Problemy Zarządzania – Management Issues, vol. 17, no. 3(83): 137–153
ISSN 1644-9584, © Wydział Zarządzania UW
DOI 10.7172/1644-9584.83.8

Management of GDPR-Related Legal Risk in Public Organizations in View of Costs of Administrative Sanctions

Submitted: 03.04.19 | Accepted: 10.05.19

Michał Gołębiowski*

The aim of this article is to identify primary risk areas related to the protection of personal data on the basis of current regulations (further referred to as "the GDPR-related legal risk") in organizations of the public finance sector. The article focuses on the matters relating to the management of personal data protection with respect to the economic impact assessment of violating the existing legal standards and in the context of possible financial and image-related sanctions for public organizations. It is based on the review of available literature, audit reports of the Supreme Audit Office (Najwyższa Izba Kontroli, NIK) and my own research.

Keywords: legal risk, GDPR, public organizations.

Zarządzanie ryzykiem prawnym RODO w organizacjach publicznych w aspekcie kosztów sankcji administracyjnych

Nadesłany: 03.04.19 | Zaakceptowany do druku: 10.05.19

Celem artykułu jest identyfikacja podstawowych obszarów ryzyka związanych z problematyką ochrony danych osobowych na podstawie aktualnych przepisów (dalej: ryzyko prawne RODO) w organizacjach sektora finansów publicznych. Opracowanie przybliża problematykę zarządzania ochroną danych osobowych z punktu widzenia ekonomicznej oceny skutków naruszania obowiązujących norm prawnych w kontekście możliwych do poniesienia sankcji finansowych i wizerunkowych dla organizacji publicznych. Artykuł opiera się na przeglądzie dostępnej literatury, wynikach kontroli NIK oraz badaniach własnych.

Słowa kluczowe: ryzyko prawne, RODO, organizacje publiczne.

JEL: H83, K23

* **Michał Gołębiowski** – MA, PhD student, Kozminski University.

Correspondence address: Kozminski University, 57/59 Jagiellońska St., 03-301 Warsaw.

Ministry of Science and Higher Education
Republic of Poland

The creation of the English-language version of these publications is financed in the framework of contract No. 607/P-DUN/2018 by the Ministry of Science and Higher Education committed to activities aimed at the promotion of education.

1. Introduction

The GDPR-related legal risk management in public organizations is an up-to-date issue, as since 25 May 2018, the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)[1] has been in force. Following the analysis of the current legal situation, it can be said that in order to comply with the GDPR regulations, organizations need to adopt a fundamentally new approach to legal risk management (Kawecki & Osieja, 2017, p. 1).

The method of the economic analysis of law has been used to study the GDPR-related legal risk because law should be economically efficient (Jabłońska-Bonca, 2017, p. 15). The development of economic analysis of law (EAL) provides for the use of economic laws to evaluate how a particular regulation works. Research conducted within the economic analysis of law addresses this issue. Cooter and Ulen (2009 p. 21) included public institutions, whose task is to tackle market failures, into EAL's field of interest. From the economic point of view, it is interesting to determine the economic and social effectiveness of legal solutions and cost-effectiveness of compliance with the law by societies and individuals. The analysis of economic effectiveness is the best tool for both the public and private sector. The problem that appears when the method of economic analysis is transferred to other scientific disciplines, such as law, is the immeasurability and incomparability of social phenomena and legal effects. For this reason, a penalty (a sanction) for failure to comply with the law or benefitting from non-compliance has been put forward as a key parameter within the economic analysis of law (Stelmach & Brożek, 2004 pp. 138–153).

In 2018, a survey was carried out in several public and business organizations in the form of a questionnaire and an in-depth interview with persons responsible for data security. The study focused on selected features of shaping risk management processes and was limited to the economic aspect (with the use of the economic analysis of law – EAL), including costs borne by public organizations to ensure and maintain the security of personal data in the context of possible costs of administrative sanctions. The results show that solutions adopted to ensure the management of legal risk are related to the holistically viewed operational management. The study reveals no differences in the approach to risk management between public and business organizations. The survey was carried out on a relatively small sample, so it can be considered as a pilot.

In terms of possible costs and in relation to failure to comply with legal obligations (Gałaj-Emiliańczyk, 2018, pp. 7–10), an attempt to answer how to reduce the GDPR-related legal risk was taken, taking into account the possible application of new solutions offered by the economic doctrine (New

 DOI 10.7172/1644-9584.83.8

Public Management) in relation to specific conditions of formal and legal nature in Polish organizations operating within the public finance system (Piątek & Postuła, 2018, pp. 201–202).

The sum of costs related to the implementation of the GDPR regulations in operational activities of public organizations has so far been connected with the entry into force of the GDPR Regulation and the Act of 10 May 2018 on the protection of personal data.[2] Since April 2019, organizations operating in the public finance sector pursue their activity in accordance with the Act of 21 February 2019 on changes of certain laws to ensure the application of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. The above mentioned law seeks to harmonize 162 acts with provisions of the GDPR regulation. As a consequence of the entry into force of the act, public organizations will be forced to adopt new solutions relating to the personal data protection, based on the evaluation of legal risk in the context of possible administrative sanctions (Litwiński, 2018, pp. 444–448).

Regardless of the identified needs and understanding of the necessity of managing security and personal data protection in numerous areas of public administration, it has become of utmost importance to meet legal requirements induced by the introduction of the General Data Protection Regulation (GDPR). Whatever the specifics of varied activities of organizations, the requirements related to the personal data of an individual are crucial in every case (Gawroński, 2018, p. 31). Relevant safeguards are important for employees, employers and clients due to the restrictions set forth in the act and the credibility of the organization involved in data processing. There are very few kinds of business or public activities that do not require access to personal data and its processing. It regards all organizations having at least one employee. The legislator reduced the scope of the GDPR for organizations employing up to 250 people.

While processing personal data, each organization has to comply with legal requirements, which impose many obligations, define limitations and specify administrative sanctions for breaches of the provisions. The fulfillment of legal requirements is very costly and limits the ease of doing business (Kępa, 2015, p. 11). However, the threat of administrative sanctions is becoming equally important. The fulfillment of the GDPR-related legal requirements is currently a key aspect of security management in organizations. The Data Security Management System (DSMS) compliant with ISO/IEC 27001 is a good example due to its market recognizability.

This paper seeks to analyze how public organizations, operating within the public finance sector, ensure the protection of personal data, which is an important part of the security management system in organizations. Moreover, it sets out key requirements in this respect and findings of NIK's

audit on the level of personal data protection in public organizations. It also presents preliminary results of author's own research including the evaluation of the level of legal risk awareness and preparation of organizations to perform their statutory tasks related to the protection of personal data.

2. Legal Basis for Personal Data Protection in Public Organizations

With regard to personal data protection, public organizations operate under the following legal acts (as of December 2018):

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, Official Journal of the European Union L119 dated 4 May 2016);
2. Act of 10 May 2018 on the protection of personal data (Official Journal (Dz.U.) of 2016, item 922, as amended);
3. Act of 17 February 2005 on the computerization of the activity of entities performing public tasks (Official Journal (Dz.U.) of 2017, item 570);
4. Regulation of the Minister of the Interior and Administration of 29 April 2004 on the documentation of personal data processing and technological and organizational conditions to be met by devices and IT systems used for personal data processing (Official Journal (Dz.U.) No. 100, item 1024);
5. Regulation of the Minister of the Interior and Administration of 11 December 2008 on the sample form of a notification of a data filing system to registration by the Inspector General for Personal Data Protection (Official Journal (Dz.U.), No. 229, item 1536);
6. Regulation of the Minister of Administration and Digitization of 10 December 2014 on the sample form of a notification of appointment and dismissal of the information security administrator (Official Journal (Dz.U.), item 1934);
7. Regulation of the Minister of Administration and Digitization of 12 May 2015 on the method of keeping the database register by the administrator of information security (Official Journal (Dz.U.) of 2015, item 719);
8. Regulation of the Minister of Administration and Digitization of 11 May 2015 on the procedure for and manner of implementing tasks aimed to ensure compliance with data protection provisions by the administrator of information security (Official Journal (Dz.U.), item 745);
9. Act of 27 August 2009 on public finances (Official Journal (Dz.U.) of 2009, No. 157, item 1240, as amended).

Due to the multiplicity of the above legal acts, the adaptation of public organizations to their security requirements is costly, organizationally difficult and requires very efficient technical solutions. This means that the

 DOI 10.7172/1644-9584.83.8

legal risk relating to the implementation of the GDPR regulatory solutions becomes the problem of not only legal but also economic nature. The act on public finances is becoming a barrier to proper implementation of solutions needed to minimize the legal risk.

The awareness of data security is often insufficient in public organizations due to their approach to information and data, as well as the requirements of their protection, as indicated by the Report of the Supreme Audit Office (NIK) of 2018.[3] A survey performed by the author in 2018 in public and business organizations reveals that the level of awareness related to the obligation of ensuring proper personal data protection among employers, employees, collaborators, clients – personal data owners – is low. This is of utmost importance not only due to legal requirements in this respect but also due to market credibility of organizations towards their partners and employees. Sensitive data has a special role here, and personal data plays the most important role in public organizations.

Compliance with legal requirements is a prerequisite for the data management system in public organizations. The author believes that the legal aspect needs to be complemented by the economic aspect in order to adopt systemic solutions. The problem discussed in this paper assumes even greater importance since, as author's own research and auditors' findings reveal, public organizations are not aware of the GDPR-related requirements and threats. Moreover, they often lack competence to ensure the protection of personal data on the EU law level. It is worth noting that the actual difficulty is to comply with the statutory requirements without having the standardized system of information protection implemented beforehand (NIK, 2018). Practical aspects of management relating to compliance with the GDPR legal requirements are a problem for both commercial and public organizations. Every employee, client or user whose data has been registered should be guaranteed that his or her personal data is safe. The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC has brought many changes for the entities involved in the processing of personal data of natural persons. It has been the biggest legislative change regarding personal data in the national legislation for the past 21 years.

3. Personal Data Security

Identification and fulfillment of legal requirements is an obligation of every organization (Fajgielski, 2018, pp. 314–369). This is a key aspect of system management of data protection security, which needs to be taken into account while developing security policy of organizations, selecting security measures, assessing legal, technical or personal risks. Nearly all

organizations are involved in personal data processing. Therefore, they have to meet relevant requirements of the General Data Protection Regulation and the national legislation.

New conditions and challenges that have emerged in the public sector following the entry into force of the GDPR and related national regulations require some reorientation of the management system in public organizations operating within the public finance sector. Searching for an answer to the question how to shape the efficient system of finance management in public organizations, the author refers to the postulates of the economic doctrine, using the New Public Management acquis and selected theoretical concepts of the New Institutional Economics. This aspect has been taken into account following, among other things, press reports[4] on the problem that emerged when the National Revenue Administration (Krajowa Administracja Skarbowa, KAS) developed and introduced the "Your e-PIT" service. The President of Personal Data Protection Office obtained information about the possible threat of access to the personal data of taxpayers by unauthorized persons. This is the first example of a potential violation of the GDPR provisions by a public organization. Legal consequences for the public organization, i.e. the Ministry of Finance, can be very serious in the context of the Act on public finances (the possibility to impose a fine and losses to the image of the public institution).

4. New Conditions of GDPR-Related Risk Management vs. Public Finances

The public finance sector is composed of organizational units that perform public tasks and are subject to public financing. Public organizations, just like any other organization, are exposed to the risk of GDPR infringement. The General Data Protection Regulation has introduced very restrictive measures relating to the protection of personal data. It needs to be noted that, at present, public organizations have huge data collections, including citizens' sensitive data, in their IT systems. Three elements are indispensable to maintain proper security of such large-scale systems:

– administrative safeguards (procedures, decision-making processes),
– technical safeguards (equipment and IT systems, databases),
– personnel safeguards (employment and trainings to the personnel).

All the above mentioned measures are very significant cost-related items in the budget of any public organization. The technical infrastructure in particular requires huge financial outlays for the acquisition and maintenance of IT systems and equipment. These costs account for ca. 20% of the total costs in public administration. Personnel costs reach ca. 60% of the total operational costs. For this reason, the author believes that it is

 DOI 10.7172/1644-9584.83.8

necessary to consider the cost-based (economic) approach to the analysis of the GDPR-related legal risk (see Figure 1).

The implementation of the efficient risk management system for personal data protection within the New Public Management economic doctrine is becoming an issue of high importance for the public sector. The adoption of a modern economic approach addresses the issue of legal risk in the field of personal data security in public organizations in a holistic manner, following the introduction of new regulations in the European Union.

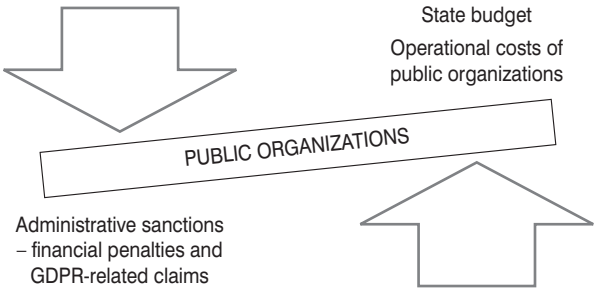

Fig. 1. Finances of public organizations in the context of the GDPR-related risk. Source: Author's own work.

The identification of instruments of efficient finance management according to the economic doctrine refers to the efficiency of finance management in the public sector and requires the identification of pro-efficiency efforts resulting from the doctrine. The Act on public finances introduces a provision of vital importance from the point of view of efficient finance management in public organizations. Pursuant to Article 44(3) of the Act of 27 August 2009 on public finances, all public expenditures should be made in a deliberate and cost-effective manner, ensuring compliance with the rules of timely achievement of the best results from a given expenditure and the optimum selection of methods and resources to reach the pursued objectives. At the same time, the Act requires that public organizations adopt certain management tools, such as:

– a multiannual financial forecast,
– management control,
– internal or external audit.

The above mentioned management tools implement financial management methods and techniques typical of the private sector into the public finance sector. The analysis of legal risk costs can also be included in this group. From the point of view of the functioning of public organizations, it is essential to prepare task-oriented budgets. This allows identifying security-critical tasks for the organization, including the personal

data security. It also improves transparency of the public funds, as information on actions taken, their costs and effects for the organization, is clearer.

Within the New Public Management doctrine that promotes the individual/natural person-oriented public servicing, various internal customer service standards are being introduced, such as electronic customer service platforms or electronic public service platforms, which fall within the scope of information security and personal data protection. The risk level relating to the personal data protection increases in technical terms. This, in turn, requires greater expenditure on technical safeguards for the used systems and databases. It needs to be remembered that a traditional management model still dominates in Poland, especially in smaller public organizations, where some personal data is protected in an old-fashioned manner. The examples provided in this paper do not cover all risks relating to personal data in public organizations.

All efforts related to the implementation of solutions connected with the GDPR legal risk should be subject to the economic analysis presented in Table 1.

The first observation that emerges from the above summary of administrative sanctions for the infringement of the GDPR provisions by public organizations refers to the level of sanctions. It is disproportionately low in comparison to the level of penalties imposed on other organizations. This means that the legislator noticed possible negative consequences for the public finance sector and seeks to reduce their extent due to the budgetary commitments of the State Treasury.

On the basis of his own research of 2018 and the findings of NIK's audit in public organizations in 2018, the author compared the implementation of the personal data protection regulation in business and public organizations (see Table 2). The Supreme Audit Office negatively evaluated the protection of electronic information resources in the audited public organizations in the Podlaskie Voiodeship. In NIK's opinion, organizational and technical measures taken in these organizations were not in line with the regulations on information security, including personal data, specified in the current legislation and did not guarantee proper security against unauthorized access, takeover or damage.

For the needs of this paper, it is important to note the following statement: "the reason why irregularities occurred was the marginalization of tasks related to the information security and protection of personal data processing by the controlled units and, in the opinion of their heads, also the lack of resources for staff training and acquisition of new infrastructure, as well as the shortage of appropriately qualified personnel in small towns and villages." (NIK, 2018).

On the basis of the NIK Report and his own research findings, the author claims that the scale and importance of irregularities found in public

 DOI 10.7172/1644-9584.83.8

Type of liablility	Legal basis	Scope of infringement	Statutory sanctions
Penal liability	Art. 107 and 108 of the Act on personal data protection	A person processes personal data although such processing is forbidden or he/she is not authorized to carry out such processing.*	A person is liable to a fine, a partial restriction of freedom or a prison sentence of up to two years.
		The offence relates to information on racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, trade union membership, genetic code, biometric data processed for the purpose of unambiguous identification of a natural person, health records, sexual life or sexual orientation.*	A person is liable to a fine, a partial restriction of freedom or a prison sentence of up to three years.
		Preventing or hindering the inspection of compliance with the personal data protection regulations by the inspector*	A fine, restriction or deprivation of liberty of up to two years
Civil liability	Art. 79 and Art. 82 of the GDPR in relation to Chapter 10 of the Act on personal data protection	1. Any person whose rights have been infringed may demand the abandonment of the infringement or an effective remedy necessary to remove the effects of the infringement, etc. 2. Any person who has suffered material or non-material damage as a result of an infringement of the GDPR has the right to receive compensation from the controller or processor for the damage suffered.	Indemnity or compensation
Administrative liability	Article 83 of the GDPR and Chapter 11 of the Act on personal data protection	For the infringement of: a. the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43 of the GDPR; b. the obligations of the certification body pursuant to Articles 42 and 43 of the GDPR; c. the obligations of the monitoring body pursuant to Article 41(4) of the GDPR.	Fines up to PLN 10,000 imposed on the unit of the public finance sector pursuant to Article 9(13) of the Act of 27 August 2009 on public finances
		For the infringement of: a. the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; b. the data subjects' rights pursuant to Articles 12 to 22;	Fines up to PLN 10,000 imposed on the unit of the public finance sector pursuant to Article 9(13) of the Act of 27 August 2009 on public finances

Tab. 1. Cont.

Type of liablility	Legal basis	Scope of infringement	Statutory sanctions
		c. the transfers of personal data to a recipient in a third country or an international organization pursuant to Articles 44 to 49; d. any obligations pursuant to Member State law adopted under Chapter IX; e. non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).	Fines up to PLN 100,000 imposed on the unit of the public finance sector pursuant to Article 9(1–12) and Article 14 of the Act of 27 August 2009 on public finances, a research center and the National Bank of Poland (NBP)

* Offences prosecuted *ex officio*

Tab. 1. Classification of legal risk related to personal data protection in public organizations in economic terms (statutory sanctions). Source: Author's own work.

Risk identification	Public organizations*	Business organizations**
Statutory scope of data	Public organizations filed and processed personal data, which was unnecessary to perform the tasks that the data filing systems were kept for.	Data was collected in accordance with the scope of services provided.
Procedures	All public organizations had data protection documentation and procedures. However, two thirds of them were outdated or incomplete (not updated even for over 10 years).[5]	Up-to-date documentation
Access authorization	Access to information was not monitored; in over a half of public organizations, employees were given the powers of administrators of operational systems used in their computers.	Access to information adapted to functions and positions
Data creation	The manner of data storage and security measures did not guarantee their proper protection.	Proper security measures

DOI 10.7172/1644-9584.83.8

Databases	Electronic information resources were not properly secured against unauthorized access, takeover or damage.	IT systems secured
IT systems	IT systems were not secured against unauthorized access, takeover or damage of data.	Security measures against access or damage
Data security	Databases were backed up in an inappropriate way or not backed up at all, while carriers and equipment used to make and keep backup copies were stored in the manner that did not guarantee their security.	Backup copies properly secured
Lack of system protection	The measures preventing unauthorized access to electronic data were not provided.	No possibility to access data without authorization
Protection of registers Reporting to supervisory bodies	Public organizations also failed to meet the obligations specified in the Act on personal data protection – information about filing systems already registered by the Inspector General for Personal Data Protection (GIODO) was not updated, new filing systems were not submitted to GIODO for registration and employees were not given authorization for personal data processing.	Registers updated in accordance with relevant regulations Infringements reported
Personal data protection (PDP) regulations	Public organizations failed to comply with the regulations on personal data protection. Nine of 13 Information Security Administrators did not perform their obligations.	Obligations fulfilled in line with law

Tab. 2. GDPR risk criteria in public and business organizations. Source: Author's own work based on NIK Audit Report of 2018, own research findings.***

organizations may give rise to justified concerns as to the soundness of the GDPR-related risk management. The currently binding provisions of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, in force since 25 May 2018, and of the Act of 10 May 2018 on personal data protection have introduced an important catalogue of administrative sanctions, including financial penalties for non-compliance. Moreover, the new legislation has introduced civil liability with respect to compensation claims brought against the organization (Kawecki, 2018, pp. 125–128).

Taking into account the size of databases available to public organizations, the scale of possible compensations for the infringement of personal data protection regulations may be very large. This also means an enormous responsibility of the State Treasury towards claimants. It is therefore important to look at the matter of personal data protection in public organizations in financial terms, as all infringements have their consequences for public finances (Malinowski, 2017, pp. 101–111).

In its audit findings, NIK also pointed to the alarming phenomenon of poor protection of information in public organizations, which – due to their very nature – have sensitive data records. Nearly all types of irregularities relating to personal data security were discovered in those organizations, including improper management of user authorizations in operational systems, lack of recurrent training, failure to provide proper authorization while logging in IT systems, inappropriate creation and storage of backup copies. The majority of the audited public organizations did not take any measures aimed to minimize the risk of information loss, which, in turn, means that the level of security was poor. Some organizations failed to comply with their own regulations and internal procedures relating to the method of data storage and protection. Data stored as paper documents was kept in public places, without the possibility of locking it. Public organizations did not make electronic backups or monitor access to information. Employees responsible for data protection did not have professional qualifications related to the management of IT systems. There were no regular internal audits of information security and data processors were not provided with relevant trainings. Moreover, operational systems used by the audited public units had no technical assistance, which means that their producers had ceased to release any security updates for them. This represents a major threat to the security of information networks in the organizations using such software.

In the opinion of the Supreme Audit Office, the irregularities were a consequence of the marginalization of responsibilities to ensure information security and protection of the processed personal data by the audited organizations. Their heads, in turn, blamed the lack of funds for training

 DOI 10.7172/1644-9584.83.8

courses and acquisition of new infrastructure, while in small towns and villages they also added the shortage of personnel with adequate qualifications. NIK submitted its conclusions to local authorities requesting them to adopt a proper approach to the evaluation of legal risk in personal data protection. All recommendations have their financial impact – the acquisition and maintenance of IT equipment and systems, attracting employees with appropriate qualifications or their training. NIK also found it necessary to implement the GDPR regulations, in force from 25 May 2018, in particular those related to the obligation to keep a register of data processing activities. Persons having access to personal data must be authorized by the personal data administrator.

The findings resulting from author's own research in organizations operating in the public finance sector coincide with the findings of NIK's audit. The personnel responsible for security of the organization and personal data confirmed the lack of training and adequately qualified staff; also, they pointed to limited financial resources for the maintenance of IT systems. Changes ensuing from new data protection regulations that should be made in IT systems were not implemented in full. System corrections were required in organizations that continued to comply with the provisions of the previous Act on personal data protection. In organizations where system solutions had not been implemented in full, the new legislation required much bigger investment in their modernization, which gave rise to the problem of financing new needs within the annual budget of a public entity. Some of them adopted minimum technical solutions to reduce costs, others limited the resources for IT system maintenance, which resulted in a significant increase of costs in the subsequent year.

On the basis of the research findings, the evaluation of the GDPR-related risk has been carried out according to the identified threats (see Table 3).

In order to evaluate the GDPR-related legal risk in view of public finances, it is necessary to specify operational costs related to the implementation and maintenance of personal data protection solutions in public organizations. This involves the maintenance of technical, organizational and procedural resources in relation to possible sanction costs, including the costs of administrative liability, such as fines and the costs of civil liability, as well as possible costs of civil claims. The calculation is not obvious. If operational costs are lower than possible sanction costs, organizations decide to bear them and avoid the legal risk. If operational costs are higher than sanction costs, organizations are willing to bear sanction costs and accept the legal risk. This is closely related to the strategy of organizations, including public institutions, which function within significant financial limits imposed by the restrictions of annual budgets. The strategic management of the GDPR-related risk is reduced to the development of the personal data protection policy or other internal regulations. Operational activities

Risk identification	Scope of actions for risk identification	Action stages for personal data
Data collection	Collecting data and defining the purpose of data processing	Subject-related planning
Data storage	Establishing an inventory of processed personal data (indicating the place of data storage – the IT system, archive, quick reference filing system, etc.)	Organizational planning
Processing	Determining whether data processing complies with the law and specifying the legal basis	Execution
Security	Developing a list of threats that may lead to the violation of personal data protection, e.g. a hacker attack, unauthorized access, breaking into a building	Implementation
Infringement event	Determining the probability of risk occurrence (based on, for instance, the frequency of its occurrence in the past)	Frequency of risk occurrence
Risk level (three levels): – low risk (0–2) – medium risk (3–5) – high risk (6–10)	Assigning risk importance/weights – e.g. the level of damage that an event may cause to the data subject	Risk significance for organization
Risk scope: – acceptable – unacceptable	Describing the consequences of a given risk, e.g. interference with the right to personal data protection, violation of the right to privacy	Data security Compensation claims
Remedial actions	Minimizing the risk when it cannot be avoided, applying risk mitigation measures, such as anti-virus software, emergency alarm in a building, etc.	Improvement

Tab. 3. GDPR risk evaluation by identified risks in organizations. Source: Author's own work based on research.

DOI 10.7172/1644-9584.83.8

focus mainly on the maintenance of necessary technical, organizational and procedural resources, specified as operational costs. In economic terms, the GDPR-related legal risk requires taking into account sanction costs, including possible administrative sanctions and possible civil claims (see Figure 2). Such an approach allows determining quickly which costs in a given organization will have an impact on minimizing the GDPR-related legal risk.

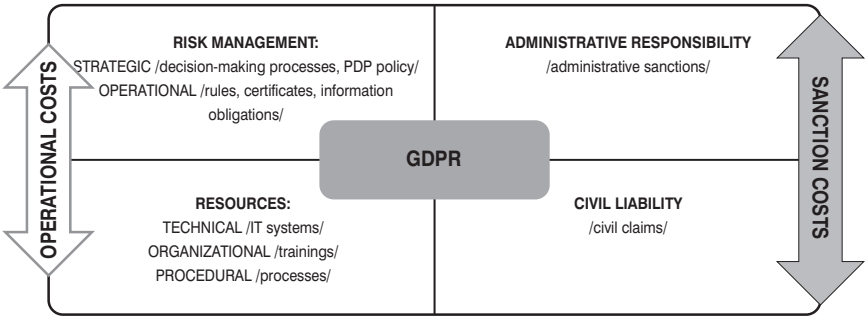

Fig. 2. GDPR's impact areas in economic terms. Source: Author's own work.

5. Conclusions

Every public or business organization needs to select a risk management model, following the economic evaluation of legal risk. It is thus necessary to build a model for analyzing the benefits of compliance or non-compliance with the law and apply it in practice. As far as public organizations are concerned, the above mentioned evaluation has to take into account sanction costs in particular. Not only due to their value but also due to the costs for the state budget and the costs of loss or damage to the reputation of the public administration.

When operational costs are higher than sanction costs, organizations are inclined not to comply with the law. When operational costs are lower than sanction costs, organizations are encouraged to introduce all solutions laid down by law. This is an economic balance, which confirms the need to adopt the economic-oriented approach to legal risk of organizations in the area of personal data protection. For public organizations, all economic aspects translate into the value of financial burdens for public finances (Bujak, 2017, pp. 50–58). This refers to both funds for operating expenses and possible sanction costs, the financial consequence of which is borne by the state budget. Therefore, the GDPR-related risk management in organizations operating within the public sector should adopt the economic approach, indicating the aspect of administrative sanction costs.

Endnotes

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, Official Journal of the European Union L119 dated 4 May 2016).

2 Act of 10 May 2018 on the protection of personal data (Official Journal (Dz.U.) of 2018, item 1000).

3 Informacja o wynikach kontroli: Bezpieczeństwo elektronicznych zasobów informacyjnych w jednostkach samorządu terytorialnego w Województwie Podlaskim, LBI.430.002.2018 (Information on audit findings: Security of electronic databases in local government units of the Podlaskie Voivodeship).

4 https://biznes.interia.pl/podatki/news/uodo-chce-wyjasnien-w-sprawie-twoj-e-pit,2603633?utm_source=paste&utm_medium=paste&utm_campaign=firefox, date: 26 March 2019.

5 Failed to meet the requirements specified in the Regulation of the Minister of the Interior and Administration on the documentation of the personal data processing and technological and organizational conditions to be met by devices and IT systems used for personal data processing.

References

Act of 29 August 1997 on the protection of personal data (Official Journal (Dz.U.) of 1996, No. 133, item 883).

Act of 17 February 2005 on the computerization of the activity of entities performing public tasks (Official Journal (Dz.U.) of 2017, item 570).

Act of 27 August 2009 on public finances (Official Journal (Dz.U.) of 2009, No. 157, item 1240, as amended).

Act of 10 May 2018 on the protection of personal data (Official Journal (Dz.U.) of 2018, item 1000).

Bujak, A. (2017). Metodyka pomiaru efektywności w jednostce budżetowej. *Polityka Ekonomiczna*, 487/2017, Wrocław.

Cooter R., & Ulen, T. (2009). *Ekonomiczna analiza prawa*. Warszawa: C. H. Beck.

Duniewska, Z., Jaworska-Dębska, B., Olejniczak-Szałowska, E., & Stahl, M. (2016). *Prawo administracyjne materialne* (2nd ed.). Warszawa: Wydawnictwo Wolters Kluwer.

Fajgielski, P. (2018). *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*. Warszawa: Wydawnictwo Wolters Kluwer.

Gałaj-Emiljańczyk, K. (2018). *Wdrożenie RODO w małych i średnich organizacjach. Praktyczny poradnik.* Gdańsk: Wydawnictwo ODDK.

Gawroński, M. (Ed.). (2018). *RODO Przewodnik ze wzorami*. Warszawa: Wolters Kluwer.

Jabłońska-Bonca, J. (2007). *Podstawy prawa dla ekonomistów.* Warszawa: LexisNexis.

Kamiński, A., & Dąbek, K. (2017). Nowe zagrożenia dla działalności przedsiębiorstw w świetle Rozporządzenia Parlamentu Europejskiego o ochronie danych osobowych (RODO). *Polityka Ekonomiczna*, 487/2017.

Kawecki, M., & Osieja, T. (Ed.) (2017). *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia.* Warszawa: Wydawnictwo C. H. Beck.

Kawecki, M. (2017). Prawo ochrony danych osobowych jako nowa dziedzina prawa, *Europejski Przegląd Sądowy*, 5/2017.

Kępa, L. (2015). *Jak w praktyce zgodnie z prawem przetwarzać dane osobowe*. Warszawa: Wydawnictwo ODO24 sp. z o. o.

Krasuski, A., & Skolimowska, D. (2016). *Dane osobowe w przedsiębiorstwie*. Warszawa: LexisNexis.

 DOI 10.7172/1644-9584.83.8

Litwiński, P. (Ed.), Barta, P., & Kawecki, M. (2018). *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*. Warszawa: Wydawnictwo C. H. Beck.

Malinowski, J. (2017). Jak przygotować samorządy do wejścia w życie przepisów UE GDPR (RODO). *Prace Naukowe Wyższej Szkoły Zarządzania i Przedsiębiorczości z siedzibą w Wałbrzychu, 41*(2).

Piątek, S., & Postuła, I. (Eds.). (2018). *Podstawy prawa w gospodarce*. Warszawa: Wydawnictwo Naukowe Wydziału Zarzadzania UW.

Polski Komitet Normalizacyjny. (2007). *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.* (Standard No. PN-ISO/IEC 27001:200).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119.

Regulation of the Minister of the Interior and Administration of 29 April 2004 on the documentation of the personal data processing and technological and organizational conditions which shall be met by devices and IT systems used for personal data processing (Official Journal (Dz.U.), No. 100, item 1024).

Regulation of the Minister of the Interior and Administration of 11 December 2008 on the sample form of a notification of a data filing system to registration by the Inspector General for Personal Data Protection (Official Journal (Dz.U.), No. 229, item 1536).

Regulation of the Minister of Administration and Digitization of 10 December 2014 on the sample form of a notification of appointment and dismissal of the information security administrator (Official Journal (Dz.U.), item 1934).

Regulation of the Minister of Administration and Digitization of 11 May 2015 on the method of keeping the database register by the administrator of information security (Official Journal (Dz.U.) of 2015, item 719).

Regulation of the Minister of Administration and Digitization of 11 May 2015 on the procedure for and manner of implementing tasks aimed to ensure compliance with data protection provisions by the administrator of information security (Official Journal (Dz.U.), item 745).

Stelmach, J., & Brożek, B. (2004). *Metody prawnicze*. Kraków: Zakamycze.