American University of Armenia
Law Department

Master's Paper

European Integration: Data protection as one of the pre-conditions for visa facilitation program in Armenia

Instructor: Mr. Armen Mazmanyan

Student: Ms. Margarita Galstyan,
LL.M second year

Yerevan, 2011

Table of Content

Introduction

Today the Armenian foreign policy and particularly European integration of Armenia and EU-Armenian relations are much talking about. The first legal document as a framework for EU-Armenian bilateral relations was Partnership and Cooperation Agreement (PCA), signed in 1996 and entered into force on July 1, 1999. Based on the PCA relations in the areas of political dialogue, trade, investment, economic, legislative and cultural cooperation were developed. Following the enlargement of the European Union, EU launched the European Neighborhood Policy (ENP) which was aimed to deepen the cooperation with non-EU Member States. By the decision taken by the European Council on 14th June 2004, the Southern Caucasus countries were incorporated into the framework. Based on this the Presidential decree was signed in November 14, 2006 adopting ENP Action Plan.

On July 19, 2010 EU and Armenia launched negotiations on EU-Armenia Association Agreement (AA). The Agreement is going to replace the PCA as the formal legal ground for EU-Armenia relations.

According to the EU Council regulation 539/2001 of March 15, 2001 Armenia is included in the Annex I (the so-called "positive list") which lists the countries and territories, the nationals of which "shall be required to be in possession of a visa when crossing the external borders of the Member States."[1]

Compared to the relatively active cooperation between the EU and Armenia on trade-related issues, the visa dialogue, despite the fact that is being mentioned in all framework documents on the EU-RA partnership, has hardly seen any development until very recent times. A real step in this area was the first meeting on EU-Armenia Association Agreement negotiating sub-committee on "Justice Freedom and Security" chapter (July 6, 2010). During the meeting beside the discussed issues on the security of travel documents and data protection, migration management, combating

[1] Council Regulation (EC) No 539/2001 of 15 March 2001

illegal migration, border management, EU side emphasized that the negotiating directives for visa facilitation and readmission agreements would be prepared by the end 2010.[2]

The following areas have been mentioned as a priority for visa liberalization:

- Document Security: this includes data protection and mainly emphasized by the introduction of electronically enabled machine-readable passports with biometric features and electronic ID Cards. Pace of the activities on introduction of biometric documents has to be coordinated with other related reforms, such as civil registry modernization and data protection
- Illegal Migration
- Public order and security
- External Relations and Fundamental Rights. [3]

The data protection is a complex system, which involves a number of related fields. It includes elements of such fundamental rights as freedom of information, right to privacy etc. A characteristic feature for data protection is that it relates to different branches of law and has a significant impact on economic and social activities as well (free trade area, free movement of goods, services etc). It has a significant importance in working relations and there are separate regulations, both national and international, for personal data protection in working relations. Data protection is highlighted in the international environment, as a part of cyber security. Special mechanisms are presented to data protection in fight against cyber terrorism and e-privacy. In all these fields a requirement of personal data protection must be satisfied.

The second article of the Justice Freedom and Security chapter of the AA states as follows: "The Parties agree to cooperate in order to ensure an adequate level of protection of personal data in accordance with the highest European and international standards, including the relevant Council of Europe instruments".

[2] Visa Liberalization Baseline Study: Armenia, http://novisa.com.ua/upload/file/ArmeniaBaselineStudy.pdf

[3] Visa Liberalization Baseline Study: Armenia, http://novisa.com.ua/upload/file/ArmeniaBaselineStudy.pdf

As it can be inferred from the preamble and the structure of the EU main legal document on personal data protection, EU directive 95/46/EC on "Protection of individuals with regard to the processing of personal data and on the free movement of such data", the main requirements for ensuring adequate level of personal data protection are presented for the legitimate collection and processing of personal data, for creating more effective protection mechanisms and for the development of the conditions for secure transfer of personal data.

Based on the above mentioned, it is essential to explore whether Armenia meets the EU requirements on data protection. For this purpose three issues will be discussed in the paper:

1) Collection and processing of personal data,

2) Data protection authorities and

3) Transfer of data to third countries.

Chapter 1

Collection and processing of personal data

Data protection, as a fundamental right, has emerged relatively later than many of other widely accepted rights. It became, and still remains, in close relation with other fundamental rights and freedoms, such as right of a person to private life, freedom of information, right to the limitation on personal data, right to anonymity, etc. These all has got more importance and need for due regulation as the use of Internet in everyday life and other IT equipments enables collection and transfer of any kind of information, as well as personal data, more than easy and fast.

The Council of Europe Convention "For the protection of individuals with regard to automatic processing of personal data" of 28.Jan.1981 can be considered as the first European legal instrument for the right to protection of personal data.

The right to data protection is closely related but not identical with the right to private life under Article 8 of the European Convention on Human Rights.

Data protection as a fundamental right is stipulated by the Art 8 of the Charter of Fundamental Rights of the European Union (hereinafter Charter). This is the first time that data protection right is not presented as a part of right to privet and family life or as an extension of the right to secrecy.

Right to data protection involves elements of several rights, which are in some instances confronting to each other (e.g. on the one hand right to privacy and on the other freedom of information): the line between them is quite delicate.[4]

In the European Union these and other rights and obligations on data protection are mainly regulated by the EU directive 95/46/EC of October 1995 on "Protection of individuals with regard to the processing of personal data and on the free movement of such data" (hereinafter Directive).

[4] Directive 95/46/EC of 24 October 1995, Art 9 of it states that Member States shall provide for exemptions or derogations from general rules for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

The Directive enshrines two of the oldest and equally important ambitions of the European integration process: the protection of fundamental rights and freedoms of individuals and in particular the fundamental right to data protection, on the one hand, and the achievement of the internal market – the free flow of personal data in this case – on the other.[5]

The main principles of the directive are that the collection and processing of personal data, the purposes of processing of that data should be legitimate, the data should be necessary and sufficient for the purpose they are collected. The data processing can be legitimate only if it is made according to the provisions set by the Directive.

According to the art 2.a of the Directive "personal data" shall mean any information relating to an identified or identifiable natural person ('data subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. From the informative point of view "personal data" includes both "objective" information (e.g. date of birth or other facts) and "subjective" information (e.g. opinions).

The data subject at least shall know what kind of data is being collected and what the purpose of processing of that data is. Transparency is an essential condition for enabling individuals to exercise control over their own data and to ensure effective protection of personal data. It is therefore essential that individuals are well and clearly informed, in a transparent way, by data controllers[6] about how and by whom their data is being collected and processed, for what reasons, for how long and what their rights are if they want to access, rectify or delete their data.

This principle is assured by the right of data subject to obtain any collected personal data at any time and by the obligation of the controller or his representative at the time of undertaking the

[5] Communication From the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions; A comprehensive approach on personal data protection in the European Union; Brussels 4.11.2010, COM(2010)609 Final,
http://ec.europa.eu/health/data_collection/docs/com_2010_0609_en.pdf

[6] "Data controller shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data…" art 2.d of the EU Directive 95/46/EC of 24 October 1995

recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed, provide the data subject with required information, if the data have not been obtained from the data subject.[7] Basic elements of transparency are the requirements that the information must be easily accessible and easy to understand, and that clear and plain language is used. This is particularly relevant in the online environment, where quite often privacy notices are unclear, difficult to access, non-transparent and not always in full compliance with existing rules.

The right to be informed (access to the data) and right to make a decision is in close conjunction with the principle of transparency. Article 8(2) of the Charter states that "everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified". Individuals should always be able to access, rectify, delete or block their data, unless there are legitimate reasons, provided by law, for preventing these. Decision-making is first explored by the data subject consent on processing the personal data. The current rules provide that the individual's consent for processing his or her personal data should be a "freely given specific and informed indication" of his or her wishes by which the individual signifies his/her agreement to this data processing.[8] If the processing of data is not in accordance with the principles of data protection then data subject has the right to demand correct, delete or not to use that data. Data processing also must be terminated if the processed data is not necessary anymore for the purpose it has been collected for. Moreover the data subject has the right on objection on the legitimate processing of their personal data, if there are sufficient grounds for objection.[9]

It is also important for individuals to be informed when their data are accidentally or unlawfully destroyed, lost, altered, accessed by or disclosed to unauthorised persons. The recent revision of the e-Privacy Directive introduced a mandatory personal data breach notification covering, however, only the telecommunications sector.[10]

[7] EU Directive 95/46/EC of 24 October 1995, art 11
[8] EU Directive 95/46/EC of 24 October 1995, art 2(h)
[9] EU Directive 95/46/EC of 24 October 1995, art 14
10.Communication From the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions; A comprehensive approach on personal data protection in the European Union; Brussels 4.11.2010, COM(2010)609 Final

Art. 8 of the Directive regulates processing special categories of data (sensitive data). The provisions of the article prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life, except cases stated in the article (explicit consent of data subject, employment law, purposes of preventive medicine, medical diagnosis, etc.).

Though the Directive states wide rights for the data subject, art 13 of it gives exhausted list when these rights can be restricted by the Member States: for the purpose to safeguard national security, defense, public security, protect the data subject or rights and freedoms of others, etc.

Another set of requirements of the Directive are addressed to the confidentiality and security of the processing personal data. Any person who has legitimate access to the personal data (including processor himself) must not process them except on instructions from the controller, unless he is required to do so by law. It is obligatory for Member States to ensure that the controller implements appropriate technical and organizational measures for protection of personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, especially in cases of the transmission of data over a network and against all other unlawful forms of processing. In this regard such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.[11]

For ensuring the rights provided by the Directive, it also allocates the institute of effective remedies. By the art 22, beside the other remedies that can be provided by the Member States, the judicial remedy for any breach of the rights shall be guaranteed. Also compensation shall be provided by the controller to any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted in accordance with the Directive.

Of course the Directive as a main instrument for data protection, gives framework of the concepts in the EU, leaving room of flexibility to Member States. Also many specific and narrow issues are

---

[11] See Art 17 of the DIRECTIVE 95/46/EC of 24 October 1995.

regulated by other documents. Moreover there are situations falling outside the scope of the Directive especially in the relations with third countries (non-EU State).

To discuss the Armenian prospective of the data protection first of all a reference should be done to the Constitution of the Armenia. Art 23 of the Constitution states as follows:

"Everyone shall have the right to respect for his private and family life.

The collection, maintenance, use or dissemination of any information about the person other than that stipulated by the law without the person's consent shall be prohibited. The use and dissemination of information relating to the person for purposes contravening the aims of their collection or not provided for by the law shall be prohibited.

Everyone shall have the right to become acquainted with the data concerning him/her available in the state and local self-government bodies.

Everyone shall have the right to correction of any non-verified information and elimination of the illegally obtained information about him/her…." [12]

After the Constitutional Amendments of the Republic of Armenia in 27.11.2005, the Constitution clearly gives data protection as a fundamental right, stated all elements that are necessary for the comprehensive realization and protection of that right[13]. But it is to be mention that Constitution gives declarative rights and for practical realization of that rights laws and other legal acts should be adopted.

Referring to the realization of the right to data protection, it is seen that the RA legislation does not fully reflect the international principles for data protection. RA Law on "Freedom of Information" (RA Law -11, 22.10.2003) and RA Law on "Archives Business" (RA Law -88, 01.07.2004) and RA Law on "Social Security Cards" (RA Law -1-N, 08.10.2003) include provisions relating to data protection.

[12] Constitution of the Republic of Armenia, as amended 27.11.2005

[13] Before the amendments, the RA Constitution only gives some elements for data protection, stressing the right to privet and family life (art 20 of the RA Constitution before the amendments).

RA Law on "Freedom of Information" mainly regulates the relations concerning the freedom of information, which defines the powers of persons holding (possessing) information, as well as the procedures, ways and conditions to receive information.[14] It relates to data protection in few provisions, stating refusal to provide data which infringes the privacy of a person and his family as one of the limitations for freedom of information.[15] Here, the data protection is presented in the scope of the right to privet and family life, though these two rights are separately presented in the RA Constitution and data protection is much wider then private and family life.

The same situation is with the RA Law on "Archives Business". Art 22 (3) of the RA Law on "Archives Business" restricts the access to the use of archival documents containing secret personal and family information for 100 years since their creation and that such documents can be disclosed only by the written permission of a person (data subject) or his heirs or court ruling.

Art 5 of the RA Law on "Social Security Cards" stipulates that the purpose of creating the system of social cards is the identification of the citizen during the process of personal data processing in the information systems … ensuring the protection of confidentiality of personal data of a citizen. Social card is a document provided to a citizen, which guarantees the exercise of the social security rights of citizens.[16] The informative database is being crated according to the presented information by citizens and state authorities and includes the following information: name, surname, date of birth, sex, in case of death the date of death. The privacy of the presented personal data must be protected according to the RA legislation.[17]

The main law that regulates collection and processing of personal data is RA Law on "Personal Data" (RA Law-422, 22.11.2002) (hereinafter Law), which regulates relations connected with the processing of personal data by state and self-governance bodies, state and community institutions, legal entities or natural persons.

[14] Art 1 of the RA Law on "Freedom of Information"
[15] Art 8 point 1.b of the RA Law on "Freedom of Information"
[16] RA Law on "Social Security Cards" 08. 10.2003, art 3(1)
[17] RA Law on "Social Security Cards" 08. 10.2003, art 7

Another legal instrument that is worth to be discussed, simultaneously with the RA Law on "Personal Data", is a Draft Law RA Law on "Protection of personal data" (hereinafter Draft Law) which reflects the RA Constitutional principles on data protection.

The rational of parallel analyses of two mentioned legal instruments, is that the Draft Law law will replace the current Law after entering into force. The Draft Law on "Protection of personal data" has already been submitted to the RA government, and it will be presented to the RA National Assembly in near future.

The purpose of the drafting new law is to have a legal act which will reflect international and especially EU standards and requirements on personal data protection, which is driven by the Armenian foreign policy toward European Integration. But as the research has shown, during the drafting, Armenian experts has used mainly Russian sources.

The comparison of two documents shows that in contrast to the acting Law, the Draft Law, though includes main principles of the acting Law, provides with wider rights to persons whose personal data is being collected and processed, clearly states the obligations of the state authorities, and what is more significant, it stipulates creation of data protection mechanism. But there are also some provisions that are better stipulated by the acting Law. The definition of personal data can be the as an example.

The art 3(a) of the acting Law defines personal data as any data recorded on medium containing facts, events and circumstances about the person, in a form that allows or may allow identifying the person. While the Draft Law define personal data as information on facts, events, circumstances which concerns a natural person where presented in a form that allows or may allow to directly or indirectly identify the natural person in question. [18] By this provision the scope of the personal data is narrowed than it is both in the acting Law and Directive, which defines "personal data" as any information, and it can be both subjective and objective one. By the given definition of the Draft Law certain amount of information falls outside of its scope.

[18] The Draft Law RA Law on "Protection of personal data" art 3 point 1 of

One of the important elements that should be stressed is that neither the acting Law, nor the Draft Law gives the distinction between the controller and processor of data. According to the art 2.d and 2.e of the Directive respectively "the controller shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data", and the "processor shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller".

It is clear, that these two definitions are different (have different functions) and the distinction is needed in cases where one has a legal ground for processing personal data, but it does not process data for itself.[19]

Giving the principles for personal data processing both Armenian legal acts states that data shall be collected and processed lawfully; it shall be collected for clearly specified or declared legitimate purposes and shall not be used for other purposes.

The transparency principle and access to the data provided by the Directive, in some instance, are reflected in the art 11 of the Law, provisions of which are more widely elaborated in the art 13(1) of the Draft Law, stating that data subject shall have the right to receive information about data processor, data processor's location and his/her possession of data subject's personal data, as well as the right to access the said personal data.... Data subject shall have the right to request the processor to modify his/her data, block access to it or destroy it, if the personal data are not complete, are inaccurate, outdated, acquired by illegal means or are not necessary to achieve the goals of processing." Based on the written request of the data subject the processor shall provide information about the existence of personal data to data subject in an accessible form. Data subject shall have the right to receive information about the processing of his/her personal data on the following; confirming the fact of personal data is being processed and goals of such processing,

[19] Typical examples are outsourced services, such as recruitment of personnel, book-keeping, training of employees and officials, medical services, IT-services. It seems that these relationships are covered by art 9 of the Law and art 12 of the Draft Law "Personal Data Processing at a Third Party Request". In that case third party (customer) in the mentioned articles means the same as controller in the sense of the Directive.

ways of personal data processing, subjects who have received or may receive personal data, list of personal data being processed and sources from which such data was obtained, time periods for the processing and storing of personal data, potential legal consequences of personal data processing for data subject.[20]

In contrast to the acting Law the data subjects' right to be informed is more efficiently prescribed by the provision of the Draft Law obligating the processor to provide requested information. If personal data were received not from data subject, except the data provided to processor on the basis of the law, as well as publicly accessible data, then the processor should be required to provide the data subject name of the processor or its legal representative (last name, first name and patronymic) and address, purpose and legal grounds for personal data processing, suggested users of personal data prior to processing such data, rights of data subject prescribed by law.[21] Like the acting Law, the Draft Law also stipulates the consent requirement. But the main difference here is that according to art 8 of the Draft Law, the personal data can be processed based on the explicit consent of the data subject, which shall be provided in the written form. The data subject can always withdraw his/her consent.

Unlike the acting Law, the Draft Law gives the definition of special category of personal data, which is personal data concerning an individual's racial or ethnic origin, political views, religious or philosophical convictions, membership in specialized organizations, health status and intimate life.[22] Art 9 of the Draft Law stipulates the exceptions when special category of personal data can be processed. In general, the exceptions conform to the requirements of the art 8 of the Directive, but there is a difference that worth to be stressed. One of the exceptions is processing of special category of personal data if that data is publicly accessible (point 2.2). The Directive clearly mentions that processing is allowed when data, had been publicized by the data subject (art 8.e), while the Draft Law doesn't give any clarification on this.

[20] Still the point 7 of art 13 states that the Data subject's right to receive information about his/her personal data may be limited only in cases directly defined by a law

[21] The Draft Law on "Protection of personal data", art 16

[22] The Draft Law on "protection of personal data", point 13 art 3

The confidentiality and security of the processing personal data are regulated by the provisions stipulating that the personal data administered by the data processor shall be confidential information and the processor shall be required to take relevant organizational and technical measures to protect information systems containing personal data from accidental loss, unauthorized access, unauthorized use, destruction, modification, blocking, copying, dissemination and other unlawful activity while processing personal data (art 10 of the Law and art 6, 17 of the Draft Law).

In contrast to the art 14 of the acting Law, the Draft Law provides the data subject with wider right to appeal, against actions or inaction of data processor , if data subject thinks that processor is processing his/her personal data in violation of the Law or is violating his/her rights and liberties in any other way.[23] This right is verified by the second provision of the art 15, which states that the data subject shall have the right to compensation for damages according to the law.

[23] Art 15 of the Draft Law

Chapter 2

Data protection authorities

The implementation and enforcement of data protection principles and rules is a key element in guaranteeing respect for individuals' rights. For that purpose art 28 of the Directive set a requirement for each Member State to establish one or more public authorities which will be responsible for monitoring the application of provisions adopted by the Member States pursuant to the Directive within its territory. These authorities shall act with complete independence and have wide range of powers in exercising the functions entrusted to them. As a supervisory body the authority shall be endowed with investigative power, such as powers of access to data, power to engage in legal proceedings, or to bring violations of data protection provisions to the attention of the judicial authorities, hear claims lodged by any person concerning the protection of his rights and freedoms in regard to the processing of personal data, etc.

The most important element for the data protection authority is the "complete independence" that must be ensured by the Member State. The guarantee of independence is intended to ensure the effectiveness and reliability of the supervision of compliance with data protection provisions, to strengthen the protection of individuals and bodies affected by their decisions.

While giving the mining of the "complete independence" the ECJ, in case Commission v. Germany, stated that independence normally means a status which ensures that the body concerned can act completely freely, without taking any instructions or being put under any pressure.[24]

The adjective "complete" implies a decision-making power independent of any direct or indirect external influence on the decision-maker. Data Protection Authorities must act impartially and must remain free from any external influence, including that of the State or Lander, and not of the influence only of the supervised bodies. Independence precludes not only any influence exercised by supervisory bodies, but also any directions or other external influence which could call into

[24] ECJ judgment of 9.3.2010, Commission v. Germany, Case C-518/07
http://ec.europa.eu/dgs/olaf/data/doc/Summary-caselaw-EU-courts.pdf

question performance of those authorities of their task consisting of establishing a fair balance between the protection of the right to private life and the free movement of personal data.[25]

The Directive requires supervisory authorities of Member States to cooperate with each other. The role of effective cooperation is especially highlighted in issues which, by their nature, have a cross-border dimension (e.g. where multinational enterprises are based in several Member States and are carrying out their activities in each of these countries).[26]

Proceeding to Armenian prospective on the issue, it is important to state that the establishment and functioning of data protection authority is provided by the art 21 of the Draft Law, which says that control over compliance with the requirements of the Law shall be exercised by the personal data protection inspection, operating within the national executive body system. The article provides almost all powers that are defined by the Directive: inspect the compliance of personal data processing with the requirements of the Law, request processor to correct, block or destroy personal data, if there are legal grounds for doing so, protect data subjects' rights and defend their interests in courts, etc.[27]

Furthermore, the Draft Law requires the data protection inspection to ensure the protection of data subjects' rights, keep a data processors' register, and maintain the confidentiality of the personal data that became available to it in the process of its activities. The decisions of the data protection authority can be appealed in the court.

While the Draft Law provides the data protection authority with these rights and duties for insuring proper protection of persons' rights involved in data protection, the most important requirement for the authority: the independence, is not provided. The essential requirement set by the Directive, to ensure the "complete independence" of the authority. The Draft Law states that the authority will

[25] ECJ judgment of 9.3.2010, Commission v. Germany, Case C-518/07

[26] Communication From the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions; A comprehensive approach on personal data protection in the European Union; Brussels 4.11.2010, COM(2010)609 Final

[27] The Draft Law on "Personal data protection", art 21

operate within the national executive body. The question is whether the independence can exist when the authority is under the subordination of executive body. This means that the decisions taken by the authority can be instructed and revised by the subordinating body. While, according to the ECJ judgment on Commission v. Germany[28], the independence of the authority is defined by 2 elements: "to act completely free" and "decision-making power". The authority to be considered independent should have the opportunity to act free, without any instructions and be able to make decisions, independent of any direct or indirect external influence of the supervisory authority. Furthermore the decision of the independent authority should not be revised by any other state authority except courts. It is obvious: establishing data protection authority under subordination of executive body, will deprive it form any independence. Moreover, according to the expert from the RA Police Legal department Nelly Manandyan (the member of working group drafting the RA Law on "Protection of Personal Data"), the potential executive body to supervise the data protection authority is the Police at the RA Government.[29] In this situation the question will be whether an authority at the Police (military service), will have any kind of independence, let alone the requirement of complete independence.

[28] ECJ judgment of 9.3.2010 in Commission v. Germany, Case C-518/07
[29] Nelly Manandyan. Personal Interview. 03. Mar.2011.

Chapter 3

Transfer of data to third countries

The preamble of the Directive states that the existing regulatory differences among EU Member States, as well as third countries on the data protection and right to secrecy, may deter the flow of information among Member States and third countries. In order to eliminate any obstacles on data flow among EU Member States, as well as with third countries, same principles and mechanisms for collecting, processing and transferring personal data should be adopted.

The data collection is a part of almost all transactions both in public and privet life. A simple example of that can be providing of personal information while using discount card in the shop (name, address, contacts, etc.). A personal data is collected while registering for an e-mail address in a web-site, and filling in an application form for getting entrance visa permission to a third country. In provided examples collected personal data is involved in trans-boarder transactions. The data subject should be sure that the collected data won't be used in other purposes that it was collected neither in the country of origin nor in the other country. Otherwise the data subject can refuse to get into transactions. Even though the data subject might be not aware of safeguards on data protection, the data controller (privet company or public authority) should undertake all necessary measures to insure that principles.

As the public authorities are called to protect rights and freedoms of individuals, they should ensure that the personal data transferred to third countries will be as protected as in the country of origin.

One of the means of enabling the transfer of personal data inside and outside EU is the so-called 'adequacy assessment'. Art 25 of the Directive provides princiclpes for the transfer of data to third countries, stating that transfer may take place only if the third country in question ensures an adequate level of protection. According to art 25(2): the adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country

of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied within that country.

Currently, the adequacy of a third country – i.e., whether a third country ensures a level of protection that EU considers as adequate – may be determined by the Commission and by Member States. But the assesment approach may very form Member State to third country or different International organizations.

For the assessment of adequacy, the Commission has adopted several decisions setting standard contractual clauses for the transactions of transferring personal data to controllers and to processors. However, Art 26(2) of Directive provides that Member States may authorize, subject to certain safeguards, a transfer or a set of transfers of personal data to third countries which do not ensure an adequate level of protection. Such safeguards may in particular result from appropriate contractual clauses, which are standard contractual clauses and relate only to data protection. [30]

On February 5, 2010 the Commission adopted a decision on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, which is the latest document on the subject.

Under these clauses the data exporter shall ensure that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law. The data importer will provide sufficient guarantees in respect of the technical and organizational security measures, ensuring that they are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing, especially where the processing involves the transmission of data over a network. The data subject should has been, or must be informed as soon as possible, about transfer of data especially if the transfer involves special

30 Commission decision on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ L 39, 12.2.2010)

categories of data where his or her data could be transmitted to a third country not providing adequate level of protection within the meaning of the Directive.[31]

Another set of obligations is presented to the importer of personal data. The importer shall process the personal data only on behalf of the data exporter and in compliance with its instructions and the standard clauses. In the case when it cannot provide such compliance for whatever reasons, the importer agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract, implement required technical and organizational security measures before processing the personal data transferred. Importer shall promptly notify the data exporter about any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, any accidental or unauthorized access etc.[32]

Clause 11 of standard contractual clauses states that the data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the clauses, without the prior written consent of the data exporter. The subcontract can be concluded only in written form and in the manner that the sub-processor shall have the same obligations as the data importer. Where the sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such contract.

The standard contractual clauses also provide safeguards for personal data protection after the termination of the data processing services. According to clause 12 of the standard contractual clauses, on the termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and

[31] Commission decision on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ L 39, 12.2.2010), Clause 4
[32] Commission decision on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ L 39, 12.2.2010), Clause 5

the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so.

For the protection of data subject rights, the data subject who has suffered damage as a result of any breach of the obligations, by any party or sub-processor, is entitled to receive compensation from the data exporter for the damage suffered.[33]

A new challenge for EU and many of the States in ensuring data protection is transfer of the passenger name record (PNR) data to third countries. This issue especially got an importance when the fight against terrorism became global concern in the international arena.[34]

The terrorist attacks of the last decade (USA 2001, Madrid 2004, London 2005, etc), led to new approach in the internal policies of the states.

PNR data is unverified information provided by passengers and collected by carriers for enabling reservations and carrying out the check-in process. It is a record of each passenger's travel requirements held in carriers' reservation and departure control systems. It contains several different types of information, for example dates of travel and travel itinerary, ticket information, contact details like address and phone numbers, travel agent, payment information, seat number and baggage information.[35]

The EU took a challenge on setting out the elements of a global EU approach on PNR and legally secured framework for PNR transfers. The result was the Communication of the Commission on 16 January 2003 to the Council and the Parliament on the Transfer of Air Passenger Name Record (PNR) Data.

The EU signed an agreement with the U.S. Department of Homeland Security for the transfer of PNR data in the interest of the fight against terrorism and serious transnational crime, which enables transfer of PNR data with proper protection of personal data. In addition the Commission

[33] Commission decision on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ L 39, 12.2.2010), Clause 6

[34] Communication from the commission on the global approach to transfer of passengers name records data to third countries, Brussels 21.09.2010, COM(2010) 492 final

[35] Communication from the commission on the global approach to transfer of passengers name records data to third countries, Brussels 21.09.2010, COM(2010) 492 final

adopted a proposal for a Framework Decision for the use of PNR data for law enforcement purposes. The Commission is currently examining, on the basis of an impact assessment, the possibility of replacing it with a proposal for a Directive on the use of PNR data for law enforcement purposes. In addition to the agreement with the US, the EU signed similar agreements with Canada and Australia. New Zealand, South Korea and Japan are also using PNR data but haven't signed agreements with EU yet. Until today, the conclusion of international agreements with third countries on PNR was "demand" driven and dealt with on a case-by-case basis. Even though all the agreements address common issues and regulate the same matters, their provisions are not identical. [36]

These developments indicate that the use of PNR data is growing and is increasingly seen as mainstream and necessary aspect of law enforcement work. At the same time, the use of PNR data involves the processing of personal data which raises important issues with respect to the fundamental rights to the protection of private life and to the protection of personal data.

PNR data is unique in its nature and its use. The main purposes to use PNR are the risk assessment of passengers and identification of "unknown" persons, i.e. persons that might

potentially be of interest to law enforcement authorities and who were so far unsuspected, identification to which persons belong specific addresses, credit cards etc, that are connected to criminal offences, and matching of PNR against other PNR for the identification of associates of suspects, for example by finding who travels together.

The collection and transfer of PNR data to third countries affects a very large number of individuals and their personal data. Thus, particular attention must be paid to the effective protection of personal data. The EU data protection laws do not allow carriers operating flights from EU to transmit the PNR data of their passengers to third countries which do not ensure an adequate level of protection of personal data, without adducing appropriate safeguards.

[36] Communication from the commission on the global approach to transfer of passengers name records data to third countries, Brussels 21.09.2010, COM(2010) 492 final

The adequate level of data protection is evaluated based on the legal regulations of third countries and compliance with international standards set by international instruments ratified by them.

Armenia has ratified some bilateral and multilateral agreements on transfer of information but they are either on criminal or civil matters. Concerning to the national legislation, the situation is not better. Art 13 of the RA Law on "Personal Data" states that the personal data can be transferred to the third countries based on the international treaties of Armenia and based on the legality provisions of the Law on the processing of personal data (the personal data is processed with the consent of the data subject; processing is envisaged by legislation or is necessary for law enforcement, processing of the personal data is required for the protection of state and public security, etc).[37]

The Draft Law on "Protection of Personal Data" includes no provisions on transfer of personal data to third countries.

The mentioned provision does not give practical mechanisms of transferring personal data to third countries, living the more detailed regulation to international agreements. Only a few governmental decrees has been adopted which also don't cover all aspects of the transfer of personal data and PNR.

One of them is the RA government decree 884-N of 22.06.2006 on "Establishing and Implementing the System of Informative Electronic Boarder Management" (hereinafter Decree). According to the Decree for the effective functioning of the system, information from the companies making international transfers, as well as airport services, services making transfer of passengers and baggage, should be collected. The information on passengers must include information that will identify the person (name, last name, date of birth, data on passports or other ID, if necessary biometric data), information on flight, luggage, details on check in, etc.

[37] RA Law on "Personal Data" art 6

The information in the system can be used only by the authorities listed in the Decree and by the international bodies based on international agreements of RA.[38]

The system is enabling users to get on-time information for the implementation of their functions. But the problem is that the information today can be used only by the national authorities as there is no international agreement signed by Armenia that will give opportunity using the system by the third countries.

Armenia is a member to International Civil Aviation Organization (ICAO) which requires Member States to enhance legislative changes encouraging open reporting systems, and protect data collected solely for the purpose of improving aviation safety. ICAO implements review of States' activities to identify gaps in their legislation, to encourage open reporting systems, develop a plan to address gaps.[39]

These all leads to the conclusion that there is a "significant" legislative gap in regulating transfer of personal data and PNR.

The presented legislative acts do not cover all aspects for insuring safe data transfer to and from third countries.

[38] RA government decree 884-N of 22.06.2006 on "Establishing and Implementing the System of Informative Electronic Boarder Management"

[39] Global Aviation Safety Plan July 2007, International Civil Aviation Organization, http://www.icao.int/icao/en/anb/gasp/docs/Gasp_en.pdf

Chapter 4

Bringing the Armenian Legislation in Line with the EU requirements

The discussed elements of both EU and Armenian regulations are to witness the complexity of data protection relations and to stress that the collection and processing of personal data should be appropriately regulated as it involves human rights issues.

Still there are many gaps in the Armenian legislation on the field, as it can be inferred from the above presented. There is a real need of improvements and amendments of the legislation, to be able to face up all challenges and to have a proper data protection system in line with the set EU requirements.

The amendments that should be done are addressed to the Draft RA Law on "Protection of personal data", as it will become the main legal document regulating the field. The concentration on the acting RA Law on "Personal data" can be considered as a waste of time in the current situation.[40]

The first inconsistency that has been mentioned in the 1st chapter is the definition of the personal data. By the wording of the art 3.1 of the Draft Law, the definition of personal data is narrowed than it is given both in the Directive and in the acting Law. The provision should be changed in accordance to the Directive. A proper solution can be to replace this provision by the corresponding provision of the Law (art 3.a), which is wider in the sense of personal data, thus provides for wider protection of data which can be considered as personal.

The second issue is to be mentioned that a clear distinction of the "controller" and "processor" should be given. Both the acting Law and the Draft Law gives definition to the "processor" of data. The Directive giving definitions of "controller" and "processor" stipulates separate rights and obligations for them. This distinction should be provided by the Draft Law, and a clear definition to the "controller" as well as rights and obligations of it, must be provided in accordance to the Directive. The clear distinction of the "controller" is important for ensuring proper data protection,

[40] As it has been mentioned, the Draft Law will replace the Law, after entering into force.

especially in cases when the data processor, having a legitimate grounds for the processing, would not process that data for itself, but based on the request of a third person (controller).

The next lack that should be mentioned, relates to the provision of art 8.1 of the Draft Law, stipulating the right of the data subject to withdraw his/her consent on data processing. Giving this right (at the first sight it seems quite logical for full implementation of data subject's rights),the Draft Law does not later detail in which cases the consent can be called back and what would be the consequences, especially when the personal data has been processed. The mentioned gaps should be fixed by the proper provisions, in order to enable the data subject to realize the right to withdraw the consent, provided by the art 8.1.

Another issue to be properly regulated is the processing of special category of personal data in cases when that data is publicly accessible (art 9 point 2.2). The Directive clearly states that special category of personal data can be processed when that data has been disclosed by the data subject (art 8.e). The purpose of this provision is to ensure that the personal data can be processed only in case of data subject's consent (the data subject's will to disclose) especially taking into consideration the sensitive nature of special category of data. Corresponding amendment should be done in the art 9 point 2.2 of the Draft Law, ensuring that special category of data can be processed if that data has been publicized by the data subject.

As it is discussed in the 2nd chapter, the essential characteristic of the data protection authority must be complete independence. The corresponding amendment should be done in the art 21.1 of the Draft Law providing complete independence to the Personal Data Protection Inspection. For this purpose first of all the independent legal status of the inspection must be provided. The second essential element for independence is appointment of the head of the Inspection. The appointment mechanism must be as to eliminate any abuse by any authority or any opportunity to influence on decision making of the Inspection.

As one of the best practices for the appointment mechanisms can be taken the Estonian practice. According to the art 36 of the "Personal Data Protection Act" of the Estonia, the head of the data

protection inspectorate shall be appointed by the Government of the Republic at the proposal of the Ministry of Justice after hearing the opinion of the Parliament Constitutional Committee. The release of the head of the data protection inspectorate shall be in the same way.[41] This system of appointment and release gives guarantees to the data protection inspectorate independence, relying on the general notion of checks and balances of the branches of government.

As regards to the transfer of personal data to third countries, it has been already discussed that the RA legislation does not provide sufficient regulations for enabling safe transfer of data. Real steps by the stakeholders should be taken for due regulation of this field, as it includes not only personal data protection and data safety relations, but also deeply relates to international relations and more important to the national security. Beside amendments in the national legislation, international agreements on transfer of personal data as well as on transfer of PNR should be concluded.

[41] "Personal Data Protection Act" of the Estonia, http://www.privireal.org/content/dp/estonia.php

Conclusion

It is true to state that today Armenian foreign policy is mainly directed to the deepening of EU-Armenian cooperation. During the last 3 days working visit of the Prim-Minister Tigran Sargsyan to the European Commission on 15 March 2011, priorities for further EU-Armenian cooperation has been discussed. The President of the European Commission Jose Manuel Barroso stated that the negotiations on "Visa Facilitation and Readmission Agreement" will be launched this year. [42]

Several preconditions has been presented to Armenia earlier in order to start the negotiations and one of them is ensuring data protection mechanisms in line with the EU requirements.

To elaborate whether Armenia meets the EU requirements on personal data protection the core elements of data protection, control and processing of personal data, data protection authorities and transfer of personal data, has been discussed.

It has been elaborated that there are several inconsistencies in the RA legislation with the EU requirements. Though the discussed RA draft Law on "Protection of Personal Data" has been drafted very recently and the purpose has been to bring RA legislation in conformity with the EU standards.

The stakeholders should take necessary measures and initiate proper legislative amendments to overcome the existing contradictions and ensure full compliance of Armenian legislation to EU standards. To make reforms in the current situation will be more easy and effective, as the RA draft Law on "Protection of personal data" is still under the discussion of the RA Government. What is worth to be mentioned is that a real challenge for the stakeholders and first of all for the Government is not the initiation of proper and necessary legislative changes to bring the Armenian regulations in conformity with EU standards, but to present a political will to do that. The Government of Armenia must express a confident political will towards enhancing European Integration of Armenia and not just create an imitation of doing so.

[42] J.M Barroso. Personal interview. 16.March.2011
http://www.enpi-info.eu/maineast.php?id_type=1&id=24541&lang_id=450

Bibliography

1. ECJ judgment of 9.3.2010 in Commission v. Germany, Case C-518/07
2. Constitution of the Republic of Armenia (adopted 5.July.1995, as amended 27.Nov.2005)
3. Charter of Fundamental Rights of the European Union, 30.Mar.2010 (2010/C 83/02), Official Journal of the European Union, http://eur-lex.europa.eu/JOIndex.do
4. Law of the Republic of Armenia on "Personal Data" (RA Law-422, 22.11.2002)
5. Law of the Republic of Armenia on "Freedom of Information" (RA Law -11, 22.10.2003)
6. Law of the Republic of Armenia on "Archives Business" (RA Law -88, 01.07.2004)
7. Law of the Republic of Armenia Law on "Social Security Cards" (RA Law -1-N, 08.10.2003)
8. "Personal Data Protection Act" of the Republic of Estonia adopted 12.Feb.2003(RT[1]2003, 26, 158)
9. The Council of the European Union: Council Regulation (EC) No 539/2001 of 15 March 2001"Listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement"
10. The European Parliament and the Council: The EU directive 95/46/EC of October 1995 on "Protection of individuals with regard to the processing of personal data and on the free movement of such data"
11. European Commission, Commission decision of on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ L 39, 12.2.2010)
12. RA government decree 884-N of 22.06.2006 on "Establishing and Implementing the System of Informative Electronic Boarder Management"

13. European Commission, Communication from the commission on the global approach to transfer of passengers name records data to third countries, Brussels 21.09.2010, COM(2010) 492 Final
14. European Commission, Communication From the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions; A comprehensive approach on personal data protection in the European Union; Brussels 4.11.2010, COM(2010)609 Final
15. Hovhannisyan, Kren, "Visa Liberalization Baseline Study: Armenia" International Center for Human Development, February 2011, Yerevan, http://novisa.eu/wp-content/uploads/2011/01/ArmeniaFINAL.pdf
16. International Civil Aviation Organization, Global Aviation Safety Plan July 2007, http://www.icao.int/icao/en/anb/gasp/docs/Gasp_en.pdf
17. National Assembly of the Republic of Armenia, Official web site, http://www.parliament.am/
18. Հայաստանի Իրավական Տեղեկատվության Համակարգ, http://www.arlis.am/
19. Europa, Gateway to the European Union, http://europa.eu/index_en.htm
20. Europa, Summaries of EU Legislation, http://europa.eu/legislation_summaries/index_en.htm
21. EUR-Lex, Access to European Union Law, http://eur-lex.europa.eu/JOIndex.do
22. Nelly Manandyan. Personal Interview. Deputy Head of the Investigations Division of the Legal Protection Department, 03. Mar.2011.
23. J.M Barroso. Personal interview. 16.March.2011, http://www.enpi-info.eu/maineast.php?id_type=1&id=24541&lang_id=450