December 2021 (№20)
Volume 7; Issue 5; Page No. 40-46
ISSN: 2346-7916 (Print)
ISSN: 2587-5043 (Online)

INTERNATIONAL JOURNAL OF LAW: "LAW AND WORLD" www.lawandworld.ge

https://doi.org/10.36475/7.5.3

Compatibility of the EU and Georgian Personal Data Protection Regimes and Data Transfer

Nika Svanidze
MA of International Law and Human Rights
Social/Resettlement Specialist at UniProfGroup Ltd.

ARTICLE INFO

Article History:

Received 1.11.2021
Accepted 22.11.2021
Published 20.12.2021

Keywords:

Personal Data,
Data Transfer,
Association Agreement

ABSTRACT

The work discusses Personal Data Protection system under the European Union law, also Personal Data Protection in Georgia and the compatibility of those two regimes. Moreover, there were mentioned ways how Georgia can adopt regulations and harmonize its legislation, to be compatible with the European Union Personal Data Protection regime. The work emphasized efforts of Georgia on the path of developing its Personal Data Protection system. The many citizens of Georgia don't even have a knowledge that their Personal Data has to be defended. Although, the court practice of Georgia revealed good developing signs in this field. If before there were not any cases concerning personal data protection, today we have some good decisions regarding the personal data protection. The data transfer between the European Union and Georgia, is also implemented in the Association Agreement between the European Union and Georgia. Here as well has to be mentioned that the Association Agreement was the greatest step for Georgia, it was the great opportunity to harmonize Georgian Personal Data system with a European. Step by step, Georgia is straining to become a member of the European Union. Thus, this work is a look through past and future of Georgian and EU relations in the field of Personal Data system.

INTRODUCTION

Modern reality is impossible to imagine without an internet. Internet commenced to be the part of our daily life. We created on the Internet our virtual reality and every day we share some kind of personal information in there. Even in case, when you buy the things online, or making flight reservations, during this time you share with the controllers your own personal data. These personal data can be many kinds of, likewise, name, age, bank card details, gender and other important minutiae which are valuable traits of your personality. But do we really need to protect this personal data?

Answers on this question are the conventions, regulations and directives adopted by the United Nations and the European Union, which are constantly here for the defence of the personal data. The first ever document which mentioned the importance of the private realm, was the UDHR in the Article 12. Next step in this field was adoption of The International Covenant on Civil and Political Rights (ICCPR), it declares that no one's privacy, home, correspondence, honour and reputation may be subjected to arbitrary and unlawful interference. After the enhance role and improvement of the modern technologies, also to revelations on mass surveillance handle in some states, since 2013 the United Nations promptly adopted two resolutions. Those regulations were emphasized the negative effects of the mass surveillance, though resolutions adopted in 2016 and 2017 made novel points, meticulously about the diminishing of the powers of intelligence agencies and denouncing of mass surveillance. The robust part of those resolutions is that they reaffirm responsibility of state authorities, moreover they indicate private sector's liability to respect Human Rights, companies are obliged to inform consumers about the gathering, usage, sharing and retention of personal data and to set forth transparency. In case of the European Union, firstly the Charter of Fundamental Rights in the Article 8 implemented the right to personal data protection, in addition it also sorted out the core values associated with the mentioned right. Take note that before the development of computers and internet and the rise of the information society, ECHR adopted the aforementioned Article 8. 1960s brought broad changes in technologies, therefore here was the demand for more detailed rules to protect individual's personal data. Thus, in 1981, a Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), was created. The main aim of the given convention is to defend and regulate transborder flows of personal data. Till the adoption of the main document for the defence of personal data, the legal tool on data protection was Directive 95/46/EC, which was adopted by the European Parliament and the Council on 24 October of 1995. The mentioned Directive implemented the protection and the free movement of personal data of the individuals with regard to the processing of personal data. In 2016 EU adopted the modernized data protection legislation, also named as the General Data Protection Regulation (GDPR). This regulation is the best fit for the modern economic and social challenges, in context of protecting fundamental rights. The interesting part is that what's happening with personal data protection in the neighboring countries of EU, in our case in Georgia.[1]

In 2014 Georgia signed Association Agreement [2] for becoming a member of the European Union. As Georgia is one of the Eastern Partnership states, it took a liability to comply with data privacy requirements. The main objective of Georgia is the harmonize its own legislation with the European standards, specifically regarding the users' rights, defence along with encouraging e-government initiatives, to implement personal data security and support their active usage between business, governments and citizens.[3] Therefore, the main hypothesis of the given research is to find out if Georgian regime of Personal Data Protection is compatible with EU regime, also to investigate if there are the issues concerning the data transfer from EU to Georgia.

1 Handbook on European data protection Law – 2018 edition; European Union Agency for Fundamental Rights and Council of Europe; Imprimerie Centrale in Luxembourg, 2018; p. 17-27.

2 Association agreement between the European Union and the European Atomic Energy Community and their Member States of the one part and Georgia, on the other part. Opened for signature 27 June 2014, [entered into force 1 July 2016]. OJ L 261/4.

3 M.Tsulukidze, K. Nyman-Metcalf, V.Tsap, I. Pappel, D. Draheim; Aspects of Personal Data Protection from State and Citizen Perspectives – Case of Georgia; Digital Transformation for a Sustainable Society in the 21st Century; Springer, 2019; p. 477.

PERSONAL DATA PROTECTION IN EU

After the Second World War, the protection of privacy commenced to be one of the most important tasks in the realm of Human Rights, thus it was implemented in several regulatory texts, at the European level. The disaster and misdeed of the mentioned period of history, disclosed what can happen when large databases of personal data were utilized for the segregation of population, meticulously of the targeted minority groups, also it was a way to ease the genocide. It was an example how menacing public invasion could be into the private realm. [4] For not repeating the history, EU has adopted several Directives. Though, nowadays the biggest instrument for the defence of the personal data in EU is the General Data Protection Regulation (GDPR). This is an impressive tool that has to be discussed in this research paper. The General Data Protection Regulation (GDPR) contrasted to its predecessors, accurately puts more points on individual control over personal data. New principles which are embedded in the given regulation reinforce individuals in obtaining more control over their data. [5] One of the key notions of data protection, which determines the material scope of the DPD and the GDPR is "Personal data'. Data protection principles, rights and obligations, which are implemented in Article 3(1) of DPD and Article 2(1) of GDPR applies solely then, when personal data is processed. Pursuant to GDPR "Personal Data' is: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[6] Anonymous data has contrary characteristic to personal data, it mostly rendered in a way that information is not identifiable or does not identifies a person, or personal data. Processing anonymous data did not fall under the realm of data protection law. Pseudonymous data acquires the traits of personal data after pseudonymisation, with this way it is plausible to identify person, and as a result it falls under the realm of the data protection law.[7] The resulting definition of personal data is broad, flexible, and adaptable to technological context.[8] To get through more precisely in the notion of "Personal Data', here has to be mentioned the court case named as Lindqvist, which took place in 2014. After this case, focus instead of comprehensive definition, was put on the big lines. There were other cases which provided more depth analyze of the particular elements of "Personal Data'. Those cases were Breyer, YS and others and Nowak.[9]

The earlier regulation on protection of personal data were not that explicit about the need for individual control, though the GDPR is not reluctant to this. Actually, fortifying individual control was one of the main objectives of the EU legislator. Despite the fact that the GDPR pays great amount of attention to data subjects "control, behavioral scientists criticized it for not being able to address threats appropriately. With the swift development of intrusive digital technologies and algorithmic decision-making, the challenges for control over data become more complex. Therefore, there are apparent threats related to individual control. [10]

European data protection law implements independent supervision as one the most significant component. Case law also highlighted importance of independent supervision. Especially, in the case named as Schrems. EU law, specifically the General Data Protection Regulation recognizes free flow of data among European Union states. Despite this, the General Data Protection Regulation conveys specific requirements affiliated with personal data transfers to third countries. This means to transfer data outside the European Union and to other international organisations. The Regulation mentions significance of this kind of data transfer in interna-

4 N. Robinson, H. Graux, M. Botterman, L. Valeri; Review of the European Data Protection Directive; May 2009; p. 6.

5 I. van Ooijen, Helena U. Vrabec; Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective; Journal of Consumer Policy; Springer; 2019; p. 91.

6 General Data Protection Regualtion (GDPR); Art 4(1).

7 N. Purtova, The law of everything. Broad concept of personal data and future of EU data protection law; Law, Innovation and Technology; Informa UK Limited, trading as Taylor & Francis Group; 02 Apr 2018; pp. 40-42.

8 D.J. Solove, P.M. Schwartz; An Overview of Privacy Law; Privacy Law Fundamentals, Chapter 2; IAPP; 2015; p. 9.

9 Opt. cit. N. Purtova, pp. 22-23.

10 Opt. cit. I. van Ooijen, Helena U. Vrabec, pp. 92-93.

tional trade and cooperation sphere, though it admits risks during the transfer of personal data. As a result, the General Data Protection Regulation provides the same amount of defence to personal data which was transferred to third countries as they harness within the EU. Data transfer is feasible if it complies with the articles written down in Chapter V of the General Data Protection Regulation. Under EU law, the flow of personal data must be free from any kind of restrictions or prohibitions throughout the EU and among Contracting Parties. In case of data transfer to third countries and to organisations, EU law set out some specific conditions. EU law implements two ways of approving data transfer to third countries and to organisations. First way is an adequacy decision made by the European Commission. This way of data transfer is implemented in Article 45 of the General Data Protection Regulation.[11] Before making an adequacy decision, there are several points which are analyzed by the European Commission. Firstly, the European Commission examines the national law and appropriate international obligations, next if country participates in regional and multilateral systems, meticulously regarding the data protection. Also, the European Commission can check other conditions on case basis. If all the conditions were met, then the European Commission issues an adequacy decision. The adequacy decision has binding effect. In case of absence of European Commission adequacy decision, the controller or processor has to convey appropriate defence, which includes legal remedies and enforceable rights for the data subject. There are several applicable safeguards, which can be established by: a legally binding and enforceable instrument between public authorities or bodies; binding corporate rules; standard data protection clauses adopted either by the European Commission or by a supervisory authority; codes of conduct; or certification mechanisms. The General Data Protection Regulations also notes other appropriate safeguards, those are the data receiver in a third country and contractual clauses among the controller or processor in the European Union. GDPR in Article 47 highlights personal data transfer based on mandatory corporate rules, which appears within the same group enterprises or a joint economic activity.[12] Moreover, the General Data Protection Regulation includes rule to transfer personal data with third country for specific purposes based on an international agreement. Although, there is written down some special rules for the cushion of personal data during the mentioned situation. [13]

PERSONAL DATA PROTECTION IN GEORGIA

Georgia its first law on personal data protection enacted only in 2011. Until this period here was not a *lex specialis* legislation on personal data protection. The Constituion of Georgia implements regular rule about private life. Pursuant to the Constitution here has to be person's consent to access its personal information.[14] Neither Civil Code of Georgia, nor General Administrative Code of Georgia, had any specific rules about the personal data protection. Specific approach to data protection was possible to found solely in laws, likewise, Tax Code of Georgia, Decree of National Commission of Communications of Georgia on Provision of Services and Protection of Consumers' Rights in the Sphere of Electronic Communications and others. Despite this, those decrees and laws were working in a narrow field and regulated solely those spheres for what they were enacted.

As it was mentioned above, Georgia in 2011 adopted law on protection of personal data. Pursuant to Neighborhood Policy Action Plan Georgia, country took liability to implement the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Therefore, Georgia took a great responsibility to at least adopt the law which could protect the person's personal data. Law of Georgia on Personal Data Protection was adopted by Parliament of Georgia on December 28, 2011. The main objective of the law is to defend the right of privacy in bond with processing personal data. The law provides some "general principles of personal data processing', likewise, lawfulness and fairness. According to it the person whose data has to be processed shall be notified about this. The

11 General Data Protection Regulation, Art. 45.

12 General Data Protection Regulation, Art. 47.

13 Opt. cit. Handbook on European data protection; pp. 249-271.

14 Constitution of Georgia, Art. 15.

"Data Subject' includes number of rights, and person's consent for processing his personal data, is obligatory. In Article 3 of the law of Georgia on Personal Data Protection[15] are mentioned some restrictions, when existed law cannot be applied. Some of them are quite vague, meticulously it is hard to comprehend why the aforementioned law cannot be applied for some specific situations.

The main strength of the law of Georgia on Personal Data Protection is that it implemented a new institute, named as Personal Data Protection Inspector. The Personal Data Protection Inspector is responsible for the lawfulness of data processing. The Personal Data Protection Inspector is elected based on an open competition that is enacted by the law. The Premier Minister of Georgia has to approve the Competition Commission. The representative of NGO, government of Georgia, Judiciary and Public Defender's Office and government of Georgia participates in the Competition Commission. This was the main novelty made by the law of Georgia on Personal Data Protection. [16]

In the end of 2013 Personal Data Protection Inspector of Georgia was finally established. The competences of Personal Data Protection Inspector contains consulting organisations on matters affiliated with data defence, managing audits of data controllers, addressing citizen investigations and growing utter level of knowledge regarding information security. The role of Personal Data Protection Inspector increments on daily basis in Georgia. Therefore, the given research paper will discuss inquires of Personal Data Protector Inspector during performance of its duties. As they investigated, by a decade in Georgia, adaptation of data defence standards and regulations preceded the implementation of electronic systems in administrative bodies. The law of Personal Data Protection requires to preserve detailed records of all manipulation when it comes to the electronically processed personal information. This precludes Personal Data Protection Inspectorate from officially obliged state entities to realize aforementioned mechanism. The automatic logging mechanism in databases including nationals' personal data is highly monitored and carried out in practice by Personal Data Protection Inspectorate. The lack of automated audit trace conveys opportunity to punish controller, even without of data revelation and mishandling. Every Data Protection Inspector Office has their filling system catalogues, which is an electronic document. This document includes the list of data categories processed by per data controller in Georgia. The mentioned electronic document is filled by controller's authorities and database inscription is there as well. One of the most significant liabilities of Personal Data Protection Inspector Office is to be the mediator among data controller authorities and citizens, with this way it is representing the interests of data subjects. Pursuant to Personal Data Protection Inspector's office the number of citizens inquires has incremented during the past couple of years for at least five times.[17] Seeing this, it is clear that Personal Data Protection is a novelty in the Georgian legislation. Despite this fact, the law implemented a robust instrument as the Personal Data Protection Inspector, whose performance harnesses the valuable assist in newly established system of personal data protection in Georgia. There was conducted the survey about users' comprehension of data safety in Georgia. The survey distinguished different results. Though, finally it can be summarized that considerable number of citizens are ready to be adopted to e-services, but the other part of the users still inclined to remain limited because of their anxiety concerning the data security in the society.

COMPATIBILITY OF TWO REGIMES AND TRANSFER OF DATA

In 2014 Georgia officially proclaimed it's willing to be the member of the European Union. After the signing the Association Agreement, Georgia took a liability to harmonize its legislation with an European standards. This concerns specifically, user's rights, defence and security of personal data together with encouraging e-government initiatives and allying for their active usage among governments, citizens, and businesses. Georgia made great effort to be compatible with the European Union regime,

15 Law of Georgia on Personal Data Protection, Art. 3

16 B. Jalagania, Regulatory Framework for Personal Data Protection in Georgia and its accordance with EU regulations; University of Oslo, 2013; pp. 25-29.

17 Opt. cit. M. Tsulukidze, K. Nyman-Metcalf, V.Tsap, I. Pappel, D. Draheim; pp. 480-482.

though still there are plenty of issues that have to be tackled. To reach the objectives Georgia is obliged to make robust steps in protection of personal data and its security. Georgia has to make amendments in the field of data controllers. Controllers should be liable to present a scripted policy on data security or foster the access control mechanisms. With the mentioned way Georgian legislation will be more compatible with the European Union regime. Moreover, throughout the whole public sector, Georgia has to assure homogeneity of personal data defence. It has to enhance interoperability and to establish protected data exchange channels among governmental entities to guarantee safe circulation of citizens' data. Country is obliged to train and develop work ethics of the public workers in the realm of citizens' personal data privacy, also their activities have to be monitored within personal databases. The citizens should have opportunity for direct and plausible monitoring how meticulously their personal data was processed. Georgia is liable for active campaign in the field of citizens' knowledge on matters pertained personal data processing.[18] Also, here should be noted that Georgia amends its law on the Personal Data Protection and in the nearest future there will be consolidated version of this law.

In case of data transfer, the Georgian legislation is not providing any defined method of data exchange. The law of Georgia on Personal Data Protection claims that the transmitted data must be defeneded from illegal disclosure oblivious of the employ. The aforementioned conveys entities discretion to accept solely secure ways of data sharing. In practice there were used mostly two ways of data transfer. Ordinary, state entities issues written inquires, where legal basis of request is indicated, after this organizations hand out citizens' personal data. [19] This emphasized the personal data transfer system on local basis. Although, here arises the question, is there any obstacles concerning cross-border data transfer from EU to Georgia?

The European Union's special rules and regulations about data transfer on third countries and organisations, which are implemented in the General Data Protection Regulation already, were discussed above. Georgian legislation also recognizes cross-border data transfer. It means that state or international organization can transfer data to the receiver which is not in the realm of Georgian jurisdiction. The law admits several rules that implements possibility of data transfer to another state or international organization. Pursuant to it, the law of Georgia on Personal Data Protection covers some grounds in this field and if there are applicable safeguards for the defence of data and data subjects by the international organization or the state then the data transfer is plausible. Another way is the international treaty or agreement, which provides the plausibility of data transfer. The last point is that data controller has to provide applicable assurance for defence of data and data subjects' rights on the ground of an agreement signed among a data controller and the corresponding state, a natural or legal person of that given state or the international organization. Those are the rules that applied in case of cross-border transfer. [20]Though, to answer on the aforementioned question, this work has to look into the Association Agreement between the European Union and Georgia. Article 188 of the given document regulates data processing and there is written down that data transfer is permissible between EU states and Georgia, there are not any obstacles, instead of this that both parties are obliged to "adopt adequate safeguards for the protection of privacy and fundamental rights, and freedom of individuals, in particular with regard to the transfer of personal data." [21]

18 Opt. cit. M. Tsulukidze, K. Nyman-Metcalf, V.Tsap, I. Pappel, D. Draheim; pp. 483-487.

19 Ibid. M. Tsulukidze, K. Nyman-Metcalf, V.Tsap, I. Pappel, D. Draheim; pp. 481-482.

20 State Inspector's Service: https://personaldata.ge/en/cross-border-data-transfer

21 Association agreement between the European Union and the European Atomic Energy Community and their Member States of the one part and Georgia; Art.118.

BIBLIOGRAPHY:

1. Handbook on European data protection Law – 2018 edition; European Union Agency for Fundamental Rights and Council of Europe; Imprimerie Centrale in Luxembourg, 2018
2. M.Tsulukidze, K. Nyman-Metcalf, V.Tsap, I. Pappel, D. Draheim; Aspects of Personal Data Protection from State and Citizen Perspectives – Case of Georgia; Digital Transformation for a Sustainable Society in the 21st Century; Springer, 2019
3. N. Robinson, H. Graux, M. Botterman, L. Valeri; Review of the European Data Protection Directive; May 2009
4. I. van Ooijen, Helena U. Vrabec; Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective; Journal of Consumer Policy; Springer; 2019
5. N. Purtova, The law of everything. Broad concept of personal data and future of EU data protection law; Law, Innovation and Technology; Informa UK Limited, trading as Taylor & Francis Group; 02 Apr 2018
6. D.J. Solove, P.M. Schwartz; an Overview of Privacy Law; Privacy Law Fundamentals, Chapter 2; IAPP; 2015
7. B. Jalagania, Regulatory Framework for Personal Data Protection in Georgia and its accordance with EU regulations; University of Oslo, 2013
8. Association agreement between the European Union and the European Atomic Energy Community and their Member States of the one part and Georgia, on the other part. Opened for signature 27 June 2014
9. General Data Protection Regualtion (GDPR)
10. Law of Georgia on Personal Data Protection
11. Constitution of Georgia
12. C-101/01
13. C-582/14
14. C-141/12
15. C-434/16
16. C-362/14
17. BS-719-715(G-17)