„Ante Portas – Security Studies”
2020, No 1(14)
DOI: 10.33674/320194

Aleksandra OLENDER[1]
Poland

RISK ANALYSIS AND DATA PROTECTION IMPACT ASSESSMENT CONDUCTED IN THE PUBLIC SECTOR

Abstract:
The European Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the repeal of Directive 95/46/EC introduced a new one, a proactive model of protection of personal data processed in the organization, based on a risk-based approach. It imposed on the administrators new obligations related to conducting analyzes of the risk of violation of the rights and freedoms of persons whose data they process. Considering the scope, scale and categories of personal data processed, public sector entities face a huge challenge to meet the restrictions of the EU legislator. An additional difficulty is often a very extensive organizational structure, complicated processing processes, limited financial resources and unadjusted IT systems. The article discusses issues of risk analysis and impact assessment for the protection of personal data processed in the public sector in order to meet the requirements of the GDPR. The key issue in this respect is the adoption of an appropriate methodology in the risk estimation process, because properly carried out it enables the implementation of security measures adequate to potential threats.

Keywords:
analysis, risk, protection, data, RODO.

Introduction

The flourishing of the information age, the development of advanced technologies and increased globalization of data flow constantly creates new challenges and threats to ensuring the security of processed information.

[1] Aleksandra Olender, PhD student in Security Science, Military University of Technology in Warsaw. The author's research interests are primarily related to issues of broadly understood security, migration, information security, personal data protection, or information warfare. Email: aleksandra.sabina.olender@gmail.com

Information has become the most valuable commodity in the modern world. Proper management of information resources and adequate protection of owned data is increasingly a priority for the proper functioning of modern organizations. The widespread use of information systems not only improves the operation of entities but also reveals new vulnerabilities used by threats. Therefore, along with technological development, it is required to constantly improve the methods of protecting our information resources.

Personal data of individuals is a model type of data processed by almost all modern organizations. The European Union law provides them with special protection, which is already grounded in the Universal Declaration of Human Rights of 1948 emphasizing that no one can be subjected to integration in his private home, family or correspondence, or become the object of attacks detrimental to his good name and honour. The protection of personal data is one of the basic aspects of the right to privacy[2]. Works on the comprehensive coverage of this issue in the EU legal act have lasted since 1990, but it was only the adoption of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free flow of such data and the repeal of Directive 95/46/EC (General Regulation – GDPR) introduced a unification of the provisions on the protection of personal data in all the European Union countries. This legal act is intended to facilitate cross-border business operations and covers all entities processing personal data within the European Union[3].

The GDPR places special emphasis on the perception of legal obligations in accordance with the pro-social approach to managing administrative and business entities. This point of view makes risk management a key element in the practice of applying and enforcing EU legislation[4].

The general regulation addresses the issues of managing personal data protection from a risk perspective, which is included in the recitals of this legal act. The EU legislator, taking into account the dynamics and diversity of the changing reality, precisely defines the expectations towards data processors, while the issues of the adequacy of the entities' behaviour to meet these expectations is left undefined. This solution requires business entities, offices, management staff and employees themselves to pay more attention to issues of social responsibility, because EU law prioritises the protection of privacy and personal rights of each person and obliges organizations to respect these overarching values, while introducing high penalties for their failure.

---

[2] M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016, p. 36.

[3] P. Litwiński, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2017, p. 17.

[4] J. Zawiła-Niedźwiecki, *Analiza ryzyka służąca spełnianiu wymagań RODO*, https://sip.legalis.pl/document-view.seam?documentId=mjxw62zogi3damjzhaydooa (15.06.2019).

The article addresses the issues of risk analysis and impact assessment for the protection of personal data processed in the public sector, serving to meet the requirements of the GDPR. The purpose of the article is to approximate the obligation to use a risk management approach when processing personal data in public entities. Given that public institutions process personal data of all citizens, often also specific categories of personal data (e.g. information on origin, race or ethnicity, political views) the processing of which may involve a high risk of violating the rights and freedoms of individuals, they pay particular attention to conducting correct risk analysis for processed data. Adopting the right methodology in the risk assessment process enables the implementation of safeguarding measures adequate to the potential threats[5]. The paper confirms the hypothesis that conducting a thorough assessment of the effects on data protection continues to be a challenge for public sector entities. The main research problem was included in the question: what is the significance for persons whose data is processed in public sector entities of conducting reliable and adequate risk analysis and assessment of personal data protection effects?

Risk-Based Data Protection Model

The Regulation 2016/679 developed by the EU authorities introduces a new, proactive model for the protection of personal data processed in the organization, set on a risk-based approach. The use of this type of solution is intended to facilitate the administrator taking appropriate steps to protect the information resources held, including in particular the personal data of natural persons. Depending on the estimated level of risk for the data being processed, the processor should implement adequate measures to minimize the negative effects of using system vulnerabilities by potential threats.

Risk is equated with uncertainty, which results from the fact that entities never operate under conditions of certainty, but only with greater or lesser probability. Risk can be understood differently. For the purposes of this article, a negative definition should be cited, which assumes that "risk means being able to fail to achieve the desired effect (damage, loss)"[6]. It can also be assumed that the risk is a "scenario that describes the event and its consequences, estimated in terms of the severity (amount of damage that an event can cause) and the likelihood of the event that constitutes a violation".

Administrators, in complying with the requirements of the GDPR, should diligently apply the issue of risk analysis and apply appropriate countermeasures. Currently, it is not the legislator who decides what safeguards should be introduced to effectively protect data, but such an obligation rests with the entities that process these data. The administrator or processor must decide for himself what protection

[5] M. Byczkowski, *Zabezpieczanie danych osobowych w RODO*, Warszawa 2017, No. 2.
[6] P. Sienkiewicz, *Ewaluacja ryzyka w zarządzaniu kryzysowym*, [in:] Ryzyko w zarządzaniu kryzysowym, P. Sienkiewicz, M. Marszałek, P. Górny (ed.), Toruń 2012, p. 25; M. Gawroński (ed.), *RODO. Przewodnik ze wzorami*, Warszawa 2018, p. 265.

measures to take. Thus, the public authority will not receive specific guidance for protecting its resources. They will have to show greater flexibility in assessing what measures should be used for the register of processing activities that they have.

The administrator is obliged to introduce technical and organizational protection of the processed data, which will be adequate to the risk scale, considered in terms of the possibility of losing information attributes (i.e. availability, integrity and confidentiality), taking into account the context, scope, purposes of processing and in particular the risk of violation of rights and freedoms of data subjects. In addition, when deciding to apply specific security measures, it should take into account the current state of technical knowledge and the cost of implementing a given solution. The introduction of security features for information resources must also have economic justification. It is possible that conducting some kind of processing is unprofitable due to the fact that the costs of data protection outweigh the profits from conducting this process. However, when referring to resources processed in the public sector, it may not be possible to opt out of certain data processing operations. This is due to the fact that public entities process data mainly based on the premise of an obligation incumbent on the administrator or an important public interest. This situation necessitates the implementation of often costly solutions to eliminate vulnerability.

Risk Management Process in Personal Data Protection

The risk management process should be one of the key issues in managing an organization as it relates to a variety of resources. In connection with the data protection requirements that the GDPR imposes on data processors, the following areas can be identified in which risk is analyzed:

- risk in processing security (associated with threats to confidentiality loss, data integrity and availability, e.g. DDoS attacks, ransomware),
- risk of failure to fulfil formal obligations (related to the requests of data subjects, e.g. the right to provide information about data processed by the administrator, to be forgotten, rectification of data, etc.),
- risk analysis and assessment / Data Protection Impact Assessment (DPIA) – related to the permanent assessment of the impact of data processing on the rights and freedoms of persons whose data subject is processing; requires implementation when designing processing as well as during data security management[7].

Information security risk management is not an innovative approach and it has been used for a long time, therefore it is a good practice to use the already developed solutions in the risk analysis for the protection of personal data. The ISO 27005 standard describes a methodology that can be implemented in both small and large organizations. However, the GDPR does not indicate that there

[7] J. Zawiła-Niedźwiecki (ed.), *Poradnik RODO. Podejście oparte na ryzyku*, vol. 2, Warszawa 2017, p. 5-25.

is any best methodology to apply the risk assessment process and its management. It is important that the result of the process is a reliable and objective assessment of the level of risk.

The main difference in the approach used so far is that the previously used information security management methodologies focused on the risk and consequences for the organization, while the GDPR places great emphasis on issues related to the risk of violation of the rights and freedoms of data subjects.

Stages of Risk Management in Data Protection

Proper risk management requires reference to the processing context, followed by identification, estimation (which makes up the risk analysis) and risk assessment. Once these steps are completed, a decision should be made about how to deal with the estimated risk and accept the residual risk.

Defining the context requires indicating all information assets, taking into account the scope, nature and purposes of the data being processed, as well as specifying the risks associated with loss, destruction or unauthorized access to data. Identification and classification of information assets in an organization should be carried out at a level of detail ensuring that the necessary information is identified for the purposes of risk analysis. The administrator at this stage should pay attention to the current state of the collateral held and specify the criteria for acceptable risk.

The next step is to identify potential threats and indicate the vulnerability to assets resulting from these threats materializing. In order to assess the risk values are assigned for the probability of occurrence of a given event and values for potential effects of hazard materialization broken down for each of the safety attributes. The risk estimate is the product of these values. Depending on the estimates decisions are made regarding the management of individual risks (reduction, behaviour, avoidance or transfer of risk)[8].

The risk analysis for the personal data being processed is the starting point for the decision about the need for further, more formal risk analysis. Pursuant to art. 35 of Regulation 2016/679, the concept of impact assessment for the protection of personal data has been introduced. This process is required when processing may pose a high risk of violating the rights and freedoms of natural persons. Unless there is a formal requirement to carry out a risk analysis of all processing activities, in practice it is necessary due to the assessment of whether a given processing process is not exposed to high risk and thus does not require the administrator to carry out an impact assessment on the protection of personal data. Therefore, the imposition of a new obligation means that in practice the entities that process personal data must constantly conduct an analysis and risk assessment for the data being processed. Activities, including the processing context, control mechanisms, risk assessment, risk management are constantly looping and are designed to permanently monitor and improve the process (near Deming).

[8] *Ibidem.*

Impact Assessment for Data Protection

The data protection impact assessment should be carried out where there is a high probability of a high risk of violating the rights and freedoms of persons whose data the controller processes. It should be used in particular in the case of data processing using new technologies. Regardless, several cases have been identified that always require an in-depth risk analysis. He belongs to them:

- making decisions based on data processed in an automated manner, based on a comprehensive and systematic assessment of personal factors of natural persons (including profiling),
- processing sensitive data and data on convictions and large scale violations of law,
- systematically large-scale monitoring of publicly available places (GDPR)[9].

The President of the Office for Personal Data Protection also published a list of types of processing operations that require an assessment of the effects on personal data protection[10].

Violations of personal data, leading to property or non-pecuniary damage or physical damage to persons whose data is processed may occur due to the use of vulnerability by threats. The GDPR lists among others the basic catalogue of threats: situations where data processing could result in identity theft, discrimination, damage to good name, financial loss, disclosure of specific categories of data, deprivation of the possibility to exercise control over own data, creation of personal profiles based on the assessment of personal factors, processing of children, processing large personal data scale. In such cases, the EU legislators propose the use of special data protection methods, e.g. in the form of pseudonymisation or encryption. There is also a high probability that in the above cases it will be necessary to carry out an in-depth risk analysis of the data subjects' rights and freedoms.

The methodology for conducting an impact assessment for the protection of personal data should be carried out taking into account all the criteria indicated in the GDPR. The use of a comprehensive approach will allow compliance of the processing with regulations. The list of criteria is presented in the Working Group Guidelines 29 on data protection impact assessment and helps determine whether processing may cause high risk for the purposes of Regulation 2016/679[11]. After a proper assessment and taking steps to minimize the risk the administrator must

---

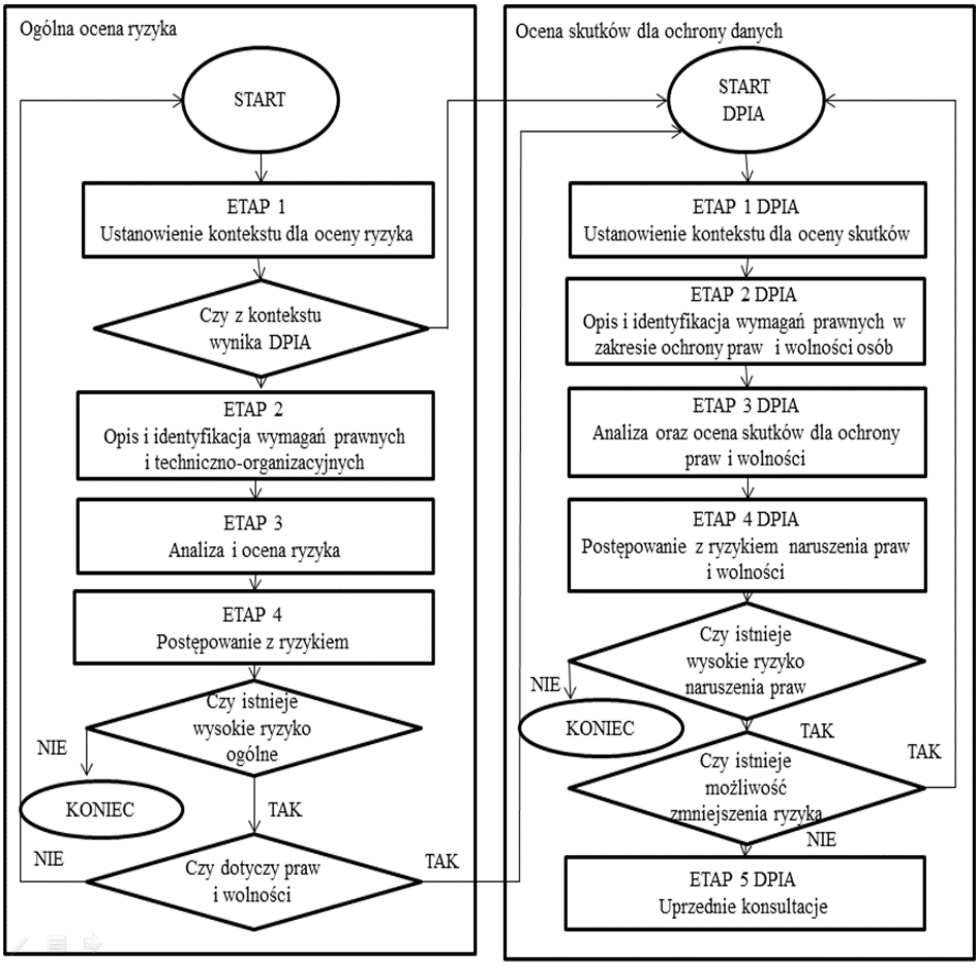
[9] *Art. 35 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*.

[10] *Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony*, (M.P. 2019 poz. 666).

[11] *Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679*, (WP 248 rev.01), <http://www.giodo.gov.pl/pl/file/12864> (15.06.2019).

decide whether the processing operation requires consultation with the supervisory authority, because if the administrator does not find sufficient resources to reduce the risk to an acceptable level (when the residual risk is still high), required there is such an action. The administrator must first of all present the purposes of the intended processing, measures to protect the processed data and an assessment of the effects on data protection. The supervisory authority issues recommendations in relation to the planned processing operation, then (after implementing the administrator's recom-mendations) decides whether the processing does not violate the provisions of the EU Regulation. A summary of the general risk assessment procedure and the data protection impact assessment is provided below at Figure 1.

Fig. 1. General risk assessment and data protection impact assessment.



Source: J. Zawiła-Niedźwiecki, *Poradnik RODO*…

According to the presented scheme, the impact assessment for data protection is carried out after an overall risk assessment, when high general risk is assessed, unless the obligation for an in-depth analysis is required by law. Consultations with the President of the Office for Personal Data Protection are required when the administrator is not able to reduce the risk of violation of the rights and freedoms of natural persons as a result of processing their data.

The introduced requirement of risk analysis is covered by such seriousness that in the event of a high level of risk of violation of the rights and freedoms of natural persons, and the administrative and technical measures taken by the administrator are not able to reduce the risk to an acceptable level, the entity will be forced to resign from such processing.

The administrator, in special cases, before starting the processing operation must consult the natural persons whom the operation will concern, their representatives or experts. Opinions can be requested in any way. Such consultations are aimed at taking into account the perspective of others. However, it is recommended that in case of doubt as to whether an impact assessment should be carried out, it is recommended to implement it.

Conducting an impact assessment for the protection of personal data by the administrator is required before processing a given data set. This is due to the principles of including data protection in the design phase (privacy by design) and default data protection (privacy by default). DPIA is a continuous process that allows you to verify the adequacy of security measures used and improve security inadequate to dynamically changing threats. It should also be noted that in the case of DPIA it is not possible to transfer the risk of processing to another entity by dealing with risk, therefore it is crucial to attach special importance to the protection of the rights of individuals not only when planning a specific processing operation, but by default, also during all processing[12].

Impact Assessment for Data Protection in Public Sector Entities

As mentioned in the previous part of the article, the obligation to carry out an impact assessment on the protection of personal data is required if the processing activities meet the conditions specified in art. 35 GDPR or the criteria indicated in the Communication of the President of the Office for Personal Data Protection regarding the list of types of personal data processing operations that require an assessment of the effects of processing on their protection. In relation to public sector entities, running a DPIA is required, for example, at labour offices when profiling the unemployed for access to various forms of assistance without their consent. The assessment of the effects on data protection is also subject to monitoring carried out with the use of cameras placed on the uniforms of public officers, e.g. police, municipal police, fire

[12] K. Pszczółkowski, *Metodyka zarządzania ryzykiem w ochronie danych osobowych, Fundacja Bezpieczeństwa Informacji Polska*, Warszawa 2018, p. 31.

brigade, because it uses elements of recognizing the properties and features of objects in the monitored area. Moreover, the recording of an intervention by an officer may involve the processing of specific categories of data, and therefore also be subject to an in-depth risk assessment.

The protection of the data subjects' rights and freedoms is directly related to the obligation to secure the processed data, contained in art. 35 GDPR. The level of security applied in the public sector raises concerns, as evidenced by the audit carried out last year (i.e. 2018) of NIK regarding the protection of electronic information resources. 31 local government units in Podlasie were inspected. In almost all entities the level of security of IT systems and network services was at an unsatisfactory or very low level[13]. This level of protection carries a risk of unauthorized access, theft and data loss. Therefore, it may lead to a violation of the privacy and property of citizens whose data is processed in the information systems.

Currently, few public sector entities are sufficiently aware in the sphere of data protection of which they are the administrator. Still, information security issues are neglected and the requirements of the general regulation based on the risk analysis of the data being processed are not respected.

According to the latest report on the activities of the President of the Office for Personal Data Protection in 2018, the President of the Office for Personal Data Protection carried out an inspection in the field of personal data processing as part of municipal video monitoring in two local government units. The audit identified weaknesses in the fact that no impact assessment on the protection of data processed under monitoring was carried out. Data processed using vision cameras, due to the lack of facial recognition and person tracking capabilities, do not constitute data of a particular category (biometric). However, given that cameras cover a large part of the city, data processing in the form of citizens' image takes place on a large scale, and therefore requires a data protection impact assessment. Because according to art. 35 section 3 letter c) GDPR, this assessment is required in particular in the case of systematic monitoring of publicly accessible places on a large scale[14].

In addition, the report emphasized that the documentation from the risk analysis carried out did not describe corrective actions and did not carry out a risk assessment for individual threats identified for processing activities requiring an assessment of the effects on personal data protection.

Another example of deficiencies in public administration turned out to be revealed in connection with the introduction by the Minister of Finance of the e-PIT portal threats resulting from the selection of authorization for the portal. Access to the taxpayer's PIT was possible after providing the amount of

[13] *Informacje o obywatelach przechowywane przez instytucje samorządowe nie są bezpieczne*, <https://www.cyberdefence24.pl/bezpieczenstwo-informacyjne/informacje-o-obywatelach-przechowywane-przez-instytucje-samorzadowe-nie-sa-bezpieczne> (15.06.2019).

[14] *Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych*, <https://uodo.gov.pl/437>, (15.09.2019).

revenues for previous years and the PESEL number of the taxpayer. Such a catalogue of information necessary for authorization meant that the circle of people who could access the data could be extended to include an employer or an accountant[15].

The introduction of a new solution related to the processing of personal data of millions of taxpayers should be preceded by an impact assessment on the protection of personal data. It is true that the data contained in e-PIT are not, by definition, a specific category of data, however, taking into account the approach of Poles to the issue of remuneration - this information is usually important and constitutes the category of data that we usually protect more. The risk to the rights and freedoms of taxpayers associated with the processing of their data should be taken into account at the design stage of the portal (privacy by design). Perhaps such an analysis would allow us to identify the risk that was revealed at the stage of using the portal. In addition, it would give the opportunity to react and minimize the likelihood of negative consequences for portal users. Even if the basic analysis showed a high level of risk of violation of rights and freedoms, mandatory consultation with the supervisory authority could help identify weaknesses in the proposed solution. Currently, issues of ensuring user privacy should be a key element in the design of new information systems. This is of great importance especially for systems used in administration, mainly due to the scale at which data is processed. Performing a detailed and reliable risk analysis and (in justified cases) impact assessment for the protection of personal data allows you to respond to any threats at the production stage, and thus prevent the materialization of threats identified for individual processing processes.

As can be seen from the examples above, conducting risk analysis and impact assessment on data protection in the public sector remains a serious challenge. Considering that public sector entities process personal data of all citizens and individual processing processes are usually not able to opt out due to the high level of risk assessment, the processing will often require additional financial resources for security.

Summary

Risk analysis and impact assessment of personal data protection are a useful tool for data controllers to implement processing operations in accordance with applicable law. Therefore, a proactive approach to data protection based on risk management should not be treated as an annoying obligation, but as support in protecting the rights of persons whose data is processed. Observing the complexity of information management processes in the public sector the

[15] S. Wikariak, *Niebezpieczeństwa wycieku informacji można było uniknąć*, <https://prawo.gazetaprawna.pl/artykuly/1399802,niebezpieczenstwa-wycieku-informacji-mozna-bylo-uniknac.html> (15.09.2019).

implementation of risk assessment methodologies for the protection of personal data into existing risk management systems seems necessary.

Undoubtedly, maintaining the security of processed data, aimed at minimizing the risk to the rights and freedoms of natural persons, is associated not only with the need to carry out impact assessments for the protection of personal data, but also analysis in areas related to the possibility of loss of confidentiality, integrity, availability of information resources or related to the claims of persons under the provisions of the GDPR. Only a holistic approach will allow the administrators to fulfil their obligations and the ability to demonstrate accountability.

Public sector units, in accordance with the National Interoperability Framework to ensure information security, should be adapted to the minimum requirements for public registers, exchange of information in electronic form and for ICT systems[16]. These national guidelines have been in operation since 2012, however, as indicated in the article, some institutions performing public tasks still have problems with managing IT systems. The attitude of management in public sector entities (especially in small entities) to the issue of ensuring information security is worrying.

It should be kept in mind that a proper management of personal data security in public sector entities is an extremely difficult task. This is due to the fact that many offices have a very extensive organizational structure and complicated processing procedures. In addition, they process specific categories of data and data on judgments that require the implementation of specific protection measures, which, with a often limited budget, can be a breakneck challenge. In addition, the use of appropriate protection measures reduces the likelihood of violations resulting in customer claims and loss of reputation. Conducting a risk analysis allows you to identify potential threats and decide what to do if it occurs. Due to reliable analysis, the administrator's reaction time is shortened when a threat materializes, which means that persons whose data have been violated have greater possibilities to minimize the possible negative effects of this event. As a result, the entity based on the risk-based model has a greater impact on the level of security of personal data being processed, and thus the security of persons whose data is being processed.

In conclusion, public sector entities, due to the scope, scale and categories of processed personal data of natural persons, should constantly monitor the level of security of processed information resources. The use of risk analysis and impact assessment for data protection is an instrument to assess what action should be taken to protect citizens' rights and freedoms. The use of risk assessment methodologies allows not only to meet the requirements of the GDPR, but also to increase the standards of the organization's functioning.

[16] *Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych* (Dz. U. 2012 poz. 526).

Nevertheless, despite the fact that the new provisions on the protection of personal data have been in existence for over a year, the examples of audits carried out in public sector entities and the introduction of technological solutions bypassing the principles of personal data protection indicate that not all entities already have developed and verified risk analyzes. Therefore, the development of reliable and adequate risk analysis and impact assessment for the protection of personal data is still a current challenge for public sector entities, which have a duty to protect the privacy of all data subjects.

BIBLIOGRAPHY:

- ✓ Byczkowski M., *Zabezpieczanie danych osobowych w RODO*, Warszawa 2017
- ✓ Gawroński M. (ed.), *RODO. Przewodnik ze wzorami*, Warszawa 2018
- ✓ *Informacje o obywatelach przechowywane przez instytucje samorządowe nie są bezpieczne*, <https://www.cyberdefence24.pl/bezpieczenstwo-informacyjne/informacje-o-obywatelach-przechowywane-przez-instytucje-samorzadowe-nie-sa-bezpieczne>
- ✓ *Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony*, (M.P. 2019 poz. 666)
- ✓ Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016
- ✓ Litwiński P., *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2017
- ✓ Pszczółkowski K., *Metodyka zarządzania ryzykiem w ochronie danych osobowych, Fundacja Bezpieczeństwa Informacji Polska*, Warszawa 2018
- ✓ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
- ✓ *Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych* (Dz. U. 2012 poz. 526)

- ✓ Sienkiewicz P., *Ewaluacja ryzyka w zarządzaniu kryzysowym*, [in:] Ryzyko w zarządzaniu kryzysowym, P. Sienkiewicz, M. Marszałek, P. Górny (ed.), Toruń 2012
- ✓ *Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych*, <https://uodo.gov.pl/437>
- ✓ Wikariak S., *Niebezpieczeństwa wycieku informacji można było uniknąć*, <https://prawo.gazetaprawna.pl/artykuly/1399802,niebezpieczenstwa-wycieku-informacji-mozna-bylo-uniknac.html>
- ✓ *Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679*, (WP 248 rev.01), <http://www.giodo.gov.pl/pl/file/12864>
- ✓ Zawiła-Niedźwiecki J., *Analiza ryzyka służąca spełnianiu wymagań RODO*, <https://sip.legalis.pl/document-view.seam?documentId=mjxw-62zogi3damjzhaydooa>
- ✓ Zawiła-Niedźwiecki J. (ed.), *Poradnik RODO. Podejście oparte na ryzyku*, vol. 2, Warszawa 2017