PROTECTION OF THE PERSONAL DATA IN ALBANIA IN COMPLIANCE WITH THE GENERAL DATA PROTECTION REGULATION

by Sara Zotaj

LL.M. Capstone Thesis

SUPERVISOR: Professor Alvaro Fernandez De La Mora

Central European University Private University

Quellenstrasse 51-55, 1100 Vienna Austria

ABSTRACT

The protection of privacy and personal data in the European Union has developed further by the enactment of the General Data Protection Regulation, which has had an impact not only in the European Union member states, but also on the countries aspiring to become part of the EU, such as Albania.

This thesis is going to provide a general overview of the General Data Protection Regulation and Albanian Law under a comparative analysis, aiming at demonstrating the differences that exist among the legislations. The first part of the thesis will be focused on two of the major differences existing between GDPR and Albanian law, specifically the usage of publicly available data, and the right to be forgotten. These two areas will be discussed in order to identify the differences, so to serve as an indication of the state of law in Albania in the area of personal data, while giving recommendations on the steps to be taken in order to be cognizant of the efforts required to comply with the best practices of the Regulation.

In order to have an efficient system of protection of personal data, an up-to-date legislation is not sufficient. There is a need for effective institutions that apply the law in practice and this thesis will discuss the level of fines imposed by the regulatory authorities in the European Union and the Information and Data Protection Commissioner in Albania. This thesis will include a critical evaluation of the level of fines, while analyzing if there is a need to change the approach towards sanctions in the Albanian practice, in order to achieve the goal of preventing further breaches of personal data.

This thesis will aim to provide a contribution to the further development of the protection of the personal data in Albania, which is an area of law that is gaining more attention after the entry into force of the General Data Protection Regulation.

TABLE OF CONTENTS

INTRODUCTION

The protection of personal data is at the center of attention nowadays, in international and national level, this due to the developments of the technology. The technological advancement and globalization, beside all the positive effects they have had, are accompanied by an increasing demand for more efficient measures in the domain of the protection of privacy.[1] The internet has created a new dimension on how the breach of privacy is understood, because of the storage and communication of the data.[2] These data are not only processed by a large number of subjects, but also are easily transferable.

We are moving from the era of processing data manually to an automated process,[3] where the use of technology is increasing significantly, which requires not only an effective legal framework, but also due emphasis has to be given to the execution of the administrative sanctions in cases of breaches.

In response to the new developments of the technology, the European Union enacted the Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, which replaced Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such, and is now applicable in all the EU Member States. The Regulation introduces new concepts, as well as an increased level of fines in cases of breaches. The increased enactment of fines towards the subjects that have breached the obligations is a demonstrating factor of the importance of protecting the personal data. The Regulation even though applicable only to the EU member states, has had an impact on countries like Albania as well, that are in the process of accession to the EU.[4] During this process Albania has to harmonize its legislation with the EU

[1] Van den Hoven, Jeroen, Martijn Blaauw, Wolter Pieters, and Martijn Warnier, "*Privacy and Information Technology*", The Stanford Encyclopedia of Philosophy (Summer 2020 Edition).
[2] Daniel J. Solove, *"The Digital Person, Technology and Privacy in the Information Age"*, New York University Press, New York and London, 2004.
[3] Tehreem Naeem, "*Data Automation: How it Transforms Enterprise Landscape"*, April 2021.
[4] This can be proven by the twinning project undertaken by Albania, that aims to provide guidance on the road to the harmonization of the legislation.

legislation, a task which requires time, engagement and a thorough understanding of the EU law and how is this law to be implemented in Albania.

The provisions of the GDPR are numerous and cover a broad range of issues related to the protection of the data, but it would be excessive for the purpose of the thesis to be engaging in an analysis of all the provisions and comparison with the Albanian Law. The purpose of this thesis is to focus on the issues I find most relevant and for which there are differences between the two legislations, such as the processing of publicly available data; the right to be forgotten and a specific chapter will be dedicated to the practical aspect of implementing the sanctions in cases of breaches.

The issue of the processing of publicly available data is relevant as it concerns the core element of the protection of personal data, that being the consent of the data subject, and for which Albanian legislation is in discrepancy with the Regulation. The second issue, that of the right to be forgotten, is a new concept for the Regulation as well, which as a novelty increases the power of the data subject over their data. The right to be forgotten is not included in the Albanian law, therefore, not guaranteeing the full protection to the data subject. But all these provisions would be futile if their implementation in practice was not effective, and therefore the thesis will include a critical analysis of the process of practical implementation in cases of breaches of personal data, consisting mostly of fines. The issues covered by this thesis aim to give recommendations for the harmonization of Albanian Law and practice, by taking as a model the positive developments of the GDPR.

I would note that the process of harmonization of the Albanian legislation with that of the EU is not an easy process, especially for countries like Albania, whose economic development is not on the same level as most of the European countries.[5] The recommendations included in this thesis should serve the Albanian legislator and enforcement institutions as an indicator on how the road to compliance should proceed in the areas covered in this thesis. GDPR has not been in force for a long period of time and its impact will be seen more in the future, but for the time being the practices set by the GDPR should be followed by EU member states, and if Albania intends to be part of the EU, it should be conscious beforehand with the requirements and the efforts needed to keep in pace with the European level.

[5] EUROSTAT, *Key figures on enlargement countries-2019 edition*, March 2019.

The area of the protection of personal data in Albania is certainly moving forward, but there is a lack of general understanding by the public of their rights,[6] as well as a lack of academic writings and non-inclusion of the topic in the academic curricula. This thesis aims to give its contribution to some aspects that might be considered by the lawmaker and the implementing authorities as necessary steps to be taken in the process of accession of Albania to the European Union.

This thesis is going to include a comparative analysis focusing on the similarities and differences existing between GDPR and the Albanian Law, having as aim to support the positive steps taken by Albania, but at the same time to highlight the necessary amendments to be made to the legal framework and the practical implementation of sanctions, to be in compliance with the best practices of the GDPR.

The thesis will be consisting of three chapters, each chapter covering different aspects of the protection of personal data.

The first chapter will begin with the introduction of the regulatory framework of the European Union and the Albanian legislation. During the analysis, it will be noted that the legislation in Albania has not changed after the enactment of the GDPR, but steps are being taken to comply with the Regulation, one of them is a twinning project funded by the European Union, which aims at assisting Albania in complying with the GDPR.

The second chapter will be focusing on some aspects of the protection of the personal data, which I find most relevant and for which I propose that Albanian Law has to change its approach. The chapter will analyze one of the most important elements of the Regulation, that being the lawful grounds for processing the personal data, which is the starting point for all the subjects that want to engage in the processing of data, by getting the clear and unambiguous consent of the person whose data are being used. This chapter will illustrate the similarities of the Albanian Law, while pointing out the differences that exist, especially in the processing and usage of publicly available information. Albanian Law in opposition to the GDPR, recognizes the usage of publicly available data as lawful if the controller carries out personal data processed for the purpose of offering

[6] The office of the Albanian Commissioner has been undertaking informative campaigns, in order to raise awareness to the general public of their rights and how to protect these rights. For more see Commissioner for the Right to Information and Personal Data Protection, National Campaign "*Digital education, play and learn - Happy onlife*", Nr. 9 & 10, December 2020.

business opportunities, if the data are taken from a public list of data. By recognizing such a right, the law explicitly provides for an "escape" from the obligations of getting the consent of the data subject.

The second chapter will proceed with the right to be forgotten, which is a new concept included in the GDPR and whose presence is missing in the Albanian Law. The GDPR introduced the "right to be forgotten" as an obtainable right, by giving the right to individuals to effectively remove their old and outdated, inaccurate, or excessive information from the search results and guaranteeing the data subject rights over the usage of their personal data.[7] In order for the protection of the personal data to be complete and effective, Albanian Law should take notice of the GDPR and include such a provision in the law, while proceeding with caution in its implementation and striking the right balance between the right to be forgotten and the right to be informed of the general public.

However, the law is not the only element of an effective system, the practical implementation plays an important role as well and the third chapter will be focused on this practical component. The European authorities have imposed enormous fines to large companies when they were found to have breached the provisions of the Regulation. These fines are high because they are considered to be an effective measure in preventing the companies from further engaging in breaches[8] that have a big impact on the right to privacy and dignity of the individuals.[9] Finding the right level of sanctions is not an easy task and European authorities have to balance the right of privacy of the individuals with the right of the company to keep functioning in the market, and at the same time to teach the company a lesson through the fines, that these behaviors are not to be tolerated and the companies should proceed carefully.[10]

[7] Article 17 of the GDPR.
[8] Recital 150 of the GDPR recognizes that the purpose of the fines is to ensure compliance with the obligations under the Regulation and to prevent the consequences of the infringement.
[9] The European Union Agency for Cybersecurity (ENISA) has noted that "Breaches of personal data can lead (and have led) to serious impact on the affected individuals' private lives, including humiliation, discrimination, financial loss, physical or psychological damage or even threat to life." *See* Personal data breaches < https://www.enisa.europa.eu/topics/data-protection/personal-data-breaches#:~:text=Data%20Protection,-Privacy%20by%20Design&text=Such%20breaches%20can%20lead%20(and,or%20even%20threat%20to%20life.>
[10] The decision of the UK's data protection authority in the British Airways (BA) case, is an example of the balancing test undertaken by the authorities. The UK's data protection authority in 2019 intended to fine BA more than £183m for breaches of the GDPR. However, the authority in the end of the process imposed a lower fine of £20m, after considering mitigating factors, such as the economic difficulties faced by BA during the coronavirus crisis. For more,

For the analysis to be comprehensive, this chapter will also include an overview of the competencies of the Albanian Information and Data Protection Commissioner, which is the central subject in passing Guidelines to help the implementation of the law, as well as to impose the necessary penalties in cases of breaches.

This chapter will highlight that even though the aim of the fines is the same as the one in the GDPR,[11] that of preventing the further engagement of companies in the infringement of personal data, the practical implementation of the law in Albania still has a long way to go. The changes needed in the implementation of the fines come as a necessity, when looking at the level of the fines imposed under the Albanian Law, which differ vastly from the level of fines under the GDPR and in certain instances, the controllers are not held responsible at all for actions which, in my opinion amount to breaches of personal data of the individuals.

As per the methodology used, it will include the doctrinal and comparative approach as it relates to GDPR and Albanian law on the protection of the personal data and will also include the comparative method between the two jurisdictions as it regards the administrative fines imposed in cases of breaches.

see: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/.

[11] Article 3(17) of the Albanian Law holds that the Commissioner supervises the processing of personal data in order to prevent further violations and, where appropriate, the imposition of administrative sanctions to ensure the implementation of its decisions.

CHAPTER I

THE REGULATORY FRAMEWORK UNDER THE GDPR AND ALBANIAN LAW

1.1 The protection of personal data under General Data Protection Regulation and Albanian Law

The protection of personal data holds an important role in the European Union, being guaranteed as a right under Article 8 of the Charter of Fundamental Rights of the European Union.[12] As a fundamental right, the protection of the personal data imposes a negative obligation upon the European institutions and member states to not illegally interfere with the personal rights, but also a positive obligation to adopt legislation that identifies the most efficient rules in their protection.[13] This is even more prominent in the era of advanced technology, where the processing of personal data happens in a large scale, affecting the rights of the individuals.

In these circumstances, in 2016 the European Union adopted the General Data Protection Regulation[14] (GDPR), which establishes the regulatory framework for the protection of the personal data. The GDPR came as a necessity, to ensure standardization among the European countries, because the previous legal framework was based on a directive,[15] for which different European countries had different methods of application.[16] These different methods of application undermined the uniformity and legal security of individuals at the same time, because they did not provide the same level of protection in different European countries and it had been noted that

[12] Article 8 of the Charter of Fundamental Rights of EU: "*Everyone has the right to the protection of personal data concerning him or her."*
[13] Mistale Taylor, "*The EU's human rights obligations in relation to its data protection laws with extraterritorial effect"*, International Data Privacy Law, 2015, Vol. 5, No. 4.
[14] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
[15] Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data.
[16] GDPR - *User-Friendly Guide to General Data Protection Regulation* < https://www.gdpreu.org/>

countries acted "opportunistically to court big tech with signals of weak enforcement and advantageous tax schemes."[17]

General Data Protection Regulation's main purpose is to ensure a consistent level of protection for natural persons throughout the Union, as well as to provide legal certainty and transparency for economic operators.[18]

Meanwhile, the protection of personal data in Albania is a constitutional right, guaranteed under Article 35 of the Constitution.[19] This legal provision, raised at the constitutional level, shows the importance of protecting the personal data of the individuals by obtaining the consent of the person whose data are being processed.

In accordance with the Constitution, currently, the protection of personal data in Albania is regulated by the Law no. 9877, "On the protection of personal data" (hereinafter The Law).[20] The adoption of this law came as a necessity in the period when Albania was trying to ensure a certain European level of data protection and the law is in compliance with Directive 95/46/EC, which although it is not nowadays in force, it contained many provisions which we now find in the Regulation. Even though Law no. 9877 governs only the protection of personal data, the right to information is treated in parallel with it, this mainly because the competent authority covering the protection of the right to information is also responsible for the protection of personal data.[21] I would consider these two areas as interrelated to one other that need to be addressed together, because there are cases where there is a need to strike a balance between the right of the data subject to the protection of its personal data and the right of the public to be informed.[22]

The Law is not the only instrument applicable to the protection of the data, there are other secondary legislation and also an important role in the legislative framework plays the Albanian

[17] Chris Hoofnagle et al., "*The European Union general data protection regulation: what it is and what it means", 28 Information and Communications Technology Law* 65 (2019), p. 71.
[18] Recital 13 of the General Data Protection Regulation.
[19] Article 35 of the Constitution of the Republic of Albania notes that: […2. The collection, use and disclosure of data about the person is done with his consent, except in cases provided by law. 3. Everyone has the right to be acquainted with the data collected about him, except in cases provided by law. 4. Everyone has the right to request the correction or deletion of untrue or incomplete data or collected in violation of the law.]
[20] Law no. 9877, dated 10.03.2008 "On the protection of personal data", as amended.
[21] This role in Albania is held by The Information and Data Protection Commissioner.
[22] Report of the Council of Ministers on the draft law "On Some Changes and Additions to The Law No. 9887, dated 10.3.2008,"On Personal Data Protection", as amended".

Information and Data Protection Commissioner, which has the competence to issue numerous guidelines on security measures to be taken in the activity of specific sectors. I can mention here the latest guidance of the Commissioner on "Protection of Personal Health Data",[23] which aims to regulate additional situations and grant wider protection to the individuals in the field of health data, which are considered as sensitive data. It is true that the guidelines do not have the same implementation and binding force as the Law and Decision of the Council of Ministers, but this should not be a disincentive in implementing these necessary supplementary acts.[24]

I would like to draw the attention to the fact that the latest amendments made to the law were in 2014, some years prior to the enactment of the GDPR. Should the fact that the law has not been amended after the enactment of the GDPR be the determining factor in assuming that Albanian Law is not in accordance with the GDPR? I would have to give a negative answer to this question, because even though there is certainly room for improvement not only in the legislative component, but also the enforcement one, Albanian legislation provides for the necessary protection of personal data. The necessary protection is supplemented by the secondary legislation adopted by the Council of Ministers and the Commissioner as well.

The Law provides that it will be applicable to the processing of data by controllers[25] established in the Republic of Albania and controllers who are not established in the Republic of Albania but that use equipment situated in the Republic of Albania.[26] The Law has tried to cover not only the processing of data by Albanian controllers, but also by foreign controllers using equipment in Albania, but the Law does not clarify whether it applies to the processing of the data of Albanian citizens by controllers not established in Albania. Meanwhile the GDPR makes it clear its extraterritorial scope by applying even to companies that are not established in the EU, but "that use personal data for monitoring the behavior of people in the EU",[27] contrary to the Albanian Law

[23] Guidance of the Commissioner No. 49, dated 02.03.2020.
[24] According to Article 116 of the Albanian Constitution, the Laws and Decision of the Council of Ministers are higher in the normative hierarchy and are mandatory upon all, compared to the Guidelines, that have an internal character and are mandatory only for the administrative units that depend on them.
[25] According to Article 4(7) of the GDPR the controller is the subject that determines the purposes and means of the processing of personal data.
[26] Article 4 of the Law no. 9877, dated 10.03.2008, "On the protection of personal data", as amended.
[27] Chris Hoofnagle et al., "*The European Union general data protection regulation: what it is and what it means*", Information and Communications Technology Law 65 (2019).

that seems to have failed to guarantee the rights of the Albanian citizens for processing happening abroad.[28]

Even though the extraterritorial application of the GDPR might raise issues[29] because of the broad interpretation given to the clause, the GDPR has tried to clarify[30] that there are various factors to be considered in deciding whether the GDPR will apply to controllers not established in the Union.

Taking into consideration these clarifications of the GDPR, Albanian Law would have to reconsider the territorial scope of application to controllers not established in Albania, but that process data of Albanian citizens. This application of the law for the processing of data of Albanian citizens should be seen in the light of the new technological developments, which make it easier for the processing of the data to happen everywhere, regardless of the physical presence in a specific territory. In order to adapt to these rapidly changing technologies that enable the processing to take place everywhere, Albania would have to amend the law. The amendment is needed in order to equally protect all Albanian citizens, without making a difference on their rights just because the controller is not established in Albania, but which nevertheless constitutes a breach of personal data.

[28] Article 3(2) of the GDPR.
[29] Toby Blyth and Jessica Yazbek*, Does the EU's General Data Protection Regulation have extra-territorial effect?,* 16 November 2020.
[30] Recital 23 of the General Data Protection Regulation.

CHAPTER II

SPECIFIC ASPECTS OF THE PROTECTION OF PERSONAL DATA

The General Data Protection Regulation is a voluminous document, aiming at regulating a broad range of issues that were included in the previous directive, but the GDPR has increased the level of protection guaranteed to the data subjects in the light of the technological developments as well. The GDPR has put a stronger emphasis on the privacy aspect, by requiring a clear, specific, and unambiguous consent of the data subject for the processing to be lawful.[31] The GDPR adds additional information that the controller has to provide to the data subject, such as the legal basis for processing, the amount of time that the controller intends to use the data and also a specification of the rights the data subjects have, and which are the means to pursue such rights.[32]

Similarly to the provisions of the GDPR, Albanian Law includes the duties of the controller in getting the consent of the data subject and informing the latter of their rights.[33] But the Law differs from the GDPR as it pertains the usage of publicly available data, where under Albanian Law the processing is lawful,[34] even without the consent of the individual, which is in contradiction to the GDPR that requires consent regardless if the data are private or public.[35]

While the GDPR has introduced novelties in its provisions such as the right to be forgotten and therefore offering the data subject more control over their data, Albanian Law does not include such a provision and consequently does not grant the full protection to the data subject.

2.1 Lawful grounds for the processing of personal data

For the processing of personal data to be lawful and not subject to fines under the GDPR, the latter recognizes six grounds, that at least one of them has to be met.[36] These grounds include: a) Getting the consent of the data subject; b) Processing is necessary to meet the requirements of a contract to which the data subject is a party; c) To enable compliance with a legal obligation; d) To protect

[31] Article 4(11) of the GDPR.
[32] Article 13 of the GDPR.
[33] Articles 5-6 of Law no. 9887, dated 10/03/2008, "On the Protection of Personal Data".
[34] Article 6(3), *supra*.
[35] Article 14(2)(f) of the General Data Protection Regulation
[36] Article 6 of the GDPR.

vital interests of individuals; e) As a public task recognized by law; f) Legitimate interests of the controller.

The first ground of getting the consent requires that the processing should only happen when the data subject has given its free consent after being informed of the purpose of the processing.[37] But getting the consent of the data subject it is not always an easy task and there has been a case decided by the Polish Data Protection Authority, where the company had processed large amount of data, claiming that it was impossible getting the consent of all the individuals whose data were being processed.[38] The decision which will be discussed in more details in the third chapter, makes it clear that if the controller has the possibility to inform and get the consent of the data subject and that it would not be burdensome for the company, then it has to perform such a duty. From this decision I can note of the importance put on getting the consent, even in circumstances of processing large amount of data.

Similarly, under the Albanian Law in order for the processing to be lawful, the same grounds as the ones mentioned under the GDPR apply, consisting of getting the consent of the data subject, to enable compliance with a legal obligation; to protect vital interests of individuals; as a public task recognized by law; and the legitimate interest of the controller.[39]

But there is one major difference with the GDPR, related to the processing and usage of publicly available information. While analyzing the Regulation, I noticed the inclusion in its articles of the duty of the controller to inform the data subject, whether the information came from publicly accessible sources, and that the term public domain has no relevance in data protection regulation.[40] The Regulation therefore recognizes the protection of personal data, even those collected through public sources. On the other hand, Article 6(3) of the Albanian Law states that the processing is lawful if the controller carries out personal data processing for the purpose of offering business opportunities or services, provided that the data were taken from a public list of data.

[37] Article 7 of the GDPR.
[38] *See* the decision of the Polish Data Protection Authority (DPA) of 25 March 2019.
[39] Article 6 of the Law no. 9877.
[40] Article 14(2)(f) of the General Data Protection Regulation.

While in the European Union measures are being taken for processing of large amount of data, that are collected from public sources without getting the consent of individuals,[41] I find the provision of the Albanian Law somehow problematic, because by recognizing such a right of the controller, we risk being faced with an abuse of this right and usage of all these data, without even considering what the primary purpose of those published data was.

By explicitly acknowledging this right the Law provides a leeway for the controllers to use the data for business opportunities, by which they would be making profits under the umbrella of publicly available data, when there might be other more appropriate approaches to be taken, one of them being the legitimate interest of the controller. From the language used in Article 6(3) of the Albanian Law, I would interpret it that the data taken from a public list of data entails a list of data held by public institutions and not every available information online. But even if the legislator intended to allow and consider lawful only the processing of those data held by public institutions, this would still not solve the problem of misusing the data contrary to the original purpose of when they were included on those lists, which would be in breach of one of the principles of the GDPR and Albanian Law.[42]

The fact that the GDPR does not unequivocally recognize the lawfulness of processing publicly available data should not be understood as if this processing is impossible, because the Regulation provides for grounds such as the legitimate interest of the controller, which is a broad concept used to justify the processing of data made publicly available, and as long as the Albanian Law recognizes the concept of legitimate interest of the controller, this can be used to legitimize the use of public information.

[41] Referring to the decision of the DPA of 25 March 2019.
[42] Article 5(1)(b) of the GDPR and Article 5(1)(b) of the Albanian Law recognize that the processing of data has to happen only for the specific purposes mentioned when the processing started and should not be further processed in a manner that is incompatible with those purposes.

2.2 The right to be forgotten in the GDPR and the lack of the right in the Albanian Law

The lawful processing of data is one component, but to grant a broader protection to the individuals, the Regulation has included a new concept, that of the right to be forgotten, a concept that was not unequivocally governed by the previous Directive.[43] Such a right has been defined as the "right to the erasure of personal data concerning the individual without undue delay"[44] if one of the conditions applies.[45] The inclusion of this concept is considered as an important part of the right of the individuals in deciding how their data are to be handled, but such a right is not without limits, otherwise we would be granting the individuals with the possibility to request the erasure of every information they consider to be in their disfavor.[46]

The "right to erasure" or "right to be forgotten" came into the spotlight in 2014, during the *Google Spain*[47] case, which resulted in the right's EU-wide acceptance and inclusion into the General Data Protection Regulation.

It is interesting to analyze the decision in the "*Google Spain*" case, which was decided under the Directive 95/46/EC, which as I mentioned above did not conceptually recognize the right to be forgotten. However, the European Court of Justice held that even publication of accurate and correct data can be in opposition with the Directive. This means a person could request removal of such data, both from the source of publication and the search engine, even when its initial publication was lawful, recognizing the right of the individual to request the deletion of those data that are not anymore relevant due to the passing of a long period of time.[48]

The Regulation recognized[49] various grounds under which the data subject has the right to request erasure, such as: when the personal data are no longer necessary for the purpose they were

[43] Article 12(b) of the Directive held that: "*Every data subject has the right to obtain from the controller the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data*". This definition covered only the erasure when the data were incomplete or inaccurate, but did not cover the situations when the erasure is required because the data are not anymore relevant.
[44] Article 17 of the Regulation.
[45] The grounds for erasure include that the data is no longer necessary; the data subject withdraws its consent; the data subjects right outweigh the legitimate interest of the controller. For more information, see Article 17 of the GDPR.
[46] This has been held as an argument against "the right to be forgotten". For more, see ARTICLE 19, "*The "Right to be Forgotten": Remembering Freedom of Expression",* 2016.
[47] Case C 131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos* (AEPD), *Mario Costeja González* [2014] ECLI:EU:C:2014:317.
[48] *Ibid*., paras. 99.
[49] Article 17 of the GDPR.

collected; when the data subject withdraws its consent; when the personal data were processed illegally, etc.[50] Analyzing these grounds recognized by the GDPR, I would hold that the inclusion of the right to be forgotten is important in shifting the power in the hands of the data subject, to limit the actions of third parties that might abuse with the rights of the individuals, under the justification of the freedom of expression.

But, as a new concept, the right to be forgotten has also been faced with criticism.[51] The critiques are mostly focused on the practical implementation and specifically on the process of balancing the freedom of expression and the availability of public information, with the right of privacy of the data subject. This balancing exercise is not an easy task and has to take into consideration the fact that the erasure might require the deletion of many data of public interest which might cause tensions in the political area within the country as well. However, the GDPR has attempted to regulate this problem by holding that the right to erasure will not apply when it conflicts with the freedom of expression, and the public interest in these cases prevails.[52] One other critique rests on the cost-increase that the companies would have to face when dealing with a request for erasure, because in itself, granting rights to a group of people, puts obligations on others, in this case the companies.[53]

If the European national authorities will be proficient in finding the correct ways of implementing the right to be forgotten, by balancing the freedom of expression and the right to information, with the autonomy given to the individuals, the right to be forgotten will have a positive impact on society. This positive impact on the society stands not only on the right of the individual to decide upon its own data, but it has a moral element as well, because people should not be indeterminately reminded of their past mistakes.[54] The right implementation by the EU authorities might as well serve as a model for Albania, where this right is not recognized, a legal omission that requires legislative amendments and additionally, guidance on its implementation.

[50] *Idem.*
[51] Christiana Markou, "*The Right to Be Forgotten" Ten Reasons Why it Should Be Forgotten, Reforming European Data Protection Law*, Serge Gutwirth, Ronald Leenes, Paul De Hert, Editors, Law and Governance Technology Series, Issues in Privacy and Data Protection, Volume 20, Springer, 2015, p. 205.
[52] Article 17(3)(a) of the GDPR.
[53] Paul A. Bernal, "*A right to delete*?", European Journal of Law and Technology, Vol. 2, No.2, 2011.
[54] ARTICLE 19, "*The "Right to be Forgotten": Remembering Freedom of Expression",* 2016, p. 14.

As mentioned, Albanian Law does not recognize the right to be forgotten, but it contains a provision dealing with the right to erasure of data, whenever the individual is informed that data relating to him are irregular, false, and incomplete or have been processed and collected in breach of the Law.[55] But, the right to be forgotten is not associated with the erasure due to the inaccuracy of the data, but is more connected with the time-factor.[56] In these circumstances, this provision of the law does not provide to the individual the right to request the erasure of information, which is not taken in breach of the Law, but nevertheless it has lost the relevance and it is not anymore necessary to be kept online.

2.3 Attempts made by Albania to comply with the GDPR and the need for legislative changes

The road to complying with the GDPR is a demanding one, but steps are being taken in this direction. In 2020 Albania became part of a Twinning Project between Italy, Austria and Albania funded by the European Union, named "*Institution-building for alignment with the Union acquis on the protection of personal data*".[57] The expected results of the Project are to provide support to the harmonization of Albanian legislation with the GDPR and the Enforcement Directive,[58] accompanied with capacity building for enforcement of the new legal framework, which would provide the knowledge and organizational instruments to handle potential challenges concerning the enforcement of the new Data Protection legal framework in Albania. It is impossible to discuss about the outcomes of this project at the time being because we will have to see the implementation during this year.

The Role of the Albanian Commissioner in raising awareness not only among the controllers and processors,[59] but also to the public of their rights protected by the Law is an important component in having an efficient system of protection and for this there is no need for legislative changes, but

[55] Article 13(1) of the Albanian Law.
[56] Recital 65 of the GDPR holds that the "In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed."
[57] *See* https://www.idp.al/twinning/
[58] Directive 2016/680 of the European Parliament and Of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.
[59] Article 4(8) of the GDPR states that the processor is a natural or legal person, public authority, agency, or other body that processes the data on behalf of the controller.

for a well-prepared institution that possesses knowledge and best practices related to the GDPR. In this regard, the office of the Commissioner is constantly undertaking information campaigns with different actors involved in the area of personal data, including the pupils in elementary schools and the public administration.[60]

Apart from the positive steps being taken, there is room for legislative amendments to be made. As the Law has not changed since 2014, I would suggest that there is a need to clarify the usage of publicly available data by the controllers, to avoid any misuse of the data which might cause breaches of the rights of the individuals. One other aspect to be considered by the legislator is the inclusion of the right to be forgotten by determining the obligation of the controller to delete personal data without undue delay. The GDPR could be of guidance in this regard, as Article 17 of the GDPR recognizes the grounds under which the data subject can require the execution of the right to be forgotten, grounds which might be included in the Albanian Law and which consist of:

- personal data are no longer needed in connection with the purposes for which they are collected or processed;
- the data subject withdraws the consent on which the processing is based and if there is not another legal reason for the processing;
- the data subject opposes the processing and there are no legitimate overriding reasons for the processing.

The legislator has to make sure to preserve the balance of the rights, by including the exceptions in which the right to be forgotten will not be applicable, such as in cases of freedom of expression, for the fulfillment of legal obligations by the state or for public interest reasons, which are reasons recognized as exceptions by the GDPR as well. It is important to emphasize that Albania does not have to limit itself only to the legislative language of the GDPR, but is advised to consult the case-law of the Court of Justice of the European Union as well, which interprets the Regulation and sheds light over the implementation of the GDPR and how is the balance of the rights to be undertaken.[61]

[60] *See* Activities of The Commissioner's Office, < https://www.idp.al/2020/06/30/training-for-the-public-administration-on-personal-data-protection-and-transparency/?lang=en>
[61] Recital 143 of the GDPR.

CHAPTER III

THE MEASURES TAKEN IN CASES OF BREACHES UNDER THE GDPR AND ALBANIAN LAW

3.1 The level of fines under the General Data Protection Regulation

Protection of the personal data requires an effective system of administrative and judicial measures taken when data protection breaches have occurred. This is one important aspect of the General Data Protection Regulation, which in its Article 83 states the level of fines to be imposed, and the factors to be considered when deciding on the imposition of the fines.

GDPR in its articles does not make a distinction as whether it will apply only to large multi-national companies or to small and medium enterprises, because its intention is to be applied broadly to every type of business. But if I were to understand the inclusion of all companies as to be imposed the same level of fines, this would not be true, because GDPR has recognized a margin of appreciation for the national authorities, because the fines depend on the circumstances of each case and the amount is variable and not fixed in all cases.[62] This is a rational standing, because every case depends on different circumstances and even though before the law everyone is equal, this does not have to be understood as the same level of fines has to be imposed on every company, because it would lead to unjust treatment.

The competent authorities for administrating the fines are the data protection regulators in each European Union country[63] and these regulators will assess whether there has been a breach of personal data and which is the appropriate level of fine. GDPR recognizes that there are two levels of fines, this based on the severity of breaches. The less severe breaches include the violation of articles concerning:[64] i. the duties of controllers and processors under certain articles of the Regulation; ii. The assessment process of the certifying organizations by the certification bodies;[65]

[62] Article 83(2) of the GDPR.
[63] Recital 79 of the GDPR and Article 83.
[64] Article 83(4) of the GDPR.
[65] Certification is a process that serves to demonstrate that the company is processing data in accordance with the GDPR. Certification is voluntary, but the companies are interested in obtaining this certification because it helps them to be more transparent and at the same time earn the trust of the data subjects that the latter's data are being processed

iii. The independence required by the monitoring bodies when dealing with complaints. In these cases, the level of administrative fines imposed varies from up to 10 000 000 EUR, or in the case of an undertaking up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.[66]

The second level of fines includes the breaches that are considered graver and include serious violations of the basic principles of processing, such as not getting the consent of the data subject,[67] breach of the data subject's rights related to the fact that the individuals have to be informed about how their data are being processed, and as discussed above they have the right to request their data to be deleted and corrected. As these infringements are more serious, the level of fines goes in proportion with that, therefore GDPR holds that they can reach up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.[68]

When looking at these numbers one might think that they are excessive and unjustifiable for the companies, but there is a valid reason why the fines are high and why they should be high, and that is related to the importance of protection of the privacy and dignity of the individuals. Living in a digitalized world has made the processing of personal data easier and in larger amount than before, creating the risks for more breaches of the rights of individuals.[69] Companies are using the internet and the search platforms to get personal data, which are later used for marketing purposes and by using these methods the companies are making huge amounts of profits.[70]

It is important to analyze what would happen if the level of fines was trivial compared to the financial benefits that the companies were making from the processing of these data. Finding the right balance between imposing the appropriate level of fines and also allowing the business to keep functioning in the market is not an easy task for the national authorities. As we will see below, there have been various cases where the national authorities have imposed very high fines, for

lawfully. The certification is issued by the certification bodies, which are accredited bodies by the competent supervisory authorities of each member State of the EU.

[66] *Ibid.*

[67] Article 7 of the GDPR clearly states the importance of getting the consent of the data subject prior to the processing of data, in order for the processing to be lawful.

[68] Article 83(5) of the GDPR.

[69] This is recognized by recital 5 of the GDPR.

[70] Mat Travizano, "*The Tech Giants Get Rich Using Your Data. What do You Get in Return?",* September 2018. < https://www.entrepreneur.com/article/319952>

which I have to say were imposed on large companies with high revenues. It is important to try to find the right balance, because if the fines would be lower, it could result in an adverse effect by not preventing the companies from processing these personal data, but on the contrary, it would encourage them to keep processing more and more, as long as the fines are low, and they would make more profit from the processing, compared to the losses they would get from being fined.

As previously mentioned, the national authorities enjoy a margin of appreciation when deciding the level of fines and they have to base their decisions on a number of factors. The regulation notes[71] that the factors to be considered include, among others: the type and severity and duration of the infringement; the willingness for committing the infringement; whether the controllers/processors took any action to reduce the damage suffered by the individuals and whether the company has breached its obligations in the past or is this the first infringement.[72]

In a research published in 2021,[73] it was noted that there had been an increase in the number of notifications towards the national authorities in cases of breaches of data,[74] which goes to showing that individuals are becoming more and more aware of their rights and protection granted by the Regulation. This increase in the number of notices should serve as a boost for Albanian individuals as well, because apart from the raising awareness campaigns by the Commissioner, the collaboration from the public is very beneficial in helping the national authority take the appropriate measures in those cases where the latter would not be able to discover on its own initiative.

[71] Article 83(2) of the GDPR.
[72] These factors are not the only factors mentioned in the Regulation and for more information, see Article 83(2) of the GDPR.
[73] Ross McKean, Ewa Kurowska-Tober and Heidi Waem *"A report produced by DLA Piper's cybersecurity and data protection team",* January 2021.
[74] In the research it is mentioned that there had been 331 notifications per day since 28 January 2020, a 19% increase compared to 278 breach notifications per day for the previous year.

3.1.1 The practical implementation of the fines by the national authorities of the European Union

Even though the Regulation has not been in force for a long period of time, its application in practice by looking at various case-law goes to showing that the national authorities are giving due importance to the protection of personal data. This can be noticed by the increased level of fines that the GDPR provides for and for which as it will be shown by the cases, the national authorities of the EU have not been reluctant on imposing such significant fines when finding a violation of the privacy and aiming therefore at preventing future breaches by the companies.

The biggest fine imposed under the GDPR thus far is the one against *Google*.[75] In this decision the French National Data Protection Commission (CNIL) imposed a €50 million fine after receiving complaints that Google was automatically processing the data of the individuals without getting their prior consent or providing information that their data were being collected. Google was found to have breached various articles of the GDPR because of the lack of transparency on the way the data were collected and failing to inform the subjects that these data were used for advertisement targeting.[76] Even though Google tried to argue that it had provided the necessary information for getting the consent, these arguments were not persuasive and the decision of the CNIL was upheld by the French court.[77]

Another decision taken is that of the Data Protection Authority of Hamburg, Germany against the clothing retailer *H&M*.[78] This decision apart from the high-level fine of €35 million, is important to be analyzed because it concerns the protection of the data of employees. The importance of processing in the field of employment is recognized by the GDPR in a separate article holding that the rules intend to protect "the data subject's human dignity, legitimate interest and fundamental rights."[79] In the *H&M* case, the employees after absences due to vacations or sick leave, had to participate in a welcome talk with the team leaders. During these meetings, some managers

[75] Decision of the French National Data Protection Commission (CNIL) of 21 January 2019.
[76] Data Privacy Manager, *5 biggest GDPR fines so far* https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/
[77] Conceil d'Etat, *RGPD: le Conseil d'État rejette le recours dirigé contre la sanction de 50 millions d'euros infligée à Google par la CNIL*, 19 June 2020.
[78] The Hamburg Commissioner for Data Protection and Freedom of Information, "*35.3 Million Euro Fine for Data Protection Violations in H&M's Service Center"*, 1 October 2020.
[79] Article 88 of the GDPR.

"acquired a broad knowledge of their employees' private lives through personal and floor talks, ranging from rather harmless details to family issues and religious beliefs."[80] These infringements were considered very serious because in such a situation the employees were the weaker party and depended on their employer, who used these data to create a detailed profile of employees for decisions concerning their employment in the future.

The application of the GDPR has seen some recent developments in the area of publicly available data, which goes beyond the cases discussed above concerning the private data of individuals. In a recent decision of March 2019, the Polish Data Protection Authority (DPA)[81] imposed a fine on a Polish company that collected data from publicly available documents and used the data to prepare reports which were later sent to clients as part of the company-verification services. The company claimed that they held more than 7.5 million records of data of natural persons and based on article 14(5)(b) of the GDPR getting the consent of the data subject would constitute a disproportionate effort. The DPA rejected these arguments by holding that the company had the addresses and the telephone numbers of the natural persons whose data the company was processing and consequently it was not an impossible duty to fulfill, which would not involve a disproportionately large effort, and subsequently imposed a fine of € 230,415.

The decision of the Polish Authority might not be considered as important in terms of economic value as the decisions rendered in cases of Google and H&M, but its importance goes beyond the numbers and focuses on the broad application of the GDPR. The decision notes that companies cannot escape their responsibilities by claiming that the data were publicly available, as long as all the personal data are considered to be equal, and the controllers have the possibility of getting the consent of the individuals without requiring disproportionate efforts.

The high-level fines imposed in these cases are an indicator that the national authorities of the EU are paying the right attention to the breaches made to the privacy of the individuals, especially by large companies which process a substantial amount of data as part of their activity. Even though the companies might consider these fines excessive and claim that it prevents them from engaging in processing activities that are necessary for the companies and their future advancements, by

[80] *Supra* at 71.
[81] Ewa Kurowska-Tober and Magdalena Koniarska "*Polish DPA issues the first fine for a violation of the GDPR – and it's harsh"* < *https://blogs.dlapiper.com/privacymatters/polish-dpa-issues-the-first-fine-for-a-violation-of-the-gdpr-and-its-harsh/#page=1*>

requiring additional efforts and financial means to comply with the requirements of the GDPR,[82] the decisions and the arguments provided by the national authorities in these cases prove that the authorities try to find the right balance between the level of fines, the breaches that have taken place and the size of the company, in order to serve the purpose of protection of individual rights.

3.2 The Role of the Albanian's Information and Data Protection Commissioner

In order to guarantee the protection of personal rights, apart from the legislation, it is important to have effective authorities in place that enforce this protection. The Regulation notes[83] that Member States have to observe the protection of personal right by independent public authorities that will monitor and enforce the application of this Regulation by imposing administrative fines as a last resort.[84]

In line with the requirements of the Regulation, in Albania this role is held by the National Information and Data Protection Commissioner. The Commissioner is an independent subject, as its functions are regulated by a special law[85] and its reporting obligations are towards the Parliament and not the executive organs.[86] The Commissioner holds an important role in protecting the personal data and some of its competences include:

- Giving the authorization for processing of the personal data for purposes not indicated in the first collection of data.
- Giving the authorization for the international transfer of personal data, by making sure to preserve that the transferred data will remain protected.
- Giving the authorization for the processing of sensitive data, under adequate measures and for a public interest.

[82] Alessandra Nistico, "*How much does EU GDPR compliance cost?"* EUGDPR, 2019. < https://advisera.com/eugdpracademy/blog/2019/09/24/how-to-calculate-your-total-gdpr-compliance-costs/>
[83] Article 51 of the GDPR.
[84] Article 58 (2)(i) of the GDPR.
[85] Aurela Anastasi, "*Independent Administrative Institutions, Issues of Administrative Law in Comparative View"*, Albdesing, 2010, p. 157.
[86] Articles 29-38 of Law no. 9887, dated 10/03/2008, "On the Protection of Personal Data".

The Information and Data Protection Commissioner in order to perform its duties has the right to conduct administrative investigations and to have access to the processing of personal data by collecting all the necessary information to carry out his supervisory duties. The role of the Commissioner is extended even in cases where the controller has not reacted after the request made by the data subject under the right to erasure, and in such instances the Commissioner can order the blocking and removal of illegal processing of personal data by the controller.[87]

One of the rights of the Commissioner concerns the notification that every controller has to give to the Commissioner prior to starting the processing of personal data for the first time.[88] This is a requirement that has to be met before the processing of the data starts and there have been various cases[89] in which the controllers have breached the obligation of notifying, which have resulted in measures taken by the Commissioner.

It is interesting to compare this obligation of the controllers under GDPR as well, because contrary to the previous Directive, under which this duty was criticized of being unrealistic, the GDPR does not require the prior notification when the company plans on engaging in any automatic processing operation.[90] As it has been mentioned, the duty for prior notification was held to be unrealistic because it produced financial and administrative burdens for the companies and an overflow of information to the national authorities as well.[91] But the fact that such a duty is not present anymore in the GDPR, does not have to be understood as excluding the controllers from their duties, because controllers have to make sure to be in conformity with the GDPR and make their own assessment if they are complying with the Regulation,[92] so to avoid potential problems that might arise when the data subject might complain about breaches.

Deriving from the GDPR, it might be advisable for Albania as well to reconsider the necessity of prior notification in order to avoid unnecessary administrative procedures for the companies, by taking into account that the Commissioner can at any time undertake controls and investigations if the companies are complying with the requirements of the law. Furthermore, if the Albanian

[87] Article 30 of the Law No. 9887/2008.
[88] Article 21, *supra.*
[89] See Recommendation of the Commissioner No. 02, dated 07.02.2019; recommendation No. 07, dated 11.02.2019; decision No. 3, dated 14.02.2020.
[90] Directive 95/46/EC, arts 18–19.
[91] Recital 89 of the GDPR.
[92] Recital 90 of the GDPR.

legislator evaluates that such a requirement should still remain, it might consider limiting the prior notification requirement only to those companies that engage in large-scale processing operations. Limiting the prior notification only to these companies might be appropriate, since these companies process large amount of data and the risk of breaches increases with the amount of data processed.

It has to be mentioned that the Commissioner has the right not only to impose administrative, financial fines, but in most cases the procedures start with a recommendation,[93] and if the recommendation does not reach its purpose, then the Commissioner proceeds with the fines. The inclusion of the right of the Commissioner to issue recommendation is an important element of the prerogatives of the Commissioner, because in certain cases the breaches occurred are not on the level that justify the issuance of a fine, especially in cases that will be discussed below when there had not been any consequence of the rights of the data subject by the noncompliance of the company with the requirements of the law.

3.2.1 Commissioner's administrative acts in cases of breaches in Albania

The Law grants the Commissioner the right to give recommendations in cases when the controllers have not complied with the requirements of the law and in cases where the breach happens again, then the Commissioner takes administrative fines.

From the analysis undertaken on the recommendations of the Commissioner I noticed two main areas in which the recommendations have been given by the Commissioner. The first area concerns the cases[94] where the controllers had continued to process and keep the data of the subjects, after their contractual relation with the subjects had ended, mostly in the employment area. The duty to keep the data only for as long as the purpose of the initial collection exists is recognized by the Albanian Law in its article 5(d) and by the GDPR as one of its basic principles.[95] The second area

[93] Article 31(a)(1), *supra*.
[94] *See* Recommendation of the Commissioner No. 21, dated 30.07.2020; No. 12, dated 18.06.2020; No. 01, dated 07.01.2021.
[95] Article 5(e) of the GDPR.

in which mostly recommendations have been given is related to the duty of prior notification, as discussed above.

Taking into account the recommendations of the Commissioner, I find that in cases where the lack of prior notification has not brought any consequence to the rights of data subjects, as long as the controller has undertaken all the measures to be in compliance with the law, regardless of the notification, which is now removed from the GDPR, then there is no need for an imposition of the fines. The other scenario, that of keeping the data after the termination of the relation, I find it more problematic, because this would be in breach of the principle of storage limitation, which is a principle recognized by the GDPR[96] and Albanian Law[97] as well, and by keeping these data for longer, the companies might misuse such data and for which it would be appropriate to impose fines.

But it has to be made clear that the recommendations are not an obligatory preliminary phase, that has to be undertaken in every case, because there are breaches that justify the direct enactment of the fines and the recommendations would be futile. In my view, this should have been how the process should have been conducted in the "*Albtelecom SH.A*" case, but the Commissioner decided to give a recommendation, instead of a fine.

In the "*Albtelecom*" SH.A case,[98] the controller Albtelecom, is a company providing services in the telecommunications domain in all areas of the country. The controller conducted marketing campaigns to certain numbers, who were not his clients, but contact persons confirmed by the clients. The strategy of this campaign aimed at increasing the portfolio of the controller's clients by informing and marketing of its products. It turned out that the controller had not tried to obtain the consent of this category of data subjects, for the purpose of direct marketing.[99] It should be noted that in the case of Albtelecom, the company was found to have committed several other violations, but again they were not considered reasonable to impose fines.

[96] *Supra*.
[97] Article 5(d) of the Law No. 9887/2008.
[98] Recommendation of the Commissioner No. 22, dated 17.02.2021.
[99] The criteria for a lawful processing of data are contained in Article 6 of Law No. 9887/2008.

In these circumstances, the Commissioner stated that the processing of data of subjects that have not given consent to the processing for marketing purposes, is contrary to the principle of legality, but was not enough to be imposed a fine.

To understand the different approaches taken by the EU authorities and Albania, it is relevant to mention the case of the Polish company that was processing large-scale publicly available data. In that case, regardless of the large amount of data that was being processed, the Polish authorities found that the controller could not be excluded from its obligations of getting the consent of the data subject, when it had the means of getting that consent and consequently the company faced a high fine by the Polish Authorities.

While in the Albanian case on the other hand, we are dealing with a company which is one of the largest companies in the field of telecommunications and had all the means of obtaining the consent of data subjects, but willingly decided not to do so. In this case the Commissioner limited its actions only with a recommendation, which I consider to be the wrong measure in preventing the company from engaging in future breaches. The risk of the company engaging in further breaches is present, because by not suffering any penalty the company might consider that it is profitable to continue engaging in such kind of behaviors when the only consequence is a recommendation. Therefore, I believe that it would have been more efficient to impose a fine, when considering the profits Albtelecom may have made from such marketing campaigns.

Analyzing the fines in the Albanian Law, I could say that their level is particularly low compared to GDPR, ranging from 200 EUR for breaches where the controllers do not inform the Commissioner prior to the processing of the data, to 16 000 EUR for breaches when the controller does not provide access to the Commissioner to computer and filing systems that process personal data.[100] In the case "*Studio Moderna Albania*",[101] a company was fined with 800 EUR because it processed large amount of data without informing the clients of their right to erasure and had kept the data after the purpose of the initial processing did not exist anymore.

In the case "*Municipality Lezhe*"[102] that concerned the actions of a public authority, the Commissioner decided to impose a fine after the municipality had not reacted in accordance with

[100] *See* Article 39 of the Law.
[101] Decision of the Commissioner No. 25, dated 27.07.2020.
[102] Decision of the Commissioner No. 66, dated 16.11.2018.

one prior recommendation of the Commissioner that required that the municipality published a Data and Privacy/Information session on their website when processing the personal data. The municipality did not include such a session on their website, violating therefore the duty to inform the data subjects and getting their prior and unequivocal consent, which is the core concept of the processing. In these circumstances, the Commissioner imposed a fine of 820 EUR.

Taking into account the analyzed cases, I would conclude that the level of fines imposed by the Albanian Commissioner is low when assessing the type of breaches that consist mainly of the duty of getting the prior consent of the individual when processing their data. Certainly, the low level of fines is to be assessed among the economic development of a country as well, but to impose such low fines in cases of serious breaches, I find it unjustifiable and at the same time failing to serve the purpose of preventing the companies from engaging in future breaches, which is the situation in the "*Municipality Lezhe"* case.

Whereas the fines in EU level are significantly higher, by causing a severe setback to large companies, I find that these measures are appropriate when taking into consideration the financial benefits that the companies can make from processing these data in breach of the law. These are important factors to be considered by the Albanian institutions if they want to protect the right of the citizens, by teaching a lesson to the companies and preventing their further engagement in breaches. It would have been noteworthy to analyze the continuation of any of these cases, if they have been appealed to the State Courts, but unfortunately accessing the court's decisions is limited at the time being, due to some changes taken that aim at anonymizing the identity of the parties to court proceedings.

CONCLUSION

The protection of personal data is getting more and more attention and emphasis due to the technological developments that require stronger rules and implementation systems by the states.

The General Data Protection Regulation has improved the situation of protection of the personal data in the European Union, and at the same time is serving as a model for Albania in the process of harmonizing its legislation with the GDPR.

The usage of publicly available data is one of the differences existing between the GDPR and Albanian Law, under the latter such a usage is explicitly recognized as lawful contrary to the GDPR. In these circumstances the usage of the publicly available data has to be reconsidered by the Albanian legislator, because at the stage the law is, it allows the companies to misuse these data without bearing any responsibility.

Apart from the usage of public data, Albanian law does not recognize the right to be forgotten, a concept included in the GDPR which grants the individuals more power on how to use their data and imposes on the controller the obligation to erase these data, when the data are not any more relevant and other factors such as public interest are not present. By not recognizing such a right, Albanian Law is lacking an important element in having a complete and efficient legal framework, which would grant a comprehensive protection to individuals in deciding over their data.

For the protection of personal data to be complete, the enactment of fines is really important and comparing the level of fines in the EU and Albania there is a substantial difference between them. The economic development of the country is a factor influencing the level of the fines, but if Albania desires an effective system of protection in compliance with the GDPR, it has to change its approach towards the fines and their levels. Taking into consideration that every case should be decided based on the circumstances of that case, there is an overall need to increase the level of fines. These increased levels of fines would serve as a lesson for the companies that their breaches are not to be tolerated and that they should proceed with caution while processing data, and also serve as a prevention in engaging in further breaches.

BIBLIOGRAPHY

Legislation

- Charter of Fundamental Rights of The European Union (2012/C 326/02)
- Directive 2016/680 of the European Parliament and Of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data
- Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data
- Guidance of the Commissioner No. 49, dated 02.03.2020
- Law no. 9877, dated 10.03.2008 "On the protection of personal data", as amended
- Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
- Report of the Council of Ministers on the draft law "On Some Changes and Additions to the Law No. 9887, dated 10.3.2008,"On Personal Data Protection", as amended"
- The Constitution of the Republic of Albania

Cases

- Case C 131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos* (AEPD), Mario Costeja González [2014] ECLI:EU:C:2014:317
- Conceil d'Etat, *RGPD: le Conseil d'État rejette le recours dirigé contre la sanction de 50 millions d'euros infligée à Google par la CNIL,* 19 june 2020
- Decision of the Commissioner No. 25 "*Studio Moderna Albania"* dated 27.07.2020
- Decision of the Commissioner No. 66 "*Municipality Lezhe*", dated 16.11.2018
- Decision of the French National Data Protection Commission (CNIL) of 21 January 2019

- Polish Data Protection Authority (DPA) decision of 25 March 2019
- Recommendation of the Commissioner No. 01, dated 07.01.2021
- Recommendation of the Commissioner No. 12, dated 18.06.2020
- Recommendation of the Commissioner No. 21, dated 30.07.2020
- Recommendation of the Commissioner No. 22 "*Albtelecom*" SH.A, dated 17.02.2021
- The Hamburg Commissioner for Data Protection and Freedom of Information, "*35.3 Million Euro Fine for Data Protection Violations in H&M's Service Center"*, 1 October 2020

Journal Articles and Papers

- Anastasi Aurela, "*Independent Administrative Institutions, Issues of Administrative Law in Comparative View"*, Albdesing, 2010,
- ARTICLE 19, "*The "Right to be Forgotten": Remembering Freedom of Expression*", 2016.
- Bernal Paul A., "*A right to delete*?", European Journal of Law and Technology, Vol. 2, No.2, 2011
- EUROSTAT, "*Key figures on enlargement countries-2019 edition"*, March 2019
- Hoofnagle Chris et al., "*The European Union general data protection regulation: what it is and what it means", 28 Information and Communications Technology Law* 65 (2019)
- Markou Christiana, "*The Right to Be Forgotten" Ten Reasons Why it Should Be Forgotten, Reforming Europian Data Protection Law*, Serge Gutwirth, Ronald Leenes, Paul De Hert, Editors, Law and Governance Technology Series, Issues in Privacy and Data Protection, Volume 20, Springer, 2015
- McKean Ross, Kurowska-Tober Ewa and Waem Heidi *"A report produced by DLA Piper's cybersecurity and data protection team",* January 2021
- Naeem Tehreem, "*Data Automation: How it Transforms Enterprise Landscape"*, April 2021
- National Campaign "*Digital education, play and learn - Happy onlife*", Nr. 9 & 10, December 2020

- Solove Daniel J., *"The Digital Person, Technology and Privacy in the Information Age"*, New York University Press, New York and London, 2004
- Taylor Mistale, "*The EU's human rights obligations in relation to its data protection laws with extraterritorial effect,"* International Data Privacy Law, 2015, Vol. 5, No. 4
- Van den Hoven, Jeroen, Martijn Blaauw, Wolter Pieters, and Martijn Warnier, "*Privacy and Information Technology*", "Privacy and Information Technology", The Stanford Encyclopedia of Philosophy

Online Articles

- Data Privacy Manager, *5 biggest GDPR fines so far* https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/
- ENISA, Personal data breaches < https://www.enisa.europa.eu/topics/data-protection/personal-data-breaches#:~:text=Data%20Protection,Privacy%20by%20Design&text=Such%20breaches%20can%20lead%20(and,or%20even%20threat%20to%20life>
- GDPR - *User-Friendly Guide to General Data Protection Regulation* < https://www.gdpreu.org/> https://advisera.com/eugdpracademy/blog/2019/09/24/how-to-calculate-your-total-gdpr-compliance-costs/
- ICO fines British Airways £20m for data breach affecting more than 400,000 customers https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/
- Kurowska-Tober Ewa and Koniarska Magdalena "*Polish DPA issues the first fine for a violation of the GDPR – and it's harsh"* < *https://blogs.dlapiper.com/privacymatters/polish-dpa-issues-the-first-fine-for-a-violation-of-the-gdpr-and-its-harsh/#page=1*>
- Nistico Alessandra*, "How much does EU GDPR compliance cost?"* EUGDPR, 2019. < https://advisera.com/eugdpracademy/blog/2019/09/24/how-to-calculate-your-total-gdpr-compliance-costs/>

- Travizano Mat, "*The Tech Giants Get Rich Using Your Data. What do You Get in Return?",* September 2018. < https://www.entrepreneur.com/article/319952>