International Journal of Innovative Technologies in Social Science

e-ISSN: 2544-9435

Scholarly Publisher
RS Global Sp. z O.O.
ISNI: 0000 0004 8495 2390

Dolna 17, Warsaw,
Poland 00-773
+48 226 0 227 03
editorial_office@rsglobal.pl

ARTICLE TITLE	THE IMPACT OF PERSONAL DATA ON MONGOLIA'S NATIONAL SECURITY
DOI	https://doi.org/10.31435/ijitss.3(47).2025.3647
RECEIVED	18 July 2025
ACCEPTED	25 September 2025
PUBLISHED	30 September 2025
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

THE IMPACT OF PERSONAL DATA ON MONGOLIA'S NATIONAL SECURITY

Munkhjargal Bayanjargal
Nomad Cyber Defense LLC, Ulaanbaatar, Mongolia

Munkhtsetseg Erdenebulgan
National Defense University, Ulaanbaatar, Mongolia

Densmaa Batbayar
University of Science and Technology, Ulaanbaatar, Mongolia

ABSTRACT

Personal data is not only a matter of citizen privacy but also a crucial resource for national security strategy and a fundamental requirement for ensuring state information security. This study explores the theoretical and practical implications of personal data breaches on Mongolia's national security, state secrecy, and the stability of its electronic infrastructure, drawing on international and domestic experiences. The research examines the enforcement of existing laws and policy documents in Mongolia and analyzes cases of data breaches in information systems critical for national security. A comparison is made between the legal and institutional frameworks for data protection in countries like the European Union, the United States, and Japan. The study highlights the importance of enhancing information security education in Mongolia, fortifying the national electronic infrastructure, and proposing enhancements to the legal framework for safeguarding personal data.

KEYWORDS

Personal Data, Cybersecurity, National Security, Data Protection Law, Mongolia

CITATION

Munkhjargal Bayanjargal, Munkhtsetseg Erdenebulgan, Densmaa Batbayar. (2025). The Impact of Personal Data on Mongolia's National Security. *International Journal of Innovative Technologies in Social Science*, 3(47). doi: 10.31435/ijitss.3(47).2025.3647

Introduction

The rapid advancement of digital transformation and information technology has elevated the importance of personal data security and value on a global scale. Personal data is now a critical strategic element impacting state systems, national security, and social stability, beyond just individual privacy and rights. Consequently, safeguarding personal data is now a crucial component of national cybersecurity.

Throughout the Covid-19 pandemic, various sectors such as banking, finance, healthcare, education, and services have significantly adopted electronic technology for their operations. This shift has led to the transition of data transmission, storage, and processing to electronic platforms. This trend has continued post-pandemic, with electronic usage becoming a regular part of daily life. While this shift has improved access to information and services, it has also created new avenues for cyber attackers to exploit sensitive data.

Personal data refers to information that can be used to identify an individual, such as their name, address, registration number, location, electronic usage history, biometric data, and health information. If this data is lost, it can lead to damage to the individual's reputation, property, life, and safety. Additionally, it can be exploited to gain unauthorized access to an organization's information system, create false records, and facilitate fraud and coercion.

Therefore, safeguarding personal data is crucial not only for protecting individual rights but also for maintaining the stability of state institutions, the integrity of the information environment, and national security.

It is essential to define key terms in this study to establish a solid theoretical foundation, ensure coherence in subsequent analyses, and maintain methodological consistency. The definitions provided are based on international standards, academic sources, and Mongolian legal documents.

a) Personal Data

Academic definition - Personal data refers to any information that can be used to identify an individual, including but not limited to their name, address, registration number, location, electronic identification, biometric data, etc.

Definition in Mongolian law - Mongolian law, personal data is defined as information such as a citizen's name, registration number, address, marital status, health status, income, and property information.

b) National Security

Scientific definition - The state of ensuring the independence, territorial integrity, stability of the state, and economic and social security of the country.

National security of Mongolia refers to the existence of favorable external and internal conditions to ensure the fundamental national interests of Mongolia.

c) Cybersecurity

International Standard Definition - Cybersecurity refers to the state and measures taken to safeguard information, systems, and networks from unauthorized access, damage, and attacks.

ENISA Definition - Cybersecurity involves protecting the confidentiality, integrity, and availability of information and services in the cyber environment.

Definition in Mongolian law - "Cybersecurity" is defined as the protection of information integrity, confidentiality, and accessibility in the cyber environment.

d) Data Weaponization

Research Definition - The manipulation of data to exert influence, cause harm, or psychologically impact political, economic, or social systems.

Study on The Impact of Status on National Security

Personal data is a crucial asset for individuals and also serves as a strategic security element for governments, organizations, and countries. It encompasses various types of information such as identification details, financial records, health records, educational history, online activities, biometric data, and images. The potential risks associated with unauthorized access, duplication, or destruction of personal data include:

Loss of personal privacy and autonomy: Unauthorized access to personal data can lead to breaches of confidentiality, reputation damage, and cyberbullying.

Heightened vulnerability to cyberattacks: Personal information can be exploited by cybercriminals for phishing attacks and credential stuffing, underscoring the importance of robust data protection measures.

Intelligence threats: Foreign intelligence agencies may leverage personal information of government officials for espionage purposes.

Manipulation of electoral processes: Utilizing user data for targeted misinformation campaigns can sow confusion and influence election outcomes.

Adverse impact on national security: Breaches involving personal data of government officials and politicians can heighten the risk of espionage activities, underscoring the need for stringent data protection policies as part of national security strategies.

Erosion of trust and e-governance: Inadequate protection of personal data can erode public trust in government institutions and online services, undermining the effectiveness of **e-governance initiatives.**

Personal data loss presents various risks not just on an individual scale, but also on organizational, state, and national levels. The numerous adverse effects of cyberbullying, intelligence exploitation, election meddling, and susceptibility to cyberattacks underscore the significance of safeguarding personal data. Consequently, the alignment and integration of elements like data protection policies, laws, technology, education, and public confidence are crucial aspects of national security. The ensuing are some instances that have impacted Mongolia's national security as a result of personal data breaches:

National data center attack (2017)

In late 2017, a Chinese hacking group known as APT27 breached Mongolia's national data center and implanted malicious code on government websites, posing a significant threat to government information security.

Criminal network operation (2019)

In 2019, Mongolian authorities conducted a special operation in Ulaanbaatar, resulting in the arrest of over 800 Chinese nationals involved in cybercrime, money laundering, and the use of counterfeit documents.

MonPass certification authority attack (2021)

Throughout 2021, Mongolia's largest certification authority, MonPass, experienced eight hacking incidents. These attacks led to the insertion of Cobalt Strike into the organization's official installer and the dissemination of malicious code to users' devices, jeopardizing information security.

Central Bank data breach (2021)

Reports emerged in 2021 of a cyberattack on the Bank of Mongolia's information system, exposing the personal data of 2.3 million Mongolian citizens and causing widespread public concern.

Khan Bank user data breach (2021)

In November 2021, it was revealed that the Khan Bank information system had been breached, resulting in the exposure of personal data belonging to 2.3 million Mongolian citizens. This significant breach affected nearly 70% of Mongolia's population, with hackers attempting to sell the compromised information.

Attack on the Ministry of Foreign Affairs website (2023–2024)

Google cybersecurity experts uncovered a cyberattack targeting Mongolian government agency websites between November 2023 and July 2024. The operation, attributed to the Russian APT29 group, utilized commercial spyware like NSO Group and Intellexa for intelligence purposes.

Vulnerabilities:

- Apple vulnerability: CVE-2023-41993
- Android vulnerabilities: CVE-2024-5274
- Google vulnerabilities: CVE-2024-5274 and CVE-2024-4671

Ministry of Defense Attack (2024)

The Chinese Red Delta group conducted cyber espionage operations targeting the Mongolian Ministry of Defense from July 2023 to December 2024. The attack utilized the PlugX backdoor malware to infiltrate the organization's systems and extract information.

Intermed Medical Data Leak (2024)

In November 2024, Intermed Medical experienced a data breach in which personal information was compromised, posing a significant threat to the security of health data.

This summary outlines the major personal data breaches in Mongolia spanning from 2017 to 2024. The incidents are classified based on the type of data compromised, the number of individuals affected, the direct financial impact, and the information sources cited from reputable international cybersecurity entities and media outlets.

Table 1. The Survey of personal data breaches in Mongolia

Year	Number of cases	Number of victims	Type of data lost	Economic loss (₮)	Source
2017	1	100,000	PII, government systems	120,000,000	Kaspersky, Cyberscoop (APT27 attack, 2017)
2019	1	800	PII, international crime	50,000,000	Independent UK (Chinese crime network in Mongolia, 2019)
2021	3	2,300,000	PII, banking, government systems	3,000,000,000	Tadviser, Security Affairs, Reddit (MonPass, Khan Bank, Bank of Mongolia, 2021)
2024	2	50,000	Health information	500,000,000	HackNotice (Intermed Hospital, 2024), Google TAG (APT29, Ministry of Foreign Affairs, 2024)

According to the data, the first major recorded breach in 2017 was an APT27 cyberattack, which resulted in the loss of 100,000 citizens' PII (Personal Identifiable Information) from government information systems. This was followed by a case involving an international criminal network in 2019, with relatively few victims (800), but the nature of the crime indicated the level of threat across national borders.

2021 saw the most extensive breach in the history of Mongolian information security, with a total of 2.3 million user data (bank customers, government system users, and e-signature service users) lost, resulting in

direct economic losses of 3 billion tugriks. This was due to the simultaneous attacks on domestic e-signature platforms (MonPass), commercial banks (Khan Bank), and the Bank of Mongolia. Two major incidents were recorded in 2024, including a health data breach (Intermed Hospital) and an APT29 cyber-espionage attack targeting a government foreign relations agency. These trends indicate that cyberattacks are becoming increasingly professional and targeted. ***Key characteristics of these incidents are:***

1. PII and sensitive data are the primary types of data compromised.
2. Targeted attacks (APTs) are increasing.
3. Economic impact is not directly correlated with the number of victims, underscoring the challenge of assessing the value of data.

The study examines data breaches in organizations handling personal data from 2017 to 2024, comparing the number of breaches in public and private sectors and the average annual percentage relative to other nations.

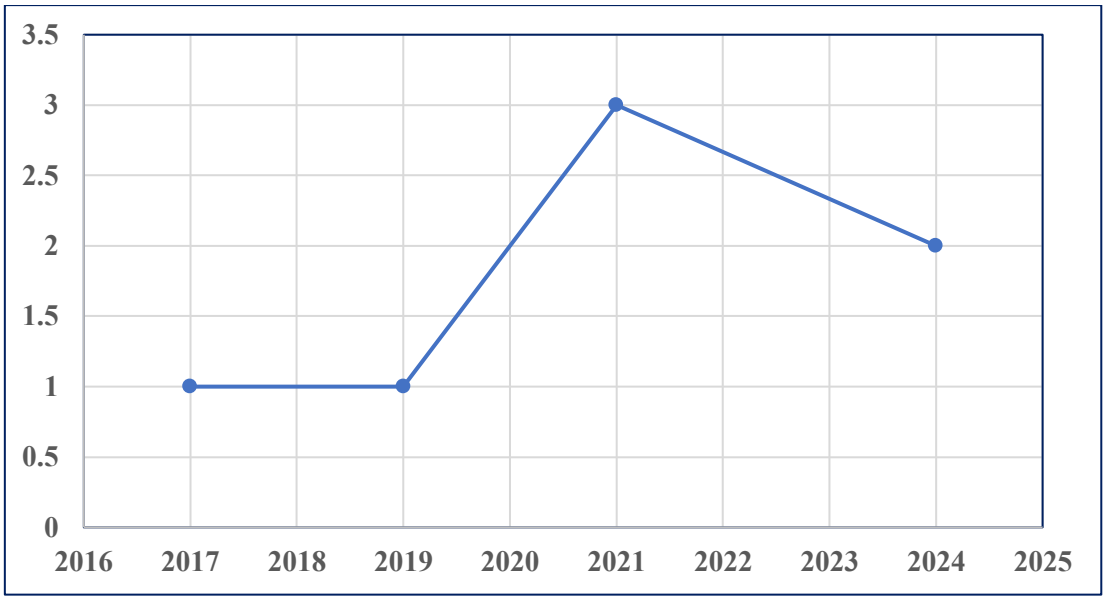

Fig. 1. *Data breaches in organizations utilizing personal data in Mongolia*

As illustrated in Chart 1, the significant rise seen in 2021 was a result of attacks aimed at major financial and government institutions.

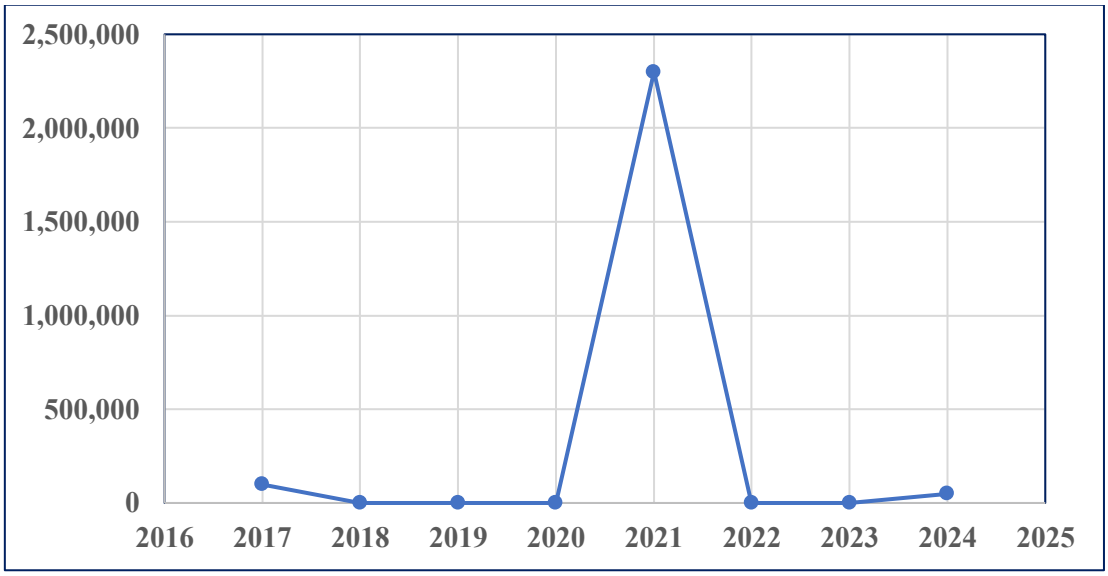

Fig. 2. *Personal data breaches reported by public and private organizations*

Chart 2 illustrates the frequency of personal data breaches in both public and private sector organizations. In public organizations, the attacks are typically politically or intelligence-driven, resulting in significant data loss in a single incident. Conversely, breaches in private organizations are often motivated by financial gain, leading to numerous smaller incidents. This discrepancy is attributed to insufficient information security measures in public organizations, while the ongoing risk of cyberattacks remains high in private organizations.

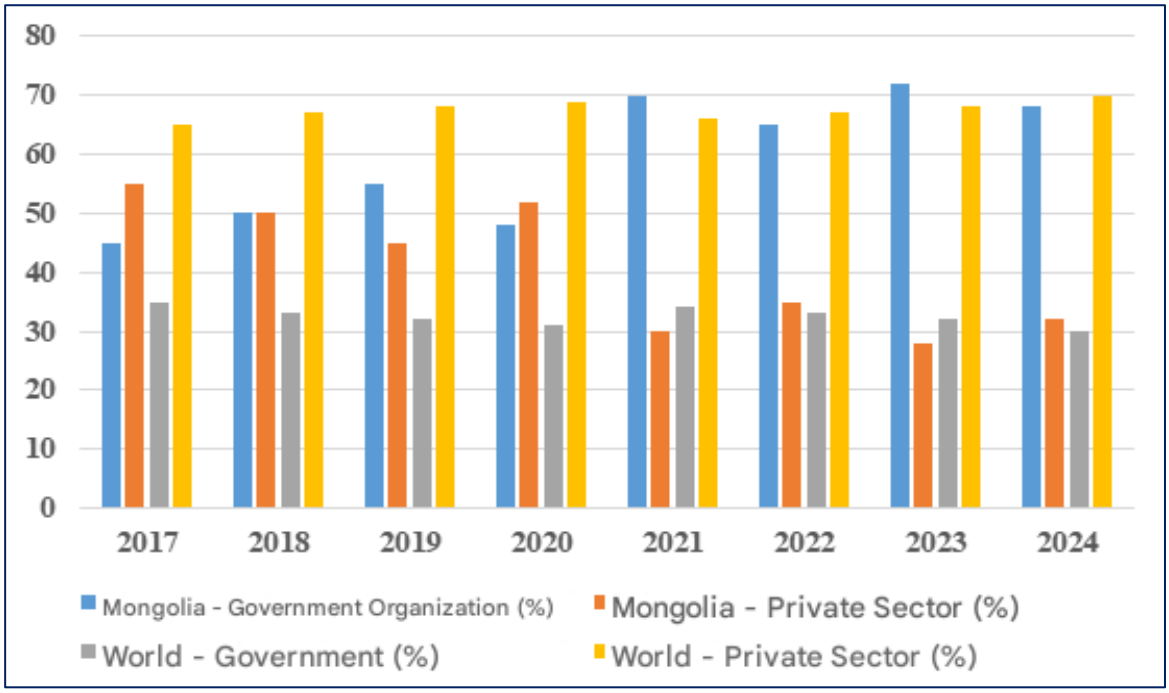

Fig. 3. *The average annual percentage of personal data lost by public and private organizations in comparison to other countries.*

Chart3 illustrates that the rate of personal data breaches in government organizations in Mongolia is notably higher than the global average. Between 2017 and 2024, the average annual data breach rate for government organizations in Mongolia was 60.4%, compared to the global average of 32.5%. In contrast, private sector organizations in Mongolia had an average rate of 39.6%, lower than the global average of 67.5%. This deviation from the international norm, where the private sector is typically more susceptible to attacks, suggests that government information systems in Mongolia are not only prime targets for cyberattacks but also have weaker security measures in place.

The relatively lower level of data protection in private sector organizations compared to global standards may be attributed to the scale of their data storage and the specific targeting by international cybercriminals. These disparities highlight the necessity for government agencies in Mongolia to enhance their information security strategies, implement dual protection mechanisms, and align their legal framework for personal data protection with international standards.

Mongolia has laws and policies in place concerning personal data, including the “Law on Personal Privacy” (1995), the “Law on Electronic Signatures” (2011), the “Law on Electronic Security” (2022), and the “Policy on Electronic Development and Information Security (2022–2030).” While these regulations offer some guidelines for data protection, there is a lack of detailed classification of personal data and mechanisms for authorized use. Additionally, Mongolia lacks an independent regulatory body, faces weak implementation control, inadequate information education for citizens, and the legal framework does not align with international standards like the GDPR. ***Some examples of countries with different data protection laws include:***

- European Union (GDPR): known for having the highest standard of data protection law, with strict fines for violations and a focus on user consent.
- Japan (APPI): places responsibility on data processing organizations and has an independent regulatory body (PPC).

- United States (CCPA, HIPAA): relies on industry-level regulations, with the private sector setting its own data protection standards.

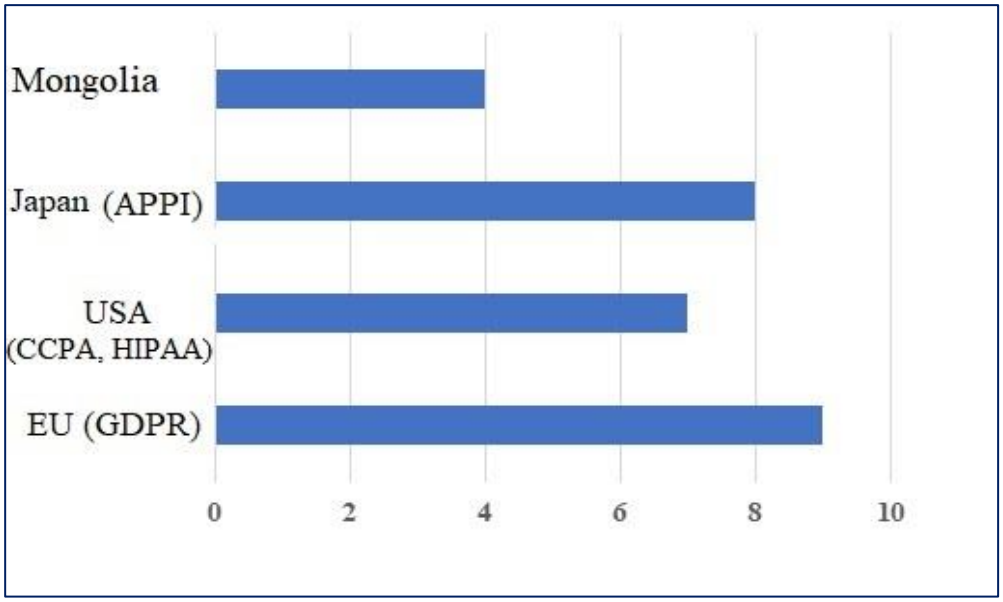

Fig 4. *Comparison of enforcement of data protection laws*

A study compared the enforcement of data protection laws in the European Union, the United States, Japan, and Mongolia on a 10-point scale. Chart 4 indicates that Mongolia may need legal reforms to align with international standards. This comparison clearly shows the necessity of updating Mongolia's data protection laws, enhancing their enforcement, and bringing them in line with global norms. It also underscores the importance of strengthening institutional supervision and the mechanisms for safeguarding individuals' data rights to enhance the efficiency of law enforcement.

Emerging Threat Trends Impacting Mongolia's National Security

In Mongolia, the loss of personal information has been shown to indirectly affect national security through various real-life incidents and attacks. As a result, there is a growing necessity to analyze emerging threat patterns that could jeopardize Mongolia's national security to proactively prevent and minimize the consequences of novel cyber attacks and information threats in the Table 2.

Table 2. Summary of actual instances of contemporary cyberattacks documented globally (2016–2025) future.

No	Type of danger	Brief description of the main mechanism	International examples	Exposure in Mongolia	Policy direction	Source
1	Deepfake	Content that uses deep learning to create realistic images and sounds	The spread of deepfake before the elections in the EU	Increasing spread on social media, risk to information trust	Source verification, forensics, annotation, information literacy	BBC News. (2023). Deepfake videos circulating ahead of European elections. BBC News.
2	AI-based attacks	Phishing, login automation, and sensitive searches	Results that pass the AI-phishing filter with high probability	The rise of language-specific targeted phishing	DMARC/SPF/ DKIM, behavioral detection, training, AI usage policy	IBM Security X-Force. (2024). Threat Intelligence Index 2024. IBM.

3	Supply chain	Attack entry via third-party channel	SolarWinds incident	Increasing dependence on cloud services and external development	SBOM, contract requirements, continuous monitoring, signature updates	Cybersecurity and Infrastructure Security Agency (CISA). (2021). Supply-chain compromises: Guidance for organizations. CISA.
4	IoT threats	Attack channels due to weak authentication and lack of segmentation	International real cases are popular	Open access to cameras and sensors has occurred.	Segmentation, encryption, access control, and update management	US CISA report warns of DDoS threat caused by Mirai.
5	Algorithm violation	Discrimination and manipulation caused by data distortions	Cambridge Analytica case	Vulnerable to digital marketing and political advertising	Algorithmic impact audit, transparency, and human rights assessment	Isaak, J., & Hanna, MJ (2018). User data privacy: Facebook, Cambridge Analytical, and privacy protection. Computer, 51(8), 56–59.

Table 2 above provides a summary of five emerging trends in modern attacks from 2016 to 2025, categorized by threat type, key mechanism, international examples, exposure in Mongolia, policy direction, and source. An example from Europe illustrates how deepfake technology can disrupt the pre-election information ecosystem, emphasizing the importance of information trust.

The increasing likelihood of AI-based phishing and automated attacks evading traditional spam filters underscores the necessity of updating security architectures and managing human factors. The SolarWinds incident exposed the systemic risk posed by third-party updates in supply chain attacks. Weak authentication and segmentation failures in IoT environments, exemplified by the Mirai botnet, can lead to widespread disruption, emphasizing the importance of update management and network isolation. The Cambridge Analytical case highlights the potential for influencing socio-political decisions through algorithmic abuse and data manipulation. Vulnerabilities specific to Mongolia include reliance on cloud and off-premise development, the susceptibility of public camera infrastructure, information literacy levels, and regulatory capacity constraints. Therefore, implementing email authentication with DMARC/SPF/DKIM, supply chain risk management and SBOM, IoT segmentation and continuous firmware updates, deepfake forensics and tagging, algorithmic impact auditing, and transparency are recommended at the policy level.

Additional Ways to Implement and Recommendations

Personal data is now considered the most valuable and vulnerable asset in today's information society. With the increasing demand for data-driven decision-making, automation, and AI-based services, safeguarding personal data has become crucial for national security. Data breaches pose a threat not only to individuals but also to a country's diplomatic, economic, and electronic independence. Therefore, the following recommendations are proposed for enhancing personal data protection:

- Establish a data transparency platform: Create an open data breach registry for citizens to check if their data has been compromised.
- Promote cybersecurity education for citizens: Provide information security training and awareness campaigns via social media. Distribute a guide on safeguarding personal data and actions to take in case of a data breach.
- Set up an Information Security Unit within the National Security Council: Form specialized teams and establish a process for enforcing and monitoring data protection laws.
- Define private sector responsibilities: Require organizations to implement data protection protocols, data destruction practices, data classification, and consent policies.
- Enhance internal data infrastructure: Mitigate data transfer risks by implementing internal servers and encryption technology.

The table below compares the current state of personal data protection with recommendations for further implementation.

Table 3. Strategies for enhancing data protection capabilities

Direction	Current situation	Suggestions and methods for implementation
Legal framework	Outdated and incomplete regulations	Develop and adopt new laws that are consistent with the GDPR model
Regulatory body	There is no independent organization.	Establish a supervisory structure such as a "Data Protection Authority"
Citizen information education	At a low level	Incorporate data protection content into educational programs and organize training for the public
Technological infrastructure	Limited, weak data center resources	Expanding internal servers and introducing data encryption technology
Private sector involvement	Unregulated, weak accountability	Enforcing organizations to implement data protection standards
International coordination	Weak real coherence, limited external relations	Developing cooperation within the framework of GDPR and APEC

Conclusions

The study revealed that the legal framework for personal data protection in Mongolia is incomplete, with weak implementation control, a lack of information literacy among citizens, and inadequate technological protection standards, posing a direct risk to national security.

In cases of data breaches, organizations and individuals often avoid responsibility, withhold information, and neglect to inform victims, indicating that the existing 72-hour reporting obligation, high fines, and compensation mechanisms based on international standards (such as GDPR, APPI, CCPA, etc.) are insufficient in Mongolia. Therefore, there is a need to revise the law, enhance the capacity of supervisory bodies, and align fine amounts with international standards.

Both public and private sector entities lack a culture of transparent reporting on data breaches, eroding citizens' trust in the government and impacting the core principles of e-governance. It is crucial to incorporate transparency requirements into internal regulations and establish a clear accountability system.

The level of technological protection is inadequate, with data transmission and storage lacking encryption. Implementing TLS 1.3 and AES-256 encryption in government systems that handle citizen data, such as E-Mongolia, E-Tax, E-Halamj, E-Daatgal, and E-Health, and developing unified key management policies and procedures are essential.

Relying on foreign hosting and international cloud services for national data storage increases the risk of losing strategically important information. Establishing a National Data Center for domestic data storage is recommended.

Citizens' awareness of data rights and security is insufficient, and there is a lack of a culture of demanding these rights. This results in citizens being unable to protect their rights in case of data loss. It is vital to emphasize the importance of personal data and educate the public on how to safeguard it through the education system and public training programs. Given the transnational nature of cybersecurity challenges, Mongolia should prioritize international cooperation and conduct regular joint actions against cyber espionage.

REFERENCES

1. Baldwin, D. A. (1997). The concept of security. *Review of International Studies*, *23*(1), 5–26.
2. BBC News. (2023, November 29). UK warns of state-backed cyber threats amid rising tensions. *BBC News*. https://www.bbc.com/news/uk-politics-67518511
3. California Department of Justice. (2024). California Consumer Privacy Act (CCPA). *Office of the Attorney General*. https://oag.ca.gov/privacy/ccpa
4. Cybersecurity and Infrastructure Security Agency. (2017, October 14). Heightened DDoS threat posed by Mirai and other botnets [Alert]. https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets
5. Cybersecurity and Infrastructure Security Agency. (2021, April 29). Defending against software supply chain attacks. https://www.cisa.gov/resources-tools/resources/defending-against-software-supply-chain-attacks
6. CyberScoop. (2018). APT27 targets Mongolia in cyber espionage campaign, Kaspersky reports. https://cyberscoop.com/apt27-mongolia-kaspersky/
7. European Union Agency for Cybersecurity. (2020). *Cyber risk management for ports* (p. 2). https://portalcip.org/wp-content/uploads/2024/11/ENISA-Guidelines-Cyber-Risk-Management-for-Ports.pdf
8. European Union. (2020). General Data Protection Regulation (GDPR). https://gdpr.eu
9. General Data Protection Regulation, Art. 4. (2016). *Regulation (EU) 2016/679*.
10. Government of Mongolia. (2010). *Mongolian National Security Concept*.
11. HackNotice. (2024, November 8). Intermed Hospital Mongolia data breach notification. https://hacknotice.com/2024/11/08/intermed-hospital-mongolia/
12. IBM Security X-Force. (2024). *X-Force Threat Intelligence Index 2024 reveals stolen credentials as top risk, with AI attacks on the horizon*. https://www.ibm.com/think/x-force/2024-x-force-threat-intelligence-index
13. *The Independent*. (2019, October 24). Mongolia and China cyber crime arrest raids target international network. https://www.independent.co.uk/tech/mongolia-china-cyber-crime-arrest-raids-a9179471.html
14. International Organization for Standardization. (2012). *Information technology — Security techniques — Guidelines for cybersecurity* (ISO/IEC 27032:2012).
15. Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytical, and privacy protection. *Computer*, *51*(8), 56–59. https://doi.org/10.1109/MC.2018.3191268
16. Japan Personal Information Protection Commission. (n.d.). Act on the Protection of Personal Information (APPI). https://www.ppc.go.jp
17. Legalinfo.mn. (2022). Electronic Security Law of Mongolia. https://legalinfo.mn/mn/detail/16574694017401
18. Parliament of Mongolia. (2021). *Cyber Security Law*.
19. Parliament of Mongolia. (2021). *Law on the Protection of Personal Data*.
20. Reddit. (2021, November 11). Central Bank of Mongolia was hacked and now [Discussion post]. *r/mongolia*. https://www.reddit.com/r/mongolia/comments/qs1i8y/central_bank_of_mongolia_was_hacked_and_now/
21. Security Affairs. (2022, January 19). Mongolian CA MonPass hack exposes citizen data. https://securityaffairs.com/119677/malware/mongolian-ca-monpass-hack.html
22. Taddeo, M. (2019). The ethics of algorithms: Key problems and solutions. In *The Oxford handbook of ethics of AI* (pp. 1–20). Oxford University Press.
23. TAdviser. (2021). Khan Bank (Haan Bank). https://tadviser.com/index.php/Company%3AHaan_Bank_%28Khan_bank%29
24. *The Hacker News*. (2025, January 15). RedDelta deploys PlugX malware to target organizations. https://thehackernews.com/2025/01/reddelta-deploys-plugx-malware-to.html
25. *The Record*. (2024). Mongolia targeted by APT29 watering hole attacks using NSO Group and Intellexa exploits. https://therecord.media/mongolia-apt29-watering-hole-attacks-exploits-nso-group-Intellexa