Data protection policy as one of the mechanisms for improving corporate compliance control (based on European, Russian and Armenian legislative systems)

Tamara Danielyan[1,*], and *Renata* Sibagatullina[2]

[1]Shushi University of technology, Armenia
[2]Financial University under the Government of the Russian Federation, Russia

Abstract. The aim of the research is to study data protection policies in developed countries and compare the same policies existing in the legal systems of developing countries. In this article, we review GDPR as a best practice for regulatory and corporate compliance. As an object, the law on personal data existing in Russia and Armenia legal system was analyzed and compared with the GDPR in the European Union. Benchmarking as a research method is used in the scientific work. Having researched the article, we can conclude that implementing and complying with a data protection policy based on GDPR contributes to regulation of two issues: developing a sustainable business and improving the data security of customers and employees.

1 Introduction

A common delusion among entrepreneurs in post-Soviet countries is the assumption that compliance with the local law is quite enough. However, companies entering the European market or dealing with residents of Europe must comply with the data protection regulation requirement (GDPR)[1]. There are several provisions in the regulation, which can be interpreted differently depending on the specific situation. The General Data Protection Regulation is similar to many other privacy laws. However, its effect applies not only to the countries of the European Union, but also to all companies that in one way or another collect, process and store personal data of citizens and residents of the EU. For non-compliance with the GDPR requirements, there is a fine of up to 20 million euros or 4% of annual income. Given the wider scope and higher fines, the media attention to the regulation is understandable. In addition, under the new law, companies are required to provide their customers with certain rights (for example, "the right to be forgotten" or "the right to export data"), as well as implement some internal corporate changes. Similar provisions with GDPR are applied in post-Soviet countries, namely, as an example, we consider identical laws working in the Russian Federation and the Republic of Armenia (In Russia, this is Federal

* Corresponding author: tamara_danielyan@yahoo.com

Law No. 152 [2] of July 27, 2006 "On Personal Data". Its purpose is also to protect personal data while processing. In Armenia, it is the RA Law "On the Protection of Personal Data" dated May 18, 2015) [3]. In this article, we will consider GDPR as one of the most effective corporate compliance control policies introduced in an organization. The purpose of the research is to propose the implementation of a GDPR policy to improve corporate compliance.

Companies that collect personal data and allow more than one employee to process the data are advised to maintain an appropriate data protection policy (DPP)[4]. You might assume this only applies to companies located in the European Union, but this is not the only case. Any company that collects data from a European resident will need to comply with the data protection regulation (GDPR) requirements. Even if a company is based on its territory and complies with its legislation, but provides online services to citizens from the EU, accordingly, this company is obliged to comply with the GDPR. Failure to comply with GDPR by local organizations can cause a number of consequences [5]:

• Financial; for non-compliance with GDPR, companies can be fined up to 4% of annual income

• Reputational; arrest on accounts in the EU or a ban on entry of the CEO, these factors are unlikely to have a good effect on the company's reputation.

• Commercial; for non-compliance with the GDPR of the company - partners may simply not cooperate with your company.

Firms in Armenia and Russia do not always decide to implement the GDPR as they consider it an unnecessary and optional component. Any processing of personal data (collection, registration, accumulation, storage, adaptation, modification, renewal, use, distribution, depersonalization and destruction) is possible only in accordance with applicable law, i.e. in the presence of consent to the processing of personal data, taken before their processing, unless life and health clearly depend on it.

This processing takes place even in such trivial cases as:

Sale or home delivery of goods. In this case, the contact details and the place of residence of the client are processed. The data should only be used for order processing. The transfer of personal data to marketers or spam sms is not included in the unconditional consent of the recipient.

Courier and mail delivery. Operators of courier services to simplify the processing of shipments collect dossiers on their customers - senders and addressees. But even reputable postal operators need to independently limit the processing of personal data.

Enrollment of a child in school or sports section. In this case, the data of the child is processed, for which the consent of the parent, guardian or guardian is required. That is, you need consent to the processing of data from two persons at once - an adult and a child.

Sale of a plane ticket. And if airlines have connections with the EU, they should take care of GDPR compliance.

Appointment to a doctor. Notice of an appointment with a doctor in one way or another implies the disclosure of information about the patient's health.

2 Methodology

We have developed a step-by-step guide for making decisions on the implementation of the GDPR.

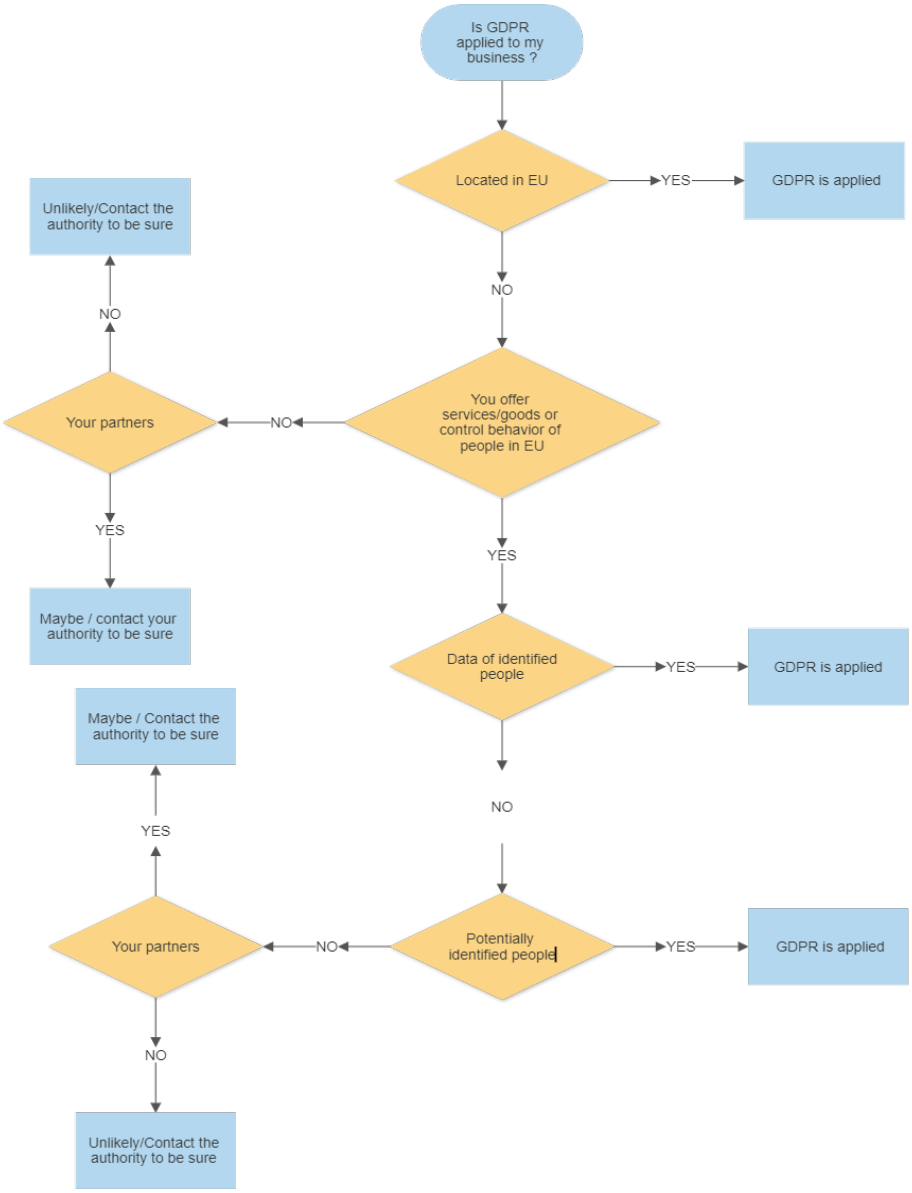

Fig. 1. Flowchart of GDPR application.

3 Checks on GDPR VS 152-ФЗ VS РН-49-U in practice

In Russia, compliance inspections are carried out superficially due to a lack of resources. In Armenia, the law is quite new and the practice of monitoring the implementation is subject to renewal and improvement every year. In Europe, compliance is based on the developed ISO 27001 certification, confirming the organization's compliance with the GDPR. Another issue present in developing countries is an issue regarding data storage conditions. Of course, it depends on the provider who will take responsibility for ensuring the protection of personal data. Both Roskomnadzor[6] and the Data Protection Agency[7] in Armenia are well aware

of the scale of the problem but it is out of focus, since in these countries such a data storage system falls under the exception.

In order to determine the basic differences between GDPR and 152-ФЗ [8] and ЗР-49-Н, we conducted *benchmark* on the principles and concepts of the same law which is in force in EU, Russia and Armenia and obtained the following results (Table 1).

Table 1. Benchmark of regulations.

GDPR	**152-ФЗ**	**ЗР-49-Н**
Controller and processor	Operator	Personal data operator
Protection of children personal data	-	-
Principles: 1)Legality, fairness and transparency. 2) Purpose limitation 3) Data minimization. 4) Accuracy 5) Storage limitation 6) Integrity and confidentiality.	Principles: 1) Legality, fairness 2) Specific and legitimate purposes of data processing 3) The impossibility of combining bases for incompatible purposes 4) Relevance of data to goals 5) No data redundancy 6) Relevance and accuracy of data 7) Storage period	Principles: 1) Legality 2) Proportionality 3) Credibility 4) Minimal involvement of subjects
GDPR Violation Notice After detecting violations related to personal data, legal entities must notify the regulatory body within 72 hours	-	-
Data Protection officer (Controller is responsible for controlling data and Processor is responsible for processing)	Data Inspector (responsible for controlling and processing)	Data Operator

From the above table, we see that, on the one hand, the legal system neither in Armenia nor in Russia guarantees complete data security and the law requires revision. On the other hand, for a sustainable and efficient business, it is imperative to implement and comply with the GDPR policy.

Based on the practice of companies operating in Armenia and Russia, we propose identifiable indicators for GDPR application.

Table 2. Identifiable signs of GDPR application in Armenian and Russian companies.

Company
Located in EU
Offers good/services in the market of EU
Monitors and processes personal data of EU people in the course of its transaction
Has offices and branches in EU
An agreement with European elements, payment in euros, execution in the EU, indicating the e-mail addresses of EU citizens in the details, if they clearly indicate the identity, etc.
Employs expats - EU citizens
There is a need to issue powers of attorney to EU citizens

4 Research outcomes

Thus, if your company deals with a large amount of EU consumer data, special categories of data, or if your data processing practices pose a security or personal data protection risk, then you should be able to prove that your business maintains safeguards and security measures in accordance with the GDPR. In other words, you will need to document and demonstrate that your organization is processing data in accordance with the GDPR, with the nature, scope, context and purpose of the data processing activities. Every business must approach data protection in a way that reflects its own individual needs and data processing procedures. Any company that collects specific categories of data which the GDPR classifies as sensitive information must include a specific clause in the DPP regarding the handling of sensitive data categories for example, data related to race, religion, sexual orientation, etc. [9]. Any Armenian and Russian company, before collecting and processing any personal data, must:

• Determine the list of collected and processed personal data.
• Determine the main jurisdictions of customers based on product localization, statistics or analysis of a specific market.
• Assess whether its activities pose a special risk to the rights and freedoms of personal data subjects.
• Determine the nature of the processing of personal data.
• Indicate the list of employees who have access to personal data.
• Determine the list of third parties (service providers, technical executors) who have access to any data.

Then, if the project enters the European market, you will need:

• Determine the target markets for the project.
• Calculate the total number of employees.
• Assess whether data processing is the main activity of the company (this group includes intermediary services, databases of individuals, social networks).
• Determine if personal data belongs to a special category - "sensitive" data - according to Article 4 of the GDPR.

Thus GDPR for effective SME is very crucial we propose the following stages of its implementation taking into account local law requirements existing the legal system of your country [10]:

Preliminary stage

A preliminary analysis of your company's activities to determine the need to comply with the GDPR requirements. Based on the results of the audit, you conclude whether or not you need to comply with the GDPR requirements.

Stage 1. Analytical

Analyzing your data will help you decide how to comply with the GDPR. At the first stage one must answer whether the company has storage/cloud space; for what purpose certain types of personal data are stored or processed; what is the legal basis for the processing; determine duration of keeping the data; define people who have access to personal data / who will have access in future; availability of appropriate technical and organizational controls.

All of these areas need to be considered before you begin the next stage. The first step in creating a holistic view is critical. If you do not know what personal data you are keeping, you will not be able to make a plan based on that data. One should analyze company's business processes to determine the necessary organizational and technical ones in order to bring the company into compliance with the GDPR requirements. You can hire an audit to analyze business processes in your company. You fill out a detailed questionnaire. The audit conducts interviews with management and specialists. You provide access to systems,

contracts and other documents for analysis. Based on the results of this work, the compliance or non-compliance of the processes with the GDPR requirements is revealed.

Stage 2. Implementation

Under the supervision and participation of lawyers and technical specialists, a plan is being implemented to eliminate deficiencies and inconsistencies in business processes with GDPR requirements. In order to eliminate or minimize risks, where applicable, the customer's business processes are adjusted. If necessary, trainings and training of the customer's specialists are carried out.

Stage 3. Accompanying + DPO

The company needs to appoint a Data Protection Officer (DPO) who will oversee GDPR compliance and provide consultations in the course of day-to-day operations.

At the accompanying stage, changes are monitored and GDPR puts into practice. In case of changes or deviations in business processes (taking account local legal requirements and law enforcement practice) recommendations should be made on adjusting measures to comply with GDPR (GDPR compliance) requirements.

5 Discussion of the outcomes

Based on the results of the internal audit and assessment of its work according to the above criteria, the company is obliged to implement an adequate legal and technical regime for the processing of personal data and notify the regulatory authorities about its activities when the law directly prescribes it.

In order to implement, first of all, you need to carefully study the regulations and highlight points that may apply to your business. The next step is to conduct a detailed audit of the data-related processes:

• Establish what personal data your project collects, where and how it is stored.
• Find out how, when, by whom and why personal data is processed.
• Develop mechanisms for protecting your data. Provide protection against burglary. Write down the data processing access policy. Limit the circle of people who have the right to work with data.
• Designate a data protection officer. Ideally, he should be well versed in the GDPR and its application in practice.

To comply with the GDPR requirements, you just need to respect the rights of users. We present to you the minimum that must be met [11]:

1. Submit information on the collection of personal data on your resource. Explain the reason for posting and the content you are going to post. Any new user should be shown a data collection notification and asked to read the policy. For example, you can do this through a pop-up window.
2. Ask users for consent to data processing. It is advisable to obtain active consent when the user takes an action to confirm. For example, it puts a tick in the checkbox “I agree with the terms of data processing”.
3. Use double opt-in. This point applies to email newsletters. Before starting to send the newsletter to a new subscriber, ask him to confirm his consent by clicking on the link in the welcome letter.
4. Provide and delete data at the first request of the user. Remember that the owner of the data is not obliged to explain the reason, his wishes are enough.
5. Report data breaches to owners and regulatory authorities. If a data leak occurs, regardless of the reason, notify users about it. And be sure to notify the supervisory authorities, at the same time providing a plan of measures to remedy the situation.

Despite the fact that the new requirements for the processing of personal data are serious, they have positive aspects for non-European players: it is easier to adhere to a single set of

data protection and processing rules than to take into account the national nuances of processing personal data of each individual EU country, as it had to be done before the introduction GDPR. Moreover, the reform aims to stimulate economic growth by reducing costs and bureaucracy for companies operating in the EU. Adherence to one rule instead of 28 (the number of EU member states) will help small and emerging companies enter new markets. According to the law, in some cases, obligations change depending on the size of the business, the nature of the data being processed and other factors.

You should also consider in advance the mechanisms for responding to requests from European regulators and subjects of personal data (users) that are possible under the GDPR (for example, on the clarification of data, their deletion, termination of processing or transfer to another company under the right to data portability).

A number of measures are proposed to minimize the risks of GDPR

It is easier for Russian and Armenian companies - subsidiaries of EU companies and members of a group of companies - to minimize risks. GDPR obliges groups of companies to implement corporate codes of conduct - binding corporate rules that regulate the mechanism of cross-border transfer of data within the group. Most likely, the parent company will issue these codes to all members of the group. But such codes minimize only a fraction of the risks. The company must take a number of steps to avoid fines and damage to its reputation in the market.

Supporting operational procedures on Personal Data. Review all internal local procedures on Personal Data for compliance with the Regulation. Provide clear instructions on what to do in case of data breaches of European citizens. It is essential that your policies are understandable to EU citizens - at least it should be bilingual.

Consent. Make up a more detailed consent form for the processing of personal data. Indicate the purposes of the processing and that the consent is specific, voluntary and informed. The form should be understandable to Europeans. Make sure consent is collected from all relevant subjects.

The procedure for storing and processing Personal Data. One must consider the procedure for storing the Personal Data of Europeans and introduce a system for recording operations for their processing or consider the need to open a representative office in the EU and the appointment of a data protection officer. Possible requests from data subjects should be prepared in order to prove that you have not violated the GDPR.

Contracts. You should review contracts with European elements to see if you are the operator or even the controller. If you are, it makes sense:

- add assurances that the party has all the necessary consents to process Personal Documents in accordance with Russian or Armenian and international legislation;
- add a ban on the use of personal data of Europeans obtained in the process of concluding and executing a contract for advertising purposes;
- if screenshots are used in the contract, make sure that they do not contain IP addresses or other information about users.

6 Conclusion

The application of the GDPR for Russian and Armenian businesses may not be required if the company does not plan to enter European markets or work with EU citizens. However, voluntary compliance with the regulations will positively affect the reputation, increase the transparency of activities for customers and partners, and increase the level of loyalty and trust from the society.

A company that does not process the data does not need this item. We recommend: 1) implementing and maintaining the Data Protection Policy, 2) educating all of your employees

how to use it 3) self-review of the privacy regulation so that you know exactly what privacy practices your business uses and what information you need to disclose to the users.

References

1. Federal'nyj zakon ot 27 iyulya 2006 g. N 152-FZ "O personal'nyh dannyh" (2006)
2. EU General Data Protection Regulation (GDPR) (2021)
3. Zakon Respubliki Armenii “O zashchite lichnyh dannyh” (2015)
4. DATA PROTECTION POLICY, IMPACT, **1** (2016)
5. Chto Takoe GDPR I kak on vliyaet na rossijskij biznes (2021). Access mode: https://academyopen.ru/journal/508
6. Roskomnadzor (2021). Access mode: https://rkn.gov.ru
7. Public Report of the Personal Data Protection Agency of the Ministry of Justice of the Republic of Armenia - Constitution of the Republic of Armenia, Ministry of Justice of the republic of Armenia (2021). Access mode: https://www.moj.am/legal/view/article/1400
8. GDPR vs 152-ФЗ, Telesputnik (2021). Access mode: https://telesputnik.ru/materials/tsifrovoe-televidenie/article/gdpr-vs-152-fz/
9. How to Build a GDPR-Compliant Data Protection Policy, Privacy Policies (2021). Access mode: https://www.privacypolicies.com/blog/gdpr-data-protection-policy/
10. GDPR Small Business Compliance Guide: Your Data & Privacy Obligations (2021). Access mode: https://article27representative.eu/gdpr-compliance/small-business/
11. GDPR tri goda: chto bylo, chto est' i chto budet (2021). Access mode: https://assets.kpmg/content/dam/kpmg/ru/pdf/2021/06/ru-ru-gdpr-three-years.pdf