www.ijecs.in
International Journal of Engineering and Computer Science
Volume 14 Issue 03 March 2025, Page No. 26920-26927
ISSN: 2319-7242 DOI: 10.18535/ijecs/v14i03.5000

Approaches to managing the risks of personal data leakage in digital ecosystems

Anton Snitavets[1]*
[1] Lead Information Security Engineer - Doumo (taxdome.com) Batumi, Georgia

Abstract
The article examines theoretical and practical aspects of managing risks associated with personal data breaches in modern digital ecosystems characterized by complex architectures and numerous distributed services. The study highlights the role of the digital economy, demonstrating that the growing number of mobile devices, cloud platforms, and IoT devices significantly increases the likelihood of unauthorized access to sensitive information. Key regulatory acts and standards were analyzed, including widely recognized U.S. federal laws (such as the Privacy Act of 1974, the Electronic Communications Privacy Act, the Health Insurance Portability and Accountability Act, and the Gramm-Leach-Bliley Act) and international standards (ISO/IEC 27001, ISO/IEC 27701). Additionally, various industry-specific guidelines and research articles published in leading scientific journals were examined Particular attention is given to information security management systems (ISMS) based on formalized risk assessment methodologies (OCTAVE, CRAMM, ISO/IEC 27005) and modern technologies (DLP, SIEM, IDS/IPS). The findings demonstrate that the most effective approach is a comprehensive one, encompassing organizational, legal, and technical measures, along with the mandatory regular updating of security policies in response to current cyber threats. The analysis underscores the importance of considering industry-specific factors (finance, healthcare, industrial IoT) and the human factor, as the degree of staff involvement and competence often determines the overall effectiveness of protection systems. In conclusion, it is asserted that achieving reliable protection of personal data requires not only compliance with formal requirements but also continuous monitoring, staff training, and proactive measures against emerging types of attacks. This article is intended for information security professionals, as well as managers and specialists responsible for safeguarding confidential data in organizations operating within digital ecosystems and facing threats of personal data breaches.

Keywords: risk management, digital ecosystems, personal data, information security, international standards, legal regulation, cyber intelligence, human factor.

1. Introduction

The modern era witnesses the emergence of a new type of economy—the digital economy—built on the foundation of digital ecosystems. A digital ecosystem is a seamless digital environment comprising proprietary and partner services of a company. The ecosystem's services operate in various market segments, including e-commerce, foodtech, DIY, e-health, fintech, and others. Contemporary digital ecosystems, which encompass cloud services, the Internet of Things, big data, and distributed platforms, introduce specific risks to the confidentiality and integrity of personal data. In the business environment, the development of ecosystems is one of the key trends. Simultaneously, the rapid advancement of digital technologies, the widespread adoption of mobile devices, and the Internet have transitioned ecosystems into an online mode of operation.

The relevance of this topic is underscored by the rapid growth in the volume of processed information and the increasing number of cyberattacks aimed at unauthorized access to confidential data. Compliance with legal regulations and standards alone does not always ensure adequate protection, as innovative technologies rapidly transform the threat landscape.

The objective of this study is to systematize existing approaches to managing the risks of personal data breaches and to identify key methodological and practical solutions that enhance the reliability of protection mechanisms within digital ecosystems.

2. Materials and Methods

This study is based on an analysis of theoretical materials, including regulatory acts, national and international standards, and scientific publications by domestic and foreign authors addressing the challenges of managing personal data breach risks. The primary focus is placed on reviewing approaches to the development, implementation, and enhancement of protection mechanisms in digital ecosystems.

The following served as the main sources:

1. The regulatory framework governing the processing and protection of personal data, including widely recognized US federal laws (such as the Privacy Act of 1974, Electronic Communications Privacy Act, Health Insurance Portability and Accountability Act, Gramm-Leach-Bliley Act) [1], and also relevant industry recommendations.
2. International standards in the field of information security, in particular ISO/IEC 27001 and ISO/IEC 27701 [2; 3].
3. Scientific articles and reviews published in peer-reviewed journals (including those indexed in Scopus, Web of Science, IEEE Xplore), which consider both fundamental aspects of risk management and specific applied solutions for the protection of personal data in various industries [4–10].

The following methods were used to identify relevant sources:

1. Bibliographic search in electronic catalogues of scientific libraries and databases (eLibrary, Web of Science, Scopus, IEEE Xplore, SpringerLink), as well as in registers of international standards (ISO, IEC, BSI, etc.).
2. Content analysis of the selected materials in order to identify key approaches to assessing and reducing the risks of personal data leakage, technical and organizational solutions, as well as the specifics of their application in various digital ecosystems.
3. Comparative analysis of risk management methodologies (OCTAVE, CRAMM, ISO/IEC 27005, etc.) discussed in foreign works, considering industry factors (e.g. healthcare, finance, industrial applications, IoT environments).
4. Systematization of the obtained data to form a holistic view of current trends, problems and best practices in the field of personal data leakage risk management.

Table 1 below provides a general overview of the key regulations and standards referred to in the article.

Table 1 - Basic Regulations and Standards in the Field of Personal Data Protection (Source: compiled by the author based on original research)

Document/Standard	Country or Region	Brief Description	Year of Adoption (Latest Revision)
ISO/IEC 27001:2022 [1]	International (ISO/IEC)	Specifies requirements for information security management systems (ISMS), including risk management processes and	2022

		controls to ensure data security.	
ISO/IEC 27701:2019 [2]	International (ISO/IEC)	Expands ISO/IEC 27001 and 27002 to include personal information management systems (PIMS), providing recommendations for preventing personal data breaches.	2019
GDPR (General Data Protection Regulation)	European Union	EU regulation on personal data protection, introducing strict breach notification requirements and heavy fines.	2018
CCPA (California Consumer Privacy Act) [3]	United States (California)	U.S. law providing residents of California with rights to access, delete, and control personal data, including obligations for businesses to ensure transparency.	2018 (latest updates in 2020)
NIST Privacy Framework (Version 1.0)	United States	U.S. framework offering a set of guidelines to help organizations manage privacy risks while aligning with global standards and regulations.	2020
HIPAA (Health Insurance Portability and Accountability Act)	United States	Sets national standards for the protection of health information, including privacy, security, and breach notification rules for covered entities.	1996 (latest updates in 2021)

All conclusions are therefore based on the synthesis and interpretation of published materials, which enabled the identification of both universal and specific aspects of the topic. This approach provides a comprehensive understanding of existing concepts, evaluates their applicability in different contexts, and formulates practical recommendations for improving the efficiency and reliability of personal data protection systems in modern digital ecosystems.

3. Results

Analysis of theoretical sources and the regulatory framework has shown that the foundation of legal regulation for the processing and protection of personal data in the United States is formed by federal laws, including the Privacy Act of 1974, the Electronic Communications Privacy Act, the Health Insurance Portability and Accountability Act, and the Gramm-Leach-Bliley Act [1]. These acts require organizations that handle personal data to implement technical and organizational measures based on risk assessment, as well as to conduct regular internal security audits. Without considering these key regulatory instruments, it is impossible to establish a comprehensive personal data protection system: these laws set forth fundamental principles, obligations, and responsibilities for operators, regulate the procedure for responding to information security incidents, and establish requirements for notifying the relevant authorities in the event of critical breaches.

Further research has shown that the cornerstones of international best practices in information security are the ISO/IEC 27001 [2] and ISO/IEC 27701:2019 [3] standards. The first describes the structure and main requirements for Information Security Management Systems (ISMS), emphasizing a formalized risk management process (identification of critical assets, determination of vulnerabilities, and selection of mitigation measures). In practice, organizations that have implemented this standard's requirements are better prepared to prevent unauthorized access to personal data because they regularly update their security policies to account for new types of attacks. ISO/IEC 27701:2019 [3], in turn, extends the existing ISO/IEC 27001 and 27002 standards by focusing on privacy issues (Privacy Information Management System, PIMS).

Research confirms that this standard provides a clear framework of control measures and processes aimed at preventing personal data breaches, as well as helping organizations demonstrate compliance with international regulations (e.g., GDPR). A review of scientific publications has revealed modern methods and models for managing the risks of personal data breaches, especially in the context of large and distributed digital ecosystems. For instance, Alekseeva E. N. [4] underscores the importance of quantitative and qualitative assessments of threats and vulnerabilities, which include analyzing business processes and constructing detailed data flow diagrams. The author points out that correctly accounting for the points where personal data is processed and stored enables the timely implementation of preventive measures (encryption, access rights segregation, etc.). Beckers K. and Epp F. A. [6] propose a "dynamic" approach to risk management (Data-Driven Risk Management), which involves systematically collecting and analyzing large datasets for continuous monitoring of the information environment. This approach makes it possible to promptly adjust security policies when new vulnerabilities are identified and to use specialized algorithms for recognizing anomalies in network traffic or database queries.

Solutions designed for big data play a crucial role in digital ecosystems. For example, Kshetri N. [9] argues that traditional, static risk management models are poorly suited to large distributed platforms, where personal data may be processed simultaneously across numerous servers and services. A more flexible approach considers vulnerabilities at each stage of the data lifecycle—from initial collection to archiving—and requires the implementation of end-to-end protection mechanisms (regular cryptographic checks, network segmentation, user role management). Kim M.'s [8] research, focused on digital healthcare, confirms the effectiveness of such a comprehensive approach. The healthcare industry is characterized by highly sensitive data (patient medical records), which is not only critical in terms of confidentiality but also subject to additional legal regulations. Consequently, proactive monitoring of all transactions, strict authentication, and mandatory encryption of communication channels are highly effective in reducing the risk of unauthorized access.

Further examination of international methodologies, presented in the works of Nemchenko A. S. and Garmash V. V. [10], has revealed a trend toward formalizing the protection process. On the one hand, strict adherence to internal regulations and standards may create additional bureaucratic hurdles and slow the adoption of new technologies. On the other hand, it provides more detailed instructions and requirements for security measures, monitoring procedures, and incident response. Most often, a model is used in which all information security events flow into a single center (SIEM), allowing for rapid response to anomalies. When analyzing risks in the Internet of Things (IoT) environment, especially against the backdrop of rapidly developing 5G networks, research by Ali S. and Islam M. [5] highlights the importance of unified approaches to encryption and key management. The authors point to the historical issue of "insufficient protection" of many IoT devices: in scenarios where data may pass through dozens of intermediary nodes, the risk of breaches increases at the weakest link. To counter these threats, they propose a comprehensive approach that includes mandatory encryption of data and control commands, multi-factor user authentication, and centralized patch management systems to quickly address firmware vulnerabilities. This approach is particularly relevant for organizations running complex IoT ecosystems, ranging from smart cities to high-tech manufacturing complexes (Industry 4.0).

Dehghantanha A. et al. [7] examine a "cyber threat intelligence" (CTI) approach, which involves collecting and analyzing information on current threats (including those in the dark web and underground forums). In this context, the risk-oriented strategy is enhanced by red team mechanisms that simulate attacker behavior and blue team mechanisms responsible for infrastructure defense. This dual approach helps assess an organization's actual resilience against modern attacks. In a rapidly changing threat landscape, proactive monitoring and prompt penetration testing make it possible to detect vulnerabilities before incidents occur and to take timely measures. This is especially important for large distributed ecosystems with numerous

proprietary and third-party services, which often include “gray zones”—nodes or applications insufficiently monitored by security teams.

Thus, the research findings indicate that the most effective approach to managing the risk of personal data breaches is a comprehensive and continuous strategy that combines legislative requirements, international standards, and modern scientific developments. First, merely formal measures aimed at complying with widely recognized U.S. laws (e.g., the Privacy Act of 1974, HIPAA, GLBA) and international standards (ISO/IEC 27001) do not guarantee data security. The key to success lies in regularly adapting security policies to evolving conditions, such as new technologies and threats. Second, ISO/IEC 27701:2019 [3] and leading studies [4–10] confirm that formalizing data management processes throughout the entire lifecycle (collection, storage, processing, archiving, and deletion) significantly reduces the risk of breaches. This requires both technical solutions (encryption, SIEM, DLP, IDS/IPS) and organizational mechanisms (access control policies, employee training, regular audits), as well as proactive tools (cyber intelligence, stress testing). Third, it is crucial to consider the unique features of each digital ecosystem, whether it be big data platforms, IoT infrastructures, cloud services, or healthcare systems. In practice, there are no universal “recipes,” and each industry has additional legal requirements for personal data protection (e.g., GDPR in the EU, HIPAA in the U.S.). Finally, the “human factor” remains one of the main causes of security breaches. The most advanced information security tools can prove useless if employees are unaware of the importance of compliance or fail to follow basic rules. Therefore, all authors [4–10] emphasize the culture of information security, maintained through regular training, testing, and strict access control policies.

As a result of this research, Table 2 presents the key measures for protecting personal data:

Table 2 - Basic Measures to Protect Personal Data at Various Stages of the Life Cycle (Source: compiled by the author based on original research)

Lifecycle Stage	Key Risks	Recommended Protective Measures
Collection	— Unauthorized or excessive data collection	— Minimize the amount of data collected
	— Data source falsification	— Verify the legitimacy of the source
		— Obtain user consent in compliance with the law
Transmission	— Data interception	— Use encryption (TLS/SSL, VPN)
	— Packet spoofing or MITM attacks	— Implement secure transmission protocols (HTTPS, SFTP)
		— Authenticate connections
Storage	— Unauthorized access to databases	— Encrypt storage systems (AES, RSA, etc.)
	— Leaks during backups	— Restrict and differentiate access rights (RBAC)
		— Conduct regular backups protected against unauthorized access
Processing	— Improper use of data	— Implement formalized security policies
	— Errors in business processes	— Deploy SIEM/DLP systems to monitor user actions
		— Maintain operation logs and conduct regular

		audits
Archiving	— Errors in long-term storage	— Encrypt archives
	— Leaks through outdated media and archives	— Control retention periods according to legal requirements
		— Ensure secure destruction or deletion of data after expiration
Deletion	— Recovery of deleted data	— Physically destroy media (if necessary)
	— Breaches during disposal of media	— Irrevocable data wiping
		— Document the destruction process

This table outlines the essential measures to ensure the security of personal data throughout its lifecycle, addressing risks at each stage and providing recommendations to mitigate potential breaches effectively. The study also presents a diagram illustrating the process of a "continuous" (cyclical) risk management model in digital ecosystems, where an organization regularly reviews and updates protective measures in accordance with emerging technologies and threats (Figure 1).

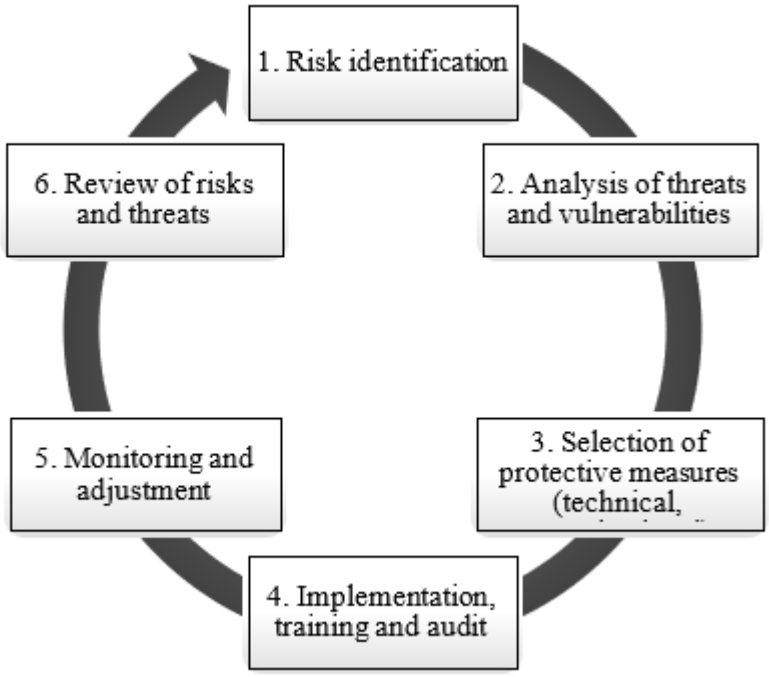

Figure 1 – Simplified Scheme for Continuous Risk Management of Personal Data Leakage

(Source: compiled by the author based on original research)

In summary, the results of the analysis demonstrate significant progress in the scientific and practical understanding of personal data protection challenges in digital ecosystems. The extensive range of considered models (from classical OCTAVE and CRAMM to the latest CTI solutions) and tools (from SIEM and DLP to AI-based predictive analytics systems) allows for the selection of optimal strategies tailored to specific conditions and objectives. At the same time, the core principle remains one of systemic and continuous action: only through the consistent consideration of emerging threats, regular updates to employed tools, and maintaining the overall competence of all personnel can the risks of personal data leakage be significantly minimized.

4. Discussion

In the context of digital ecosystems, where the volume and value of processed personal data are continuously growing, managing the risks of data breaches takes on strategic importance. An analysis of the literature and regulatory documents shows that creating an Information Security Management System (ISMS) that merely complies with legal requirements does not guarantee effective protection. Combining widely accepted legal frameworks (e.g., HIPAA in the U.S. or GDPR in the EU) with the implementation of international standards (ISO/IEC 27001, 27701) provides a methodological foundation and a "minimal level of security." However, practical experience demonstrates that many serious incidents occur in organizations that formally meet these requirements yet fail to adapt their internal risk management processes to a rapidly changing environment.

The research results highlight that traditional methodologies (OCTAVE, CRAMM, etc.) and approaches from ISO/IEC 27005 were primarily developed for relatively static IT systems. Contemporary digital ecosystems, on the other hand, are complex, heterogeneous platforms with numerous external integrations, technology stacks, and cloud services. Risk management must be adaptive and proactive, continuously gathering data on new vulnerabilities, leveraging big data to assess threat levels, and regularly revising protection strategies. A separate emphasis is placed on end-to-end protection at all stages of the personal data lifecycle (collection, transmission, storage, processing, disposal/archiving). Many studies note that focusing on just one aspect—e.g., encryption only during storage—does not solve the problem if vulnerabilities exist in business processes, cloud service configurations, or user awareness. Nearly all authors point out the dominant role of the human factor: improper access rights configuration, weak passwords, and delayed system updates can negate even the most advanced technical measures. Another important aspect of the discussion is industry specificity. Risk management in digital healthcare requires not only high standards of confidentiality and adherence to local laws but also the formalization of procedures at the level of clinical protocols and medical ethics. IoT systems in industry require mechanisms for quick firmware updates, comprehensive encryption key management, and physical access controls to equipment. This underscores the fact that there is no universal "security recipe": each ecosystem—whether in education, healthcare, industry, or finance—imposes its own constraints and requirements.

Given these complexities, researchers propose using risk management models based on real threat and vulnerability data (CTI), regularly conducting penetration tests, and employing simulation attack mechanisms (Red/Blue Team). These proactive methods have a significant advantage in helping to prevent incidents rather than just responding to them after the fact. However, for many organizations—especially smaller ones—such a high level of technology remains out of reach due to limited resources and a shortage of qualified personnel.

Another major topic of discussion is the depth of integration of technical tools (SIEM, DLP, IDS/IPS) into business processes. On the one hand, automation and AI-based algorithms increase the efficiency of threat detection [10]. On the other hand, security fatigue (alert fatigue) and a surge in false positives can lead to the opposite effect. Moreover, deploying expensive tools without adequate staff training and clearly defined roles can result in chaos and actually increase the risk of mistakes. Finally, there is a pressing question about balancing security with business efficiency. Excessive control measures can slow down operations, prompting employees to circumvent cumbersome regulations and thereby creating vulnerabilities. The challenge for specialists is to find the optimal balance between the level of security and the convenience of business processes.

5. Conclusion

The analysis demonstrated that managing the risks of personal data breaches requires a comprehensive approach that combines a legal framework, compliance with international standards, and dynamic methods for threat monitoring.

The legal foundation and regulatory acts governing personal data protection in the public sector play a key role in ensuring information security and the confidentiality of citizens' data. One of the primary legislative instruments is represented by international regulations and widely recognized laws, such as the General Data Protection Regulation (GDPR) in the EU or the Privacy Act of 1974 in the United States, which establish principles and rules for collecting, storing, and processing personal data.

It is particularly important to consider the specific characteristics of various industries and technologies, involving all organizational levels in the process. Universal technical measures (encryption, SIEM, DLP, IDS/IPS), combined with organizational tools (formalized regulations, staff training, audits), are most effective when paired with proactive vulnerability analysis and cyber threat intelligence. Such an integrated and continuous risk management mechanism minimizes the likelihood of data breaches, strengthens trust in digital services, and maintains a high level of information security.

As a solution to the challenge of ensuring personal data protection, it is necessary to improve the knowledge of employees in all companies that process personal data regarding information security threats, methods for recognizing them by primary indicators, and ways to counteract them. This is critical since the dependency of information security on human factors remains significant.

References

1. Privacy Act of 1974 (5 U.S.C. § 552a), Electronic Communications Privacy Act (18 U.S.C. §§ 2510–2523), Health Insurance Portability and Accountability Act (Pub. L. No. 104-191) и Gramm-Leach-Bliley Act (Pub. L. No. 106–102).
2. ISO/IEC 27001:2022. Information security, cybersecurity, and privacy protection — Information security management systems — Requirements. Geneva: International Organization for Standardization, 2022.
3. ISO/IEC 27701:2019. Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. URL: https://www.iso.org/standard/71670.html (дата обращения: 25.12.2024).
4. Alekseeva E. N. Digital ecosystems and risk management for personal data protection // Journal of Information Security. – 2020. – No. 3. – Pp. 31–41. URL: https://www.jinfsec.org/articles/digital-ecosystems-and-risk-management (дата обращения: 25.12.2024).
5. Ali S., Islam M. A comprehensive approach to personal data protection in digital ecosystems based on the Internet of Things // IEEE Access. – 2021. – Vol. 9. – Pp. 12345–12357. DOI: https://doi.org/10.1109/ACCESS.2021.3058234.
6. Beckers K., Epp F. A. Data-driven risk management in modern IT environments // Computers & Security. – 2021. – Vol. 102. – Article No. 102117. DOI: https://doi.org/10.1016/j.cose.2020.102117.
7. Dehghantanha A., Conti M., Dargahi T. Cyber threats: Implementing a risk management approach to data protection in digital ecosystems // IEEE Systems Journal. – 2019. – Vol. 13, No. 2. – Pp. 1818–1829. DOI: https://doi.org/10.1109/JSYST.2018.2866925.
8. Kim M. Risk management approach to personal data leakage in digital health ecosystems // Healthcare Informatics. – 2020. – Vol. 26, No. 2. – Pp. 99–108. DOI: https://doi.org/10.4258/hir.2020.26.2.99.
9. Kshetri N. Privacy and security issues in big data ecosystems // Journal of Big Data. – 2021. – Vol. 8, No. 1. – P. 4. DOI: https://doi.org/10.1186/s40537-021-00409-9.

10. Nemchenko A. S., Garmash V. V. Models and methods for managing personal data leakage risks in the context of digitalization // Issues of Cybersecurity. – 2022. – No. 5. – Pp. 45–54. URL: https://cybersecjournal.ru/.