SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2023
ORGANIZATION AND MANAGEMENT SERIES NO. 184

IMPROVING THE SYSTEMIC APPROACH TO INFORMATION SECURITY MANAGEMENT IN THE CONTEXT OF INCREASING THE LEVEL OF DATA PROTECTION IN LOCAL GOVERNMENT ENTITIES

Aneta WYSOKIŃSKA[1*], Katarzyna ZAWIERUCHA-KOZŁOWSKA[2]

[1] Faculty of Command Management, War Studies University, Warsaw;
a.wysokinska-senkus@akademia.mil.pl, ORCID: 0000-0001-9021-6355
[2] Faculty of Command Management, War Studies University, Warsaw; k.zawierucha@akademia.mil.pl,
ORCID: 0000-0002-9439-5589
* Correspondence author

Purpose: The article presents the requirements of the ISO/IEC 27001 standard and the implementation status of the information security management system in Poland and worldwide. Additionally, the role of modern technologies in ensuring the security of organizations was presented and the threats that may accompany the use of technology in the aspect of personal data in public administration were indicated.
Design/methodology/approach: The analysis conducted allowed us to identify differences in the number of international certificates awarded and to determine the relationship between the implemented systems and the represented sectors.
Findings: The article identifies threats that may occur when using information technologies in the context of personal data protection, determines which of these threats pose the greatest threat to personal data processed in the analysed organizations, and identifies technological factors that influence the increase in the level of security in the context of personal data protection. The study also analyses the number of information security management system certificate according to the ISO 27001 standard, taking into account individual sectors.
Practical implications: The research indicates fundamental issues regarding the implementation of the information security system in Poland and around the world.
Originality/value: The information contained in the article discusses the relationship between the implemented international certificates and the type of services provided and verifies the world leaders in terms of the number of ISO 27001 certificates in the public administration sector.

Keywords: information security management system, new technologies, data protection.

Category of the paper: research and review publication.

1. Introduction

Changes taking place in the modern world have made information technology play a huge role in human functioning, and personal data have become a kind of modern currency. The aim of the article is to identify threats that may occur when using information technologies in the context of personal data protection; determining which of these threats pose the greatest threat to personal data processed in the analysed organizations and identifying technological factors that influence the increase in the level of security in the context of personal data protection. The study also analyses the number of information security management system certificates according to the ISO 27001 standard, taking into account individual sectors. The research used the diagnostic survey methods. The survey was conducted among 372 Polish local government units. The research conducted showed that by the end of 2020, 44,499 certificates of compliance with the ISO 27001 standard had been granted worldwide. Despite the growing number of ISO 27001 certificates granted worldwide, the share of certificates granted in the public administration sector is relatively small compared to other sectors. The conducted survey research allowed us to isolate factors that generate threats in the context of personal data protection. According to the surveyed local government units, the human factor, resulting from the possibility of accidental, unintentional disclosure of personal data, is a key risk category that may have a negative impact on the personal data protection process. There is a limited number of studies on the issue discussed, and it should also be pointed out that people processing data are insufficiently aware of possible threats. Analysis of the risks arising from the use of information technologies in the context of personal data security in the public sector is still a current and important trend in research, because activities aimed at limiting and counteracting risks contribute to increasing the efficiency and improving the security of organizations.

2. Requirements of the ISO/IEC 27001 standard and the implementation status of the information security management system in Poland and worldwide

PN-EN ISO/IEC 27001 is the most well-known standard in the world regarding the Information Security Management System (ISMS). On August 22, 2023, a new version of the PN-EN ISO/IEC 27001:2023-08 standard (English version) was published. The ISO/IEC 27001 standard is an important element of the information security management system. In the context of increasing cybercrime and the constant emergence of new threats, a key strategic task of every organization is information security management. This may seem complicated and

sometimes even unattainable. The PN-EN ISO/IEC 27001 standard is used to help organizations purposefully secure collected data, create secure data processing processes and take into account evolving external and internal risks.

PN-EN ISO/IEC 27001 promotes a holistic approach to information security, identifying key areas for building security, such as: people, processes and technologies.

The Information Security Management System, created in accordance with this standard, is an instrument for creating appropriate security measures, taking into account the context in which the organization operates, its business strategy and goals.

It sets out the necessary safeguards to ensure that personal data and/or personally identifiable information are properly managed in a transparent and systematic manner. This standard specifies the safeguards that are appropriate when an organization acts as a processor or controller of personal data. The control measures included in the standard connect the entire cycle of obtaining, analysing, storing, sharing and deleting information, thus enabling this identification. The data subject remains at the centre of the security measures applied to the requirements of the GDPR (McDonagh, 2018, p. 4).

The most important standards in the field of information security management developed by the International Organization for Standardization ISO include:

PN-EN ISO/IEC 27000:2017-06 Information technology. Security techniques. Information security management systems. Overview and terminology.

This International Standard presents the fundamentals of information security management systems, along with terminology often used in the ISMS set of standards. It is used by organizations of all types and sizes, such as commercial companies, government institutions and non-profit organizations.

PN-EN ISO/IEC 27001:2023-08 Information security, cybersecurity and privacy protection. Information security management systems – Requirements.

This document defines the criteria for creating, implementing, maintaining and improving an information security management system in an organization. It also includes requirements for assessing and managing information security risks, tailored to the needs of a given organization. The provisions contained in the document are universal and apply to all organizations, regardless of their type, size or nature. Omission of any requirement from Chapters 4 to 10 is unacceptable if the organization declares compliance with this document.

PN-EN ISO/IEC 27002:2023-01 Information security, cybersecurity and privacy protection. Securing information.

This document presents a reference set of information security standards along with instructions for their implementation. It was created for organizations to use in the context of an information security management system (ISMS) in accordance with ISO/IEC 27001, implement information security based on globally recognized best practices and create their own dedicated information security management guidelines.

PN-ISO/IEC 27004:2017-07 Information technology. Security techniques. Information security management. Monitoring, measurement, analysis and evaluation.

This document provides guidance to assist organizations in assessing their information security performance and the effectiveness of their information security management system to meet the requirements of ISO/IEC 27001. The document is suitable for organizations of all types and sizes.

PN-EN ISO/IEC 27006:2021-05 Information technology. Security techniques. Requirements for entities auditing and certifying information security management systems.

This International Standard defines requirements and provides guidance for institutions auditing and certifying information security management systems. Its aim is to facilitate the accreditation process for bodies certifying information security management systems.

It should be noted that as a criteria document, this International Standard may be used in accreditation, peer review or other audit processes

PN-EN ISO 27007:2022-06 Information security, cybersecurity and privacy protection – Guidelines for auditing information security management systems

This document provides guidance on managing an information security system, conducting audits, and qualifying information security system auditors.

ISO/IEC 27007 is intended for those who need to understand or conduct interna lor external audits of an information security system, or manage an information security system audit program.

PN-EN ISO/IEC 27017:2021-07 Information technology. Security techniques. Practical rules for information security based on ISO/IEC 27002 for cloud services

This standard provides information security guidelines specifically designed for the provision and use of cloud services.

PN-EN ISO/IEC 27701:2021-09 Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Requirements and guidelines.

This document defines the requirements and provides guidance for the establishment, implementation, maintenance and continuous improvement of a Privacy Information Management System (PIMS) as an extension of ISO/IEC 27001 and ISO/IEC 27002 for managing privacy in an organization. It contains PIMS requirements and guidelines for personal data administrators and processors. It is used for organizations of all types and sizes, including public, private, governmental and non-commercial entities managing personal data as part of an Information Security Management System.

The research conducted showed that by the end of 2020, 44,499 certificates of compliance with the ISO 27001 standard had been granted around the world. Compared to the number of certificates obtained in 2013, which was 21,604, this value doubled in comparison to 2020.

Comparing the number of certificates obtained in the world with certificates of other management systems, it should be stated that it ranks 4^{th} in terms of implemented systems.

The most certificates obtained by the end of 2020 concern the ISO 9001 standard – 916,842 certificates, ISO 14001 – 348,473, ISO 45001 – 190,481 and ISO/IEC 27001 – 44,499.

Data on the number of cerificates obtained, divided into various ISO standards, is presented below (Figure 1).

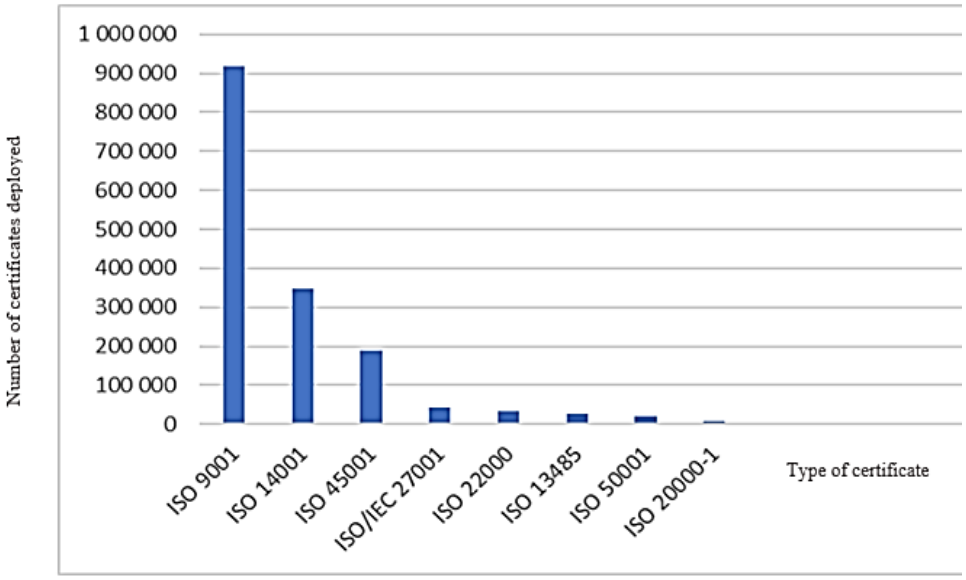

Figure 1. Number of management system certificates in the world – as of the end of 2020.

Source: own study.

Figure 2 shows the number of ISO 27001 certificates in the 20 countries with the highest number of certificates.

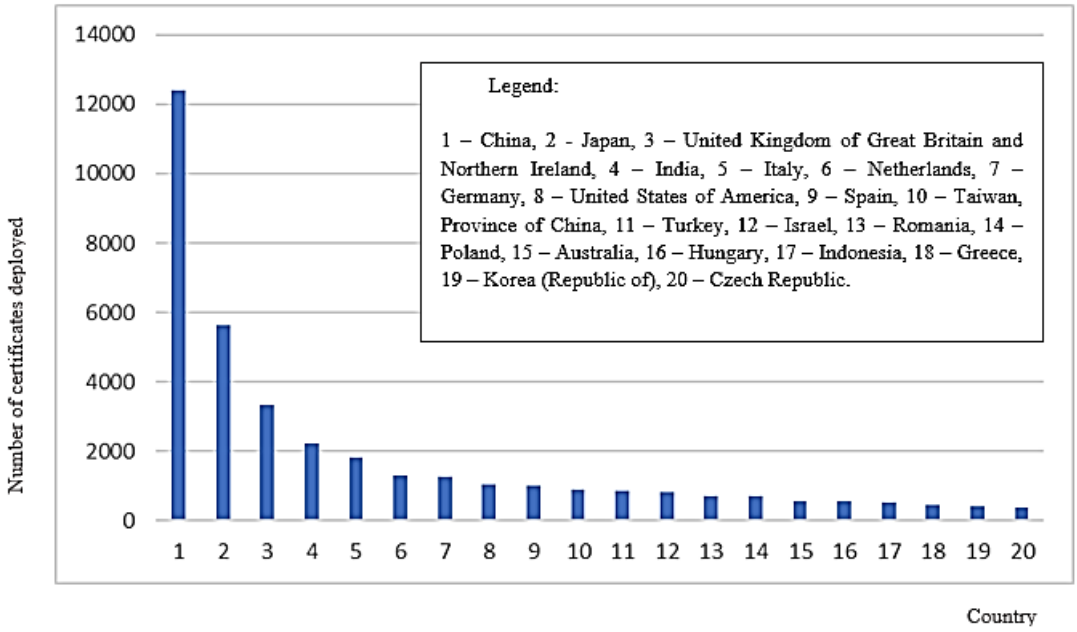

Figure 2. Number of ISO/IEC 27001:2013 Information technology certificates awarded. Security techniques. Information security management systems – Requirements – in 20 countries in 2020.

Source: own study.

The world leader in the number of ISO 27001 certificates obtained by the end of 2020 is China – 12,403, then Japan – 5,645, United Kingdom of Great Britain and Northern Ireland – 3,327, India – 2,226, Italy – 1,827, Netherlands – 1,326, Germany – 1,281, United States of America – 1,058, Spain – 997, Taiwan, Province of China – 10,895. Poland ranked 14th with 710 certificates.

Figure 3 presents the 10 industries with the largest number of implemented ISO 27001 certificates in 2020.

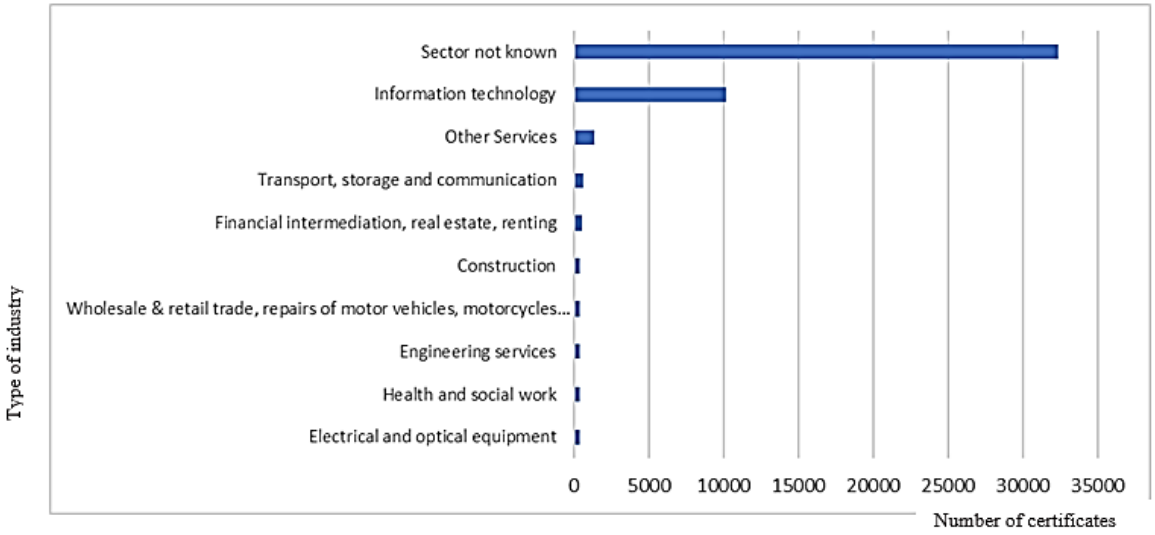

Figure 3. 10 industries with the largest number of implemented ISO 27001 certificates in 2020.
Source: own study.

Analysing the 10 sectors in the world in which the largest number of ISO 27001 certificates have been granted, the following can be indicated: Sector not known – 32,372, in turn – Information technology – 10,167, Other Services – 1,359, Transport, storage and communication – 620, Financial intermediation, real estate, renting – 564, Construction – 417, Wholesale & retail trade, repairs of motor vehicles, motorcycles & personal & household goods – 404, Engineering services – 399, Engineering services – 399, Health and social work – 389, Electrical and optical equipment – 388.

In Poland, the most popular sectors when it comes to the implementation of information security management systems are: Health and social work – over 30% of the total number of ISO 27001 certificates, Sector unknown – 30% of the total number of ISO 27001 certificates and Information technology – 21%.

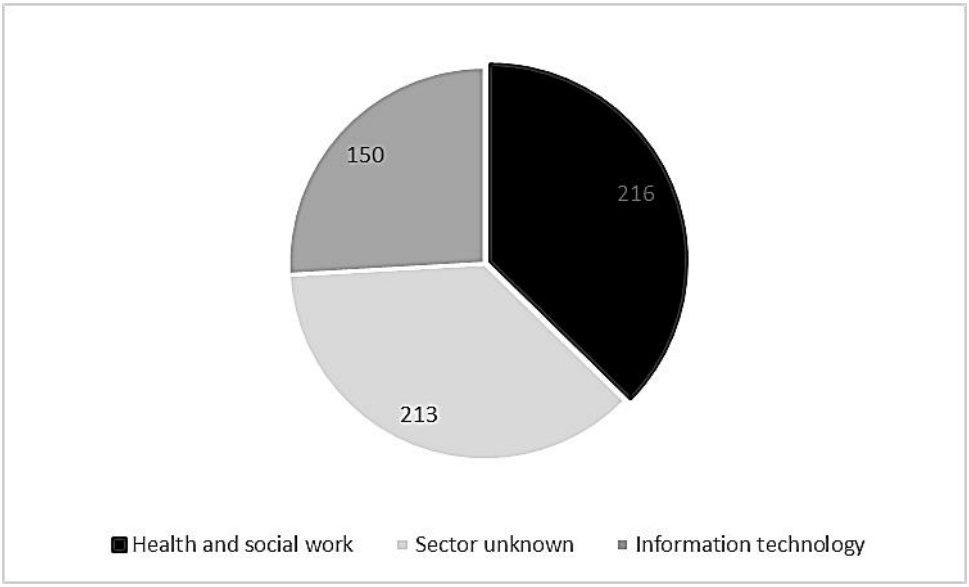

Figure 4. Sectors with the largest number of ISO 27001 certificates granted in Poland in 2020.

Source: own study.

Figure 5 presents the 5 countries that hold the leading position in terms of the number of certificates confirming compliance with the ISO 27001 standard in the world in the public sector.

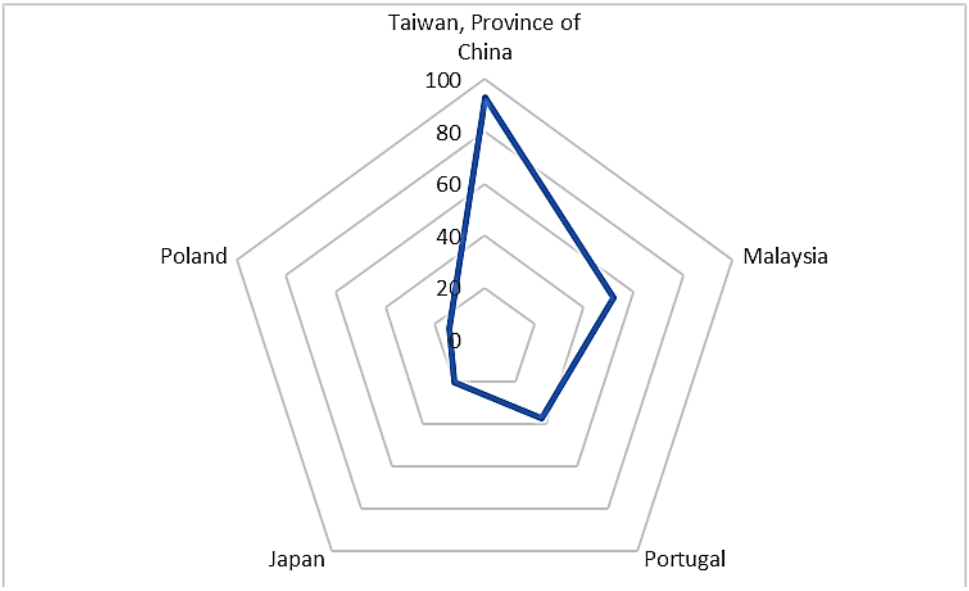

Figure 5. World leaders in terms of the number of ISO 27001 certificates in the public administration sector.

Source: own study.

The world leaders in terms of ISO 17021 certificates held include: Taiwan, Province of China – 93 certificates, Malaysia – 52, Portugal – 37, Japan – 20, Poland – 14. Statistics show that despite the growing number of certificates granted in the world, relatively small is the share of certificates awarded in the public administration sector in relation to other sectors. Therefore, it is recommended to pay attention to the establishment, implementation, operation, monitoring,

review, maintenance and improvement of the Information Security Management System, because a properly implemented and certified system brings many benefits to the organization.

Information security management system according to the ISO 27001 standard:

- contributes to minimizing the risk of events related to information security,
- enables the organization to be prepared for information security incidents,
- increases the credibility of the organization in the eyes of customers, investors and shareholders (all stakeholders),
- has a positive impact on protecting and improving the organization's reputation,
- ensuring the security of the Client's interests as a result of a properly functioning information management system,
- guarantees an appropriate level of quality of protection of information assets,
- increased employee awareness of information security.

Based on the above information, it can be seen that the implementation of the Information Security System affects the quality of the services provided, therefore private, public and non-profit organizations should implement their activities based on ISO 27001.

3. The role of modern technologies in ensuring the security of the organization

The dynamic development of the real and virtual world has led to the emergence of numerous benefits. However, despite the positive aspects, digitization has brought with it new forms of threats. The rapid development of technology that blurs reality has created many dangers. Thanks to computerization, new technologies and artificial intelligence introduced to all economic sectors, as well as the collection of data in IT systems, ease of access to this data has arisen. Total surveillance and loss of privacy are a huge disadvantage of new technologies that are difficult to oppose. The development of computerization has made it possible to "crack" any password, and the prospect of not being able to exchange information generates huge problems.

However, the constant development of civilization favours the development of the organization and the increase in profits achieved and facilitates functioning, and new technologies regularly adapt to the needs and influence economic development because effective management can determine success in the organization (Bauman, 2000, p. 5). Modern technologies provide many new opportunities for effective, innovative and more efficient operation of enterprises, increasing the effectiveness of services provided and the number of product offers. However, with such dynamic development, information security must be taken into account. The ongoing changes in the management of organizations mean that personal data is becoming a kind of modern currency and it is very easy to lose it or leak it.

The autonomy of modern technology or its improper use may reduce safety. Technology users often do not protect their personal data or that of other people whose data they process. This may result from ignorance, intentional action or the desire to achieve convenience over the loss of privacy. That is why it is so important to create appropriate regulations, procedures, conduct training and build appropriate security measures.

Modern technologies that ensure organizational security include, for example:

- working time monitoring systems,
- technologies that provide Internet services for organizations,
- identity verification systems,
- e-mail monitoring,
- monitoring of websites viewed by the employee,
- monitoring of the software used,
- access cards to specific rooms,
- access keys to the processed data.

The need for security is one of the most important issues for both individuals and entire organizations. Therefore, modern organizational management requires proper management of information security and personal data. For this purpose, each organization, regardless of whether it is a data controller or a processor, must appoint a personal data inspector who will supervise the accuracy of the processed data.

The most direct use of knowledge and modern technologies for security includes support in making current decisions that improve security, as well as consistent actions related to data integrity violations. The latest knowledge and modern technologies are a key factor in the organization's security level and the fundamental importance of implemented security strategies. That is why it is so important to use the potential of the mentioned factors in practice. Modern technologies, while knowing them properly, currently concern all aspects of security that organizations face every day (Kleiber, 2014, p. 61).

More and more important information is collected on various types of digital media and processed on a large scale. Providing them with the appropriate level of security requires the organization to take multi-directional actions to protect data against modification, loss or theft. However, the multidimensionality of activities must concern all factors that threaten the data, i.e.: human factors (staff), organizational factors (organizational structure), technical factors (technologies used, communication means and software) and emergency factors (unexpected, such as fire, flood). Although it is worth mentioning that, unfortunately, many crimes are committed using IT tools and methods.

The dynamics of organizational development in other parts of the world necessitates the need to constantly modernize technologies and adapt them to constantly emerging new threats. Today, it is difficult to imagine a modern, well-organized and safe organization without the use of modern technologies. The use of information technology in running a company has a positive

impact on innovation, but creates completely new threats. Undoubtedly, modern technologies influence safety, but not always by improving it, but also by reducing it. However, they allow for the ability to prevent threats, not just react to them. Technologies provide the opportunity to address all types of risks related to information integrity. It is not only about solving existing problems, but also about taking a broader look at security in order to reduce the risk.

Therefore, if an organization approaches modern technologies rationally and does not threaten its own safety and the safety of its stakeholders, it can derive many benefits from modern methods, systems and management techniques. New technologies, despite creating many threats, are still being improved and implemented. They help create the future reality, improve the quality of life and increase the security of the organization, but unfortunately, at the same time creating a space of action for people who threaten the processed data.

4. Research methodology

The aim of the study is to identify threats that may occur when using information technologies in the context of personal data protection; determining which of these threats pose the greatest threat to personal data processed in the analysed organizations and identifying technological factors that influence the increase in the level of security in the context of personal data protection. The study also analyses the number of information security management system certificates according to the ISO 27001 standard, taking into account individual sectors.

Research questions:

- What types of threats may occur when using information technologies in the context of personal data protection and which of these threats pose the greatest threat to personal data processed in the analysed organizations?
- What technological factors (information technologies) influence the increase in the level of security in the context of data protection?

The research used a diagnostic survey method using a questionnaire, which was addressed to personal data protection inspectors and personal data administrators as well as people with knowledge in the field of personal data protection in all Polish local government units processing personal data.

The target population of local government units included 2807 entities, consisting of municipal governments (2477), district governments (314) and voivodeship governments (16). The minimum sample size with a known population size – 2807, maximum allowable estimation error – 5% and confidence coefficient – 95% was estimated at 338 units according to the formula:

$$n_{min} = \frac{p(1-p)}{\frac{d^2}{z^2_{1-\frac{\alpha}{2}}} + \frac{p(1-p)}{N}}, \quad (1)$$

where:

p – estimated fraction size,

d – maximum allowable estimation error,

N – size of the general population,

$z_{1-\frac{\alpha}{2}}$ – quantile of the $1-\frac{\alpha}{2}$ order in a standardized distribution $N(0,1)$.

Ultimately, in the study carried out for the purposes of the doctoral dissertation, the survey was sent to 372 local government units representing municipal, district and voivodeship governments in all voivodeships. It was taken into account that in order to maintain representativeness, the structure of the research sample according to the voivodeship and the type of local government unit should largely correspond to the structure of the entire population.

The study involved 177 women, representing 47.6% of respondents, and 195 men, representing 52.4% of respondents.

The majority of respondents were people between 41-50 years old (35.5% of respondents) and 31-40 years old (32.5% of respondents). The youngest group consisted of respondents under 20 years of age (0.03% of respondents), which is also the smallest group. The oldest group were people over 50 years old (23.1% of respondents), and the group between 20-30 years old (8.6%).

Most respondents responded from local government units operating in rural areas, which constituted 170 local government units (45.7%). A city under 20,000 inhabitants (small town) was represented by 108 local government units (29%), a city with 20-99.9 thousand inhabitants (medium-sized city) was represented by 72 local government units (19.4%), a city over 200,000 (big city) inhabitants by 12 local government units (3.2%). The smallest group consisted of representatives from a city of 100-199.9 thousand inhabitants (big city) by 10 local government units (2.7%).

5. Findings

In the study, factor loadings were calculated using the principal components method with the Varimax rotation. Table 1 includes only significant factor loadings, after rounding, in absolute value not less than 0.7 (Table 1).

Table 1.
Factor loadings obtained using the principal components method after the Varimax rotation in the analysis of the most important technological factor influencing the improvement of the systemic approach and increasing the level of security in the context of data protection in local government units

Type of technology	Component		
	1	2	3
Website monitoring	0.837		
Monitoring of IT systems and software used	0.828		
Access cards	0.755		
Identity verification for access control	0.752		
Monitoring of e-mail IT systems	0.736		
Monitoring systems for entrances to specific rooms			
Devices, applications and platforms using the Internet of Things		0.812	
Technologies implementing Internet services		0.769	
Employee working time monitoring systems			
Profiling systems			
Settlement and recording systems			
Systems for reporting irregularities (related to, e.g., corruption)			
Computing cloud			
Video surveillance			
Fingerprint readers			0.804
Biometric gateways (facial recognition system)			0.794

Source: own study.

Finally, in order to interpret common factors, variables that were correlated with individual factors were separated. The "Website monitoring, "Monitoring of IT systems of the software used", "Access cards", "Identity verification for access control" and "Monitoring of e-mail IT systems" variables have high factor loadings (0.837, 0.828, 0.755, 0.752 and 0.736, respectively) with the first factor. The "Devices, applications and platforms using the Internet of Things" and „Technologies implementing Internet services" variables have high factor loadings (0.812 and 0.769, respectively) with the second factor. In turn, the "Fingerprint readers" and "biometric gateways" variables have high factor loadings (0.804 and 0.794, respectively) with the third factor.

The first of the distinguished technological factors influencing the improvement of the systemic approach and increasing the level of security in the context of data protection in local government units is therefore described by five important IT solutions:

- website monitoring,
- monitoring of IT systems of the software used,
- access cards,
- identity verification for access control,
- monitoring of e-mail IT systems.

Due to the variables that describe it, it has been defined as "IT monitoring". The share of this factor in the total variance of the variables included in the study was 28.4%.

The second of these factors is described by two IT solutions:

- devices, applications and platforms using the Internet of Things,
- technologies providing Internet services (e.g., e-mail, social media).

The share of this factor in the total variance of the variables included in the study was 28.1% and was defined as "Internet services technology and the Internet of Things".

The last factor was also described by two elements:

- fingerprint readers,
- biometric gateways (face recognition system).

and was defined as "Biometric security". The share of this factor in the total variance of the variables included in the study was nearly 17%.

6. Summary

An appropriate management system promotes the proper implementation of processes carried out in private and public organizations. In order to improve and develop the organization and operational effectiveness, it is recommended to implement international standards also in terms of the security of processed information. This also applies to local government units, where the amounts of data processed are huge. The security of data processed in local government units is paramount to the implementation of administrative activities in connection with access to the data of all residents of municipalities, poviats and voivodeships, where unfortunately data leakage or theft also occur. The popularity of implementing systems according to international standards is increasing, both in the area of quality, corporate social responsibility and the above-mentioned information security. Which is why it is so important to conduct risk analyses that take into account threats to the security of processed data in order to eliminate risks or turn them into opportunities for further development of the organization.

References

1. Barczak, A., Sydoruk, T. (2003). *Bezpieczeństwo systemów informatycznych zarządzania*. Warszawa: Bellona.
2. Bauman, Z. (2000). *Globalization: The Human Consequences.* Warszawa: Biblioteka Myśli Współczesnej.
3. Bógdał-Brzezińska, A. (2012). *Teleinformatyczne zagrożenia bezpieczeństwa Polski. Uwarunkowania wewnętrzne i międzynarodowe*. Warszawa: WUW.

4. Journal of Laws of 2022.1526, art. 92, https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/samorzad-powiatowy-16799844/art-92, 2.09.2023.
5. Kleiber, M. (2014). Nauka i technologia na rzecz bezpieczeństwa państwa w polskich realiach. *Kwartalnik Bezpieczeństwo Narodowe*. Warszawa: Biuro Bezpieczeństwa Narodowego.
6. McDonagh, K. (2018). *Regulacje dotyczące ochrony prywatności. Zrozumienie roli normy ISO/IEC 27701, Biała księga.* Warszawa: BSI.
7. PN-EN ISO 27007:2022-06 Information security, cybersecurity and privacy protection – Guidelines for auditing information security management systems.
8. PN-EN ISO/IEC 27000:2017-06 Information technology. Security techniques. Information security management systems. Overview and terminology.
9. PN-EN ISO/IEC 27001:2023-08 Information security, cybersecurity and privacy protection. Information security management systems – Requirements.
10. PN-EN ISO/IEC 27002:2023-01 Information security, cybersecurity and privacy protection. Securing information.
11. PN-EN ISO/IEC 27006:2021-05 Information technology. Security techniques. Requirements for entities auditing and certifying information security management systems.
12. PN-EN ISO/IEC 27017:2021-07 Information technology. Security techniques. Practical rules for information security based on ISO/IEC 27002 for cloud services.
13. PN-EN ISO/IEC 27701:2021-09 Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Requirements and guidelines.
14. PN-ISO/IEC 27004:2017-07 Information technology. Security techniques. Information security management systems. Monitoring, measurement, analysis and evaluation.
15. 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 Protection Regulation data), https://uodo.gov.pl/pl/404, 2.09.2023.
16. Zieliński, A. *Bezpieczeństwo danych osobowych*. Urząd Ochrony Danych Osobowych, www.uodo.gov.pl, 2.09.2023.