ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 05,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

REQUIREMENTS FOR PROTECTING THE PERSONAL DATA OF NETWORK USERS

Rustamov Alisher Bahodirovich
Associate Professor, University of Information Technologies and Management

Annotation: In today's digital age, technological advancements have penetrated almost every aspect of our lives and play a significant role in increasing the efficiency of human activities. In particular, the internet offers a wide range of services such as communication, online commerce, education, and information sharing, making life more convenient and connected. However, while these digital services provide numerous advantages to users, they also introduce serious risks related to the protection of personal data. Personal data includes information such as a user's name, surname, date of birth, residence address, phone number, email address, and financial details. If such sensitive data is misused or accessed by unauthorized parties, it can lead to various types of harm or exploitation. Therefore, ensuring data security in the digital environment and protecting users' personal information have become critical and urgent issues. This article explores the key requirements, international standards, and modern approaches related to safeguarding personal data of internet users. It also highlights various cybersecurity policies and outlines practical steps that users themselves should follow to minimize the risk of data breaches. By understanding and implementing these protective measures, users can engage with the digital world in a more secure and reliable manner.

Keywords: Information Technologies, Information Systems, Information Confidentiality, Personal Data, Digital Technologies, Internet, Data Security, Encryption, Security Protocols

In the current era, characterized by the rapid and relentless development of information and communication technologies, safeguarding personal data belonging to each individual from cyber threats has become an increasingly critical priority. Protecting such data from unauthorized access, misuse, and malicious exploitation demands much greater attention and effort than ever before. The continuous advancement of digital technologies has significantly elevated the importance and value of personal information for individuals, organizations, and society as a whole. Alongside this, however, concerns and anxieties surrounding the management, privacy, and security of personal data have also escalated dramatically.

As these concerns intensify, it becomes progressively more challenging for individuals to maintain effective control and oversight over their personal information. Factors such as the widespread collection, processing, and sharing of data by multiple digital platforms complicate personal data management, making it harder for users to protect their privacy. Furthermore, international legal frameworks and national legislations provide individuals with the right to access, search, store, disseminate, and utilize information freely, which, while vital for transparency and freedom of information, simultaneously adds complexity to the challenge of safeguarding data privacy.

The growing globalization and interconnectedness of information systems have led to increased interest and focus on addressing data privacy concerns worldwide. Numerous scientific studies and practical investigations have been undertaken to analyze the problem from various perspectives. These efforts have highlighted the urgent need to develop robust and effective mechanisms to protect personal information in the digital environment. Initially, research efforts focused mainly on establishing regulatory frameworks and legal standards designed to govern data privacy. However, these mechanisms often overlooked the influence of

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 05,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

external factors such as technological innovations, cross-border data flows, and differences in cultural or legal interpretations between countries. As a consequence, a variety of data confidentiality issues have emerged, varying widely among nations and regions simultaneously.

To effectively resolve these multifaceted challenges, it is imperative to develop comprehensive requirements and standards that ensure data security in digital technologies. Such requirements should address not only technical aspects but also legal, organizational, and ethical dimensions of personal data protection.

Table 1

Requirements for Ensuring the Security of Personal Data When Using Digital Technologies

Encryption and security protocols	When transmitting digital data, encryption protocols (such as SSL/TLS) are required. These protocols encrypt data and provide security during transmission.
Secure passwords and authentication	Users are required to create secure passwords and use authentication methods. Secure passwords should be strong and random, and users should be given the opportunity to update their passwords regularly. Authentication methods ensure that the user is authenticated by entering the user's ID and the correct password.
Collect data to a minimum	Digital platforms and service providers are required to use personal data only for the purposes for which it was collected. This requirement requires the user to give consent and requires them to provide information about the purposes for which the user's data is collected and how it will be used.
Data retention, expiration and deletion	Digital platforms are required to specify how long they must retain and delete personal data after it has been transferred. The data must be deleted after a specified period of time has passed since the transfer.
Security check and changes	Digital platforms and service providers are required to establish monitoring and security assurance systems for security audits and updates. These systems should be responsible for protecting data from misuse through false settings or documentation, from inaccuracies and attacks, and from errors in data documentation.
Legal basis for the protection of personal data	Organizations using digital technologies are required to comply with legal requirements and legal frameworks for the protection of personal data. Implementations such as granting user permissions, data protection, data transfer and setting terms of use must meet legal requirements.
Educating users on security settings	Digital platforms and service providers are required to help users learn about security settings and configure them correctly. Users should be provided with information about security settings, such as learning about security settings, protecting their passwords, being vigilant against attacks and errors, collecting and using data correctly, and using systems to protect against attacks.

Personal data refers to any information related to individuals that is transmitted or stored through the internet, computers, mobile devices, personal documents, and other electronic equipment. Such data may include, but is not limited to, a person’s full name, date of birth, residential address, phone number, email address, bank account details, passport information,

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 05,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

and other similar personal identifiers. These pieces of information can be used to identify a specific individual and therefore require careful handling to ensure their security. The security of personal data encompasses the protection of these details during their collection, transmission, storage, and access by authorized or unauthorized parties. This involves implementing various security measures and protocols to prevent data breaches, unauthorized disclosure, and misuse. Common practices to safeguard personal data include encrypting sensitive information, protecting access with strong passwords, and utilizing security protocols designed to secure data flows.

Additionally, maintaining the integrity and confidentiality of personal data often involves thorough verification processes, documentation controls, and monitoring mechanisms. These steps ensure that personal data is only accessed by authorized individuals under appropriate conditions, thus preserving individuals' privacy and preventing identity theft or fraud. Overall, the safeguarding of personal data is a critical aspect of modern information security practices, given the increasing volume of data being generated and shared across digital platforms.

When utilizing digital technologies, it is crucial to follow several important recommendations to ensure the security and protection of personal data:

- Use strong and unique passwords. Passwords should be at least eight characters in length and include a combination of lowercase letters, uppercase letters, numbers, and special symbols. This complexity helps to prevent unauthorized access by making passwords difficult to guess or crack.
- Implement two-factor authentication (2FA). Two-factor authentication adds an extra layer of security by requiring a second form of verification beyond just the password. Common methods include receiving a code via SMS, using dedicated authentication apps, or biometric verification. This approach significantly reduces the risk of unauthorized account access.
- Employ encryption tools. Encryption is a vital technique that protects data by encoding it during transmission and storage. By using encryption protocols, sensitive information is rendered unreadable to anyone without the appropriate decryption key, thereby safeguarding data from interception or unauthorized viewing.
- Regularly review and update security settings. It is essential to periodically check the security configurations on your operating systems, applications, and web browsers to ensure they are up-to-date and properly configured. These settings often include privacy controls, firewall rules, and permissions that help prevent vulnerabilities.
- Share personal information only on official and trusted websites. Always verify the URL of websites before submitting any personal data, ensuring that the web address begins with "https://" and employs secure communication protocols such as SSL/TLS. This helps confirm the authenticity of the site and that data is transmitted securely.
- Provide your personal data to organizations, websites, or applications solely for necessary and legitimate purposes. Avoid oversharing or submitting information to unverified sources, thereby minimizing the risk of data misuse or leakage.
- Store personal data correctly and securely. Personal data should be saved primarily in secure databases or encrypted storage locations. When processing data temporarily during operations, ensure it is handled with adequate protections to prevent accidental exposure.
- Distribute data carefully and responsibly. When sending personal information, use secure communication channels and verify that data is transmitted only to intended and

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 05,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

authorized recipients. This practice reduces the chance of data being intercepted or sent to incorrect parties.

- Properly dispose of personal data when no longer needed. To protect against risks such as data breaches, phishing attacks, or identity theft, personal data should be irreversibly deleted or destroyed once its purpose has been fulfilled.
- Permanently erase personal data from reviewed files, obsolete devices, or discontinued services. This involves clearing data from storage media and ensuring that residual information cannot be recovered by unauthorized individuals or software.

Following these guidelines helps maintain the confidentiality, integrity, and availability of personal data in the digital environment, thereby protecting individuals' privacy and enhancing overall cybersecurity.

Recommendations and Suggestions	Description and Reasons
1. Make strong and unique passwords a habit	Use unique, complex passwords for each account, with at least 8 characters including uppercase, lowercase, numbers, and symbols, to reduce hacking risks.
2. Enforce two-factor authentication (2FA)	Add an extra layer of protection to accounts by requiring a second verification step such as SMS codes or authentication apps, preventing unauthorized access.
3. Widely implement data encryption technologies	Protect the confidentiality of data during transmission and storage by encrypting it, minimizing the risk of hacking and data theft.
4. Regularly update and review security settings	Continuously monitor and update system and software security settings to fix vulnerabilities and enhance protection.
5. Provide personal data only through trusted and official websites	Verify website authenticity and use only secure platforms to avoid phishing, fraud, and data theft.
6. Share personal data only for necessary purposes and avoid excessive use	Limit data sharing to legitimate and essential reasons to prevent misuse or overexposure of personal information.
7. Establish secure and organized data storage practices	Use secure databases or encrypted storage solutions to protect data from theft, loss, or unauthorized access.
8. Use secure communication channels and verify recipients when sharing personal data	Ensure data is transmitted only to intended and authorized parties to avoid interception or accidental disclosure.
9. Safely delete unnecessary or outdated data	Permanently erase data to prevent recovery and reduce the risk of breaches or identity theft.
10. Fully remove personal data from obsolete devices and services	Completely clear all data from old devices or discontinued services to prevent data recovery or unauthorized access.

By following these recommendations, you can significantly improve the security and privacy of your personal information.

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 05,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

Protecting personal data is one of the most critical tasks in today's digital environment. Strong passwords and two-factor authentication effectively safeguard accounts from unauthorized access. Encryption and regularly updating security settings help ensure the confidentiality of sensitive information. Providing data only to trusted websites and using it strictly for necessary purposes enhances overall security. Special measures must be taken to store and share personal information safely. Secure deletion of unnecessary data protects against cyberattacks and data breaches. Thus, personal data security plays a vital role in preserving privacy and preventing digital threats.

References:

1. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020.
2. Mitnick, K., & Simon, W. L. The Art of Deception: Controlling the Human Element of Security. Wiley, 2012.
3. Grimes, R. A. Cybersecurity Basics. Microsoft Press, 2019.
4. Hadnagy, C. Social Engineering: The Science of Human Hacking. Wiley, 2018.
5. Stallings, W. Network Security Essentials: Applications and Standards. Pearson, 2017.
6. Schneier, B. Secrets and Lies: Digital Security in a Networked World. Wiley, 2015.
7. Ross, S. J. Information Security Management Principles. BCS Learning & Development Limited, 2017.
8. Alsmadi, I., & Karabatis, G. Social Computing and Big Data Analytics: Security and Privacy Issues. CRC Press, 2016.
9. O'Gorman, G. Understanding Social Engineering Attacks: Defending Against Human Threats. Syngress, 2021.
10. Kaspersky Lab. "What is Phishing?" https://www.kaspersky.com/resource-center/threats/phishing
11. Symantec. Internet Security Threat Report. Volume 25, 2023.
12. Microsoft. "Protecting your account with Two-Factor Authentication". https://support.microsoft.com
13. Cisco Systems. Annual Cybersecurity Report. Cisco Press, 2023.
14. UzbekCERT. "Kiberxavfsizlik bo'yicha milliy strategiya tavsiyalari". 2024-yil.
15. Karimov, B., & Xasanov, I. Axborot xavfsizligi asoslari. Toshkent: TDYU nashriyoti, 2021.
16. Norqulov, A. Tarmoq texnologiyalari va axborot xavfsizligi. Toshkent: Innovatsiya, 2022.
17. Rustamov, A., and A. Amirov. "TARMOQLARDA AUTENTIFIKASIYA PROTOKOLLARIGA QO'LLANILADIGAN NAMUNAVIY HUJUM TURLARI." Прикладные науки в современном мире: проблемы и решения 1.31 (2022): 12-14.
18. Bahodirovich R. A. jamiyatni xabardor qilishda kiber xavfsizlikni ta'minlash //ta'limdagi zamonaviy muammolar va ularning ilmiy echimlari. – 2024. – Т. 1. – №. 2. – С. 429-431.
19. Normurodov, A. D., and A. B. Rustamov. "INTERNET-BUYUMLAR IOT AFZALLIKLARI VA XAVFSIZLIK MUAMMOLARI." INNOVATSION IQTISODIYOTNI SHAKLLANTIRISHDA AXBOROT KOMMUNIKATSIYA TEXNOLOGIYALARINING TUTGAN O'RNI 1.1 (2023).