GDPR and personal data protection in non- EU countries: Albanian case of data protection legislation

Gliqiri Riza

University of Tirana, Faculty of Economics, Tirana, Albania

Abstract

GDPR, which stands for the General Data Protection Regulation, is the European legal framework, that aims to simplify the regulatory environment for businesses and organizations in all EU member countries, but with clear implications for businesses and individuals located in any other country, where domestic or foreign companies process personal data of the European citizens. It is a set of rules designed to give European citizens more control over their personal data, at a time when almost every aspect of life revolves around data. From the companies we work for, social media giants, banks, health care systems and governments, every service we use in our daily lives, involves the collection and analysis of our personal data. Being such an important development in protecting the security of personal data, this paper aims to give a brief analysis of some of the most important concepts of GDPR, the affected companies and citizens and the administrative fines applied in case of violation. Furthermore, it will provide a comparison of Albanian legal framework for Data Protection with the GDPR, followedby some conclusions and recommendations.

Keywords 1

Personal data, legislation, protection, security, controller, processor, administrative fines

1. Introduction

While the technologhy is being developed in an unstoppable way, people and authorities are nowadays more aware and conscious of the risk we all face while sharing the virtual reality over the Internet. As a result, in January 2012, the European Commission began setting targets for Data Protection Reform across the European Union [6], so that the changes would make Europe fit the digital era we live in. This period needed many years of preparation, but almost four years later agreement was reached on what was called the GDPR, one of the most powerful legislations of the last 20 years. The regulation was adopted bythe European Parliament in April 2016 and the directives were published in the Official Journal of the European Union in all official EU languages, while two years later, on 25 May 2018, the legislation came into force all over the Europe. It followed the 1995 Data Protection Directive [4], which had been implemented until then. As a result, under the terms of the GDPR, organizations must not only ensure that personal data is collected lawfully and under strict security conditions, but on the other hand, even those who collect, process or save the data are obliged to protect it from misuse and exploitation. At first glance, the GDPR may seem complex, but the essence of the legislation is based on the fundamental human right to privacy, where data owners are the ones who choose what to do or not to do with their personal data.

Thus, since the protection and security of personal data are the foundamentals in which the GDPR is based, first of all we should all know what is considered personal data under the current legal framework. Personal data is any information related to an identified or identifiable living individual which can lead to the identification of a particular person. According to the European Commission (2020) [5], earlier the types of data that were considered personal included name, address and photos, but the GDPR extended the definition beyond that, considering personal data even an IP address or other similar digital data that can identify us on the network.

Proccedings of RTA-CSIT 2021, May 2021, Tirana, Albania
EMAIL: gliqeririza@hotmail.com

Furthermore, General Data Protection Regulation states that genetic and biometric data, which can be processed to uniquely identify an individual are also defined as sensitive personal data. Based on the new GDPR rules, the types of information that should be addressed and treated with special care as they constitute personal data include: name, address, date of birth, social security numbers, etc.; internet-based data, including user location, IP address, cookies and RFID[1] tags; health card data (HIPAA[2]) and genetic data; biometric data; racial and/or ethnic background; political convictions; religious faith and sexual orientation.

On the other hand, when it comes to dicussing the responsibility for processing and having control over the personal data, GDRP specifies that there are two main stakeholders, Data Controllers and Data Processors. A Data Controller can process the collected data using its own processes, or in some cases the controller can also work with a third party/ outsourced service for processing procedures. However, even in this case, the Data Controller should not relinquish the control of the data over the third-party service. The Data Controller continues to be in control, specifying how the data will be used and processed by the external service. Thus, the Controller has the greatest responsibility when it comes to protecting the rights of the data subject. As a result, the Data Processor, simply processes any data given to it by the controller. The Data Processor can also be a company or a third-party outsourced organization, subcontracted by the Data Controller for data processing service, even though the processor neither possesses the data being processed, nor controls it. This means that a processor is neither able to change the purpose, nor the means in which the data is processed. Therefore, Data Processors are obliged to operate under the instructions given by the controller.

2. The GDPR's important changes

According to the General Data Protection Regulation, a company or organization, either it is located within the EU, or it is operating in any country outside the European Union, must implement and be compliant with the GDPR, if it meets any of the following conditions:

- The business is operating in any European Union country;
- Even if it is not located in any of the EU countries, the company still processes personal data of European citizens;
- The company has more than 250 employees;
- The company has less than 250 employees, but the data processing being performed during the daily activity affects the rights of its data subjects.

According to the GDPR, there are two declarations which analyze the territorial scope and clearly specify the rules that must be followed by a company located outside the European Union, but is still processing the data of a European entity or citizen [7]. There are two cases that analyse when an organization outside the European Union is affected by the legal framework of the GDPR and will have to apply increased measures and controls, in order to be compliant with the legislation [3]. This happens in the case of:

- *Providing goods and / or services to European citizens/ The Offering Test*

One of the ways the internet is making our lives easier is the fact that with just one click, goods and services become accessible very easy from anywhere in the world. From the GDPR perspective, it adds challenges for companies and organizations operating globally [2] because the legislation states that, no matter where the organization is located, as long as it provides goods and services to European citizens, it is obliged to be compliant with the GDPR. Thus, even if the company is not operating in a European country, it should be compliant with the GDPR.

- *Monitoring their behavior/ The Monitoring Test*

If an organization uses tools that allow it to track cookies or IP addresses of people from any of the European Union countries who visit its website, then it is obviously affected by the GDPR legislation. As e result, the company will have to take responsibility for tracking this data. In contrast to the provision of goods and services, monitoring does not specifically require any indication of why it occurs, even though GDPR guidelines state that "use of the word "monitoring" means that the controller has a specific purpose in mind for the collection and subsequent activities of reuse of relevant data relating to the conduct of an individual within the EU." Furthermore, according to the legal framework explanations, although it is not required a concrete reason why someone's activity on the network is being monitored, the main consideration is the fact that it is believed that any observed behavior can later be used to profile the monitored subject [2].

[1] RFID- Radio-frequency Identification
[2] Health Insurance Portability and Accountability Act

On the other hand, according to the changes GDPR brought inthe European legal framework for Personal Data Protection, a data subject, i.e. the person whose data are collected and processed, has some fundamental rights [9], which must be respected during the processing of his personal information. These rights are explained in the Articles 15-22 of the General Data Protection Regulation and in case of violation, the Data Controller, i.e. the company which is processing the data will have to face the administrative fines stated by the regulation. These rights include:

- The data subject's right of access: the right to obtain from the controller the confirmation as to whether or not the personal data of the subject are being processed.
- The right to rectification: the right to obtain from the controller without undue delay the rectification of the innacurate personal data concerning the subject.
- The right to erasure/ "The right to be forgotten": the right to obtain the erasure of the personal data concerning the subject, where the controller shall have the obligation to erase the data without undue delay.
- The right to restriction of processing: the right to obtain the restiction of processing him/her personal data.
- The right to be informed: the right to being informed from the controller, in case your personal data is being collected, processed or saved for any aim.
- The right to data portability: the subject's right to receive the data concerning him/her, in a structured, commonly- used and machine-readable format.
- The right to object: the right to object at any time the processing of data concerning the subject.
- The right not to be subject to a decision based on automated processing: the right not to be subject to a decision based solely on automated processing, including profiling, that affects the subject and produces legal effects concerning him/ her.

GDPR administrative fines

One of the most discussed factors whenever GDPR is being analysed is undoubtedly the ability of regulators to penalize businesses that do not comply with the regulation. Thus, if an organization does not process the individual's data properly, any of the subject's rights is violated, or there are found other compromising factors, the company can be fined. The GDPR has two main levels of fines: it states that minor violations can result in fines up to € 10 million or 2% of a firm's global turnover (whichever is higher), while major violations may have more serious consequences: fines up to € 20 million or 4% of a firm's global turnover (whichever is higher). The maximum fines of course do not mean that by default it is applied the highest level of administrative measures. The exact level of the fine depends on many factors, such as the severity of the non-compliance or possible breach of personal data; the measures taken to comply with the GDPR; the degree to which the organization fails to establish and provide essential mechanisms to prevent violations of personal data or to provide answers to the requests of entities; willingness to respond to these requests; the degree to which privacy is respected; additional measures or even the will of the data subject for how the information that has been collected will be further handled [1]. The GDPR summarizes that the first level applies specifically to data breaches. The maximum amount is set at 2% of a company's global revenue or 10 million euro, whichever is higher. To avoid this fine, it is suggested that organizations should apply high levels of security, demonstrate cooperation with the authorities, conduct a Data Protection Impact Assessment, and potentially hire Data Protection Officer. On the other hand,the second level covers the will or the consent of a data subject on how the data that is being collected or processed, should be treated. It also covers compliance with the eight rights of data subjects under the GDPR. Violations of these rights can be punished with a maximum of 4% of a company's global revenue or 20 million euro, whichever is higher [8].

3. Albanian legal framework for Personal Data Protection

After it is given above a brief analysis of some of the most important concepts of the GDPR, this part of the paper is dedicated to the Albanian legal framework for Personal Data Protection. At the time being, Albania has a dedicated law for Personal Data Protection, the Law nr. 9887 on Personal Data Protection, dated 10.03. 2008, which was promulgated by decree number 5671dated 21. 03. 2008. It acts as a legal framework for personal data protection and security in the Republic of Albania, but its

territorial scope affects: (a) all data controllers located in the Republic of Albania; (b) all diplomatic missions or consular offices of the Albanian state; and (c) all data controllers, who may not be located in Albania, but perform their activity through the use of any means located within the territory of the Republic of Albania.

Similar to the General European Regulation on Personal Data Protection GDPR, even in the Albanian legal framework, there are two main stakeholders, the Data Controller and the Data Processor and for each of them, the law clearly states the responsabilities and obligations in order to guarantee the protection and security of thesubject's personal data [10]. Furthermore, the legal framework analyses also the Data Subject, whose personal data are being collected, processed or saved by the Controller and the Processor. Even in the Albanian legislation for personal data protection, the legal framework states that the Data Subject has some foundamental rights which should be taken in consideration when processing the personal data and the legal way how it must be protected by the controllers and/or processors.

Personal Data Protection Commissioner

On the other hand, in the Albanian legal framework it is stated that the responsible and supervisory authority/ institution for the lawful and fair processing of personal data is the Commissioner for Personal Data Protection, who contributes to the protection of the rights and freedoms of the citizens. The Commissioner main purpose is supervision of the process and it is obliged to respect the principle of confidentiality even after the end of his / her duty. It acts as a mechanism to ensure the proper implementation of the protection and security of personal data. It is an independent authority, with full power and has at its disposal all the necessary human and technical means and resources, to ensure the protection required by European standards. Having said that, the collection, processing, storage and all the processes through which personal data passes, must be based on some basic principles of justice and security.

According to Article 30 of the Law on Personal Data Protection, the Commissioner has the right to conduct an administrative investigation, to have access to the processing of personal data, as well as to collect all the information necessary for the performance of supervisory duties. It can also order the blocking, deletion, destruction of data, or even suspend the processing of personal data when the process is considered illegal. Moreover, in cases of serious, repeated or intentional violations of the law by a controller or processor, especially when his recommendations have not been implemented even after repeated warnings, the Commissioner may publicly denounce the case or report the matter to the Assembly and the Council of Ministers.

Albanian administrative fines in case of violation

As stated in the legislation, the data processing, must be based on the principles of justice, security and legality. In the same way, Albanian legal framework also states that entities have their rights, which must be strictly respected by controllers and processors. In case the subject faces a violation of his rights, those responsible become subject to sanctions and adminisatrative measures, which are intended to punish legal offenses. Since the controller is responsible for the data of a subject and its proper processing, it is the main stakeholder affected by fines. In case of violations, the authority responsible for assessing the situation and imposing fines is the Commissioner, which also attaches to the documentation all the necessary notifications about the violations by the controller, of the obligations set by law. After that, 30 days after the fine or notification that a violation has been committed, the controller has the right to appeal to the court, but if this does not happen, 30 days within the notification, the offender must pay the imposed fine, the amounts of which are collected on behalf of the State Budget.

Furthermore, when it comes to the level of administrative fines applied to a controller which has conducted an unfair processing of personal data of a subject, in the Albanian legal framework, it is said that the lowest level of fines is 10 000 ALL, which is applied when controllers use personal data in contradiction with Chapter II of the Law, "Processing of personal data", while the highest level is calculated around 50 000 ALL, applied when controllers, do not fulfill the obligation to notify the subject, according to the definition in article 21 of this law [10]. Surely, the maximum amount of a fin does not mean that by default it is applied the highest level of the administrative measure, because the exact level of the fine depends on many other factors, analysed by the Commisioner.

But what is the result of the Albanian legal framework for Personal Data Protection and is it enough helpful to address all recent challenges that technologhy has created, in the same way GDPR has been to the European Union citizen? First of all, people are still not fully aware that their personal data is a very valuable asset that needs to be protected. Exposure to the web and cyberspace, or even the flow of

information along the way, still causes Albanian citizens data to fall into the hands of unauthorized parties and people still do not consider it as a major problem. Last month, the media published details of a large database leak that contained the personal information of more than 910,000 voters. It included members of the public, journalists, members of civil society, and well-known personalities, allegedly taken from the Civil Registry e-Albania, provided to the Socialist Party for use in the electoral campaign. The data included the subject's ID number, name, fathers name, surname, date of birth, voting center, place of birth, residence code, list number, phone number, whether they are an emigrant and if so, which country, whether they are likely to vote for the Socialist Party, birthplace, employer, and their Patron. This is undoubtedly one of the biggest data breaches in the history of Albania, but the authorities have not launched any responsible person/ party, stating that verifications are still being conducted. Furthermore, despite of being part of the legislation, Albanian legal framework for Personal Data Protection is not enough to bring helpful results for personal data security and privacy, because compared to GDPR, in the Albanian legislation, the amount of fines reach modest levels and in case of violation it would cost a company less to pay the fine, rather than to hire a professional/ information security specialist responsible for data security and protection, which would provide a persistent experience and assistance in that field.

4. Conclusions and future work

In this paper it was stated that the GDPR is the strictest regulation ever adopted so far to protect the personal data and under certain circumstances, its global impact affects even companies and organizations outside the European Union. On the other hand, the Albanian law on protection of personal data, is currently not sufficient to provide the necessary security and protection and without the necessary changes and/ or interventions, it is not be ready to face the changes of the European legislation. As a result, first of all I would recommend that for the Albanian society, the first step towards the necessary changes would be rising awareness on personal data protection. Moreover, the Albanian law on data protection is currently very old and can not address cyber security attacks of the last years, when the technology is being developed rapidly. Thus, not only it is needed the law to be changed, but also to follow the best international/ European practices. Higher administrative fines and other strict sanctions similar to GDPR, would be a recommended solution.

5. Acknowledgements

I am very thankful to Prof. Assoc. Dr. Edlira Martiri for leading me in this research and for always supporting, helping and inspiring me to become a good professional in the Information Security field, since the beginning of my studies.

6. References

[1] Boardman R., Mullock J., Mole A., "Guide to General Data Protection Regulation", Bird& Bird Publications, 2020

[2] Ingley C., Wells P., "GDPR: Governance Implications for Regimes outside the EU", 14th European Conference on Management, Leadership and Governance, Victoria, Australia, 2018

[3] Sorensen J., Kosta S., "Before and after GDPR: The changes in third party presence at public and private European websites", The World Wide Web Conference, 2019

[4] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and onthe free movement of such data", Official Journal L 281, 23/11/1995 P. 0031– 0050: EUR-Lex - 31995L0046 - EN (europa.eu)

[5] The e-Privacy Directive (Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 (OJ L 201, 31.7.2002, p. 37) and Regulation (EC) No 2006/2004) of the European Parliament and of the Council of 27 October 2004 (OJ L 364, 9.12.2004, p. 1).

[6] "Reform of EU Data Protection rules", European Commission: (europa.eu), 2012

[7] "The Territorial Scope", Article 3, The General Data Protection Regulation, 2016

[8] "General conditions for imposing administrative fines", Article 83, The General Data Protection Regulation, 2016

[9] "European Regulation (EU) 2016/679 (General Data Protection Regulation)" | https://gdpr-info.eu/

[10] Albanian Law nr. 9887 on Personal Data Protection, dated 10. 03. 2008: http://www.pp.gov.al/web/ligj_mbrojtja_e_te_ dhenave_personale_40.pdf