.2.

3. The personal information systems which are not required to be registered in accordance with the decision of relevant executive body.

The relevant executive body within this context Is Cabinet of Ministers of AR[181], which adopted decision N 237 on approval of "Personal Information Systems which are not required to be registered"[182]. In accordance with the decision, the following information systems are exempted from state registration:

1. The public information systems containing anonymized data, information made publicly available by the data subject;
2. The information systems containing archived personal data;
3. The information systems of state or municipal bodies, where those systems contain personal data of less than 1000 subjects;
4. The information systems containing data necessary for protection of life and health of data subjects, where those systems contain personal data of less than 1000 subjects;
5. The information systems containing data for the purpose of scientific or statistical researches, where those systems contain personal data of less than 1000 subjects;
6. The information systems of social unities, trade-unions and other non-commercial organizations, containing the personal data of their members, subject to condition that the data could not be given to 3rd parties without the consent of data subject, where those systems contain personal data of less than 1000 subjects;
7. The information systems containing personal data collected and processed with the written consent of data subjects(name, address, phone number, sex, data of birth, occupation, photo and etc.) in the field of telecommunications, mail service and other fields, which are intended to provide information to the

[181] "Fərdi məlumatlar haqqında" Azərbaycan Respublikası Qanununun tətbiq edilməsi barədə" Azərbaycan Respublikası Prezidentinin 2010-cu il 4 iyun tarixli 275 nömrəli Fərmanı

[182] "Dövlət qeydiyyatına alınması tələb olunmayan fərdi məlumatların informasiya sistemləri"nin təsdiq edilməsi haqqında Azərbaycan Respublikası Nazirlər Kabinetinin 2012-cu il 17 dekabr tarixli 237 nömrəli Qərarı.

public and open to consultation, where those systems contain personal data of less than 1000 subjects;

The application for registration of personal information systems shall contain at least the information: the name, address of the controller, the legal basis of processing, the purposes and means of processing, the description of the categories of personal data, the categories of data subjects, brief description of security measures taken by the controller or processor, the categories of users of data and etc. All this information shall be kept in state registry of personal information systems. [183]

The relevant executive body responsible in sphere of processing, collection and protection of personal data, which is Ministry of Telecommunications of AR[184], shall check the compliance with the rules by the controllers and processor. It has rights to check the compliance of the processor and controller with the provisions of this law. Where the provisions of the Law are violated, the body has the right to demand the controller and processor to put an end to the violation, bring the perpetrators to legal responsibility and ban the processing of personal data by the latter.[185]

3.2.3.4.Rights of the data subject

The Law grants the data subjects a wide specter of rights in regard to processing of their data. First and foremost, the data subject has a **right to access** to his/her data, which implies the getting information at least about whether his data is undergoing processing, the identity of the controller and processor, the purposes and means of processing, the approximate duration of processing, the legal basis of the processing, the intended transfer of data to 3rd parties and whether there is legal basis for the transfer. This right also implies the possibility to get acquainted with his/her personal data that is intended to go under processing. This right is a prerequisite of the **right to rectification** of the data, whereas the subject is allowed to analyze his data and rectify it, in case the data is inaccurate or incomplete.[186] Data subject is also legally empowered to get

[183] Fərdi məlumatlar haqqında qanun, m 16.1
[184] "Fərdi məlumatlar haqqında" Azərbaycan Respublikası Qanununun tətbiq edilməsi barədə" Azərbaycan Respublikası Prezidentinin 2010-cu il 4 iyun tarixli 275 nömrəli Fərmanı, m 1.2.
[185] Fərdi məlumatlar haqqında qanun, m 17
[186] Fərdi məlumatlar haqqında qanun, m.7.1.

information about the source of collection of his personal data, where such data was collected not from the data subject.

The data subject has a **right to object** to collection and processing of his data, unless the collection and processing are based on mandatory provisions of law. The objection has to be raised in a written form to the controller and processor. The objection does not have to be justified. Where the controller or processor get the objection, they have to immediately stop the processing. The right to object also covers the automated individual decision-making, where such decisions negatively affect the interests of the data subject, unless such decisions are based on mandatory provisions of law. Where such objection is raised, the processing has to be temporarily suspended until the data subject gives his consent to processing by means other than the automated means.

Article 7.4 deals with the right to legal remedy of the data subject which covers the right to administrative remedy, right to apply to the court, and right to compensation for material and moral damage incurred by the illegal collection and processing of his data, as well as not ensuring the adequate security of personal data. This right is based on article 60 of the Constitution, which establishes the right to legal remedy.

3.2.3.5.Transfer of personal data to 3rd countries

The transfer of personal data to other countries is regulated by article 14 of the Law. However, the article only lays down the basic prohibitions, principles and rules of transfer. The regulation is not so thorough and comprehensive as in EU. The transfer of personal data to other countries is prohibited where

1. Such transfer poses risk to the public and state security;
2. Where the other country does not provide sufficient legal protection equal to protection granted in Azerbaijan;

The Law follows an "equality" rather than "adequacy" approach. Accordingly, the data can be transferred to a country which ensures not adequate protection as in EU, but protection equal to that granted in Azerbaijan. However, the data could still be transferred to other country where the data subject has given his consent or where the transfer of data is essential for protection of life and health of the data subject. In principle, unless there is a consent of the data subject or it is for the vital interest of the data subject, the transfer

of data to other states is prohibited, if the state in question does not provide legal protection equal to AR.

3.2.3.6.Enforcement, legal remedies and sanctions

The right to an effective remedy is a prerequisite for effective protection of any right. Without effective remedies under national law, it would be impossible to effectively enforce any right which is granted under this Law. Under the Law, the data subject has a right to complain to relevant administrative body or court, and to claim for material and moral damages, where his rights are violated by the unlawful collection, processing or any other act of controller and processor.[187] The controller and the processor are liable for the any material or moral damage suffered by the data subject as a result of collection, processing or inappropriate security measures. The data subject has three possibilities: complain to the controller or processor, complain to the relevant executive body and to lodge a claim within the court. Neither of the first two instances are obligatory: the subject can directly apply to the court at any time.

Complaining to controller or processor. Where the data subject deems that his rights were violated as a consequence of collection or processing of his data, he can make a written request to the controller about the alleged violation, which has to be considered and responded by them within 7 working days. In case the response of the controller or processor is not satisfactory, the data subject can refer the matter to the relevant executive body within the meaning of article 17 of the Law. This body is responsible for promoting compliance with the provisions of the Law, and bringing the violations to the end. The body can bring the controllers and processors to legal responsibility in accordance with the laws of Azerbaijan. Accordingly, the natural persons, legal entities or other state bodies are legally responsible for violation of the provisions of this Law.[188]

There are three types of responsibility in information sphere.[189] Where the legal wrongdoings have a malicious character, such wrongdoings incur criminal liability. The norms regulating the criminal acts in sphere of information are gathered in chapter 30 of

[187] Fərdi məlumatlar haqqında qanun, m 7.4
[188] Fərdi məlumatlar haqqında qanun, m 19.
[189] Xropanyuk VN. Dövlət və hüquq nəzəriyyəsi (ixtisarla). Bakı: Qanun, 2007, s 223.

the Criminal Code of AR, namely the Cybercrimes. Accordingly the criminal acts like unlawful access to the computer systems(Art. 271 of CC[190]), the unlawful collection of information(Art 272 of CC), unlawful access to the information systems(Art 273 of CC) are criminally punishable.

The civil liability in information sphere is characterized by the material character of sanctions imposed for the wrongdoings. This sanctions comprise fines, compensation for damages, compensation for moral damages and etc. This civil-legal sanctions are aimed for the restoration of violated rights in information sphere.[191]

The violation of legislation on information could also lead to administrative legal responsibility. The Chapter 16 of the Code on Administrative wrongdoings[192] provides for acts that are subject to administrative sanctions. These acts are: the violation of norms of personal data protection(art 181.4), violation of data security norms(182), non-registration of personal information systems(183) and etc. The sanction for such wrongdoings is up to 500AZN.[193]

3.3. Other Laws.

Article 3.2 of the Law on Personal data explicitly excludes the processing and accumulation of personal data in the sphere of intelligence, operational-search activity, the processing of data classified as state secret and data collected in National Archive of Azerbaijan Republic from the scope of regulation. Such activities are regulated by relevant legal acts of AR. As long as intelligence and operational-search activities require the processing of personal data which may have serious legal implications for the individuals, detailed data protection rules and safeguards in these areas are especially necessary.

Operational-search activity. The law of AR on Operational-search activity regulates the legal issues and relationships arising as a result of carrying out operational-

[190] Azərbaycan Respublikasının Cinayət Məcəlləsi. Bakı, 30 dekabr 1999-cu il №787-IQ.
[191] Tağıyeva GZ. Mülki hüquq məsuliyyəti və onun nəzəri-təcrübi problemləri // Dövlət və hüquq. Elmi-nəzəri metodik jurnal, Bakı, 2003, № 5-6, s. 104.
[192] Azərbaycan Respublikasının İnzibati Xətalar Məcəlləsi. Bakı, 11 İyul 2000-ci il № 906-IQ.
[193] 1 AZN = 0.52 EUR. 'XE: Convert EUR/AZN. Euro Member Countries To Azerbaijan New Manat' (*Xe.com*, 2017) <http://www.xe.com/currencyconverter/convert/?Amount=1&From=EUR&To=AZN> accessed 24 June 2017.

search activity and sets out legal safeguards in carrying out such activity.[194] Operational-search activity is carrying out measures specified in the law by the relevant state authorities in open and covert manner. The main purposes of such activity are the prevention, disclosure of crimes, determining the person who committed a crime, and finding the persons evading the investigation, inquiry or serving a criminal sentence.[195] Operational-search activity is based on principles of legality, humanism, respect to human right and freedoms and principle of conspiracy.[196] Operational-search activity involves measures such as tapping the phones, inspection of home, mail and correspondence, extraction of information from telecommunication or other technical channels.[197] These measures restrict the rights and obligations of a person, in particular right to private and family life guaranteed under article 32 of the Constitution. Therefore, a special set of safeguards and legal remedies are envisaged in order to minimize the risks posed by such an activity.

First of all, the activity can be carried out only for the purposes mentioned in article 1.3 of the Law. Second, the dissemination of information containing data regarding private and family life, as well as his honor, dignity without the consent of the data subject is strictly prohibited. Third, the violation of rights and freedoms of people envisaged in the Constitution is prohibited. Temporary limitation of those rights is only permitted where such limitation is necessary for the purposes enumerated in article 1.3, and where it is proportionate. Fourth, any person whose rights and freedoms are deemed to be violated can apply to public prosecution office, who is in charge of checking the compliance of operational-search activity with the provisions of this law. This would be without prejudice to judicial remedy and right to apply to the court. Fifth, where the data is irrelevant to the purpose of the operational-search activity, such data shall be prohibited to use and has to be immediately erased. Sixth, the data obtained in violation of the provisions of this Law shall be immediately erased. Seventh, the data obtained in a course of operational-search activity containing information related to private and family life of a person shall be immediately erased, even if it was obtained legitimately. Eighth, the access to the data obtained in a course of legitimate operational-search activity shall be

[194] Əməliyyat-Axtarış Fəaliyyəti haqqında Azərbaycan Respublikasinin Qanunu. Bakı, 28 oktyabr 1999-cu il № 728-IQ.
[195] Əməliyyat-Axtarış Fəaliyyəti haqqında Qanun, m 1.3.
[196] Əməliyyat-Axtarış Fəaliyyəti haqqında Qanun, m 3.
[197] Əməliyyat-Axtarış Fəaliyyəti haqqında Qanun, m 10.

granted only to investigator, prosecutor or court in accordance with Criminal Procedural Code of AR. Ninth, the dissemination of information regarding private and family life of a person without his consent shall incur legal responsibility in accordance with other legal norms of AR. Finally, the person whose rights and freedoms were violated shall be entitled to compensation for material and moral damage. Article 21.3 explicitly mentions that except the measures envisaged in this Law, recording the photos, videos and audio of a person, or having him shadowed without his/her consent shall give a rise to legal responsibility in accordance with law. These safeguards are aimed to mitigate the potential adverse effect of such activity.

Activity in sphere of intelligence. The processing of data in relation to activities in sphere of intelligence is excluded from the scope of Law on Personal Data. Therefore, special safeguards are introduced in Law on Intelligence and Counter-Intelligence of AR. The main purposes of such activity are ensuring the national interest of AR and creating an environment for successful realization of state security policy.[198] The Law on Intelligence and Counter-Intelligence of AR sets out similar safeguards to those introduced in Law on Operational-search activity. Accordingly, the intelligence and counter-intelligence activity have to be based on principles of legality and respect to human rights and freedoms. Except the cases specified in the law, the limitation of right to private and family of a person is prohibited. The dissemination of information regarding private and family life shall be punished in accordance with law. The abuse of powers granted to intelligence and counter-intelligence authorities shall incur legal responsibility in accordance with law. The Law also stipulates the principle of purpose limitation: the personal data which are not relevant to the purposes specified in this Law shall be immediately erased. The right to effective remedy implies the right to apply to relevant administrative instance or to a court. The person whose right and freedoms are violated shall be entitled to compensation for material and moral damage.

Activity in sphere of State Security. The processing of personal data in sphere of state security are excluded from the scope of Law on Personal data of AR by virtue of article 3. The activities in sphere of state security are regulated by Law of AR on State Security. The main objective of this law is the establishment of legal foundation of state

[198] Kəşfiyyat və əks-kəşfiyyat haqqında Azərbaycan Respublikasinin Qanunu. Bakı, 29 iyun 2004-cü il № 711-IIQ, m 1.2.

security policy for the sake of development of AR as an independent, sovereign and democratic state. The activities in state security sphere can also come in touch with the processing of personal data. Therefore, adequate legal safeguards are put forward to strike a proper balance between the state security and right to private and family life guaranteed under article 32 of Constitution. The limitation of human rights and freedoms guaranteed under Constitution is only permissible in cases and for purposes specified in this law. [199] The person whose rights and freedoms were adversely affected is entitled to compensation. The abuse of competences granted under this Law shall incur legal responsibility in accordance with law.

Some provisions of data protection norms can also be found in Law of AR on Mass Media. Pursuant to article 10-1 of the Law, the secretly recorded audio, visual, photo and video recordings of a person can only be disseminated with the consent of the person in question or with the decision of the court.

One of the important issues in data protection is the reconciliation of freedom to obtain information under article 50 and right to private and family life of a person guaranteed under article 32 of Constitution of AR. This issue is dealt with in Law of AR on Freedom of Information. Pursuant to article 2.1 the mentioned Law, the freedom of information in Azerbaijan is guaranteed. This freedom implies the right to obtain information. However, there are some legal constraints in regard to personal data. The personal data is classified as confidential data and defined as information regarding private and family life.[200] Pursuant to article 38.2, the freedom of information is limited in regard to data about political views, religious or other beliefs, racial or ethnic origin, criminal convictions and proceedings, data related to health, sexual life, marital status, adoption and other data connected to family life, data relating to disability or mental incapability, the data relating to taxation. The right to obtain information is limited from the moment it is obtained.[201]

[199] Kəşfiyyat və əks-kəşfiyyat haqqında qanun, m 13.2.
[200] Kəşfiyyat və əks-kəşfiyyat haqqında qanun, m 34.4, 38.1.
[201] Kəşfiyyat və əks-kəşfiyyat haqqında qanun, m 38.4.

CHAPTER IV. ASSESSMENT OF ADEQUACY OF PROTECTION IN AR VIS-À-VIS EU

In a bid to evaluate the transfer of personal data from EU to third countries, the group of Member States' national data protection supervisors, the so-called Article 29 Working Party (the Working Party), formulated a range of core data protection principles and effective enforcement mechanisms compliance with which would allow a determination that a third country's data protection system is adequate.[202] Although there is no adequacy decision of the Commission in regard to transfer of personal to Azerbaijan[203], taking into consideration of other adequacy decisions of the Commission, I strongly believe that Azerbaijan offers an adequate level of protection for personal data, both within the meaning of its national data protection laws and international commitments.

In accordance with the opinion of the Working Party, any meaningful analysis of adequate protection must comprise the two basic elements : the content of the rules applicable and the means for ensuring their effective application. The Working Party identified the core data protection principles, which would be prerequisites for adequate protection of personal data. These principles are purpose limitation principle, the data quality and proportionality principle, the transparency principle, the security principle, the rights of access, rectification and blocking and the rules regulating the transfers to other third countries. Three additional issues to are to be considered into in cases of specific types of data processing, namely, the processing of sensitive data, processing of data for direct marketing purposes and regulation of automated individual decisions. In terms of enforcement requirements, the Working Party identified three core elements: a good level of compliance, support and help to individual data subjects as well as appropriate redress.[204]

---

[202] Article 29 Working Party Working Document of the of on 24 July 1998 entitled "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EC Data Protection Directive". DG XV D/5025/98.

[203] 'Commission Decisions On The Adequacy Of The Protection Of Personal Data In Third Countries - European Commission' (*Ec.europa.eu*, 2017) <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm> accessed 25 June 2017.

[204] Ibid (n 196) 6-7, see also Commission Decision (EC) 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act [2002] OJ L2/13

On the other hand, as regards the CoE Convention 108, the Convention could be said to include the first five of the six 'minimum conditions'[205]. This brief analysis seems to indicate that most transfers of personal data to countries that have ratified Convention 108 could be presumed to be allowable. Azerbaijan ratified the Convention on 03.05.2010.

As discussed in Chapter ,in regard of core principles of data protection, the Law of AR explicitly provides for all of them. The data subjects are also endowed with the same rights which the DPD grant. These rights include the right to access, rectification and blocking of personal data, right to object to processing of his/her personal data, right to security of processing and right to object to automated individual decision-making.

In regard to processing of sensitive personal data, the Law of AR grants even more protection than that afforded by DPD: the special categories of personal data include not only the categories enumerated in Article 8 of the DPD, but additionally, the personal data relating to family life of a person. In this relation, the Law of AR treats the data relating to family life as a special category of data which is afforded special protection. In regard to grounds for processing sensitive data, both DPD and Law of AR provide for same legitimate grounds.

However, in regard to processing of data for direct marketing purposes, the Law of AR does not provide specific 'opt-out' rights where data are used for direct marketing purpose. It rather provides a general right to object to processing of his/her personal data, unless the processing is carried on the basis of mandatory provisions of law. As long as there is no mandatory provision in regard to processing of personal data for direct marketing purposes, the data subject may object to processing whenever the controller or processor informs the data subject about the intended transfer of data to 3rd party in accordance with article 13 of the Law.

The data subject is explicitly endowed with a power to object to automated individual decision making about him, whenever the such a decision infringes upon the rights and interests of the data subject. The scope of this right is almost similar to that granted by DPD.

[205] Ibid (n 202) 8.

In terms of enforcement requirements, the Working Party identified three core elements: a good level of compliance, support and help to individual data subjects as well as appropriate redress.[206]

The institutional support to individual shall be considered adequate where support is ideally be impartial, independent and equipped with the necessary powers to investigate any complaint from a data subject.[207] In Azerbaijan, such an institution is The Ministry of Telecommunications and High Technologies of AR within the meaning of article 17 of the Law. The authority is endowed with effective investigative and interventive powers, such as to order the blocking of processing of data, investigating the complaints of data subjects and referring the matter to the court.

The level of compliance is connected to several factors, such as the degree of awareness of the code's existence and of its content among members, on the steps taken to ensure transparency of the code to consumers in order to allow the market forces to make an effective contribution, on the existence of a system of external verification and, perhaps most crucially, on the nature and enforcement of the sanction in cases of non-compliance.[208] In this regard, the level of compliance is ensured with several factors. First, the controllers and processors are legally obliged to comply with the provisions of the data processing. Second, the relevant executive authority within the meaning of article 17 is legally obliged to promote the compliance by controller and processor, by means of regular requests, checks and informatory measures. Third, subject to some limitations, any personal information systems intended to process the personal data have to be registered in accordance with Decision of Cabinet of Ministers. Fourth, the violation of provisions of this law and other norms by controllers and processors shall invoke legal responsibility. These sanctions are both remedial, which are simply requires a data controller, in a case of noncompliance, to change its practices so as to bring them into line with the Law, as well as punitive, where the controller or processor is subject to administrative, civil or criminal liability.

Appropriate redress, or adequate legal remedy implies the compensation for material and moral damage for the data subjects. In this respect, the Law of AR provides for a right of data subject to apply to relevant executive body within the meaning of article

[206] Ibid 7.
[207] Ibid 12.
[208] Ibid 40.

17 or to apply for a judicial remedy, where his rights and freedoms were adversely affected. The data subject shall be entitled to adequate compensation for both material and moral damage.

Nevertheless, there are also some weak points in the Law. First and foremost, the Law does not envisage the appointment of Data Protection Officer, in order to simplify the registration of Personal Information Systems, as well as to guarantee more protection to personal data.

Second, the Law does not treat biometric data as a special category of personal data. Biometric data, within the meaning of article 9.5 of the Law, shall be treated as personal data, without any other specific protection.

Third, the regulation of transfer of personal data to other countries is quite superficial. The law merely stipulates the transborder flow of data where the receiving state ensures data protection equal to that in Azerbaijan. However, the law does not specify any derogation from this rule except where data subject has given his consent or where the transfer is necessary for the vital interests of the data subject. The transfer of data of data for performance of a contract, or implementation of precontractual measures is, in principle, prohibited by virtue of Article 14 of the Law. Moreover, the Law does not envisage the transfer of data on important grounds of public interest or exercise of legal claims. In other words, the data could not be transferred to other state in any case except there is explicit consent of the subject. DPD provides for transfer of data to third states where the controller adduces adequate safeguards or appropriate contractual clauses to the intended processing. Such a rule is absent from Article 14.

Fourth, the law does not provide for prior examining of checking operations which are likely to pose a specific risk to the data subject. All the Personal Information Systems are subject to state registration. The application for registration shall contain, inter alia, the means, purposes and categories of data undergoing processing. However, the Law does not specify the prior authorization of processing operations which would have serious adverse effects on data subject. Nor it does not specify the cases where the controller intends to process any other category of data which is not previously specified in the application for registration.

Fifth, as mentioned above, the legal age of a valid consent is 18 years old. In an increasingly technologized society, children already could be expected to understand the

implications of giving consent in certain cases, for instance, giving consent to processing of their personal data in order to get a particular product or service in internet. Moreover, the children aged 14-18 already have civil legal capacity, although limited.[209] They have rights to conclude a broad array of transactions[210], right to work, right to participate in commercial cooperatives and etc.[211] Therefore, in my point of view, the legal age of a valid consent could be lowered to 16 years old.

Sixth, the definitions of personal data within the Law on Personal data and Law on Freedom of Information significantly vary. The latter defines the personal data as data "relating only to personal and family life", whereas the Law on Personal data has a much broader scope, defining as "any data relating to identified or identifiable natural person". To this reason, such discrepancies within the Laws should be eliminated.

Seventh, pursuant to article 8 of the Law, consent should be only in written form or in an electronic form with an electronic signature. Such a requirement would make the processing of personal data based on oral consent or consent which can be implied from the behavior of the data subject illegal. To this end, the provision of the Law is very limited and strict in its scope.

Eighth, where the personal data was inaccurate and was rectified, the Law does not impose an obligation on the controller or processor to notify the recipients and users of the data about such rectification. This situation could have a potential adverse effect on the data subject, where the recipients or users process inaccurate data.

Summing above all the mentioned points, it could be concluded that Azerbaijan's legal system, in particular, The Law on Personal data, despite of this shortages and week points, does provide an adequate protection of personal data, by means of principles, grounds of processing, effective implementation mechanisms, sanctions and remedies, the rights of data subject, as well as by international commitments of Azerbaijan. The Law of AR provides a protection almost equal to the protection afforded in EU. Although the activities in the spheres of intelligence, counter-intelligence, operational-search are explicitly excluded from the scope of the Law, the relevant acts and laws do place adequate safeguards for processing.

[209] Azərbaycan Respublikasının Mülki Məcəlləsi, m 28.3.
[210] Azərbaycan Respublikasının Mülki Məcəlləsi, m 29.
[211] Azərbaycan Respublikasının Mülki Məcəlləsi, m 30.

CONCLUSION

The right to privacy is a one of the most important parts of human dignity. In an increasingly globalizing society, information is the most important asset one can possess. The integration of borderless communication across the boundaries of different jurisdictions, their incorporation in our everyday lives made it inevitable to adopt special laws to protect our privacy against such developments. To this end, on an international plain, many international organizations made an attempt to regulate the right to privacy. However, the protection of privacy, in particular with regard to processing of personal data have to be regulated not only on international plain, but also on a national level.

Protection of right to private and family life is the positive obligation of states party to ECHR, which means they have to not only refrain from infringing the right, but also take positive measures to protect it. As a positive obligation to protect the personal data, both EU and AR have their data protection laws, which aim to protect the individuals, their right to privacy in the context of processing of personal data. The data protection laws set out detailed rules and principles of processing of personal data, grant the data subjects rights to enhance the protection, as well set out remedies and sanctions to mitigate the potential risks of abuse.

Nevertheless, the scope of protection of personal data varies from one jurisdiction to another. The principal aim of this thesis was to conduct a detailed analysis of data protection laws of EU and AR, to evaluate the regulatory approaches of those jurisdictions, and to reach a logical conclusion in regard to adequacy of data protection in AR. As a conclusion of this thesis work, it is essential to mention these implications found out in this work:

1. In regards to human rights, article 12 para.1 of the Constitution stipulates that the ensuring the human rights and freedoms, and providing the deserving life to the people and citizens are the ultimate goals of the state. Pursuant to second paragraph of that article, the right and freedoms enshrined in the Constitution are applied in a manner consistent with international agreements, to which AR is a party to. Article 71 para 5. States that no provision of the Constitution may be interpreted in a manner to restrict or limit the rights and freedoms of a person. In accordance with para. 6, the rights and freedoms of a person are

directly in force in the territory of AR. All these once more approve that the human rights issues in AR is one of the main policy concerns.

2. AR provides an adequate level of protection by means of its Law on Personal data. The Law on Personal data sets out all the principles and rules in regard to processing that are found in EU laws. The scope of the rights granted under the Law is almost same to that granted under EU laws. The legislation of AR provides for effective remedies and sanctions for violations of right to privacy, in particular right to data protection. The laws provide for administrative, civil and criminal liability of perpetrators.
3. AR provides an adequate level of protection by means of its international commitments. AR is a party to CoE Convention 108, which forms a part of legislation of AR pursuant to article 148 of the Constitution.
4. The activities in sphere of intelligence, counter-intelligence and operational-activity are excluded from the scope of the Law on Personal data. However, these areas are regulated by specific laws and place adequate safeguards to enhance the protection of private and family data and to mitigate the potential risks of adverse effect.
5. The provisions for protection of personal data can be found in other legislative acts and norms, such as the Law on Mass Media, the Law on Freedom of Information, the Law on Information and etc.
6. The gaps, unclear provisions and other discrepancies can in no manner affect the adequacy of protection in AR. Such problems and unclear provisions are of a minor and individual character, which do not affect the overall picture of data protection in AR.

TABLE OF CASES

CJEU Cases

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado (C-468/10 and C-469/10) [2011] ECR 2011 I-12181.

Bodil Lindqvist [2003] (C-101/01) ECR 2003 I-12971, para 31.

European Commission v Federal Republic of Germany (C-518/07) [2010] ECR 2010 I-01885, para 27.

Productores de Musica de Espana v. Telefonica de Espana Sau (C-275/06) [2008] ECR 2008 I-00271

Volker and Markus Schecke Gbr and Hartmut Eifert v. Land Hessen (C-92/09 and C-93/09) [2010] ECR 2010 I-11063, para 48.

ECtHR Cases

Amann v Switzerland App no 27798/95 (ECHR, 16 February 2000), para 50.

Axel Springer AG v. Germany App no 39954/08 (ECHR, 7 February 2012).

Leander v Sweden App no 9248/81 (ECHR, 26 March 1987), para 58.

Mosley v. the UK App no 48009/08 (ECHR, 10 May 2011).

Peck v the United Kingdom App no 44647/98 (ECHR, 22 October 2002).

P.G. and J.H. v UK App no 44787/98 (ECHR, 25 September 2001), para 56.

Vereinigung bildender Kunstler v. Austria App no 68345/01, (ECHR, 25 January 2007).

Von Hannover v. Germany App no 40660/08 (ECHR, 7 February 2012).

TABLE OF LEGISLATION

International

Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR)

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR)

Council of Europe Convention for the Protection of Individuals with regard to automatic processing of personal data (opened for signature 28 January 1981, entered into force 1 October 1985) (Convention 108) art 4(1).

EU

Primary Law:

Consolidated Version of the Treaty on European Union [2008] OJ C115/13 (TEU), art 286.

Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C326/47 (TFEU), art 263(4).

Charter of Fundamental Rights of the European Union, [2012] OJ C 326/02, art 51 (Charter of Fundamental Rights).

Secondary Law:

Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (Data Protection Directive).

Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention [2000] OJ L316 (Eurodac regulation).

Council Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L8/1 (Community Institutions Regulation).

Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in electronic communications sector [2002] OJ L201/37 (E-privacy Directive).

Council Decision No 2007/533/JHA of 8 June 2004 establishing the Visa Information System(SIS) [2004] OJ L213 (Visa Decision), art 5.

Rules of Procedure No 2005/C 68/01 of 24 February 2005 on the Processing and Protection of Personal Data at Eurojust approved by the Council, OJ [2005] C 68/01 (Eurojust rules).

Council Decision No 2007/533/JHA of 22 June 2007 on the establishment, use and operation of second generation Schengen Information System(SIS) [2007] OJ L205 (Schengen II Decision), art 57.

Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime [2008] OJ L210/1 (Prüm Decision).

Council Decision No 2008/633/JHA of June 23 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, [2008] OJ L218.

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 [2008] OJ L350/60 (Council Framework Decision).

Council Decision of 6 April 2009 establishing the European Police [2009] OJ 2009/371/JHA (Europol Decision).

Council Decision No 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes [2009] OJ L323 (CIS Decision).

Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (General Data Protection Regulation).

Council Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89 (Police and Criminal Authorities Directive).

Commission Decision (EC) 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of

personal data provided by the Canadian Personal Information Protection and Electronic Documents Act [2002] OJ L2/13.

Working party opinions:

Article 29 Working Party Opinion 1/2010 of 16 February 2010 on the concepts of "controller" and "processor" 00264/10/EN WP 169.
Article 29 Working Party Opinion 4/2007 of 20 June 2007 on the concept of personal data 01248/07/EN WP 136.
Article 29 Working Party Opinion 15/2011 of 13 July 2011 on the definition of consent 01197/11/EN WP187.
Article 29 Working Party Opinion 03/2013 of 2 April 2013 on purpose limitation 00569/13/EN WP 203.
Article 29 Working Party Working Document of 24 July 1998 entitled “Transfers of personal data to third countries: Applying Articles 25 and 26 of the EC Data Protection Directive”. DG XV D/5025/98.

Azerbaijan:

“Dövlət qeydiyyatına alınması tələb olunmayan fərdi məlumatların informasiya sistemləri”nin təsdiq edilməsi haqqında Azərbaycan Respublikası Nazirlər Kabinetinin 2012-cu il 17 dekabr tarixli 237 nömrəli Qərarı.
“Fərdi məlumatlar haqqında” Azərbaycan Respublikası Qanununun tətbiq edilməsi barədə” Azərbaycan Respublikası Prezidentinin 2010-cu il 4 iyun tarixli 275 nömrəli Fərmanı.
Azərbaycan Respublikasının Cinayət Məcəlləsi. Bakı, 30 dekabr 1999-cu il №787-IQ.
Azərbaycan Respublikasinin Cinayət-prosessual Məcəlləsi. Bakı şəhəri, 14 iyul 2000-ci il № 907-IQ.
Azərbaycan Respublikasinin Əmək Məcəlləsi. Bakı şəhəri, 1 fevral 1999-cu il № 618-IQ.
Azərbaycan Respublikasının İnzibati Xətalar Məcəlləsi. Bakı, 11 İyul 2000-ci il № 906-IQ.

Azərbaycan Respublikasının Konstitusiyası. Bakı: Biznes xəbərləri, 2012.

Azərbaycan Respublikasının Mülki Məcəlləsi. Bakı şəhəri, 28 dekabr 1999-cu il, № 779-IQ.

Əməliyyat-Axtarış Fəaliyyəti haqqında Azərbaycan Respublikasinin Qanunu. Bakı, 28 oktyabr 1999-cu il № 728-IQ.

Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanunu. Bakı şəhəri, 11 may 2010-cu il № 998-IIIQ.

İnformasiya əldə etmək haqqında Azərbaycan Respublikasinin Qanunu. Bakı, 30 sentyabr 2005-ci il № 1024-IIQ.

Kəşfiyyat və əks-kəşfiyyat haqqında Azərbaycan Respublikasinin Qanunu. Bakı, 29 iyun 2004-cü il № 711-IIQ.

BIBLIOGRAPHY

(2017) <http://www.coe.int/en/web/conventions/full-list/ /conventions/treaty/108/declarations?p_auth=B7TntMsT> accessed 23 June 2017.

Bainbridge D and Platten N, *European Data Protection Directive* (Butterworths 1996)

Bygrave L, *Data Protection Law* (Kluwer Law International 2002)

'Commission Decisions On The Adequacy Of The Protection Of Personal Data In Third Countries - European Commission' (*Ec.europa.eu*, 2017) <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm> accessed 25 June 2017.

European Commission, Taking data protection into a digital and globalized era: Joint Statement by Vice-President Ansip and Commissioner Jourová ahead of the 2017 Data Protection day Brussels, 27 January 2017, STATEMENT/17/154, available at: http://europa.eu/rapid/press release_STATEMENT-17-154_en.htm [accessed 25 June 2017]

Full list, 'Full List' (*Treaty Office*, 2017) <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=B7TntMsT> accessed 23 June 2017.

Handbook On European Data Protection Law (Publications Office of the European Union 2014)

Hondius F, *Emerging Data Protection In Europe* (North-Holland Pub Co 1975)

Kilkelly U, *The Right To Respect For Private And Family Life* (Directorate General of Human Rights, Council of Europe 2001)

'Privacy And Human Rights - Overview' (*Gilc.org*, 2017) <http://gilc.org/privacy/survey/intro.html> accessed 25 June 2017.

'Read About "Right To Privacy" On Constitute' (*Constituteproject.org*, 2017) <https://www.constituteproject.org/search?lang=en&key=privacy> accessed 23 June 2017.

'Reform Of EU Data Protection Rules - European Commission' (*Ec.europa.eu*, 2017) <http://ec.europa.eu/justice/data-protection/reform/> accessed 28 June 2017

Roagna I, *Protecting The Right To Respect For Private And Family Life Under The European Convention On Human Rights* (Council of Europe 2012)

***

Cəfərov İM. Azərbaycan Respublikası Konstitusiyasının Şərhi. Bakı: Hüquq ədəbiyyatı, 2003, s 180.

Əsgərov ZA. Konstitusiya hüququ: Dərslik. Bakı: Bakı Universiteti nəşriyyatı, 2006, s102.

Azərbaycan dilinin izahlı lüğəti. Dörd cilddə. I cild. Bakı: Şərq-Qərb, 2006, s 251.

Xropanyuk VN. Dövlət və hüquq nəzəriyyəsi (ixtisarla). Bakı: Qanun, 2007, s 223.

Tağıyeva GZ. Mülki hüquq məsuliyyəti və onun nəzəri-təcrübi problemləri // Dövlət və hüquq. Elmi-nəzəri metodik jurnal, Bakı, 2003, № 5-6, s 104.

ANNEX

Abstract.

Title:

Comparative analysis of data protection systems and regulatory approaches in Azerbaijan and EU.

Rapid expansion of information technologies nowadays, their penetration in all spheres of life, collection and processing of personal data through the use of new technologies makes inevitable to ensure the protection of personal data on the international and regional level. Therefore, I would like to write a thesis in the sphere of data protection law. To be more certain, my main intention is to make a comprehensive and detailed analysis of data protection systems, respective laws and regulatory approaches in AR and EU.

The main purpose of this thesis is to assess the adequacy and sufficiency of data protection in Azerbaijan. To this end, the following tasks are to be undertaken:

1. To analyze the right to privacy and right to data protection in relation to each other;
2. To assess the Data Protection Laws of EU in a detailed and comprehensive manner;
3. To examine Data Protection Laws of Azerbaijan ;
4. To evaluate the adequacy of protection of data in Azerbaijan in comparison with EU;
5. To analyze the possibility and future perspectives of development of Data Protection Systems in Azerbaijan based on evaluation of adequacy.

First and foremost, the research focuses on the definition and notion of right to privacy which is a fundamental human right. Here the main question is what is “the right to data protection” in the light of general right to privacy. The second question is the role of international organizations in creation of instruments to ensure the right to data protection.

In analysis of respective data protection systems in EU and Azerbaijan, I will focus first of all, on the purposes and scope of respective data protection laws. The analyzed legal issues shall cover the main legal definitions in laws, the core principles of data processing, the main rules of data processing, the rights of data subject, and rules for promoting compliance. Due regard shall be given to grounds for lawful processing of data and in particular, sensitive data. As far as rights of the data subject are concerned, the analysis shall focus on rights such as right to access, right to object to "profiling" and processing for marketing purposes, as well as right to legal remedies. In addition, the thesis shall emphasis on the rules for promoting of compliance, such as the authorization by relevant authorities, institutional support and sanctions. The due attention has to be given to the rules of transfer of data to other states.

The adequacy of protection in AR shall be evaluated in the light of Adequacy Decisions of Commission, the opinions of Article 29 Working Party, as well as based on all the legal issues and criteria (core principles, rules, rights of data subject, rules of compliance and etc.) analyzed in respective laws of both jurisdictions. Finally, based on the evaluation of data protection system in AR, the research will try to make assumptions about possible improvements and development of data protection systems in Azerbaijan.

Vorschläge für Masterarbeiten.

Titel:

Vergleichende Analyse der Daten-Schutz-Systeme und Regulierungsansätze in Aserbaidschan und der EU.

Die heutzutage rasche Expansion der Informationstechnologien, deren Eindringen in allen Bereichen des Lebens, Erhebung und Verarbeitung personenbezogener Daten durch den Einsatz von neuen Technologien macht es unumgänglich, den Schutz von personenbezogenen Daten auf internationaler und regionaler Ebene zu gewährleisten. Daher möchte ich eine Abschlussarbeit im Bereich des Datenschutzgesetzes verfassen. Mein wichtigstes Ziel ist es daher, eine umfassende und detaillierte Analyse der Daten-Schutz-Systeme, entsprechende Gesetze und Regulierungsansätze in der AR und der EU durchzuführen.

Das Anliegen dieser Arbeit ist die Beurteilung der Angemessenheit des Datenschutzes in Aserbaidschan. Zu diesem Zweck sind die folgenden Aufgaben durchzuführen:

1. Analyse des Rechts auf Privatsphäre und Recht auf Datenschutz im Verhältnis zueinander;
2. Daten-Schutz-Gesetze der EU auf eine detaillierte und umfassende Weise beurteilen;
3. Daten-Schutz-Gesetze von Aserbaidschan überprüfen;,
4. Die Angemessenheit des Schutzes der Daten in Aserbaidschan im Vergleich zur EU bewerten;
5. Die Möglichkeit und Perspektiven der Entwicklung des Datenschutz-Systems in Aserbaidschan analysieren, basierend auf der Beurteilung der Angemessenheit.

In allererster Linie, konzentriert sich die Forschung auf die Definition und den Begriff des Rechts auf Privatsphäre wie ein grundlegendes Menschenrecht. Hier ist die wichtigste Frage: Was ist "das Recht auf Datenschutz" im Lichte der allgemeinen Recht auf Privatsphäre? Die zweite Frage ist die Rolle der internationalen Organisationen bei der Schaffung von Instrumenten für das Recht auf die Gewährleistung des Datenschutzes.

In der Analyse der jeweiligen Datenschutzsysteme in EU und Aserbaidschan konzentriere ich mich zunächst über den Zweck und Umfang der jeweiligen Datenschutzgesetze. Die analysierten Rechtsfragen umfassen die wichtigsten rechtlichen Definitionen in Bezug auf Gesetzen, den Grundprinzipien der Datenverarbeitung, den wichtigsten Regeln der Datenverarbeitung, den Rechten der betroffenen Person und Regeln für die Förderung der Grundregeln. Insbesondere sollte man Rücksicht auf die Gründe der rechtmäßigen Verarbeitung der Daten und besonders den sensiblen Daten geben. Soweit wir über die Rechte der betroffenen Personen diskutieren möchten, konzentrieren wir uns auf die Analyse der Menschenrechte wie z.B. Recht auf Zugang, Widerspruchsrecht gegen Verarbeitung zu Marketingzwecken sowie Recht auf Rechtsmittel. Darüber hinaus wird die These auf den Regeln für die Förderung der Einhaltung etwa von der Genehmigung durch die zuständigen Behörden, institutionelle Unterstützung und Sanktionen betont. Besondere Aufmerksamkeit muss man den Regeln der Weitergabe der Daten an andere Staaten geben.

Die Angemessenheit des Schutzes in der AR soll im Lichte der Angemessenheit Entscheidungen der Kommission, der Meinungen der Artikel 29 Working Party, sowie basierend auf den rechtlichen Fragen und Kriterien, die bei der Beurteilung der jeweiligen Gesetze der beiden Länder herausgefunden werden, ausgewertet werden. Schließlich, basierend auf der Auswertung des Daten-Schutz-Systems in AR, versucht die Forschung Annahmen über mögliche Verbesserungen und Entwicklung von Daten-Schutz-Systemen in Aserbaidschan durchzuführen. analysiert (Kernprinzipien, Regeln, Rechte der betroffenen Person, Regeln der Compliance usw.)