SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2023
ORGANIZATION AND MANAGEMENT SERIESNO. 171

PERSONAL DATA SECURITY SYSTEM IN LOCAL SELF-GOVERNMENT UNITS

Katarzyna ZAWIERUCHA-KOZŁOWSKA

Faculty of Command Management, War Studies University; k.zawierucha@akademia.mil.pl,
ORCID 0000-0002-9439-5589

Purpose: The article deals with the topic of personal data security systems in various local government units (LGUs) located in Poland. In addition, the personal data security system, information technology and personal data were defined. The aim of the article was to draw attention to the importance of data processed in local government units and to present the results of research in this area.
Design/methodology/approach: The considerations and analysis made it possible to identify the causes of the negative impact on personal data and to present the types of threats that may occur in connection with incorrect processing of personal data.
Findings: The article presents the essence of the information security management system and the most important threats resulting from improper management of personal data. The article defines local government units in the context of knowledge of legal provisions in the field of personal data processing. In addition, the article recommends the use of good practices in the field of proper data protection.
Practical implications: Research proves important issues regarding the quality of personal data processing in local government units.
Originality/value: The information contained in the article deals with the subject of the functioning of local government units, personal data protection and the growing importance of technology used for data processing, supplementing the limited number of publications on the presented topic.

Keywords: personal data security system, security, personal data protection.

Category of the paper: research and review publication.

1. Introduction

The personal data security system is one of the most important elements of the organization's functioning, taking into account the value of the processed personal data. Some kind of organization's assets, such as data processing, determine the success or failure of the organization's functioning. The factors determining the proper management of personal data

are human, technical and technological, organizational factors and those resulting from sudden, unexpected events. Including them in the personal data security system contributes to the sustainability of organizations, which are local government units, and to the reduction or elimination of administrative and financial penalties imposed on units by the supervisory authority, which is the President of the Office for Personal Data Protection.

The introduction and application of regulations related to the proper processing of data determines the correct functioning in the three-tier structure of local government (gmina, poviat, voivodship), and thus determines the correctness of personal data processed in their structures, also with the use of information technology. Creating registers of residents, placing information in the Public Information Bulletin (BIP), using monitoring, or commissioning IT services to other entities requires proper protection of personal data.

Information security is currently one of the most important elements of the data security system in public, private and non-profit organizations. Public security is *a state based on legal norms, in which the conditions for the efficient functioning of a state organization are ensured [...]* (Fehler, 2010).

The functioning of the described organizations is based on the dynamism of world development, which is why it is so important to adapt to the changing environment or create such organizations that will be able to exist in the unpredictable future, where personal data and protection determine the safety of the individuals to whom the data relate. The protection of personal data, constituting the information security system, concerns the new provisions governing data processing, which have gained great importance since 2018. Although data protection is not something new, its value has increased after the introduction 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 movement of such and the repeal of Directive 95/46/EC (General Data Protection Regulation).

What is worrying, however, is the fact that the provisions on the protection of personal data in local government units are often unknown or known only to a small or moderate extent. Often, only inspectors or administrators of personal data are familiar with the regulations, while other people who process huge amounts of personal data on a daily basis, e.g. in the process of communication, collecting data about employees and residents, or recording the results of training, are not familiar with the regulations.

The main purpose of the article is to identify the risks associated with incompetent data processing or resulting from ignorance of the law, define the concept of information, personal data, personal data security system, present the benefits of proper data processing and present the essence of the functioning of local government units based on huge amounts of processed data. In order to achieve the main goal, the results of research carried out for the purposes of the doctoral dissertation, corresponding to the aspects of the subject matter, were presented, the functioning of local government units in the aspect of information processing and the effectiveness of the data security system were verified.

2. Information security management system as the basis for the functioning of local government units

The system, i.e. *a set of relations between mutually coupled elements* (Sienkiewicz, 1994, p. 159) can function on the basis of the system and information, thus creating an information system defined as a multi-level structure enabling the processing of indicated information. The information system is also one of many elements of the sequence of events that creates the decision chain in the management system. The management system, in turn, is a set of activities, which includes activities that create subsequent parts of the resource management process along with their mutual relationships. In addition, the management system should be supported by the information system, while the technical means constituting the management infrastructure should be identified with the IT system of a given organization, i.e. *the automated data processing system* (Klonowki, 2004).

Information security management and personal data protection are aimed at minimizing the risk of theft, negative use of data or data loss. So what is personal data? According to Art. 4, point 1 of the GDPR: *personal data means information about an identified or identifiable natural person ("data subject"); an identifiable natural person is a person who can be identified, directly or indirectly, in particular on the basis of an identifier such as name and surname, identification number, location data, online identifier or one or more specific physical, physiological, genetic, mental factors, economic, cultural or social identity of a natural person* (GDPR, point 1). Information, on the other hand, is perceived as a specific amount of data, it is the source of the proper functioning of the organization, as well as the opportunity to achieve a competitive advantage. Thus, information is the number of conclusions that can be obtained from a particular message. Very often the word "data" is equated with the word "information", which is why these words are used interchangeably, according to the glossary of synonyms (Ludwiczak et al., 1998). Increasing the security of information and personal data is a series of activities aimed at determining the procedure for securing data and information. For optimal security of the processed data, it is necessary for organizations to comply with all standards regulating the functioning of the organization in this aspect, i.e. standards regulating the functioning of the Information Security Management System (ISMS), procedures, policies, audits, services of the personal data protection officer, social engineering tests and training which additionally complement the knowledge obtained from international standards, relevant laws or the GDPR.

The Information Security Management System - ISMS, operating on the basis of international standardization standards, indicates the model of the continuous improvement cycle (PDCA) in accordance with the concept of W.E. Deming. The process approach in information security management draws users' attention to procedures and rules ensuring the security of IT systems and networks (Wołowski, et al., 2012) (Figure 1 and 2).

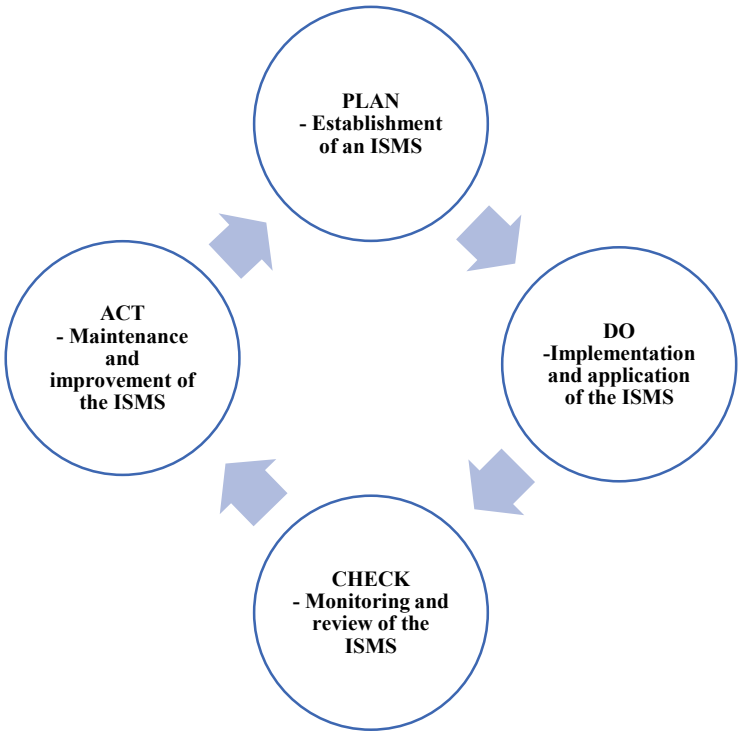

Figure 1. PDCA model used in ISMS processes.

Source: own study based on PN-ISO/IEC 27001:2017-06.

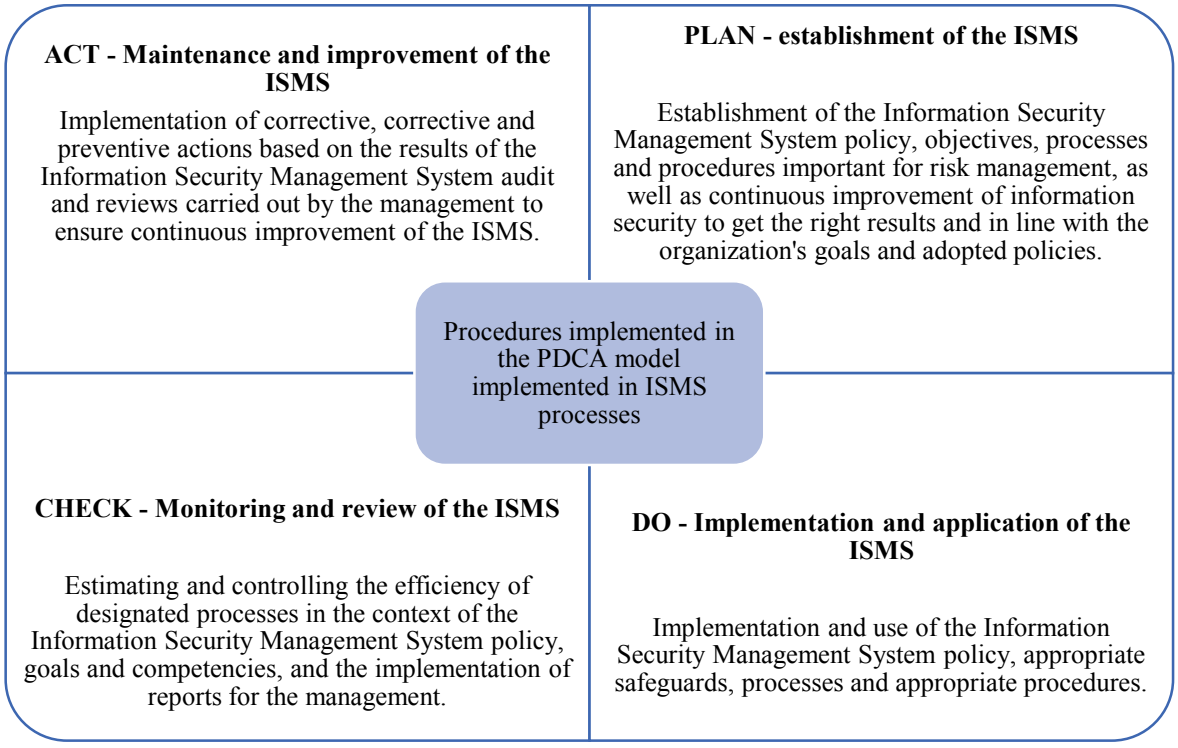

Figure 2. Procedures implemented in the PDCA model implemented in ISMS processes.

Source: own study based on F. Wołowski, J. Zawiła-Niedźwiecki, Bezpieczeństwo systemów informacyjnych edu-Libri, Kraków-Warszawa 2012, s. 17.

When determining the methods of personal data processing, when designing the IT system and during data processing, all organizational and technical measures should be taken to effectively implement the principles of personal data protection, comply with the requirements of the GDPR, and protect the rights of persons whose data is processed (Schwartz, Solve, 2010). This mainly applies to local government units due to the amount of data processed in their structures, also with the use of information technology. The register of residents requires the identification of the local population and the creation of appropriate information clauses, or a register of processing activities also in the aspect of sharing personal data, where very often data processing is automated. Undoubtedly, therefore, the Information Security Management System should be implemented at entities performing public tasks. Because it covers not only the protection of personal data, but also other information that needs protection, including classified information.

3. Data security in local government units

Surveys conducted among local government units were conducted in 2021. The research tool was a questionnaire addressed to 372 local government units representing both commune, poviat and voivodeship governments in all voivodeships. The target population of local government units included 2,807 entities (16 voivodeships - voivodeship offices, 314 poviats - poviat starosty, 2,477 communes - commune office, municipal office/city and commune office, municipal office, city hall) (Samorząd…, 2023).

The results obtained from the conducted survey gave the opportunity to obtain conclusions that allowed the assessment of the current data security in local government units and the recommendation to ensure acceptable protection of personal data.

177 women (47.6% of respondents) and 195 men (52.4% of respondents) participated in the survey. The characteristics of the respondents indicate that a greater number of people dealing with the subject of personal data protection in local government units are men. It is worth noting, however, that this indicator is not significantly higher compared to the number of women. The number of respondents by gender is presented in the Figure 3.

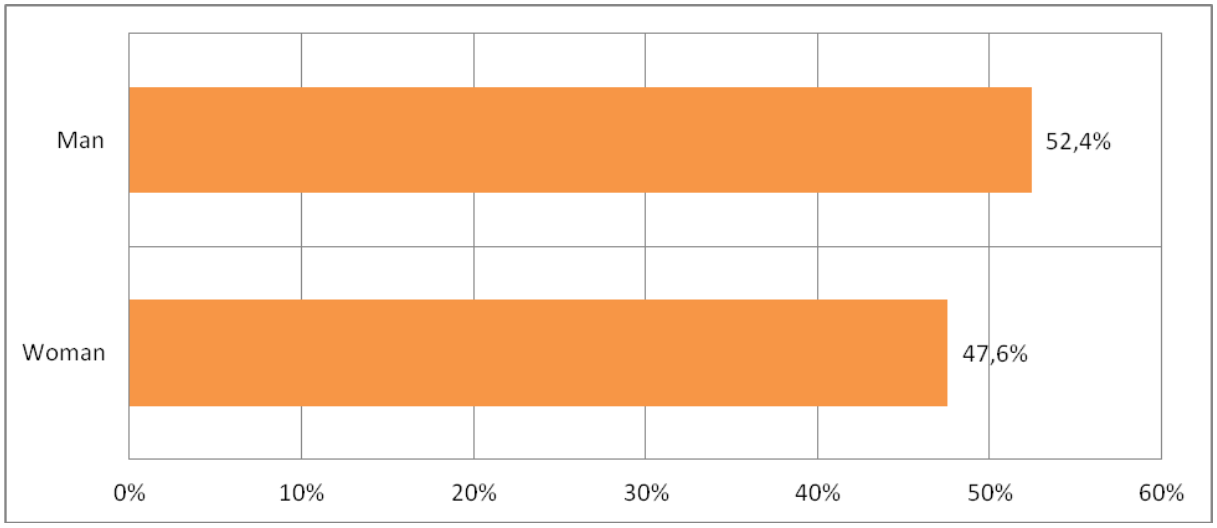

Figure 3. Characteristics of the respondents by gender.

Source: own study based on conducted research.

The type of self-government represented by local government units is presented in figure 4. Most of the respondents were from commune self-governments, which accounted for 236 local government units (63.4%). Poviat self-government 128 local government units (34.4%). The smallest group was constituted by the voivodeship self-government, i.e. 8 LGUs, which accounted for 2.2% (Figure 4).

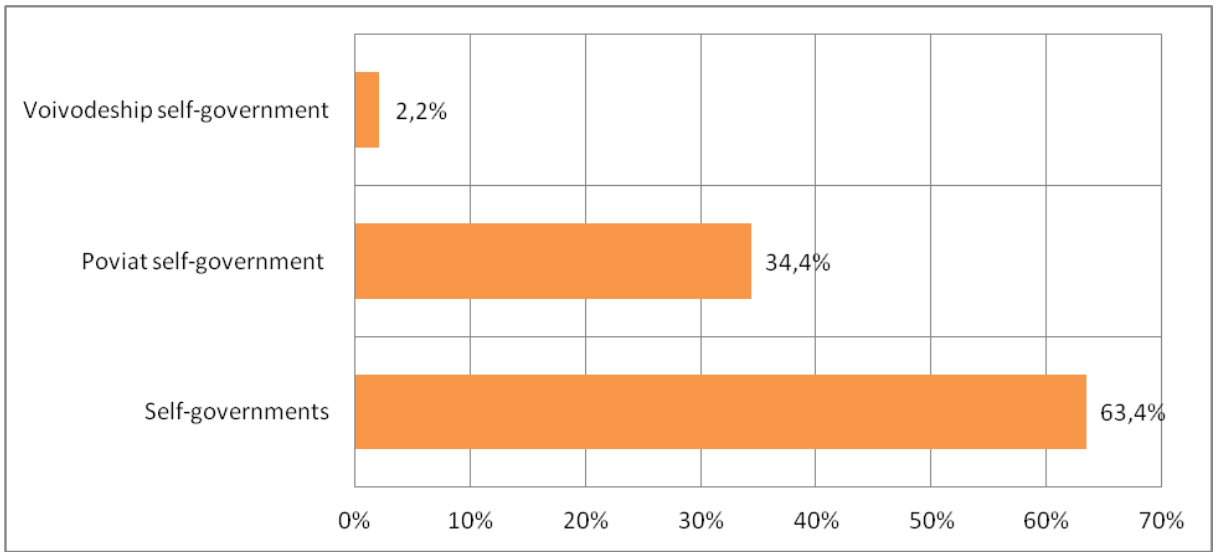

Figure 4. Characteristics of the respondents due to the represented local government.

Source: own study based on conducted research.

In the analysis of the results obtained from the conducted research, it was important to maintain the consistency of the structures with regard to the spatial distribution and type of local government unit, which made it possible to view the representativeness of the research sample and the possibility of generalizing the results obtained in the questionnaire.

Respondents were asked to indicate the answer regarding the presence of documents regarding the protection of personal data in a given LGU. It was recognized that the necessary documents creating security in local government units are: a template for the register of recipients of personal data, a cookie policy, a monitoring policy, an information clause on data processing in e-mail correspondence, a list of personal data files, a template for the incident register, a register of categories of personal data processing, policy clean desk, requirements to ensure confidentiality, integrity and accountability, template of the contract for entrusting the processing of personal data, clause of consent to the processing of ordinary personal data, instruction for managing the IT system, templates of information clauses, register of personal data processing activities, instruction in the event of threats and incidents, register of persons authorized to process personal data, employee statements regarding knowledge of data protection rules, authorization to process personal data. The above-mentioned types of documents were presented to the respondents, then they were asked to mark the answer whether a specific document is included in the LGU (Figure 5).

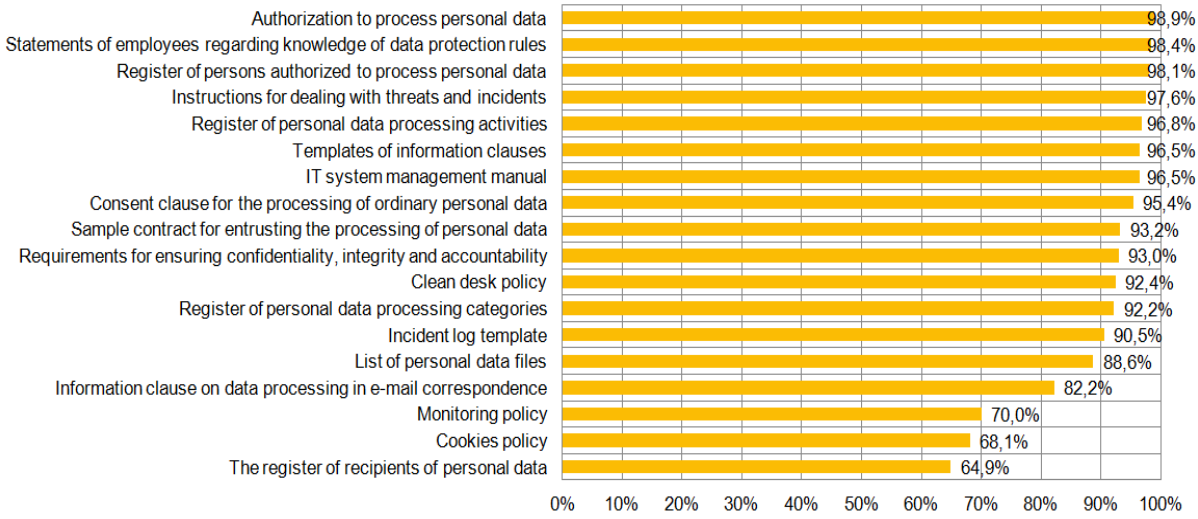

Figure 5. Types of documents used in units.

Source: own study based on conducted research.

Respondents almost unequivocally indicated that the above documents are included in local government units. Authorization to process data is available in local government units. This was the answer of 98.9% of local government representatives. Similarly, employees' statements regarding knowledge of data protection principles (98.4%), or the register of persons authorized to process personal data (98.1%). The fewest representatives of local government units indicated the register of recipients of personal data (64.9%), cookie policy (68.1%) and monitoring policy (70.0%).

The answers given regarding the use or implementation of implementation plans for particular types of monitoring mostly prove the presence of a given technology among LGUs. 64% of representatives of local government units answered that video monitoring is used in their organizations. 54% of respondents also reported the presence of monitoring of IT systems

of the software used, 43% of monitoring of websites, 40% of monitoring of IT systems of e-mail and 23% of the use of monitoring systems for entrances to specific rooms. Noteworthy, however, is the information on the use of various types of monitoring by LGUs, and the lack of a document on the monitoring policy in 30% of local government units (Figure 6).

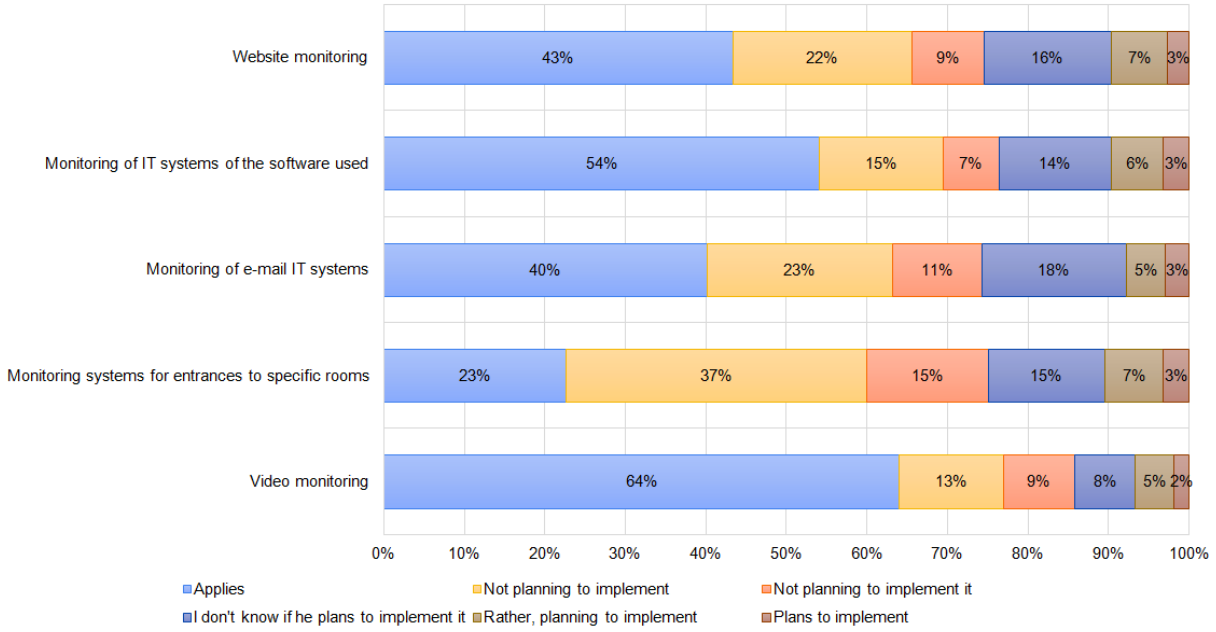

Figure 6. Types of monitoring used in local government units.

Source: own study based on conducted research.

Knowledge of the provisions of the GDPR in terms of individual scopes should not raise doubts that the respondents of individual local government units know the provisions on the protection of personal data to a large extent and to a very large extent. However, unfortunately, also local government units do not comply with the provisions of the GDPR, despite the fact that 46% of local government representatives (the survey was addressed to personal data inspectors, personal data administrators or people dealing with issues related to personal data protection) answered that they know the provisions to a very large extent concerning breaches of personal data protection, and 36% that they know this scope of the provisions of the GDPR to a large extent. 44% of respondents know the provisions on the processing of personal data to a very large extent, and 35% to a large extent. Similarly, in terms of the scope of the provisions on data protection breaches: 41% of respondents indicated that they know these provisions to a very large extent, and 36% to a large extent (Figure 7).

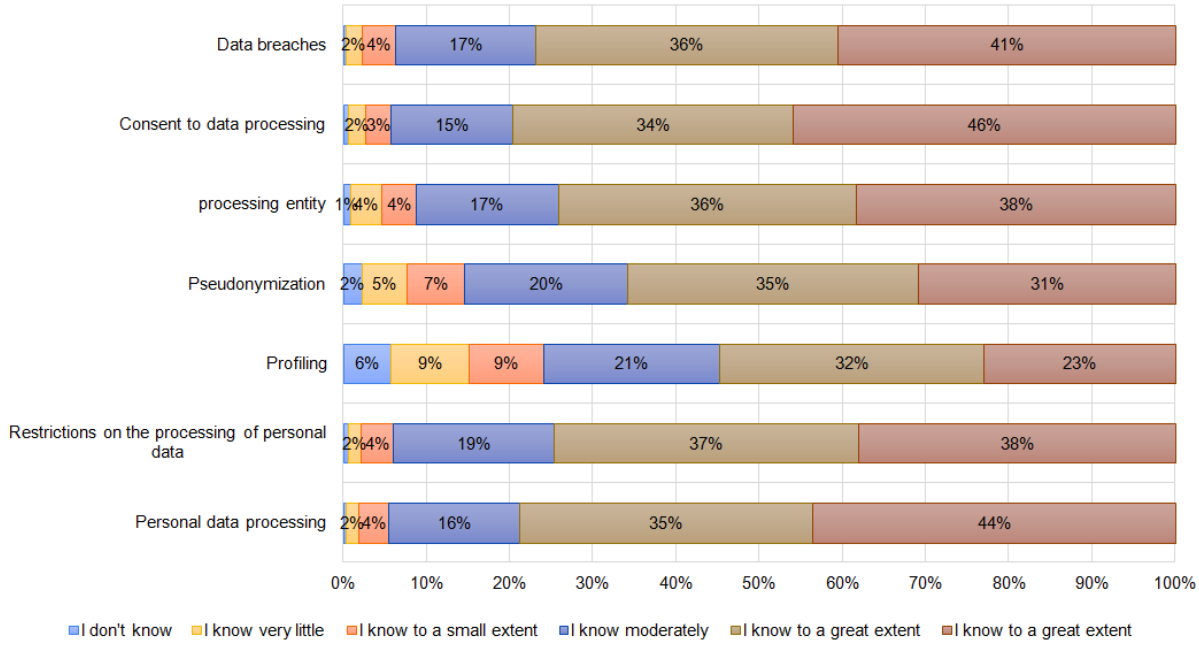

Figure 7. Knowledge of GDPR regulations in local government units.

Source: own study based on conducted research.

Questions regarding administrative and financial penalties issued against the unit show that 94.6% of the units were not subject to administrative and financial penalties, unfortunately, however, a disturbing fact applies to 5.4% of the surveyed local government units that inform about the imposed penalties (Figure 8).

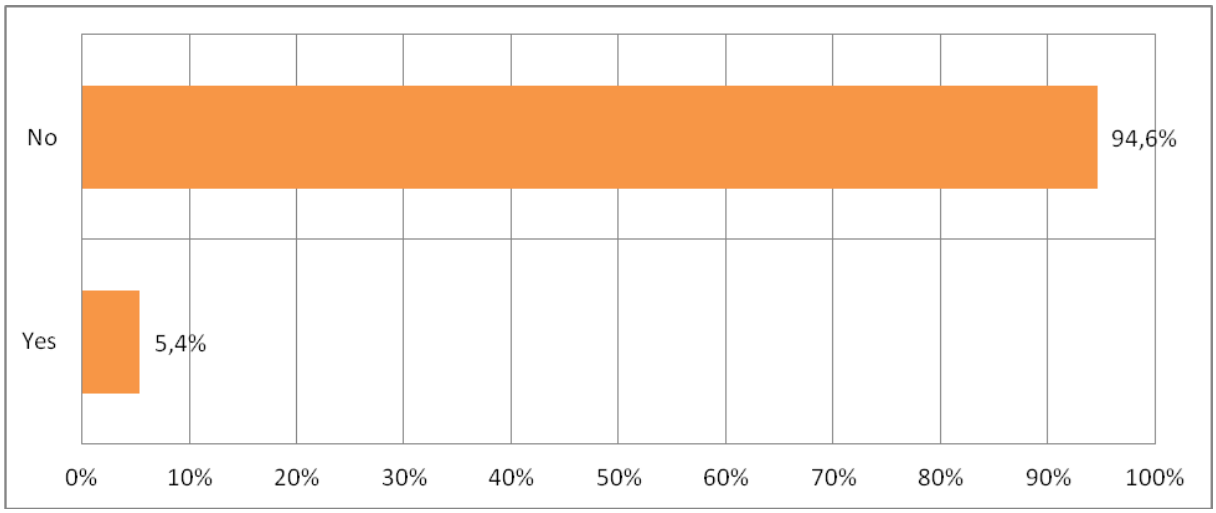

Figure 8. Penalties applied to LGUs by the supervisory authority.

Source: own study based on conducted research.

Administrative money penalties were imposed on 5% of the surveyed LGUs, out of 5.4%, and corrective measures on 95%. Unfortunately, this shows the premises regarding the lack of knowledge of local government employees in the aspect of the GDPR and other provisions governing the data security system (Figure 9).

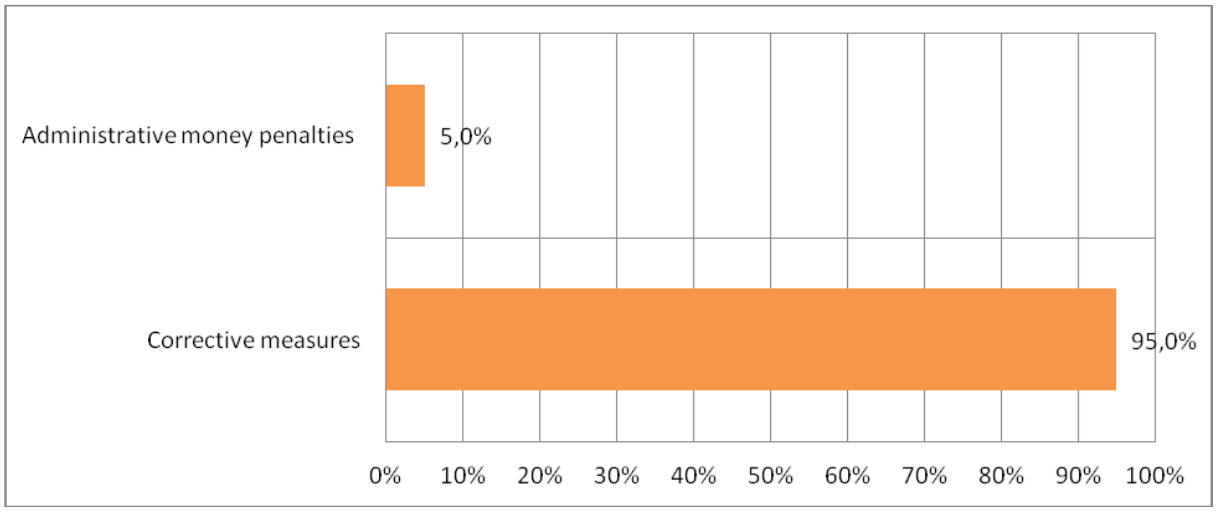

Figure 9. Types of penalties imposed on is by the supervisory authority.

Source: own study based on conducted research.

The highest type of penalty imposed by the President of the Personal Data Protection Office was applied to Mayor Aleksandrów Kujawski (personal data controller). The fine granted is PLN 40,000, and the basic premises for imposing it were:

- lack of a contract for entrusting the processing of personal data with entities to which the data was transferred,
- lack of internal procedures regarding the review of resources available in the Public Information Bulletin in terms of determining the period of their publication.

On the other hand, examples of administrative penalties belonging to the category of corrective measures imposed by the supervisory authority on local government units include:

- conducting additional risk analysis and conducting additional training,
- two-step login to e-mail accounts,
- fulfilling the information obligation towards a natural person,
- recommendations regarding the data set and assigning them to individual employees,
- removal of personal data from the documentation published in the Public Information Bulletin.

It should therefore be noted that the management of organizations in the aspect of security and data protection should display elements of continuous improvement, taking into account the changes taking place in the modern world and the regulations that adapt to the changing environment of the organization's functioning. In addition, organizations must take into account the risks that accompany data processing and the factors that may cause such risks.

4. Types of threats related to the loss of personal data

Each processed personal data may bring many benefits to the organization and to the data subjects, however, in connection with the implementation of the processing process, there may be as many threats. Recital 75 of the GDPR informs about the negative aspects of the processing of personal data that may lead to physical or material or non-material damage, which primarily concerns (GDPR, recital 75):

- identity theft,
- discrimination,
- financial loss,
- identity fraud,
- violation of the confidentiality of personal data protected by professional secrecy,
- infringement of good name,
- significant social damage,
- significant economic damage,
- unauthorized reversal of pseudonymisation,
- deprivation of the ability to exercise control over your personal data,
- deprivation of the possibility of exercising rights or freedoms.

However, it is worth bearing in mind that the risk of violating the rights or freedoms of natural persons always has a different probability of occurrence and a different severity of the threat, therefore, when assessing the possibility of threats, one should always take into account (Izydorczyk, 86a):

- scientific studies with practical applications,
- administrator's own experience,
- experience of other administrators,
- guidelines, codes and/or opinions developed and disseminated by national and international social organizations and protection authorities.

According to T. Izydorczyk, hazard identification is one of the most difficult processes, and the field of organization and management uses the following methods to identify hazards (Izydorczyk, 86b):

- using the experience and methods developed by external experts,
- use of prepared catalogs of threats,
- brainstorming among people involved in hazard identification.

The General Data Protection Regulation does not provide information on how to identify threats, therefore knowledge in this area begins with the application of the provisions of the GDPR. This is due to the legal requirement of risk assessment in connection with violations of the rights or freedoms of natural persons.

In the literature, the most common causes of potential threats are mentioned (Bógdał-Brzezińska, 2012):

- incorrect protection of servers, cryptographic devices and auxiliary devices,
- damage to devices and/or telecommunications line connections,
- inappropriate or insufficient software,
- gaps and errors causing data loss,
- lack of awareness of users in the field of ICT security, validity of processed data, the possibility of personal data protection, expected penalties related to violations, etc.,
- intentional damage to IT systems,
- intentional attacks,
- short technology lifetime,
- deliberate incidents committed by users (management staff, employees), e.g. connecting devices to an unsecured network or connecting external devices containing malware,
- unauthorized actions by administrators and/or users.

Appropriate data protection is the supervision of information security, i.e. the system by means of which the functioning of the organization (its activities) in the field of information security is controlled and managed (Figure 10).

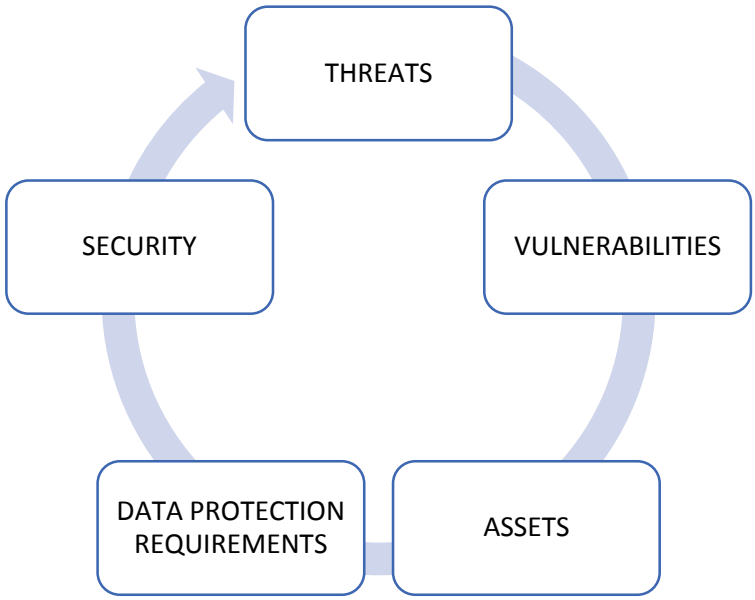

Figure 10. Elements of the information system in JST.

Source: own study based on Zieliński, www.uodo.gov.pl, 8.02.2023.

In accordance with the security requirements contained in art. 39 of the Act on the protection of personal data processed in connection with prevention and combating crime, the personal data controller is obliged to apply the following measures (Dz.U. 2018, point 39):

- technical means,
- organizational measures,

which will ensure proper protection of the processed personal data. Measures must be appropriate to both the type of threat and the category of data protected and appropriate to ensure a level of security that corresponds to the specific threat.

The proper functioning of local government units with regard to the protection of personal data, i.e. the functioning of an appropriate data protection system, is a requirement of the currently applicable provisions of law and a necessity to ensure adequate protection of processed data, which today are invaluable for humans.

The undertakings undertaken by local government units in connection with the processing of personal data should be included in the risk-based approach, include an assessment of the impact on the protection of personal data, check the level of ICT security and verify the facts in connection with the correctness of processing. Activities related to the dissemination of the code of good practice will allow for the improvement of the personal data processing process while ensuring compliance with the provisions of law on the protection of personal data and increasing the sense of responsibility among employees of local government units in this regard.

5. Summary

A proper data protection system allows for effective management of local government units and for precise determination of the possibility of risk to personal data. Local government units processing numerous personal data, both of employees and citizens, have created sufficient reasons to focus on their functioning and to verify them in terms of the protection of the processed data. Compliance with the provisions on the protection of personal data and the implementation of good practices in the field of correctness of data processing should be participatory in order to involve all employees in the protection of personal data and taking into account all factors affecting the protection of such data.

References

1. Babbie, E. (2004). *Badania społeczne w praktyce.* Warszawa: PWN.
2. Bógdał-Brzezińska, A. (2012). *Teleinformatyczne zagrożenia bezpieczeństwa Polski. Uwarunkowania wewnętrzne i międzynarodowe.* Warszawa: WUW.
3. Dz.U. 2018, point 39, https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU 20180002177, 5.02.2023.

4. Fehler, W. (2010). *Bezpieczeństwo publiczne jako składnik wewnętrznego bezpieczeństwa państwa.* Bezpieczeństwo teoria i praktyka, https://repozytorium.ka.edu.pl/handle/11315/27355.
5. Izydorczyk. T.(2017). Analiza oparta na ryzyku. In: M. Kołodziej, *Vademecum ABI. Część II – Przygotowanie do roli Inspektora Ochrony Danych.* Warszawa: C.H. Beck.
6. Kisielnicki, J (2013). *Systemy informatyczne zarządzania.* Warszawa: Placet.
7. Klonowski, Z.J. (2004). *Systemy zarządzania przedsiębiorstwem. Model rozwoju i właściwości funkcjonalne.* Wrocław: Oficyna Wydawnicza Politechniki Wrocławskiej.
8. Kołodziej, M. (ed.) (2017). *Vademecum ABI. Część II – Przygotowanie do roli Inspektora Ochrony Danych.* Warszawa: C.H. Beck.
9. Ludwiczak, D., Piskadłowa, A, Tarka-Huczek, E. (1994). *Słownik wyrazów bliskoznacznych.* Warszawa: Wiedza Powszechna.
10. *Samorząd terytorialny w Polsce.* Ministerstwo Spraw Wewnętrznych i Administracji, Baza JST, http://administracja.mswia.gov.pl/adm/baza-jst/843,Samorzad-terytorialny-w-Polsce.html, 5.02.2023.
11. 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), https://uodo.gov.pl/pl/404, 5.02.2023.
12. Sienkiewicz, P. (1994). *Analiza systemowa. Podstawy i zastosowania.* Warszawa: Bellona.
13. Szostek, D. (ed.) (2018). *Bezpieczeństwo danych i IT w kancelarii prawnej*. Warszawa: C.H. Beck.
14. Schwartz, P.M., Solve, D.J. (2010). *Information Privacy. Statutes and Regulations*. New York: Wolters Kluwer.
15. Wołowski, F., Zawiła-Niedźwiecki, J. (2012). *Bezpieczeństwo systemów informacyjnych*. Kraków-Warszawa: edu-Libri.
16. Zieliński, A. *Bezpieczeństwo danych osobowych.* Urząd Ochrony Danych Osobowych, www.uodo.gov.pl, 8.02.2023.