AMERICAN UNIVERSITY OF ARMENIA

ՀԱՅԱՍՏԱՆԻ ԱՄԵՐԻԿՅԱՆ ՀԱՄԱԼՍԱՐԱՆ

LL.M. Program

ԻՐԱՎԱԳԻՏՈՒԹՅԱՆ ՄԱԳԻՍՏՐՈՍԻ ԾՐԱԳԻՐ

Collection of personal Data: The issues of formulation and request of the consent of the subject of data

Whether the regulations set forth in Articles 9 and 10 of the RA Law on Protection of Personal *Data* are sufficiently clear for the data subject to understand the purpose of and give his informed consent for processing his personal data.

by

ANAHIT ELOYAN

SUPERVISOR

PROF. NSHAN MATEVOSYAN

Contents

INTRODUCTION

When entering into a contractual relationship, the parties may collect personal data for marketing or other purposes not related to the performance of the contract. States have adopted rules and laws to regulate the collection of personal data. The relevance of the issue of personal data protection is also related to the development of innovative technologies and the access to personal information on social networks. Many websites, the primary purpose of which is not collecting and processing personal data may become a source of personal information where the consent of data subject is absent. A similar popular web source in the Armenian reality is www.elections.am website. The corresponding section of the above website, where the personal data of voters is published, serves as a register of voters.

First, to assess the activities of personal data collectors, domestic legislation needs to be studied. In no circumstances, the conduct of the collectors may contravene the Article 34 of the Constitution of the Republic of Armenia, adopted on 5th of July, 1995 (the "RA Constitution").

According to Article 34(1) of the RA Constitution: *"[e]veryone shall have the right to protection of data concerning him or her.* According to the second part of the same article: *"The processing of personal data shall be carried out in good faith, for the purpose prescribed by law, with the* ***consent*** *of the person concerned or without such consent in case there exists another legitimate ground prescribed by law".*

On 25th of January 2001, Armenia became a full member of the Council of Europe. Following Article 13 of the Parliamentary Assembly Opinion No. 221(2000), Armenia upon its accession to the Council of Europe has undertaken to sign the European Convention on Human Rights (the "ECHR"), as amended by Protocols Nos. 2 and 11 thereto, and Protocols Nos. 1, 4, 6 and 7.[1]

According to to Article 8 of the ECHR: *"Everyone has the right to respect for his private and family life, his home and his correspondence. 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 other".*

Later, the European Court of Human Rights referred to personal data in one of its judgments *(S. and Marper v. the United Kingdom, judgment (Grand Chamber) of 4 December 2008, § 103)*, according to which *"The protection of personal data is of fundamental importance to a person's enjoyment of his or her*

[1] Council of Europe, *Membership, available at* https://www.coe.int/en/web/yerevan/membership (last visited March 31, 2020).

right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article ... The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored ... [It] must also afford adequate guarantees that retained personal data were efficiently protected from misuse and abuse ..."[2]

In respect to duties towards citizens Republic of Armenia law on the Protection of Personal Data No. HO-49-N, was adopted on 18th of May, 2015 (the "RA Law on Protection of Personal Data"), according to Article 1(1) of which, *"This law shall regulate the procedure and conditions for processing personal data, exercising state control over them by state administration or local self-government bodies, state or community institutions or organizations, legal or natural persons*."

According to Article 10 (1) of RA Law on Protection of Personal Data, the data processor shall notify the data subject about the intention of processing data in order to obtain his **consent.**

Obviously, the consent of data subject is a requirement mentioned by both the RA Constitution and the RA Law on Protection of Personal Data aimed at the protection of the person's right to enjoy his or her right to respect for private and family life, as guaranteed by Article 8 of the ECHR.

The RA Law on Protection of Personal Data defines data related terms, such as **personal data, processing of personal data, transfer of personal data to third parties, use of personal data, processor of personal data, data subject, database, depersonalization of personal data, blocking of personal data, destruction of personal data, data on personal life, biometric personal data, special category personal data, publicly available personal data, authorized person** and **third party.**

Perhaps, while collecting personal data the definition of the aforementioned terms is crucial, however RA Law on Protection of Personal Data does not include the definition of the word "consent", which has its expression in the well-known European Union Regulation 2016/679 of the European Parliament and of the Council of 27th of April, 2016, known as General Data Protection Regulation ("GDPR"). GDPR interprets the term **"Consent"** as follows:

"Consent" *of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*

[2] European Court of Human Rights, *Factsheet – Personal data protection*, *available at* https://www.echr.coe.int/Documents/FS_Data_ENG.pdf (last visited May 12, 2020).

Analyzing the above definition, we can say that the consent must be freely given and everyone should be informed about the purpose of the processing of his/her data in order to understand why his/her rights to privacy are restricted.

Fist of all, the legal grounds of data collection must be disclosed to data subject. The legal grounds of data collection can be either contractual or provided by law. However, whatever the legal ground is, the disclosure of the legal basis is not possible if the law is not precise and cause ambiguity.

Moreover the processing of personal data must be stored for specified and legitimate purpuses, which should be stated in the notice and which will give apportunity to data subject to be informed about the purpose of providing the information

"Data minimization" is another principle which should be taken into account while data collection. The required information should be as much as necessary to achieve the purpose of the transaction.

The data should be accurate in a form and in value. Each time the information is provided to a third party, the person must be given an additional notice, in order to be informed of how many people have their data at that moment. In the event of change of personal information, the data subject can be obliged to notifie about such changes to all data processors and will be able to guarantee data accuracy.

The Identification of personal data should be limited to the purpose of the transaction. The data collector has to erase the information when the goal of the data collection is reached

Data must be secured as well, and most of all the data subjects should be given the chance to be informed of measures of their data security.

As, nowadays, the data collection through the websites is common, the RA Law on Protection of Personal Data should contain rules directed to properly formed consents on the websites, which will make such consents freely given and informed.

CHAPTER 1: COMPARATIVE ANALYSES INTERNATIONAL AND ARMENIAN DATA PROTECTION LAWS

"GDPR highlights the importance of informed consent while collecting personal data. The expanded rights granted to data subjects can generally be characterized as giving them more control over their data and increasing their understanding of what is being done with it."[3] In addition, "GDPR specifies that anyone that has and processes personal data is accountable for ensuring that such data is:

• Processed in a legal, fair and transparent fashion *(lawfulness)*;

• Collected and used only for specified, explicit and legitimate purposes *(purpose limitation)*;

• Limited only to what is necessary for the specific purpose of processing *(data minimization);*

• Accurate, with inaccurate data rectified and erased *(data accuracy);*

• Retained only as long as needed *(data retention)*

• Protected *(integrity and confidentiality)."* [4]

LAWFULNESS

The Councel of Europe treaty for the protection of individuals with regard to automatic processing of personal data is adobted in 1981 (the "Convention"). All members of the Council of Europe have ratified the treaty. Being non–Council of Europe states, Argentina, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia, and Uruguay have acceded to the treaty. Armenia ratified the convention on 09th of May 2012.[5]

According to Article 5 (a) of the Convention, personal data undergoing automatic processing shall be obtained and processed fairly and lawfully.

According to Article 10(1) of RA Law on Protection of Personal Data, "[t]he processor of personal data or the authorised person thereof, for obtaining the data subject's consent, notifies of the intention to process the data." According to the point 2 of the second part of the same article, the notification for obtaining the data subject's consent (the "Notification") shall include legal grounds and purpose of the processing of personal data.

[3] Alan Cardel, *EU GDPR & EU-U.S. Privacy Shield*, § 4 (2019).

[4] Peter H. Chase, *Perspectives on the General Data Protection Regulation Of the European Union*, May 7, 2019

[5] Council of Europe, *Chart of signatures and ratifications of Treaty 108, available at* https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures (last visited May 12, 2020).

In accordance with 34(1 and 2) of RA Constitution, "everyone shall have the right to protection of data concerning him or her. The processing of personal data shall be carried out in good faith, for the purpose prescribed by law, with the consent of the person concerned or without such consent in case there exists another legitimate ground prescribed by law."

Pursuant to Article 9(4) of RA Law on Protection of Personal Data, "[t]he data subject's consent shall be considered given and the processor shall have the right to process it, where:

1. personal data are indicated in a document addressed to the processor and signed by the data subject, except for the cases when the document, by its content, is an objection against processing of personal data;

2. the processor has obtained data on the basis of an agreement concluded with the data subject and uses it for the purposes of operations provided for in that agreement;

3. the data subject, voluntarily, for use purposes, verbally transfers information on his or her personal data to the processor."

According to Article 9(5) of the same law, "[p]ersonal data may be processed without data subject's consent, where the processing of data is directly provided by law."

Article 9(4)(1) of RA Law on Protection of Personal Data is not clear enough to understand whether the person can process data based on the Power of Attorney provided for entering into contractual relations. It is not clear whether the other party can use the data collected from due diligence documents if a data subject does not sign a non-disclosure agreement ("NDA").

"The individual's right to be informed requires providing people with information about lawful basis for processing. This means the data processor needs to include these details in his/her privacy notice."[6]"Article 6(1) of GDPR sets out the conditions that must be met for the processing of personal data to be lawful.

They are:

(a) The data subject has given consent to the processing of their personal data for one or more specific purposes;

(b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) Processing is necessary for compliance with a legal obligation to which the [processor] is subject;

[6] Information Commissioner's Office, *Guide to the General Data Protection Regulation (GDPR): Lawful basis for processing, available at* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ (last visited May 12, 2020).

(d) Processing is necessary in order to protect the vital interests of the data subject;

(e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the [processor];

(f) Processing is necessary for the purposes of the legitimate interests pursued by a [processor], except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to the processing carried out by public authorities in the performance of their tasks.

These conditions are all equally valid and organisations should assess which of these grounds are most appropriate for different processing activities and then fulfill any further requirements the GDPR sets out for these conditions (GDPR Article 5)."[7]

In comparison with detailed regulation of GDPR, under Armenian legislation, data processor can collect personal data on two grounds, with the consent of the person and in the absence of such consent in other cases provided by law. The RA Law on Protection of Personal Data does not list the legal grounds on which the data of data subjects may be processed in the absence of consent. Perhaps at least partial enumeration by law would enable the data processor to understand the legitimacy of his actions faster and easier. By comparing the two legislative acts, it becomes clear that EU law provides for a more comprehensive and clear regulation.

However, while searching for some legal grounds for data collection, one can find some specifications in the Convention, especially Article 9(2) that provides for a possibility of derogation from the provisions of Articles 5 (Quality of data), 6 (Special categories of data) and 8 (Additional safeguards for the data subject). "Derogation shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a. Protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

b. Protecting the data subject or the rights and freedoms of others."

PURPOSE LIMITATION

In accordance with Article 5(a and b) of the Convention: "Personal data undergoing automatic processing shall be stored for specified and legitimate purposes and not used in a way incompatible with those purposes."

[7] Philippa Donn, *GDPR Legal Grounds for Processing – Consent? Legitimate Interests*?, *available at*https://dpnetwork.org.uk/gdpr-legal-grounds-processing-consent-legitimate-interests/ (last visited May 12, 2020).

According to Article 8(a) of the Convention: "Any person shall be enabled to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file."

"Purpose limitation is a key personal data protection principle, which requires that the collection and processing of personal data has a clearly defined purpose and that such data cannot be reused for another purpose that is incompatible with the original purpose."[8]

The data subject must be aware of the purpose for which he/she is giving his/her consent.

According to Article 4(2) of RA Law on Protection of Personal Data: "Personal data shall be processed for legitimate and specified purposes and may not be used for other purposes without the data subject's consent."

In accordance with Article 5(1) of RA Law on Protection of Personal Data: "The processing of data must pursue a legitimate purpose; measures to achieve it must be suitable, necessary and moderate."

As mentioned above, under article 10(2)(2) of RA Law on Protection of Personal Data, the Notification shall include the purpose of the processing of personal data.

Overall, the purpose of collecting personal data under Armenian legislation and the European Union Regulation is interpreted in the same way, with few differences.

According to Article 5 (1) (b) of GDPR, "Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, not be considered to be incompatible with the initial purposes". [9]

"The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes under GDPR should be subject to appropriate safeguards for the rights and freedoms of the data subject under this Regulation.

Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation.

The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the [processor] has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data).

---

[8] IsITethical, *Purpose Limitation, available at*http://www.isitethical.eu/portfolio-item/purpose-limitation/ (last visited May11, 2020).

[9] 2016/679 GDPR § 5 (2018 through May 25).

Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles.

The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials."[10]

Compared to GDPR, RA Law on Protection of Personal Data, does not make reference to scientific, historical research or statistical purposes. The lack of specifific regulation makes the processing of personal data for other perpeses than mentioned in the agreement incomprehensible.

Currently many entities use data for economic purpuses, particularly for advancing marketing strategies. For instance, many companies send massages to individuals for product offerings. This approach is commonly known as personalized marketing.

"In order to enable the users to effectively and efficiently manage the risk caused by data processing for the purpose of "personalized marketing" against their internal freedom of behavior, the following aspects must be determined.

At first, it must be clear which entity gets access to the information about the user. As described before, this is the startup itself. However, if further entities shall obtain access to the data, such as advertising or media partners, it must be clarified which entity is best suited for informing the user about which entity of them has which knowledge about the user."[11]

According to Article 10(2) of RA Law on Protection of Personal Data, "the Notification for obtaining consent to process personal data shall include the name (surname, name, patronymic, position) of the processor or his or her representative requesting the data subject's consent." The Notification shall also contain information on registered office or place of registration (actual residence) and the scope of persons to

[10] 2016/679 (GDPR) Recital 156.

[11] Maximilian von Grafenstein, *The Principle of Purpose Limitation in Data Protection Laws* 628 (1st ed. 2018).

whom personal data may be transferred. In regards to the regulation of RA Law on Protection of Personal Data, once the person gives his/her consent on processing his/her data, all the information provided can be transferred to the person indicated in the notice. However, in the future, when the data is transmitted to designated persons, they will not be obliged to notify the person about the use of specific information, as the law does not provide for such an obligation. The absence of such a requirement does not allow the data subject to be informed about the number of entities processing the information at the moment. However, it is worth mentioning that according to article 15(1) and (2) of the RA Law on Protection of Personal Data, "[t]he data subject shall have the right to information on his or her personal data, processing of data, grounds and purposes for processing, processor of data, the registered office thereof, as well as the scope of persons to whom personal data may be transferred. The data subject shall have the right to get familiarized with his or her personal data, require from the processor to rectify, block or destruct his or her personal data, where the personal data are not complete or accurate or are outdated or has been obtained unlawfully or are not necessary for achieving the purposes of the processing." Later in the 5th part of Article 15, it is mentioned that "data subject shall be provided with personal data based on a written request of the data subject or a representative acting by virtue of a power of attorney, or of a legal representative. The request may be filed electronically validated by an electronic digital signature."

Perhaps some companies may also collaborate and transfer the data without additional consent. In this case, it will be hard to control the information flow.

"Correspondingly, it must be clarified about what the individual is informed of. If the user is able to know what others know about him or her, he or she has to know, at least, the profiling criteria under which personal data is categorized and which make him or her "unique", in relation to the other users in the profiling system. Furthermore, the user also needs information about where the data originates from and what type it is. The reason for this is that it also determines the information about the individual. Finally, the user should know which entity specifically has that information."[12]

Armenian legislation covers clarification about what the individual is informed of. Especially according to article 10(2) of RA Law on Protection of Personal Data, the Notification shall include a list of personal data subject to processing.

The data processor should implement protective instruments against unspecific risks the processing of personal information can cause. The protection instruments must be clarified in the notice that is sent to data subject. In case the data processor does not implement such protection instruments against the risks, the data subject cannot rely on data processor and cannot be sure that the data and/or information is not

[12] Maximilian von Grafenstein, *The Principle of Purpose Limitation in Data Protection Laws* 628 (1st ed. 2018).

misused. Thus, the processor should inform the the data subject about these precautionary protection instruments. In that case, the disclosure of such protective measures to data subjects can increase trust between parties of transaction.[13]

RA Law on Protection of Personal Data does not stipulate that the Notification should indicate information on measures that will prevent, manage, or eliminate the risks of information leakage. Perhaps, the data subject must be aware of such rules to assess the risk of leakage of his / her information and to give informed consent thereon.

"Finally, it must be assessed, how this information should be presented to the individual so that he or she is able, in terms of cognitive capacities available in the daily online life, to understand that information."[14] The information, as well as the purpose for which the information is collected, should be certain.

As soon as the data subject is informed about later transfers as well as modifications of his/her personal information, given consent can be qualified not only as informed but also freely given. As one of the conditions for data subject's consent set forth by Article 4(11) of the GDPR is that consent must be freely given.

The GDPR further clarifies the conditions for consent in Article 7(4):

"When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

"Freely given" consent essentially means you have not cornered the data subject into agreeing to you using their data. For one thing, that means you cannot require consent to the data processing as a condition of using the service. They need to be able to say no. According to Recital 42 [of GDPR], "*Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment*."

One exception is if a piece of data is necessary to provide the subject data with a service. For example, the service provider may need data subject's credit card information to process a transaction or his/her mailing address to ship a product.

Recital 43 [of GDPR] discusses freely given consent. It explains that one must get separate consent for each data processing operation. [Therefore], if [one] wants [his/her] email address for marketing purposes and

[13] Id.

[14] Maximilian von Grafenstein, *The Principle of Purpose Limitation in Data Protection Laws* 628 (1st ed. 2018).

their IP address for website analytics purposes, one must give the user an opportunity to confirm or decline each use.[15]

According to Article 9(4) of RA Law on Protection of Personal Data

"4. The data subject's consent shall be considered to be given and the processor shall have the right to process, where:

1. personal data are indicated in a document addressed to the processor and signed by the data subject, except for the cases when the document, by its content, is an objection against processing of personal data;

2. the processor has obtained data on the basis of an agreement concluded with the data subject and uses it for the purposes of operations prescribed by this Agreement;

3. the data subject, voluntarily, for use purposes, verbally transfers information on his or her personal data to the processor."

In order to discuss the application and possible modification of Article 9(4) based on GDPR, the employment agreement can be taken as an example.

According to Article 13 of the Labour Code of the Republic of Armenia, adopted on November 9, 2004 (the "RA Labour Code"), "Employment relations are relations based on mutual agreement of employees and employers, under which employees shall personally perform official functions (work with certain profession, qualification or in a certain position) with certain remuneration adhering to internal disciplinary rules, and employers shall ensure conditions of employment provided for by the labour legislation, other regulatory legal acts containing norms of labour law, collective agreements and employment contracts."

Assuming, after the conclusion of the employment agreement, the new internal disciplinary rule is adopted, which requires additional personal information from an employee such as fingerprints authentification. The fingerprints authentification will be used to control the exits and entrances of the employee.

In regards to Article 9(4) of RA Law on Protection of Personal Data, the aforementioned requirement on fingerprints authentification will not be considered as a breach, as the processor has obtained data on the basis of an agreement concluded with the data subject and uses it for operations prescribed by employment Agreement.

To find out the legal consequence of the employee's conduct, we can assume that the employee rejects to give his consent and does not want to provide fingerprint authentification.

Regulations of Article 218 of RA Labour Code state as follows:

[15] Ben Wolford, *What are the GDPR Consent Requirements?, available at*https://gdpr.eu/gdpr-consent-requirements/ (last visited May 12, 2020).

"1. The workplace discipline shall be the rules of conduct established by the labour legislation, other regulatory legal acts containing norms of the labour law by collective agreement and employment contract, by internal legal acts of the employer, which all employees shall be obliged to follow.
2. The internal disciplinary rules (internal legal act of the employer) of the organisation shall regulate the procedure of accepting for employment and dismissal of employees, the fundamental rights, obligations and liability of the parties to the employment contract, the working regime, the time for rest, the measures for encouragement and disciplinary liability being applied to employees, as well as other issues relating to employment relations."

According to Article 220 of RA Labour Law: *Lack of performance of employment duties or improper performance of such duties due to the fault of the employee shall be deemed as violation of workplace discipline*.

According to Article 113(1)(5) of RA Labour Law "the employer shall have the right to rescind the employment contract concluded with the employee for an indefinite time limit, as well as the employment contract concluded for a fixed time limit before the end of the validity period, if the employee regularly fails to fulfill the obligations reserved for him or her by the employment contract or the internal regulatory rules, with no good reason." Accordingly, the employee might be fired based on his/her refusal to provide further personal data that may qualifyfor a breach of internal regulatory rules.

DATA MINIMIZATION

Under Article 5(b) of the Convention, personal data undergoing automatic processing shall be adequate, relevant and not excessive in relation to the purposes for which they are stored.

Article 5(2) of RA Law on Protection of Personal Data reads as follows, "[t]he processor of personal data shall be obliged to process the minimum volume of personal data that is necessary for achieving legitimate purposes."

"GDPR states that personal data [one] collect[s] and/or process should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". This means that you should hold no more data beyond what is strictly required. After all, it is challenging to lose information that you don't have. Some organisations are more prone to carrying excess information than others, particularly those in the healthcare industry or the financial services sector. The UK's Information Commissioner's Office offers this example: A recruitment agency places workers in a variety of jobs. It sends applicants a general questionnaire, which includes specific questions about health conditions that are only relevant to particular

manual occupations. It would be irrelevant and excessive to obtain such information from an individual who was applying for an office job. In this instance, the purpose for processing is to ensure that the applicant is placed into an appropriate role for which they are qualified. As the indicated medical conditions are not relevant to office jobs, there is no need to collect this information, and the principle of data minimisation says that it should not be collected or processed." [16]

Thereby, in order to reach the goal of transaction the processor should require as minimal personal information as possible. That can be a good reason why, in a bank, transactions for currency exchange, bank transfer or lending a credit are treated in different ways. For several cases, the passport will be enough to conclude the contract but for the other cases, taking into account several potential risks, the scope of due diligence documents may be broader.

The relevance of the issue is also related to the development of innovative technologies. "The online service provider would have access to bare minimum personal data, e.g, if YouTube wants to know that you are above 18 years to watch a particular video, it does not need to know your birthdate, a simple yes or no answer would suffice."[17]

DATA ACCURACY

In accordance with Article 5(d) of the Convention: "Personal data undergoing automatic processing shall be accurate and, where necessary, kept up to date."

"In his book Data Quality: The Accuracy Dimension, Jack Olson explained that data accuracy refers to whether data values are correct. To be correct, Olson argued, a data value must be both the right value and be represented in an unambiguous form, which is why he declared the two characteristics of data accuracy are **form** and **content**.

"Form is important because it eliminates ambiguities about the content," Olson explained. Form dictates how a data value is represented, and Olson used his birth date (December 13, 1941) as an example of how you can not always tell the representation from the value. If a database was expecting birth dates in United States representation, a value of *12/13/1941* would be correct, *12/14/1941* would be inaccurate because it's the wrong value, and *13/12/1941* would be inaccurate because it's the wrong form since it's in the European representation where the day is followed by the month.

[16] IT Governance Privacy Team, *EU General Data Protection Regulation (GDPR)* 51-52 , (3rd ed. 2019).

[17] Shraddha Kulhari, *Building-Blocks of a Data Protection Revolution* 45 (2018).

In the case of February 5, 1944, the United States representation is *02/05/1944*, whereas the European representation is *05/02/1944*, which could be misunderstood as May 2, 1944. Because of this ambiguity, a user would not know whether a birth date was invalid or just erroneously represented. "A value is not accurate," Olson explained, "if the user cannot tell what it is."

As for content, Olson explained that "two data values can be both correct and unambiguous yet still cause problems." This is a common challenge with free-form text, such as a city name. "The data values *ST Louis* and *Saint Louis* may both refer to the same city, but the recordings are inconsistent, and thus at least one of them is inaccurate." Consistency is a part of accuracy, according to Olson, because "inconsistent values cannot be accurately aggregated and compared. Since much of data usage involves comparisons and aggregations, inconsistencies create an opportunity for the inaccurate usage of data."[18]

In Armenia there probably will not be an issue regarding the form of the data under circumstances mentioned above, as though there is no clear way of writing dates by law, it is accepted to write the day first, then the month and then the year. However, Armenian regulation can cause some issues regarding the accuracy of the content. To avoid inaccuracy of data content, data subject should have the obligation to tell the data processor about any change of his given personal data. This will allow the parties to avoid data inaccuracies for future use or transfer. This obligation is frequently mentioned in the agreements and is formulated as an obligation to send written notices on changes of requisites. However, as long as there is no obligation for data subject to notify about changes, pursuant to Article 4(1) of RA Law on Protection of Personal Data the processor of personal data shall be obliged to follow and ensure that the data are processed in observance of the requirements of the law. In accordance with Article 6 of the same law, the personal data being processed must be complete, accurate, simple, and, where necessary, kept up to date. In case of incomplete, inaccurate, outdated, unlawfully obtained personal data or those unnecessary for achieving the purposes of the processing, the processor of personal data shall be obliged to carry out necessary operations for making them complete, keeping up to date, rectifying or destructing.[19] Perhaps, it is fair to mention that the data processor cannot be informed about changes of personal data objectively. Therefore, this obligation of personal data processor will be hard to fulfill.

DATA RETENTION

[18] Jim Harris, *The Two Characteristics of Data Accuracy, available at* http://www.ocdqblog.com/home/the-two-characteristics-of-data-accuracy.html (last visited May 12, 2020).

[19] *RA Law on Protection of Personal Data*, Article 18(2), (Adopted: 18 May 2015. Entry into force: 01 July 2015)

According to Article 5(e) of the Convention: "Personal data undergoing automatic processing shall be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored." The provisions of the RA Law on Protection of Personal Data on the term of personal data are in line with the Convention. "[p]ersonal data must be stored in such a way as to exclude the identification thereof with the data subject for a period longer than is necessary for achieving predetermined purposes."[20]

Following Article 5(e) of GDPR "Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')." In order to determine retention periods, organizations must consider several factors including to what extent they need to keep a record of a relationship with an individual once that relationship ends, to what extent they need to keep information to defend themselves from possible future legal claims, industry standards and guidelines, and any legal or regulatory requirements. Unless there is some reason for keeping it, personal data should be deleted or anonymized.

*"**Example***

A bank holds personal data about its customers. This includes details of each customer's address, date of birth and mother's maiden name. The bank uses this information as part of its security procedures. It is appropriate for the bank to retain this data for as long as the customer has an account with the bank. Even after the account has been closed, the bank may need to continue holding some of this information for legal or operational reasons for a further set time."[21]

By deleting unnecessary information, data processor will avoid unnecessary expenses. As according to Article 19(2) "In the course of processing personal data the processor shall be obliged to use encryption keys to ensure the protection of information systems containing personal data against accidental loss, unauthorised

[20] Id. Article 5(5)

[21] Lydia F de la Torre, *What does "storage limitation" mean under EU Data Protection law?*, available at https://medium.com/golden-data/what-does-storage-limitation-mean-under-eu-data-protection-law-fc6459ecb26c (last visited May 12, 2020).

access to information systems, unlawful use, recording, destructing, altering, blocking, copying, disseminating personal data and other interference."

INTEGRITY AND CONFIDENTIALITY

"Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination."[22] In the course of processing personal data, the processor shall be obliged to use encryption keys to ensure the protection of information systems containing personal data against accidental loss, unauthorised access to information systems, unlawful use, recording, destructing, altering, blocking, copying and disseminating personal data and other interference. The processor shall be obliged to prevent the access of appropriate technologies for processing personal data for persons not having a right thereto and ensure that only data, subject to processing by him or her, are accessed by the lawful user of these systems and the data which are allowed to be used.[23] It is evident that under Armenian legislation, personal data should have sufficient protection, however, the law does not require that a data subject be informed of the measures of protection of his personal information before giving his consent. Modifications should be made, particularly in Article 10(2). In particular, the notice shall specify all measures to be taken by the data collector against accidental loss, unauthorised access to information systems, unlawful use, recording, destructing, altering, blocking, copying, and disseminating personal data and other interference. Perhaps, when the measures of protection of own data security are stated, the person's consent can be qualified as informed.

CHAPTER 2: THE FREELY GIVEN AND INFORMED CONSENT IN THE CONTEXT OF TECHNOLOGY DEVELOPMENT

As it was mentioned before the relevance of the issue of personal data protection is directly related to the development of innovative technologies and to the access to personal information on social networks. Since most of the consents are being given and will be given by gadgets and electronic devices, it is essential to understand the scope of online data that is subject to protection. "Personal data shall mean any information relating to a natural person, which allows or may allow for direct or indirect identification of a person's

[22] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, art. 7, Jan. 28, 1981, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

[23] *RA Law on Protection of Personal Data*, Article 19(2) and (3) (Adopted: 18 May 2015. Entry into force: 01 July 2015).

identity."[24] "Natural persons may be associated with online identifiers provided by their devices, applications, tools, and protocols, such as internet protocol addresses, cookie identifiers, or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of natural persons and identify them."[25] The scope of online identifiers is not defined by Armenian legislation. "Online identifiers under the GDPR include Cookie identifiers."[26] "Using cookies or similar technologies to track an individual across websites involves the processing of personal data if this tracking involves online identifiers that are used to create a profile of the individual."[27]

The latest guidance on the Information Commissioner's Office website states that "[i]f you are relying on implied consent, you need to be satisfied that your users understand that their actions will result in cookies being set. Without this understanding, you do not have their informed consent. The Guide is intended to help website operators categorize the cookies they use and assist the website operators in preparing suitable methods of obtaining informed consent, as well as aiding communication with web site visitors by offering them standard notice language explaining in simple terms what cookies are and how they are used." [28]

How do reputable sites send similar notifications? For instance, the notification sent by www.adidas.co.uk website is as follows:

"*By selecting 'Accept tracking', you allow Adidas to use cookies, pixels, tags, and similar technologies. We use these technologies to collect your device and browser information in order to track your activity for Marketing and Functional purposes, like featuring personalised ads and improving the website. adidas may share this data with third-parties - including social media advertising partners like Google, Facebook, and Instagram - for Marketing purposes. Please visit our privacy notice (see Cookies Notice section) for more information and to understand how we use your data for Required purposes (e.g. security, shopping cart features and logging in).*"

There are two options, a person can either accept the notice, or he/she can manage the purpose of the operation: such as marketing purpose or functional purpose, which means that you agree to share devise and browser information. It is noteworthy that the site does not allow refusing to provide information.

---

[24] *Id.*Article 3(1)(1)

[25] 2016/679 GDPR Recital 30.

[26] Thomson Reuters Practical Law, *Glossary: Online Identifiers, available at* https://uk.practicallaw.thomsonreuters.com/w-014-8191?originationContext=document&transitionType=DocumentItem&contextData=(sc.Default)&firstPage=true&bhcp=1 (last visited May 12, 2020).

[27] Information Commissioner's office, *What are identifiers and related factors?, available at*

[28]https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-are-identifiers-and-related-factors/ (last visited May 12, 2020).

Robert Bond, *The EU E-Privacy Directive and Consent to Cookies,* 68 The Business Lawyer 219 (2012).

While visiting another prestigious website www.ielts.org (IELTS website), the notification includes the following phrase:

"We use cookies to ensure that we give the best experience on our website. If you continue, we will assume that you are happy to receive all cookies on the IELTS website".

The website user can choose between "Continue" or "More about cookies" bottons. Thus, in this case, one cannot give his free consent as well. As if you chose to use the service, accordingly, you consent to share your information. Perhaps, the information shared with the processors can be qualified as personal data, as 'personal data' means any information relating to an identified or identifiable natural person ('data subject'). Under GDPR "[a]n identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[29] In order to come to the conclusion that the use of cookies is the use of personal data, the "more about cookies" bottom of the IELTS website can become a convincing way.

In the IELTS website, it is written: "Please be aware that we use cookies on our website. We use cookies to track the interests of our users so that we can subsequently enhance their experience on our website. If your browser rejects a cookie, you may still use our website. Our website uses cookies to distinguish you from other users of our website without storing any personally identifiable information about you. This helps us to provide you with a good experience when you browse our website and also allows us to improve our site. A cookie is a small file of letters and numbers that we store on your browser or the hard drive of your computer. Cookies contain information that is transferred to your computer's hard drive."

By sending notifications of such content, the data collector may have a problem with the right of freely given consent. "Freely given" consent essentially means you have not cornered the data subject into agreeing to you using their data. For one thing, that means you cannot require consent to the data processing as a condition of using the service. They need to be able to say no. According to Recital 42 of GDPR, "Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."

But it should also be noted that it is gratifying that such notifications are at least sent. For example, in Armenia, there is no practice of sending similar notifications. This does not mean that there is no or cannot be any abuse in Armenia. Merely, in the case of poor regulatory compliance, the data subject may not know about the use of his or her online identification.

[29] 2016/679 GDPR § 4(1).

CONCLUSION

Everyone shall have the right to protection of data concerning him or her. Everyone shall be free to give his or her consent, and most of all, everyone should be aware of what information he/she provides and the purpose for which he/she restricts the right to privacy.

At first, the disclosure of personal data must have legal grounds about which the data subject must be informed. This ground can be either contractual in which case there is a mutual agreement on disclosing the data or provided by law, such as state security, public safety, the monetary interests of the State or the suppression of criminal offences, protecting the data subject or the rights and freedoms of others.[30] *However, in both cases, the data subject and data collector should be aware of the grounds on which the data can be collected. In this case, the law must be precise and give no grounds for ambiguity.*

Second, Personal data undergoing automatic processing shall be stored for specified and legitimate purposes and not used in a way incompatible with those purposes. The purpose of collecting information is stated in the notice, which enables the person to be aware of the purpose of providing the information. Taking into account the importance of the purpose of data collection, and the possibility of excluding personalization and possible contractual risks, the approach to law regulation should be different. For instance, if the agreement (purpose) does not need a wide scope of due diligence documents, there is no need to require such documents. The aforesaid statement can also be made for data minimization, as there is a considerable link between purpose limitation and data minimization. For instance, to reach the goal of the transaction the processor should require as minimal personal information as possible. That can be a good reason why, in a Bank, transactions for currency exchange, bank transfer, or lending a credit are treated in different ways.

The data also should be accurate, both in a form and in value. The data subject should be aware of all third parties that might get the personal information not only while giving consent, but also should be notified about such transfers when some time has passed since giving consent. In that case, when there is a personal data change, the data subject can be obliged to notify about the change of outdated data.

When there is no need to keep the personal data for achieving the purpose of data collection, the data collector has to erase the information or if the information is used for statistics or research makes it impossible to identification. Moreover, keeping extra information is expensive, as that information must be secured.

[30] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, art. 9(2), Jan. 28, 1981, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

Security measures for keeping the personal information should be defined in the Notification that shall be sent to data subject for getting confirmation. As the data subject should have the right to be informed about measures for his/her data protection.

Finally, perhaps there is a need for updates among definitions mentioned by RA Law on Protection of Personal Data*, as artificial intelligence is developing day by day, and there are new ways of communication and transactions. While defining such terms, it is crucial to follow up on the principles of data processing. Without such compliance, data collection can be qualified as not informed or not freely given.*

LIST OF SOURCES

Publications

1. Council of Europe, Membership
   https://www.coe.int/en/web/yerevan/membership

2. European Court of Human Rights, Factsheet – Personal data protection,
   https://www.echr.coe.int/Documents/FS_Data_ENG.pdf

3. Alan Cardel, EU GDPR & EU-U.S. Privacy Shield, § 4 (2019).

4. Peter H. Chase, Perspectives on the General Data Protection Regulation Of the European Union

5. Council of Europe, Chart of signatures and ratifications of Treaty 108
   https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures

6. Information Commissioner's Office, *Guide to the General Data Protection Regulation (GDPR): Lawful basis for processing,*
   https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

7. Philippa Donn, *GDPR Legal Grounds for Processing – Consent? Legitimate Interests*?, https://dpnetwork.org.uk/gdpr-legal-grounds-processing-consent-legitimate-interests/
8. IsITethical, *Purpose Limitation,*
   http://www.isitethical.eu/portfolio-item/purpose-limitation/

9. Maximilian von Grafenstein, *The Principle of Purpose Limitation in Data Protection Laws* 628 (1st ed. 2018).

10. Ben Wolford, *What are the GDPR Consent Requirements?,*
    https://gdpr.eu/gdpr-consent-requirements/

11. IT Governance Privacy Team, *EU General Data Protection Regulation (GDPR)* 51-52 , (3rd ed. 2019).

12. Shraddha Kulhari, *Building-Blocks of a Data Protection Revolution* 45 (2018).

13. Jim Harris, *The Two Characteristics of Data Accuracy*,
    http://www.ocdqblog.com/home/the-two-characteristics-of-data-accuracy.html

14. Lydia F de la Torre, *What does "storage limitation" mean under EU Data Protection law?*,

    https://medium.com/golden-data/what-does-storage-limitation-mean-under-eu-data-protection-law- fc6459ecb26c

15. Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, art. 7, Jan. 28, 1981, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

16. Thomson Reuters Practical Law, *Glossary: Online Identifiers,* https://uk.practicallaw.thomsonreuters.com/w-014 8191?originationContext=document&transitionType=DocumentItem&contextData=(sc.Default)&firstPage=true&bhcp=1

17. Information Commissioner's office, *What are identifiers and related factors?,* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-are-identifiers-and-related-factors/ (last visited March 31, 2020).

18. Robert Bond, *The EU E-Privacy Directive and Consent to Cookies,* 68 The Business Lawyer 219 (2012).

Legal Documents

1. The Constitution of the Republic of Armenia, July 5, 1995
2. The European Convention on Human Rights, November 4, 1950
3. Armenia law on the Protection of Personal Data No. HO-49-N, May 18, 2015
4. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, January 28, 1981
5. Regulation (EU) 2016/679 of the European Parliament and of the council of 27 april 2016
6. Labour Code of the Republic of Armenia, November 9, 2004