Goshadze Kakhaberi,
The University of Georgia, Georgia

The Principle of Secure Processing of Personal Data

Data protection is an emerging field of law that is challenging for legislators and the actors from public and private sector. It establishes standards for processing personal information and sets certain requirements to any party which is handling one's personal data. The article is oriented on the issues regarding the security of data, namely to keep personal data safe and secure in an organization, public or private, if they are using such data. The emphasize is made on the features of organizational and technical security measures and on their role in processing operations. The aim of this article is to show that these measures are not only mere rules, instead, they deserve to be considered as the data processing principles alongside with the five universally acknowledged principles of data handling. Additionally, to reach the high standards of security, the government should prescribe the standards of security for both private and public actors.

Keywords: Personal Data, personal information, organizational and technical security measures, high standards of security, government, private and public actors.

Introduction

In a modern society, personal data is widely used in many situations and for various purposes. It is not hard to imagine that technical development triggers new and complicated means and methods for data processing. A few decades ago, special legal acts regarding data processing came into place on a national as well as on an international level. The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal data, known as Convention #108 entered into force in 1981. It is the very first international, legally binding document which prescribes general principles and rules for personal data processing. Since then European countries have been passing legal acts establishing rules for data processing practices.

Today we have a reality where legal norms are keeping up with data processing methods step by step. The vast majority of economic and professional business activities are based on the usage of personal data. Moreover, this kind of data is often considered to be a commodity, which can be used by enterprises and companies for trade purposes. The need to have a strong legal basis for developed processing practices is continuous, as the IT technology creates new challenges for the legal background of data processing. To address this issue effectively, one must assume that legal norms cannot regulate every detail in this complicated process and therefore it depends on how general norms, known as principles, would be interpreted in order to serve the best interests of individuals and data controllers.

Law of Georgia on Personal Data Protection establishes 5 general principles for handling and using personal data in various circumstances. The rule, which obliges any data controller to process personal data securely is not regarded as a principle in this act; it is a separate norm (see art. 17). By carefully reading this norm, one will understand that data security is required at every step of processing, starting with collecting personal data to the point when the data is no longer needed and has to be deleted or destroyed.

Additionally, this act (see art. 17 (5)) prescribes that the *"data security measures must be established by legislation of Georgia."* By making this mandatory requirement, it is worth searching if there such standards for every type of private and public data controllers have been established so far.

This article aims to review several issues: 1.) Understanding data security requirements as a principle, along with five general ones; 2.) Describing what kinds of methods do the rules of secure processing include; 3.) To inquire what kind of standards for security have been established and adopted for legal and private entities and to find out if these security measures are applicable to every data controller.

1. The Five General Principles of Personal Data Processing and the Rule of Secure Processing

In data protection law, there are internationally acknowledged principles, which should always be adhered to when the data processing starts. These principles form one of the main parts of legislation on data protection. The importance of them is evident from the general conception of processing, in other words, if a data controller has legal grounds for processing, but he fails to ensure principles, the process cannot be started. For further clarification, let's discuss each of them briefly.

- **General principle of fairness, lawfulness and dignity.** Law of Georgia on Personal Data Protection, art. 4 (a), states that *"data must be processed fairly and lawfully, without impinging on the dignity of a data subject;"* This requirement can be considered as the most general principle, as it defines that the prerequisite for every single aspect of data processing should be those mentioned above. By this prescription, norms require general standards, such as equality, impartiality and etc. to be in place. The fact that this prescription mentions the word "dignity", indicates a dual purpose of the act, that

is, not only the protection of personal data, as a part of the right to privacy, but also it ensures that the fundamental right of the protection of dignity is guaranteed.

- **Purpose specification principle**. Art. 4 (b) establishes as follows: *"data may be processed only for specific, clearly defined and legitimate purposes. Further processing of data for purposes that are incompatible with the original purpose shall be inadmissible;"* Purpose specification or as it is also called purpose limitation principle is the one which must not be avoided, due to the simple consideration that if a data controller has not specified the purpose in advance, processing cannot commence.

- **Proportionality principle.** The requirement of proportionality is prescribed in art. 4 (c) of the act, *"data may be processed only to the extent necessary to achieve the respective legitimate purpose. The data must be adequate and proportionate to the purpose for which they are processed;"* This principle has strong connection with the previous one, as it requires the processing of only those data which are needed for the purpose specified in advance. Accordingly, processing excessive data can be considered as not only violating the proportionality principle, but as a breach of the purpose limitation principle by simply assuming that there is no purpose for processing excessive data.

- **Accuracy principle.** The fourth data protection principle in art. 4 (d) states that *"data must be valid and accurate, and must be updated, if necessary. Data that are collected without legal grounds and irrelevant to the processing purpose must be blocked, deleted or destroyed;"* Any modification of already processed data is required if it is "necessary". There is no further definition of "necessity", but to analyze this norm in connection with the purpose specification principle, it is clear that any modification is only permissible if there is such purpose;

- **Timely deletion principle.** It is obvious that data no longer needed must be deleted or destroyed in order to avoid the violation of other principles as well. Art. 4 (e) of the Law of Georgia on Personal Data Protection prescribes that *"data may be kept only for the period necessary to achieve the purpose of data processing. After the purpose of data processing is achieved, the data must be locked, deleted or destroyed, or stored in a form that excludes that identification of a person, unless otherwise determined by Law."* Timely deletion principle is the last principle of our act, which requires that data controllers delete/destroy or depersonalize data if there is no need to keep it in a manner which enables the identification of a data subject. Of course, we have to see this in light of the purpose specification, according to which keeping data that is no longer needed would be a violation of a second principle – purpose limitation.

As we see through the analysis of the legal prescriptions these principles apply on the overall process of data processing, starting with gathering personal information onward to the point where it should be deleted and disposed of. Now, if we turn to the previous norm, stating the requirement of secure processing, we may find common points with the principles discussed. Law of Georgia on Personal Data Protection, art. 17.1, points out that *"A data controller shall be obliged to take appropriate technical measures to ensure protection of data against accidental or unlawful destruction, alteration, disclosure, collection or any other form of unlawful use, and accidental or unlawful loss."* According to this norm, the requirement covers all the activities made upon personal data, from collection to any other form of use, and ending with destruction. So, taken together, these activities can be regarded as processing, upon which security is an unavoidable prerequisite. Considering all of this together, secure processing can be regarded as a principle, due to the fact that it applies on every stage of the process in a same way as principles apply on every step of data processing. Moreover, for example, in the Data Protection Act of 1998 of the United Kingdom (part I,

schedule I), data security is already mentioned as a principle, it states that *"Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."*

Finally, we should also mention the three characteristics of data protection principles, these are: 1. Cumulative approach – mostly, in data processing there is more than one principle involved at the same time, for example, purpose limitation and proportionality are always together at place; 2. Ensuring principles in advance – it means that data controller who wishes to use data, should always define in advance the purposes of processing and quantity of data; 3. Lifecycle coverage – principles cover all stages of data processing, from collection to disposal.

It is evident that, all three characteristics are relevant to data security. Therefore, it can be easily regarded as a principle, which is an indication of logical approach to regulate data protection practices.

2. Organizational and Technical Security of Personal Data and Respective Standards

Data security can be ensured in a two-way approach. This approach involves establishing organizational and technical measures. These two sub-division of data security have different aspects and definitions. Let's describe each of them.

2.1. Organizational Security of Personal Data

Under the notion of organizational data security, we may assume that there are activities which effectively address these issues. This approach depends on the ways of processing the data, stages of it and the persons involved in it. It is hard to stipulate and describe all possible ways of ensuring organizational

data security, besides they may differ, as the approach must be shaped differently for every particular situation, but for clarification purposes, a few examples are needed, which are general by their nature.

If the data is being processed without using automated means, these activities apply to organizational measures. For example, in a company, papers containing personal files should not be left without a control on a desk to which every person, including, staff and other individuals doing business with the company would have access. Therefore, repositories of personal files containing hard copies should be locked when they are not in use to avoid data security breaches. To ensure an advanced level of protection, one has to distinguish sensitive and non-sensitive personal data from each other and apply stricter security to the papers with sensitive data, say simply, lock them in a more secure manner, for example in a safe to which access is restricted. Here, we can mention filing systems as well, best practice of handling filing systems, requires to keep sensitive data apart from an ordinary ones, if possible. The Council of Europe recommends that *"health data covered by medical secrecy should be separate from other categories of personal data held by the employer. Security measures should be taken to prevent persons outside the medical service having access to the data"* (Council of Europe, Committee of Ministers, Recommendation no. R (89) 2 of the Committee of Ministers to Member states on the Protection of Personal Data Used for Employment Purposes, 1989, art. 10 (5)).

To raise awareness about organizational security issues, newcomers and members of a company's staff should have specific trainings on these matters; there will be even better outcomes if such trainings are mandatory. It is important to consider that these procedural activities are not a mere everyday routine occurring inside of a company. It is important to think that having these activities in place leads us to ensuring that we meet legal requirements.

Organizational security measures are not methods of securing company's personal data from the "rest of the world." Accordingly, data must be

protected inside an organization, between departments and divisions of an institution. For example, if a client in a bank decides to sign a loan and mortgage agreement, the information held about this individual should not be communicated, for instance, to the deposits department and vice versa.

Finally, those measures of organizational security would be ineffective if there is not a requirement of confidentiality. Law of Georgia on Personal Data Protection, art. 17.4 states that *"Any employee of a data controller and of a data processor, who is involved in processing of data, shall be obliged to stay within the scope of powers granted to him/her. In addition, he/she shall be obliged to protect data secrecy, including after his/her term of office terminates."* As we see, this confidentiality clause covers all kinds of employees, that is, of both private and public legal entities.

2.2. Technical Security of Personal Data

Today, when we are talking about data security, we mostly are referring to IT systems and measures taken to protect data electronically. It is not uncommon to think this way, because a vast majority of personal data held by organizations are being processed by automated means. As time goes by, these means are developing, raising new challenges for legislators to effectively address complicated issues. Technical security measures can vary company to company, but let's review some basic approaches that every data controller should take into consideration.

Using information technologies for data processing most commonly means using computers, internet, smartphones and other portable technology. It is obvious that the simple security of data requires having antivirus software installed and relevant firewalls activated. Further, if a company has its own server room, access to it should be restricted to avoid any unauthorized data processing. Every employee who works on his computer or any other

automated mean to process data, should always use a password and user name combination to keep the data safe. The more digits that are used for creating a password combination, the stronger the protection will be. Using an email can also have issues if an employee is not properly informed, for example, for communicating files containing personal data one must not use Gmail, Yahoo or any kind of email which is out of the control of the employee, rather, for purposes mentioned above, the organization should use its own email, which is protected by special measures to avoid unauthorized access. For those employees who are using special software for data processing, additional features, such as logging of activities must be at place. This logging enables a company to trace any use and modification of personal data in order to asses whether it was done in accordance with data protection principles and the legal grounds for processing. Additionally, the existence of an IT audit department will be efficient in controlling activities done by employees via automated means (for more information visit these web-pages: ttps://www.dataprotection.ie/docs/Data-security-guidance/1091.htm; http://www.infosec.gov.hk/english/technical/guidelines.html#id2; http://www.bu.edu/infosec/howtos/how-to-choose-a-password/).

Both for organizational and technical data security there are additional measures which strengthen the methods in place: 1.) The Georgian data protection act requires that *"Measures taken to ensure data security must be adequate to the risks related to processing of data."* For example, if an organization processes sensitive and non-sensitive data, measures taken to protect sensitive data should be stricter than those for "ordinary" information; 2.) Having a data protection officer at an organization is a good way to ensure that data processing practices are compatible with the provisions of legislation. But in contrast to the first method, this is not established by the Law of Georgia on Personal Data Protection. However, in Germany data protection audit is prescribed by law as follows *"in order to improve data protection and data security, suppliers of data processing systems and programs, and bodies conducting data processing may have independent*

and approved experts examine and evaluate their data protection strategy and their technical facilities and may publish the results of this examination. [...]" (Federal Data Protection Act of 2009 of Federal Republic of Germany, section 9a). Additionally, the German data protection act states what kind of security measures should be taken to meet the requirements of legal provisions, they should be in a manner to:

"*1.* Prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control); 2. Prevent data processing systems from being used without authorization (access control); 3. Ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control); 4. Ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control); 5. Ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control); 6. Ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control); 7. Ensure that personal data are protected against accidental destruction or loss (availability control); 8. Ensure that data collected for different purposes can be processed separately." (Ibid, annex to section 9, first sentence).

3. Standards for Ensuring Data Security

There are variety of ways according to which data security standards can be shaped. This is due to the fact that each company, enterprise or any other organization needs standards that are suitable for each particular entity's situation and needs. Therefore, measures guaranteeing data security cannot be shaped in a detailed way. But in any case, general requirements must be

established and are welcomed to serve as guidelines for more detailed internal security provisions.

Law of Georgia on Personal Data Protection, art. 17 (5) mandates as follows *"the data security measures shall be defined by the legislation of Georgia."* This legal provision obliges the legislature to establish standards for data security. In 2012, the Law of Georgia on Information Security was passed. In the first article of the act we read *"this Law aims to promote efficient and effective maintenance of information security, define rights and responsibilities for public and private sectors in the field of information security maintenance, and identify the mechanisms for exercising state control over the implementation of information security policy."* As it is described, the act covers activities done both by private and public actors, but let's see if this law is fully applicable on every activity performed by those entities.

For further examination, we need to mention two definitions offered by this act:

1. Critical information system – an information system whose uninterrupted operation is essential to national defense and/or economic security, as well as to normal functioning of the state authority and/or society (art. 2 (f));

2. Critical information system subject – a state body or a legal person whose uninterrupted operation of the information systems is essential to the defense and/or economic security of the state, as well as to the maintenance of state authority and/or public life (art. 2 (g)).

As we see, this act covers entities which hold information that can be mentioned under one header "information of public importance". Then, we have to find out how far the applicability of this act extends. On this issue answer is given in art. 3 (1) *"This Law shall apply to all legal persons and state authorities that are critical information system subjects. This law shall also apply to the organizations and agencies that are subordinated or related to*

critical information system subject through labor, internship, contractual, or other relationships and that provide access to information assets under such relationships." This means that the law obliges only those entities, which hold and use "information of public importance." It is obvious that the notion of "information" contains various kinds of data, including, personal data, therefore, the act is applicable to personal data processing only if it is regarded as a part of critical information system, that is, "information of public importance." However, if we continue to discuss the issue of applicability, art. 3 (6) gives us following regulation: *"the provisions of this law shall not affect the application of the norms provided for by the legislation of Georgia that governs […], personal data processing, […]."* At first, it may seem that this norm excludes the applicability of this act on personal data processing, but from a teleological and systematic interpretation of the norms, it is clear that this act does not affect the rules of data processing which are given by another legal act, but at the same time ensures security measures for information, including, personal data, if it is a part of critical information system. Additionally, this act does not apply to mass media, editorial offices of publishing houses, scientific, educational, religious and public organizations, as well as to political parties regardless of the importance of their activities to the national defense and/or economic security and to the maintenance of state authority and/or public life (see art. 3 (3)). The main idea behind excluding these entities and activities done by them, was not to impede freedom of expression generally, and more interesting is that *"any legal person and public authority that is not a critical information system subject may voluntarily assume the obligations deriving from this Law."* It simply gives an opportunity to every entity to adhere stated norms, but this is not mandatory. We cannot say that this act applies to all public and private sector entities; therefore it can't be regarded as establishing personal data protection mandatory standards of data security for every entity.

Moreover, in 2013, the President of Georgia issued an Edict #157 on the Approval of the List of Critical Information System Subjects, according to

which these subjects were defined. By reading this list one will clearly see that entities mentioned in an edict are public organizations, such as, ministries, public legal entities and private organizations, which are functioning as public entities and are established by the state. Therefore, the Law of Georgia on Information Security does not provide sound basis for organizational and technical data security for every data controller.

The issues of information security are addressed in the Order #2 on Minimal Requirements of Information Security Standards issued by the Chairman of Data Exchange Agency, in which measures of security are described. It also includes best practices of the ISO 27001 standard, which is on information security. However, this document can't be seen as a remedy for data security, due to the fact that by this order it only applies to the critical information system subjects, which were recently mentioned.

As we see, there is no mandatory minimal requirements for data security established by legislation to every data controller. The remedy may be found in the international standard, namely, ISO 27001, which is on information security management. It helps organizations to keep information assets secure, such as financial information, intellectual property, employee details or information entrusted to data controllers by third parties. It can be applied to small, medium and large business in any sector for data security (http://www.iso.org/iso/iso27001).

Another way to ensure data security is to implement a modern approach for data processing practices, namely, conception of Privacy by Design, introduced by Ann Cavoukian – former Information and Privacy Commissioner of Ontario, Canada. This conception lies on seven general principles, which are flexible for any institution to be adopted. These seven principles can be seen as a rephrase of data protection principles, but gives us explanations and definitions from the different angle. Let's review only those, which have relation to the data security to see how useful they are for maintaining effective protection of data in IT systems.

- *Proactive and preventive approach* – This is the first principle of PbD. In order to avoid any risks to be materialized, data controllers should shape and implement measures in advance that will prevent privacy invasive events (Privacy by Design in Law, Policy and Practice, Cavoukian, A., Ontario, Canada, 2011, 20). These measures can easily be regarded as ensuring data security too, because preventing risks, among other things, includes safeguarding personal data from unauthorized access and use.

- *Privacy as the default* – It aims to deliver the maximum degree of privacy protection by automatically protecting it in any IT system or business practice (ibid.). This principle requires that a data controller put in place measures that will form a sound basis for data security as it is oriented on information technology issues. Therefore, a data controller should not only establish default rules for security, but also think of the adequacy of protection for various kinds of data, particularly, for non-sensitive and sensitive information.

- *Privacy embedded into Design* – The main idea of this principle is that privacy should be an essential component of the core functionality being delivered (ibid.). This is not meant to diminish the productivity of a service. The essential point of this principle is to maintain efficiency alongside with securing the data in IT systems. Therefore, it can serve as a requirement for data security.

- *End-to-end lifecycle protection* – This principle mandates protection of data from the time when it is collected to the end of the process, when it should be timely deleted (ibid.). Of course, this principle can be regarded as a main requirement for data security, due to the idea of the security itself – measures guaranteeing security, should cover every aspect of data processing, that is, to extend on entire lifecycle of the process.

Conclusion

The aim of this article was to examine ways for ensuring organizational and technical data security. As it appeared, the requirement established by the Law of Georgia on Personal Data Protection to ensure data security can easily be regarded as the principle requirement with 5 general principles of data protection. So, the importance of these mandatory requirements is evident. By guaranteeing data security, data controllers are guaranteeing that the five general principles of data protection, provided for by law, will be complied with and data processing practices will be in accordance with the requirements established by these general provisions.

Another important aim was to find legal regulations for establishing mandatory standards on organizational and technical data security. However, such standards are provided only for public legal entities and government organizations, such as, ministries. It somehow seems that the Georgian legislature has avoided regulating private organizations, which results in an approach, when every private entity establishes such standards which are suitable according to their own considerations.

Georgia shares a European model of data protection and according to the EU-Georgia Association Agreement (art. 14), Georgia is obliged to establish the same level of data protection that it is in European Union, particularly, as guaranteed by the Directive 95/46/EC, but the fact is that overall data protection culture is not at the same high level in Georgia as it is in European Union. Even the Law of Georgia on Personal Data Protection, which was passed at the end of 2011, entered into force in its entirety in 2013, but still today data controllers are still having issues with the implementation of this act in their everyday processing activities (see Annual Report of Personal Data Protection Inspector's Office on the State of Personal Data Protection and Activities of the Inspector of Georgia, 2015, p. 9). Accordingly, it is now legislators turn to regulate this new field of law efficiently. It worth noting that at first prescribing minimum security standards for every data controller may

not be easy to implement, but doing so, we can achieve the standards of data protection which have been established in the European model and therefore protect one of the most important human rights – privacy

References

Publications:

Cavoukian, A. (2011). Privacy by Design. Ontario, Canada. Information Commissioner's Office.

Annual Report of Personal Data Protection Inspector's Office on the State of Personal Data Protection and Activities of the Inspector of Georgia. (2015). Tbilisi, Georgia. Personal Data Protection Inspector's Office of Georgia.

Webpages:

Data Protection Commissioner of Ireland. (2016). Data Security Guidance. Retrieved 07/20/2016 from: https://www.dataprotection.ie/docs/Data-security-guidance/1091.htm.

InfoSec. (2016). IT Security Standards and Best Practices. Retrieved 06/16/2016 from: http://www.infosec.gov.hk/english/technical/guidelines.html#id4.

Boston University Information Services & Technology. (2016). Information Security. Retrieved 06/29/2016 from: http://www.bu.edu/infosec/howtos/how-to-choose-a-password/

International Organization for Standardization. (2016). ISO/IEC 27001 – Information Security Management. Retrieved 07/07/2016 from: https://www.iso.org/isoiec-27001-information-security.html.

Legal Acts:

Chairman of Data Exchange Agency. (2013). Order #2 on Minimal Requirements of Information Security Standards. Retrieved 07/05/2016 from: http://dea.gov.ge/?action=page&p_id=127&lang=geo.

Council of Europe, Committee of Ministers. (1989). Recommendation no. R (89) 2 of the Committee of Ministers to Member states on the Protection of Personal Data Used for Employment Purposes. Retrieved 07/01/2016 from: http://www.coe.int/t/dg3/healthbioethic/texts_and_documents/Rec(89)2E.pdf.

Data protection Act of the United Kingdom. (1998). Retrieved 06/30/2016 from: http://www.legislation.gov.uk/ukpga/1998/29/contents.

EU-Georgia Association Agreement. (2014). Retrieved 07/20/2016 from: https://eeas.europa.eu/sites/eeas/files/association_agreement.pdf.

Federal Data Protection Act of Federal Republic of Germany. (2009). Retrieved 07/15/2016 from: https://www.gesetze-im-internet.de/englisch_bdsg/.

Law of Georgia on Information Security. (2012). Retrieved 06/24/2016 from: https://matsne.gov.ge/ka/document/view/1679424?impose=translateEn.

Law of Georgia on Personal Data Protection. (2011). Retrieved 07/01/2016. From: https://matsne.gov.ge/ka/document/view/1561437?impose=translateEn.

President of Georgia. (2013). Edict #157 on Approval of the List of Critical Information System Subjects. Retrieved 07/07/2016 from: https://matsne.gov.ge/ka/document/view/1867646.

The Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Retrieved 07/20/2016 from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37.