ACTIONS TO ENSURE PERSONAL DATA PROTECTION IN A BUSINESS ENTERPRISE

Gintarė Kulbeckienė
Šiauliai State College
Lithuania

Nijolė Litevkienė
Šiauliai State College
Lithuania

Annotation

The General Data Protection Regulation is related to fundamental changes in business enterprises as they need to radically rethink how to process customers' personal data. The following principles of personal data protection have been established: the principle of lawfulness, fairness and transparency; purpose limitation in data handling; the data minimisation principle; the principle of periodicity; the principle of storage limitation; the principle of integrity and confidentiality; and the principle of responsibility. The study revealed problem areas in the implementation of the personal data protection policy in the business enterprise: ensuring management of access to personal data; informing individuals about the nature of the use of their personal data; and development of a description of the procedure for rules on a new consent to the use of personal data. Hiring external experts and leader support in implementing the personal data policy in the organization are to be assessed as the enterprise's weaknesses.

Keywords: General Data Protection Regulation, personal data protection, business enterprise, implementation, problem areas.

Introduction

Relevance and novelty of the topic. The concept "personal data" defines a significant area of application of data protection, which, although is broad, according to W. G. Voss (2016), still needs to be further expanded and applied exponentially due to the growing diversity of situations. This is so because opportunities are created for developing countries to interpret this concept and summarize data themselves, which also means progress in data analysis. According to D. Barnard-Wills (2017), as our environment is rapidly approaching what some call "onlife," where everyday existence is mediated by information technologies, everything in this environment is increasingly "assessed", and literally any data are likely to be personal. The above-mentioned context presupposes the idea of the following fundamental changes related to the field of personal data protection (de Hert, Papakonstantinou, 2016):

- The difference between reality and virtuality;
- Reduction of differences between the man, machine and nature;
- Information lag ranging from the lack of information to abundance of information;
- Transition from separate objects, properties to binary preference relationships, preference to interaction, processes, and networks.

It is noted that the EU data protection law can become an "overall law" aimed at ensuring the highest level of legal protection in all circumstances, but according to Rodrigues et al. (2016), it is practically impossible to comply with it; therefore, personal rights are ignored or discredited, they are abused. Many scholars (Petraitytė, 2011; de Hert, Papakonstantinou, 2012, 2016; Štitilis, 2014; Civilka, Šlapimaitė, 2015; Voss, 2016; Zaleskis, 2017; Purtova, 2018) analysing personal data protection issues criticized the concept of personal data as far too broad.

It becomes clear that most attention is drawn to one element of the concept of personal data – determining the person's identity on the basis of corresponding direction of technological development; i.e., re-identification and de-anonymization algorithms. However, N. Purtova (2018) notes that conducted research shows that, given technological advances in data processing and the amount of data to be analysed, absolute and irreversible anonymity no longer exist. The above-mentioned author draws attention to the difference between identifiable and unrecognizable information. N. Purtova (2018) proposes to keep personal data (or information for determining personal identity) as a security threshold grounded on zero identification risk when the risk of identification is associated with a different degree of information processing. It should be underlined that the above-mentioned author does not distinguish another problem area related to protection of personal data: the concept of personal

data is not limited to simple identification because another essential element of the concept of personal data is related to personal information.

In the age of the Internet of things, data transfer, advanced data analyses, and data management in decision-making determine that any information is related to the person, as defined in the EU data protection law (Barnard-Wills, 2017). From the data protection perspective, it can be seen that all data can affect people; therefore, all data must have some protection against possible negative effect. Based on the said context, it can be stated that it is the novelty of the General Data Protection Regulation (GDPR) that determines the relevance of this topic.

Topic issues. According to G. Miglicco (2018), the GDPR is associated with fundamental changes in business enterprises because they need to rethink fundamentally how they intend to handle customers' personal data. R. Kucęba and G. Chmielarz (2018) emphasize the issues of information and personal data security management in organizations and accentuate the need to analyse personal data security breaches in organizations as an important factor determining the necessity of improving previously applied solutions in this field. In addition, it is important to assess the level of organisational preparedness in the field of personal data protection, seeking to ensure compliance with the General Data Protection Regulation (GDPR) that has entered into force.

Based on the said context, the following **problem questions** can be raised: How business enterprises are able to secure personal data protection implementing the essential provisions of data protection policy? What changes have been undertaken in the business enterprise in the field of personal data protection? What problem areas have been disclosed applying personal data protection in business enterprises?

Exploration of the topic. Theoretical and practical problems of personal data protection are thoroughly analysed in various aspects by Lithuanian and foreign researchers. E. Žiobienė (2002, 2005) raises the issue of privacy protection enshrined in the Constitution of the Republic of Lithuania, revealing differences in the dissemination of information about public and private persons, emphasizes relevant problems of protection of the constitutional right to privacy. I. Petraitytė (2011) reveals the fundamental ideas of legal regulation of Lithuanian personal data protection, shows the link between this field of legal regulation and the person's natural right to privacy (its inviolability, protection) as well as the influence of this link on the system, content and development of legal provisions on personal data protection. D. Štitilis (2014) discusses the current situation and problems of the electronic health record and legal environment in the context of personal data protection. M. Civilka and L. Šlapimaitė (2015) reveal the constantly changing conception of personal data in the electronic space. Analysing the essential components of the concept of personal data, these authors criticize the conception enshrined in the Directive 1995/46/EC of the European Parliament and of the Council on protection of individuals with regard to personal data processing and on free movement of such data, critically analyse the recommendation on the concept of personal data adopted by the Article 29 Data Protection Working Party on June 20, 2007. E. Jarašiūnas (2017) draws attention to the topics of the Charter of Fundamental Rights of the European Union in the jurisprudence of the Court of Justice. J. Zaleskis (2017) defines the framework for the activities of the Data Protection Officer under the EU General Data Protection Regulation.

E. Mraznica (2017) contemporises the issue of harmonization of personal data protection at the EU level, emphasizing the necessity to control management of personal data and ensure greater risk management in this field. M. Goddard (2017) notes the impact of the GDPR on a global scale. N. Purtova (2018) accentuates the broad field of the concept of personal data, emphasizing flexibility, adaptability, and uncertainty of this concept. M. Jasztal (2018) addresses the problem of reducing the risk of the role of internal audit, which is related to personal data protection in implementing the GDPR. A comparative analysis performed by B. Custers et al. (2018) revealed the presence of significant differences in the way the Member States of the EU implemented personal data protection at the levels of national laws, policies, and practices. R. Kucęba et al. (2018) analyse personal data security breaches in organizations as an important factor determining the necessity of improving previously applied decisions in this field. S. Xander et al. (2018) raise the question of the links between confidentiality management and the GDPR: What steps were taken by the organizations in Europe to adapt to new privacy rules?

The object of the research: protection of personal data in the business enterprise.

The aim of the research: to analyse actions undertaken by the business enterprise in fulfilling the requirements for protection of personal data.

Research objectives:

1. To establish the principles of personal data protection;

2. To investigate how personal data protection is implemented in the business enterprise;

3. To highlight problem areas in implementing the personal data protection policy in the business enterprise.

Research methods:

1. Theoretical analysis. The analysis of the scientific literature on personal data protection.

2. The quantitative research. A questionnaire survey of employees of the business enterprise was conducted in order to determine how protection of personal data is implemented in the specific organization.

Literature Review

Advantages of General Data Protection application. The EU Parliament adopted the General Data Protection Regulation (GDPR), which substantially changed the Data Protection Directive valid until then, adopted in 1995. These rules apply to all organizations and enterprises whose activities are related to the EU customers, regardless of their geographical location. According to "Legaltech News", legislation defines new data and privacy rights for the EU consumers, regulates and transmits as well as handles the EU data, seeking stricter implementation of data management by punishing organizations for non-compliance with the rules provided by the GDPR (EU Approves GDPR, 2016).

The GDPR is intended for changing national laws of the Member States of the EU; there will be only one central supervisory institution to monitor access to the EU data. The EU maintains that such standardization will save 2.3 billion euros.

The following advantages of the GDPR are provided (EU Approves GDPR, 2016):

- Gives the EU citizens the right to be forgotten, which means that data controlers, data processors and third parties must delete the EU citizen's personal data online at his or her request, unless there are legitimate reasons to keep such information (historical, statistical, public health, scientific need, the right to freedom of expression or legal or contractual obligations);
- Clear and positive consent is required; e.g., the EU citizen indicates on the website that he or she agrees that his or her personal data are stored or processed;
- Provides the right to EU citizens to transfer data; e.g., allows the exchange of personal data between service providers as information from one e-mail provider to another;
- Demands that the EU enterprises and providers inform their representatives of national supervisory service about significant data management breaches more rapidly;
- Limits the use of profiling that collects personal information to predict the person's behaviour without his/her consent;
- Parental consent is required for children aged 13-16 to create an account on the social media.

General Data Protection Regulations. A new Directive of the EU on handling of cross-border cooperation data as well as on processing of criminal and judicial investigations was adopted along with the GDPR. The Directive lays down minimum standards for handling of data related to the rights of EU citizens and to criminal or judicial nature limitations of data transfer and allows for cooperation between law enforcement agencies of Member States.

According to M. Jasztal (2018), every business organization must implement the new regulation, which will be the basis for handling personal data of EU residents. Any entity can be prosecuted and punished for violating the provisions of the GDPR in every Member State of the EU if personal data have been breached. M. Jasztal (2018) draws attention to the established rules that the data controller should follow each time when processing personal data. The following rules are distinguished:

1. The principle of lawfulness, fairness and transparency, related to the obligation to apply general and national legal provisions in the field of data processing to the person to whom this is related.

2. Purpose limitation in data handling, which means that the collection of data should take place only for specific, explicit and legitimate purposes, except for the prohibition on further processing of data for archival, public, scientific, statistical, and historical purposes.

3. The data minimisation principle related to limitation of data collection; i.e., personal data will be accumulated to the extent that is necessary to achieve the purposes for which they are processed.

4. The principle of periodicity, according to which it is required that the data are accurate, updated and incorrect data are removed or corrected.

5. The principle of storage limitation, according to which the possibility of identification would appear only for that period which is exactly needed.

6. The principle of integrity and confidentiality, related to the obligation to keep personal data protected, in particular against unauthorized persons or their unlawful processing.

7. The principle of responsibility, which defines the responsibility of the data controller for personal data processing in accordance with the provided rules.

Methodology of Personal Data Protection regulation implementation. It is maintained that personal data is any information about the identified or identifiable natural person. An identifiable person is the one whose identity can be established directly or indirectly, in particular by indicating the identity number or one or several specific factors that describe the person's physical, physiological, mental, economic, cultural or social characteristics. Information that allows the person's identification is not taken into account if this requires excessive costs, time or activity. Organizational entities operating in the legal and economic space must perform their tasks reliably, legally, purposefully, economically, publicly and efficiently. The enforcement mechanisms described above are related to all areas of activity, including the activity-related territory, in processing personal data. Tasks need to be performed properly, seeking to ensure appropriate and efficient mechanisms granting the rights and the limits of responsibility in performing tasks, following established rules, and properly supervising data as well as seeking to ensure efficient data protection (Goddard, 2017).

The said context reveals that the most appropriate method for acting objectively and independently in the above-mentioned activity areas is an internal audit investigation. Although, according to E. Mraznica (2017), for many years the internal audit investigation was attributed to the economic sector to familiarize the enterprise's board members, the head of the finance department with the obtained findings so that the latter know in advance what to do in case of at least the least risk. However, it must be emphasized that risk reduction is necessary not only in the economic sector but also in the field of personal data processing in order to prevent breaches and fraud cases in this area. Therefore, it can be stated that the organization also needs professional staff who can control the activities related to personal data processing, including the risks in this field (de Hert, Papakonstantinou, 2016).

The following advantages of the GDPR have been distinguished: it gives EU citizens the right to be forgotten; clear and positive consent is required; gives EU citizens the right to transfer data; requires to inform about important data management breaches more rapidly; restricts the use of profiling. The following principles of personal data protection have been established: the principle of lawfulness, fairness and transparency; purpose limitation in data handling; the data minimisation principle; the principle of periodicity; the principle of storage limitation; the principle of integrity and confidentiality; and the principle of responsibility.

Methodology

To conduct the empirical research, the research aim was raised: to identify the actions that the business enterprise performs in implementing personal data protection. It was sought to determine actions taken by the business enterprise in planning to move to personal data protection under the new Regulation (GDPR) as well as to identify problem areas encountered by the business enterprise in the field of personal data protection. Based on this context, it was decided to investigate how personal data protection was implemented from the standpoint of business enterprise's employees. In the theoretical part of the research, after analysing the scientific literature that is closely related to the topics under investigation, it was decided to conduct a case study by selecting a Lithuanian business enterprise.

In the opinion of K. Kardelis (2016), one of the most important requirements for sampling is the representativeness of the sample, which correctly reflects the proportions of possible values of the studied feature in the population. In this case, the sample of interview participants was formed on the basis of the research aim and on the criteria provided for the participants (Rupšienė, 2007; Bitinas et al., 2008); i.e., their purposeful sampling was applied.

Respondents were selected for the questionnaire survey using the purposeful sampling method because the following respective respondents' selection criteria were developed prior to conducting this survey:

• The employee must be employed by the enterprise for at least 1 year;

• The employee's position must be related to management and/or implementation of personal data protection;

• Employees must by their will and voluntarily agree to complete the questionnaire;

• Employees who have agreed to participate in the questionnaire survey must fully complete the questionnaire checklist.

According to the data of January 1, 2020, the business enterprise has 106 employees. Based on respondents' sampling criteria to conduct the questionnaire survey, 63 employees of this enterprise were selected, for whom the prepared survey questionnaires were provided. 56 questionnaires were selected for the analysis of the research data as not all questionnaires

were fully completed and were assessed as damaged and unsuitable for further processing. It can be stated that the return rate of the questionnaires is almost 100 per cent; therefore, the survey data can be treated as reliable and representative. A quantitative study was conducted on October 19-27, 2020. The analysis of the written survey data was performed by calculating the means of respondents' opinions and applying the method of descriptive statistics.

The questions of the survey questionnaire were designed based on the Likert scale, seeking to measure and determine the extent to which the respondent agrees or disagrees with the presented statements or other indicators defining the phenomenon or process. The answers to the statements in both questionnaires ranged from "strongly agree" (5 points) to "strongly disagree" (1 point). Respondents had to choose one answer and mark it with the symbol "X". The formulated questions in the questionnaire are presented in a certain order. Respondents were asked a total of 8 questions (6 closed-ended questions and 2 open-ended questions). The groups of questions in the compiled research questionnaire were divided into 4 groups.

Conducting the empirical research, the requirements for research ethics were followed. Therefore, in order not to violate the ethics of social research, prior to conducting the interview with the manager of the enterprise and questionnaire surveys of employees, their oral consent was obtained and the possibility of conducting the research was discussed with them during the information meeting. The aims and objectives of the research were clearly and comprehensibly explained to the enterprise's manager and employees, and they were asked to participate in the study. The principles of voluntary participation in the study and anonymity as well as the possibility of self-determination to refuse to participate in the research or to withdraw from it were emphasized to the subjects.

It is assumed that the obtained research results can be applied in other Lithuanian business enterprises due to similarities in managing personal data protection processes.

Results

The aim of this empirical research is to identify the actions the organization undertook in planning the transition to personal data protection under the new Regulation (GDPR). Primarily, it was sought to identify actions related to the analysis of the situation of privacy measures; therefore, respondents had to evaluate the actions of their organization, related to application of privacy measures, undertaken to ensure personal data protection (see Table 1).

Table 1

Actions related to the application of privacy measures, undertaken in the business enterprise, seeking to ensure personal data protection

Criterion / Statement	Strongly agree	Partially agree	Neither agree nor disagree	Partially disagree	Strongly disagree
A personal data processing and review system has been developed	54%	19%	11%	11%	5%
An analysis of gaps in personal data protection has been performed	44%	31%	21%	4%	0%
Personal Data Protection Impact Assessment (DPIA) has been performed	28%	17%	44%	0%	11%
Risk assessment in the field of personal data protection has been carried out	51%	22%	17%	5%	5%
The level of implementation maturity in the field of personal data protection has been identified	32%	27%	43%	0%	0%

As it can be seen from the data given in Table 1, many employees of the business enterprise maintain that the following three steps related to application of privacy measures, undertaken in this business enterprise in order to ensure personal data protection, are the most important:

1. Development of the personal data processing and review system;
2. Performance of risk assessment in the field of personal data protection;
3. Performance of the analysis of gaps in personal data protection.

The analysis of the research data has shown that more than a third of enterprise's employees who took part in the research (44 per cent and 43 per cent respectively) did not have the opinion on the enterprise's actions such as performance of the Personal Data Protection Impact Assessment (DPIA) and identification of the maturity level of implementation in the field of personal data protection, which are related to application of privacy measures, undertaken by the business enterprise, seeking to ensure the protection of personal data. In addition, it has

been found that a share of respondents (11 per cent) strongly disagree with the statement that the Personal Data Protection Impact Assessment (DPIA) was carried out in this enterprise.

In summary, it can be stated that seeking to ensure the protection of personal data, the business enterprise paid most attention to the process of development of the personal data processing and review system; risk assessment in the field of personal data protection was carried out, and gaps in the personal data protection system were addressed. However, this enterprise did not pay enough attention to other areas that were also closely related to application of privacy measures, seeking to ensure protection of personal data: no Personal Data Protection Impact Assessment (DPIA) was performed and the maturity level of implementation in the field of personal data protection was not identified.

This leads to the conclusion that the business enterprise has only undertaken partial actions related to application of privacy measures, seeking to ensure personal data protection. Therefore, it should be assumed that this enterprise underestimated the importance of the field of personal data protection in its activities and did not purify a clear concept of personal data protection, which would be understood by all employees of this enterprise.

This study also addressed the actions of the business enterprise, related to the enterprise's adaptation to the new requirements for processing personal data. During this empirical research, respondents had to evaluate the actions undertaken by the organization, seeking to adapt to the new requirements for processing personal data (see Table 2).

Table 2

Actions undertaken by the business enterprise, seeking to adapt to the new requirements for processing personal data

Statement \ Criterion	Strongly agree	Partially agree	Neither agree nor disagree	Partially disagree	Strongly disagree
Security of address data	57%	28%	5%	5%	5%
Data leakage from the EU has been prevented	33%	28%	17%	11%	11%
Transfer of address data	44%	34%	17%	0%	5%
Use of anonymous data	22%	40%	22%	5%	11%
Purpose limitation of address data	49%	17%	18%	11%	5%

The analysis of the research data has shown that most of the employees of the business enterprise, who participated in this empirical research, distinguish three specific actions that were undertaken in the business enterprise, seeking to adapt to the new requirements for personal data processing:

1. Security of address data;
2. Transfer of address data;
3. Purpose limitation of address data

Analysing respondents' answers to this question, it was identified that more than a third of them (40 per cent) only partially agreed that actions such as the use of anonymous data had been undertaken in their enterprise in order to adapt to the new requirements for processing personal data. It should be emphasized that 11 per cent of research participants even strongly disagreed with the statement that the business enterprise used anonymous data. The same number of enterprise's employees (11 per cent) also strongly disagreed with the fact that the enterprise had prevented data leakage from the EU. Only a third of respondents (33 per cent) strongly agreed with this statement that the enterprise had prevented data leakage from the EU; 28 per cent of the enterprise's employees partially agreed with this.

In summary, it can be stated that seeking to adapt to the new requirements for personal data processing, the business enterprise has prioritized actions that are related to security of address data, transfer of address data, and purpose limitation of address data. It was found that this enterprise had not paid enough attention to the actions related to the use of anonymous data and prevention of data leakage from the EU.

It can be concluded that the business enterprise only partially adapted to the new personal data processing requirements as the enterprise's actions related to adaptation to the new personal data processing requirements do not encompass all areas relevant to personal data processing under new personal data protection requirements. Based on the said context, the following assumption can be made: seeking to adapt to new requirements for personal data processing, the business enterprise became more focused on the field of address data and underestimated the importance of the use of anonymous data and prevention of data leakage from the EU.

This study also sought to identify actions related to the development and improvement of the personal data protection management and control system. Respondents had to evaluate the actions of the business enterprise, related to the development and improvement of the personal data protection management and control system (see Table 3).

Table 3

Actions related to the development and improvement of the personal data protection management and control system in the business enterprise

Statement \ Criterion	Strongly agree	Partially agree	Neither agree nor disagree	Partially disagree	Strongly disagree
Improvement of the privacy policy	46%	38%	11%	0%	5%
Implementation of privacy by activity area	17%	61%	17%	0%	5%
Introduction of privacy by default	51%	27%	8%	4%	0%
Improvement of the security policy	54%	28%	18%	0%	0%
Planning of GDPR implementation	17%	5%	73%	0%	5%
Improvement of outsourcing contracts	29%	17%	21%	11%	22%
Improvement of data log management	47%	24%	12%	17%	0%
Improvement of the continuity plan	54%	28%	13%	5%	0%
Development of Binding Corporate Rules	22%	45%	28%	5%	0%
Training of employees to work with personal data	48%	33%	19%	0%	0%

As it can be seen from the data presented in Table 3, more than a half of respondents (respectively 54 per cent for each statement) emphasize the improvement of the security policy and the improvement of the continuity plan as those fundamental actions that are related to the development and improvement of the personal data protection management and control system at JSC “Lietuvos žinios”. A similar number of research participants (51 per cent) strongly agree that the introduction of privacy by default in this enterprise is also to be attributed to the actions related to the development and improvement of the personal data protection management and control system in the business enterprise.

The analysis of the research data has shown that slightly less than a half of respondents strongly agree that the business enterprise is taking steps to improve its privacy policy and data log management and that employees are trained to work with personal data.

It was found that more than a half of respondents (61 per cent) only partially agreed that privacy implementation actions were carried out in this enterprise according to the activity area. In addition, it showed up that more than a third of respondents (45 per cent) only partially saw the enterprise’s actions related to the process of developing Binding Corporate Rules, while almost a third of them (28 per cent) did not even have an opinion about the enterprise’s actions in this activity area.

Analysing the research data, it should be noted that the majority of research participants (as many as 71 per cent) do not have an opinion on whether the GDPR implementation process was planned in the business enterprise.

It has been found that a share of respondents either partially or strongly disagree with some of the actions related to the development and improvement of the personal data protection management and control system in this business enterprise. Although nearly half of research participants agreed that the enterprise was improving data log management processes, the research showed that 17 per cent of respondents nevertheless partially disagreed with such statement.

Based on the analysis of research data, respondents assess the improvement of outsourcing contracts in this enterprise more negatively than positively: almost a third of them (22 per cent) do not agree that the business enterprise is improving the process of outsourcing contracts, which is also enhanced by 17 per cent of respondents who state that they partially disagree with the statement that outsourcing contracts are being improved in this enterprise.

In summary, it can be stated that the improvement of the security policy and continuity plan as well as introduction of privacy by default are essential steps that are to be related to the development and improvement of the personal data protection management and control system in this enterprise. It has been found that the actions of improving the privacy policy and data log management are taking place in the business enterprise and that employees are being trained to work with personal data. It was found that most employees did not have an opinion about planning steps for implementation of personal data protection under the new regulation. It showed up that this enterprise had not taken any steps related to improvement of its outsourcing contracts as part of its personal data protection policy.

It can be assumed that implementing the personal data protection policy, the business enterprise did not pay enough attention to one of the most important elements of the enterprise's management – planning the implementation of new requirements for personal data processing. Hence, the development and improvement of the personal data protection management and control system in this business enterprise have weaknesses that need to be eliminated in improving the currently employed data protection management and control system as partially adapted to the new requirements for personal data processing.

Supplementing and broadening the scope of actions related to adaptation to new requirements for personal data processing, it was also sought to find out the actions of this business enterprise, related to internal human resources and external partners in implementing the personal data protection policy (see Table 4).

Table 4

Actions related to internal human resources and external partners in implementing the personal data protection policy in the business enterprise

Statement \ Criterion	Strongly agree	Partially agree	Neither agree nor disagree	Partially disagree	Strongly disagree
A Data Protection Officer or a person responsible for implementing the personal data protection policy in the organization has been appointed	43%	29%	18%	0%	0%
Informing the employees about the personal data protection policy and training to work on the basis of it	51%	34%	5%	5%	5%
A team has been assembled, whose work is related to introduction, management, and control of the personal data policy in the organization	17%	45%	22%	0%	16%
Cooperation with external partners in implementing the personal data policy in the organization	53%	31%	11%	0%	5%
Hiring external experts in implementing the personal data policy in the organization	22%	17%	28%	17%	16%
Leader support in implementing the personal data policy in the organization	17%	22%	34%	22%	5%

To find out the actions undertaken by the business enterprise with regard to internal human resources and external partners in implementing the personal data protection policy in this business enterprise, it was identified that half of respondents (51 per cent) distinguished informing the employees about the personal data protection policy and training to work on the basis of it in implementing the personal data protection policy in the area of internal human resources and external partners as well as cooperation with external partners in implementing the personal data policy in the organization, as stated by 53 per cent of respondents. More than a third of respondents (43 per cent) note that this business enterprise has appointed the Data Protection Officer or the person responsible for implementing the personal data protection policy in the business enterprise.

The analysis of the research data has revealed that more than a third of respondents (45 per cent) only partially agree that this business enterprise assembled the team whose work is related to introduction, management and control of the personal data policy in the organization, while 16 per cent of research participants strongly disagree with this distinguished statement. This confirms one of the management functions discussed earlier – planning – as the weakness of this enterprise in implementing the new regulation in the field of personal data protection.

Respondents indicated that this business enterprise had not hired external experts for implementation of the personal data policy in accordance with the requirements set out in the new regulation. Assessing the leader support for the implementation of the personal data policy in the organization, one third of respondents (34 per cent) do not have an opinion about it, and almost a third of them (22 per cent) partially disagree with such statement.

In summary, it can be stated that actions related to internal human resources and external partners in the implementation of the personal data protection policy are particularly prominent in the areas of informing the employees about the personal data protection policy, training to work on the basis of it, and cooperation with external partners. However, it was found that there was no specific team in this business enterprise whose work would have been related to introduction, management and control of the personal data policy in the organization and no external experts were hired to help implement the personal data policy in accordance with the

requirements set out in the new regulation. Assessment at the level of internal human resources revealed that during the implementation of the personal data policy in this business enterprise, employees had missed the leader support in implementing the process of adapting to new requirements for processing personal data in the organization.

In the said context, it can be assumed that the process of adapting to new requirements for personal data processing in the business enterprise was not smooth as the enterprise's management did not assemble the team clearly supported by the leader in the internal management structure, which together with hired external experts would be responsible for smooth process of development and improvement of the personal data protection management and control system.

Supplementing and broadening the scope of analysing the situation of privacy measures, it was also sought to find out what specific actions the enterprise had undertaken in implementing the personal data protection policy (see Table 5).

Table 5

Actions undertaken by the business enterprise in implementing the personal data protection policy

Statement \ Criterion	Strongly agree	Partially agree	Neither agree nor disagree	Partially disagree	Strongly disagree
Ensuring control of access to personal data	34%	51%	11%	0%	4%
Ensuring security of personal data	51%	33%	11%	0%	5%
Ensuring accuracy of personal data	41%	54%	0%	0%	5%
Ensuring erasure or forgetting of personal data	45%	22%	17%	11%	5%
Development of a database for processing information related to personal data	34%	28%	28%	5%	5%
Informing individuals about the nature of the use of their personal data	44%	28%	28%	0%	0%
Development of the description of the procedure for rules on a new consent to the use of personal data	34%	34%	22%	5%	5%
Application of precautionary measures, seeking to reduce harm due to potential problems related to personal data protection	22%	39%	34%	0%	5%
Monitoring of the location of physical data	22%	11%	57%	5%	5%

Based on the data presented in Table 5, it can be seen that half of respondents (51 per cent) strongly agree with the statement that security of personal data is ensured in this business enterprise as a key action undertaken by this enterprise in implementing the personal data protection policy. More than a third of respondents note assurance of erasure or forgetting of personal data as well as informing individuals about the nature of the use of their personal data, which should be considered as important steps in the enterprise, implementing the personal data protection policy.

It is observed that half of respondents (51 per cent) partially agree that the personal data access control and accuracy of personal data are ensured in this business enterprise.

It should be accentuated that although more than a third of respondents (39 per cent) partially agrees that this business enterprise applies precautionary measures, seeking to reduce harm due to potential problems related to personal data protection, a similar percentage of research participants (34 per cent), however, has no opinion on this matter.

As to monitoring of the location of physical data, implemented in this business enterprise, it showed up that more than a half of all respondents (57 per cent) cannot answer this question – they do not have an opinion on this area.

To sum up, it can be stated that the business enterprise is able to ensure security of personal data by implementing key provisions of the personal data protection policy, one of which is to ensure erasure or forgetting of personal data and informing the individuals about the nature of their personal data use. However, only partial personal data access control and accuracy of personal data are ensured in this business enterprise. Weaknesses identified in the implementation of the personal data protection policy in this business enterprise are as follows: non-compliance with precautionary measures in order to reduce damage due to potential problems related to personal data protection, absence of monitoring of the location of physical data.

Seeking to further supplement and expand the scope of actions related to adaptation of the business enterprise to new requirements for personal data processing, it is important to

identify problem areas that showed up in implementing the personal data protection policy in this business enterprise (see Table 6).

Table 6

Problem areas that emerged in implementing the personal data protection policy in this business enterprise

Statement \ Criterion	Strongly agree	Partially agree	Neither agree nor disagree	Partially disagree	Strongly disagree
Ensuring control of access to personal data	44%	34%	22%	0%	0%
Ensuring security of personal data	5%	39%	34%	0%	22%
Ensuring accuracy of personal data	5%	22%	51%	0%	22%
Ensuring erasure or forgetting of personal data	17%	17%	27%	11%	28%
Development of the database for processing information related to personal data	22%	17%	22%	5%	34%
Informing individuals about the nature of the use of their personal data	45%	22%	22%	11%	0%
Development of the description of the procedure for rules on a new consent to the use of personal data	56%	33%	11%	0%	0%
Application of precautionary measures, seeking to reduce harm due to potential problems related to personal data protection	17%	34%	17%	17%	15%
Monitoring of the location of physical data	22%	5%	40%	22%	11%
Training the employees to work with personal data	22%	5%	17%	39%	17%
Cooperation with external partners in implementing the personal data policy in the organization	11%	11%	17%	50%	11%
Hiring external experts in implementing the personal data policy in the organization	12%	6%	24%	39%	19%
Leader support in implementing the personal data policy in the organization	5%	28%	17%	45%	5%
Appointment of the Data Protection Officer or the person responsible for implementation of the personal data protection policy in the organization	17%	5%	22%	11%	45%
Informing the employees about the personal data protection policy and training to work based on it	11%	17%	28%	16%	28%
Assembling the team whose work is related to introduction, management, and control of the personal data policy in the organization	22%	0%	44%	0%	34%

Based on the analysis of the research data, three problem areas that emerged in implementing the personal data protection policy in this business organization can be identified:

1. Ensuring control of access to personal data;
2. Informing individuals about the nature of the use of their personal data;
3. Development of the description of the procedure for rules on a new consent to use personal data.

It has been found that respondents have no opinion on the areas such as monitoring of the location of physical data and assembling the team whose work is related to introduction, management and control of the personal data policy in the organization. Based on the previous analysis of research data, the latter areas are to be attributed to problem areas, which can be considered as a weakness in this business enterprise.

In respondents' opinion, the following areas of the business enterprise should not be attributed to problem areas in implementing the personal data protection policy in this business organization:

1. Ensuring erasure or forgetting of personal data;
2. Development of the database for processing information related to personal data;
3. Training of employees to work with personal data;
4. Cooperation with external partners in implementing the personal data policy in the organization;
5. Hiring external experts in implementing the personal data policy in the organization;
6. Leader support in implementing the personal data policy in the organization;
7. Appointment of the Data Protection Officer or the person responsible for implementing the personal data protection policy in the organization;

8. Informing the employees about the personal data protection policy and training to work based on it.

In summary, it can be stated that problem areas of the business enterprise that showed up in implementing the personal data protection policy in this business organization are related to ensuring the personal data access control, informing individuals about the nature of their personal data use, and the process of development of the description of the procedure for rules on a new consent to the use of personal data. Thus, all problem areas identified in the business enterprise include areas of personal data protection.

Although the previous analysis of research data revealed that hiring external experts and leader support in implementing the personal data policy in the organization were to be assessed as weaknesses, the employees of this business enterprise did not treat them as problem areas.

Based on the said context, the following assumption should be made: the employees of the business enterprise do not have a clear concept of improving the implementation, management and control of personal data protection in the business organization as their answers often contradict each other. The emerging contradiction allows to consider the low maturity level of implementation in the field of personal data protection as there is no uniform approach of all employees to implementation of the personal data protection policy under the new regulation.

Responding to the given questions, employees of the business enterprise had to indicate how, in their opinion, implementation, management and control of personal data protection in this business enterprise should be improved. Three notional categories were distinguished, revealing the employees' attitude to the areas of personal data protection improvement in the business enterprise (see Table 7).

Table 7

Improvement of implementation, management and control of personal data protection in the business enterprise

Category	Subcategory	Proof statement
Assembling the team	–	"I think it was necessary to assembly such team which would be responsible for protection of personal data in our organisation in accordance with its members' positions"
Leader support	–	"It is strongly felt that there is no that key person with an exclusive interest in the protection of personal data; i.e., there would be the one who would advise in that area".
Hiring external experts	–	"I am for hiring an external specialist who would help make the transition to the appropriate personal data policy easier and smoother".

Analysing the responses of business enterprise's employees about the improvement of personal data protection in this business organization, the category "Assembling the team" was distinguished. According to research participants, the enterprise needs such team whose work would be related to introduction, management, and control of the personal data policy in the organization. This is confirmed by the following statement: "I think it was necessary to assembly such team which would be responsible for protection of personal data in our organisation in accordance with its members' positions".

Another important area for improvement, related to improving personal data protection in the business enterprise, is leader support. It came to prominence that the employees of this business organization particularly valued leader support in implementing the personal data policy in the organization ("It is strongly felt that there is no that key person with an exclusive interest in the protection of personal data; i.e., there would be the one who would advise in that area").

Employees also emphasize the need of hiring external experts in implementing the personal data policy in the business organization. This is illustrated by the following statement of the subjects: "I am for hiring an external specialist who would help make the transition to the appropriate personal data policy easier and smoother".

To sum up, it can be stated that employees of the business enterprise associate the improvement of implementation, management and control of personal data protection in the business enterprise with three segments: teamwork, leader, and external consulting assistance.

Conclusions

1. Advantages of the GDPR have been distinguished: gives EU citizens the right to be forgotten; clear and positive consent is required; gives EU citizens the right to transfer data; requires to inform about important data protection breaches more rapidly; and limits the use of profiling. The principles of personal data protection have been established: the principle of

lawfulness, fairness, and transparency; purpose limitation in data handling; the data minimisation principle; the principle of periodicity; the principle of storage limitation; the principle of integrity and confidentiality; and the principle of responsibility.

2. It has been established that the business enterprise is able to ensure security of personal data by implementing the essential provisions of the personal data protection policy, one of which is to ensure erasure or forgetting of personal data and to inform individuals about the nature of the use of their personal data. However, this business enterprise ensures only partial control of access to personal data and accuracy of personal data. Weaknesses in the implementation of the personal data protection policy in this business enterprise have been distinguished: precautions are not taken to reduce the damage due to potential problems related to protection of personal data, monitoring of the location of physical data is not carried out.

3. The research has revealed problem areas in implementing the personal data protection policy in the business enterprise: ensuring control of access to personal data; informing individuals about the nature of the use of their personal data; and development of the description of the procedure for rules on a new consent to use personal data. Hiring external experts and leader support in implementing the personal data policy in the organization are to be assessed as a weaknesses of the enterprise. It is assumed that the employees of the business enterprise do not have a clear concept about the improvement of implementation, management and control of personal data protection in the organization because a share of answers contradict each other. This contradiction allows to consider the low maturity level of implementation in the field of personal data protection as there is no uniform approach of all employees to implementation of the personal data protection policy under the new regulation.

References

1. Barnard-Wills, D. (2017). The technology foresight activities of European Union data protection authorities. *Technological Forecasting & Social Change*, *116*, 142–150. EBSCOhost: Business Source Complete.

2. Bitinas, B., Rupšienė, L., ir Žydžiūnaitė, V. (2008). Kokybinių tyrimų metodologija. Vilnius: Socialinių mokslų kolegija.

3. Civilka, M., ir Šlapimaitė, L. (2015). Asmens duomenų samprata elektroninėje erdvėje. *Teisė, 96*, 126–148. doi: https://doi.org/10.15388/Teise.2015.96.8761

4. Custers, B., Dechesne, F., Sears, A. M., Tani, T. and van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law & Security Review*, *34* (2), 234–243. EBSCOhost: Business Source Complete.

5. de Hert, P., and Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, *32* (2), 179–194. EBSCOhost: Business Source Complete.

6. de Hert, P., and Papakonstantinou, V. (2012). The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. *Computer Law & Security Review*, *28* (2), 130–142. EBSCOhost: Business Source Complete.

7. EU Approves GDPR. (2016). *Information Management Journal*, *50* (4), 7–8. EBSCOhost: Business Source Complete.

8. Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, *59* (6), 703–705. doi: 10.2501/IJMR-2017-050.

9. Jarašiūnas, E. (2017). Europos Sąjungos pagrindinių teisių chartija teisingumo teismo jurisprudencijoje. *Jurisprudencija*, *1* (24), 6–34.

10. Jasztal, M. (2018). The Role of Internal Audit in Reducing Risk Related to Personal Data Protection Following GDPR Implementation. *Research Papers of the Wroclaw University of Economics / Prace Naukowe Uniwersytetu Ekonomicznego we Wroclawiu*, *521*, 69–78. doi: 10.15611/pn.2018.521.07.

11. Kardelis, K. (2016). *Mokslinių tyrimų metodologija ir metodai*. Šiauliai: Liucijus.

12. Kucęba, R., and Chmielarz, G. (2018). Issues of Personal Data Management in Organizations - GDPR Compliance Level Analysis. *Business Informatics / Informatyka Ekonomiczna*, *1* (47), 58–71. EBSCOhost: Business Source Complete.

13. Miglicco, G. (2018). GDPR is here and it is time to get serious. *Computer Fraud & Security*, *9*, 9–12. EBSCOhost: Business Source Complete.

14. Mraznica, E. (2017). GDPR – a New Challenge for Personal Data Protection. *Bankarstvo Magazine*, *46* (4), 166–177. doi: 10.5937/bankarstvo1704166M.

15. Petraitytė, I. (2011). Asmens duomenų apsauga ir teisė į privatų gyvenimą. *Teisė, 80*, 163–174. Retrieved from: http://www.zurnalai.vu.lt/teise/article/view/158.

16. Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation & Technology*, *10* (1), 40–81. doi: 10.1080/17579961.2018.1452176.

17. Rodrigues, R., Barnard-Wills, D., de Hert, P., and Papakonstantinou, V. (2016). The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR. *International Review of Law, Computers & Technology, Taylor & Francis*. 2016, *30* (3), 248–270. EBSCOhost: Business Source Complete.

18. Rupšienė, L. (2007). *Kokybinio tyrimo duomenų rinkimo metodologija*: metodinė knyga. Klaipėda: Klaipėdos universiteto leidykla.

19. Štitilis, D. (2014). Elektroninis sveikatos įrašas ir teisinė aplinka: esama situacija bei problemos. *Sveikatos politika ir valdymas*, *1* (6), 63–79. doi: 10.13165/SPV-14-1-6-05.

20. Voss, W. G. (2016). European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield and the Right to Delisting. *Business Lawyer*, *72*, 221–234. EBSCOhost: Business Source Complete.

21. Xander, S., Hannu, S., and Rutkowski, A.-F. (2018). Privacy Governance and the GDPR: How Are Organizations Taking Action to Comply with the New Privacy Regulations in Europe? *Proceedings of the European Conference on Management, Leadership & Governance*, 371–378. EBSCOhost: Business Source Complete.

22. Zaleskis, J. (2017). Duomenų apsaugos pareigūno veiklos pagrindai pagal ES bendrąjį duomenų apsaugos reglamentą. *Teisė*, *104*, 159–170. Retrieved from: http://www.zurnalai.vu.lt/teise/article/view/10851/8986

23. Žiobienė, E. (2005). Aktualios konstitucinės teisės į privatų gyvenimą apsaugos problemos. *Jurisprudencija*, *64* (56), 124–131. Retrieved from: https://www3.mruni.eu/ojs/jurisprudence/article/view/3135/2936

24. Žiobienė, E. (2002). Lietuvos Respublikos Konstitucijoje įtvirtinta privataus gyvenimo apsauga: informacijos skleidimo apie viešuosius ir privačius asmenis skirtumai. *Jurisprudencija*, *30* (22), 91–99. Retrieved from: https://www3.mruni.eu/ojs/jurisprudence/article/view/3567/3359

Received: 4 February 2021
Accepted: 31 May 2021