IRSHAD Uzbek Journal of Law and Digital Policy | Volume: 3, Issue: 6
2025

Comparative Legal Analysis of Personal Data in the Legislation of Uzbekistan, Europe and the USA

Khushnazar Juraev
Tashkent State University of Law

Abstract

This article presents a comprehensive comparative analysis of the legal frameworks governing the protection of special categories of personal data in Uzbekistan, the European Union, and the United States. The study examines the Law of the Republic of Uzbekistan "On Personal Data" (2019), the European Union's General Data Protection Regulation (GDPR), and the sectoral approach adopted in the United States through HIPAA and state-level legislation such as the California Consumer Privacy Act. Through doctrinal legal analysis of legislative provisions, examination of enforcement cases in Europe, and comparative methodology, the research identifies significant gaps in Uzbekistan's current legal framework, particularly the absence of the right to be forgotten, inadequate data breach notification requirements, and insufficient penalties for violations. The article concludes with four specific legislative recommendations to strengthen Uzbekistan's personal data protection regime and align it with international best practices.

Keywords: Personal Data, GDPR, HIPAA, Data Protection, Right to be Forgotten, Biometric Data, Genetic Data, Privacy Rights

APA Citation:

Juraev, K. (2025). Comparative Legal Analysis of Personal Data in the Legislation of Uzbekistan, Europe and the USA. *Uzbek Journal of Law and Digital Policy, 3*(6), 94–104. https://doi.org/10.59022/ujldp.482

I. Introduction

The rapid advancement of digital technologies and the exponential growth of data processing activities have fundamentally transformed how personal information is collected, stored, and utilized across all sectors of society (Paul et al., 2024). Among the various categories of personal data, special or sensitive personal data including health records, genetic information, biometric identifiers, and data revealing racial or ethnic origin demands heightened protection due to its potential for causing significant harm if misused. The unauthorized disclosure or improper processing of such data can lead to discrimination, identity theft, reputational damage, and violations of fundamental human rights. Consequently, jurisdictions worldwide have developed increasingly sophisticated legal frameworks to address these concerns, though with varying approaches and levels of effectiveness.

Uzbekistan, as part of its broader digital transformation agenda and commitment to integrating into the global digital economy, adopted the Law "On Personal Data" (Law No. LRU-547) on July 2, 2019, which entered into force on October 1, 2019. This landmark legislation represents the country's first comprehensive attempt to establish a regulatory framework for personal data protection, including provisions specifically addressing special categories of data. However, as digital technologies continue to evolve and cross-border data flows intensify, questions arise regarding whether Uzbekistan's current legal framework provides adequate protection for sensitive personal information, particularly when compared to more established regimes such as the European Union's General Data Protection Regulation (GDPR) and the sectoral approach adopted in the United States.

The primary objective of this research is to conduct a comprehensive comparative analysis of the protection methods and guarantees for special personal data across these three jurisdictions. By examining the substantive provisions, enforcement mechanisms, and practical application of these legal frameworks, this study aims to identify gaps in Uzbekistan's current legislation and propose concrete recommendations for legislative reform. The research question guiding this analysis is: How can Uzbekistan strengthen its legal framework for protecting special categories of personal data while learning from the experiences of the European Union and the United States?

The significance of this study extends beyond academic interest, as it addresses pressing practical concerns for policymakers, legal practitioners, and data controllers operating in Uzbekistan. With the country's increasing participation in international trade and digital commerce, alignment with global data protection standards becomes not merely aspirational but essential for economic competitiveness and the protection of citizens' fundamental rights. Furthermore, real enforcement cases from European jurisdictions provide valuable lessons on the practical challenges and effective strategies for protecting sensitive personal data in the digital age.

II. Methodology

This research employs a combination of doctrinal legal analysis, comparative legal methodology, and case study examination to achieve its objectives. The doctrinal approach involves a systematic analysis of primary legal sources, including the Law of the Republic of Uzbekistan "On Personal Data" (Law No. LRU-547), the Regulation on Requirements for Protection of Personal Data approved by the Cabinet of Ministers, the European Union's General Data Protection Regulation (Regulation 2016/679), and relevant United States federal and state legislation including the Health Insurance Portability and Accountability Act (HIPAA) and the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA).

The comparative methodology enables systematic identification of similarities and differences across jurisdictions, facilitating the assessment of relative strengths and weaknesses in each approach. Secondary sources, including scholarly articles, official guidance documents from regulatory authorities, and reports from the European Data Protection Board, supplement the primary legal analysis. Case study examination focuses on significant enforcement actions and judicial decisions in European jurisdictions, providing practical insights into how data protection principles are applied and violations are sanctioned. The research covers the period from 2018 (when GDPR entered into force) to 2024, capturing the most recent developments in data protection enforcement.

III. Results

A. Definition and Categories of Special Personal Data across Jurisdictions

The analysis reveals significant variations in how each jurisdiction defines and categorizes special personal data. Under Article 25 of Uzbekistan's Law on Personal Data, special personal data encompasses information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, political party and trade union membership, health-related data (physical and mental health), data concerning a person's private life, and criminal record. Additionally, Article 26 separately addresses biometric and genetic data, defining biometric data as personal data relating to the anatomical and physiological characteristics of a subject, and genetic data as personal data relating to inherited or acquired genetic characteristics derived from biological sample analysis.

The European Union's GDPR, under Article 9, prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for uniquely identifying individuals, health data, and data concerning sexual orientation. The GDPR's approach is notably broader in explicitly including sexual orientation as a protected category and providing detailed definitions for genetic and biometric data within Article 4. Furthermore, Member States retain the authority under Article 9(4) to

maintain or introduce additional conditions, including limitations, for processing genetic, biometric, or health data.

The United States lacks a comprehensive federal data protection law comparable to the GDPR, instead relying on a sectoral approach. HIPAA specifically protects individually identifiable health information (Protected Health Information or PHI) held by covered entities such as healthcare providers, health plans, and healthcare clearinghouses. The California Consumer Privacy Act, as amended by the CPRA, introduces the concept of "sensitive personal information" encompassing Social Security numbers, financial account information, precise geolocation, racial or ethnic origin, religious beliefs, union membership, contents of mail and messages, genetic data, biometric information processed to identify consumers, health data, and information about sexual orientation. This represents the most comprehensive definition of sensitive data in U.S. state-level legislation to date.

B. Processing Conditions and Legal Bases

Uzbekistan's Law on Personal Data establishes that special personal data may only be processed with the explicit consent of the data subject, except in cases related to the implementation of international treaties, administration of justice, enforcement proceedings, and other cases provided by law. Article 26 similarly requires consent for processing biometric and genetic data used for identification purposes. The law mandates that consent requests must be presented in an easily accessible form and clearly indicate the purpose of processing. Where the initial processing purpose changes, additional consent must be obtained.

The GDPR's Article 9(2) provides ten specific exceptions to the general prohibition on processing special category data, including explicit consent, employment and social security law obligations, vital interests protection, processing by non-profit bodies, data manifestly made public, legal claims, substantial public interest, preventive or occupational medicine purposes, public health reasons, and archiving or research purposes. Each exception is accompanied by specific conditions and safeguards. Notably, Member States may require explicit consent even where other exceptions might apply, demonstrating the flexibility built into the European framework.

Under HIPAA, covered entities may use and disclose PHI without patient authorization for treatment, payment, and healthcare operations. Other disclosures generally require written authorization from the patient. The Privacy Rule establishes the "minimum necessary" standard, requiring covered entities to make reasonable efforts to limit PHI use and disclosure to the minimum amount needed to accomplish the intended purpose. The CCPA/CPRA takes a different approach by granting consumers the right to limit the use and disclosure of their sensitive personal information, requiring businesses to provide a clear mechanism for consumers to exercise this right.

C. Protection Guarantees and Security Requirements

Article 27 of Uzbekistan's Law on Personal Data establishes general guarantees for personal data protection, requiring the implementation of organizational and technical measures based on identified security threats. The Cabinet of Ministers establishes security levels for personal data processing depending on security threats, requirements for ensuring protection, and requirements for material carriers of biometric and genetic data. The Regulation on Requirements for Protection of Personal Data further specifies four categories of personal data processed in databases: special, biometric, genetic, and publicly available data. Personal data of employees must be processed in separate databases from data of non-employees.

The GDPR's Article 32 requires controllers and processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. These measures may include pseudonymization and encryption, ensuring ongoing confidentiality, integrity, availability and resilience of processing systems, ability to restore data availability following incidents, and regular testing of security measures. The regulation specifically mentions that when assessing appropriate security levels, particular account shall be taken of risks presented by processing, including accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data.

HIPAA's Security Rule establishes national standards for protecting electronic PHI, requiring covered entities to ensure confidentiality, integrity, and availability of all e-PHI; identify and protect against reasonably anticipated threats; protect against reasonably anticipated impermissible uses or disclosures; and ensure workforce compliance. The rule mandates administrative, physical, and technical safeguards, with specific implementation specifications that may be required or addressable depending on organizational circumstances. The CCPA/CPRA requires businesses to implement reasonable security procedures and practices appropriate to the nature of the personal information.

D. Enforcement Cases in Europe: Lessons for Uzbekistan

European enforcement actions provide valuable lessons for Uzbekistan's developing data protection regime. One significant case involved Dedalus Biologie, a French company that was fined €1.5 million in April 2022 following a massive data breach affecting nearly 500,000 individuals. The breach exposed sensitive medical information including data related to HIV status, cancers, genetic diseases, pregnancies, and drug therapy. The French data protection authority (CNIL) found multiple violations including extraction of more data than required during software migration, failure to ensure security of personal data under Article 32 GDPR, lack of encryption, absence of automatic deletion procedures, no authentication requirements for internet access to server public areas, use of shared user accounts, and no procedure for monitoring security alerts. This case demonstrates the severe consequences of inadequate technical and organizational measures for protecting

health data.

In Portugal, Centro Hospitalar Barreiro Montijo received a €400,000 fine—one of the first major GDPR fines - for violations related to indiscriminate access to patient data. The investigation revealed that 985 registered doctor profiles existed in the system while only 296 doctors were employed, and nine technical employees had access levels reserved for medical staff, enabling them to access all patient clinical processes. The hospital was found to have violated the principle of minimization and the integrity and confidentiality principle due to inadequate technical and organizational measures. The authority emphasized that the involvement of special categories of health data significantly increased the severity of the violation due to heightened risks to data subjects.

A German hospital in Rhineland-Palatinate was fined €105,000 for GDPR violations arising from a patient mix-up during admission, which resulted in incorrect invoicing and revealed structural technical and organizational deficits in patient and privacy management. The Commissioner for Data Protection emphasized that the fine was intended not merely as a sanction but as a signal that data protection authorities are particularly vigilant regarding health data protection. Similarly, an Irish hospital (Cork University Maternity Hospital) was fined €65,000 after personal data of 78 patients, including sensitive health information such as medical histories and planned care programs, was found in a public recycling facility, highlighting the importance of secure data disposal procedures.

The landmark Google Spain case (C-131/12) before the Court of Justice of the European Union in 2014 established the right to be forgotten within European data protection law. Spanish citizen Mario Costeja González sought removal of links to 1998 newspaper announcements about attachment proceedings concerning his social security debts, arguing the information was no longer relevant sixteen years later. The Court held that even initially lawful processing of accurate data may become incompatible with data protection principles when, considering all circumstances, the data appears inadequate, irrelevant, no longer relevant, or excessive in relation to processing purposes and elapsed time. This decision was subsequently codified in Article 17 of the GDPR as the right to erasure (right to be forgotten).

E. Comparative Analysis of Data Subject Rights

Uzbekistan’s Law on Personal Data grants data subjects the right to access their personal data, the right to request correction of inaccurate or incomplete data, and the right to request destruction of data when purposes are achieved or consent is withdrawn. The operator must destroy personal data within three days of consent withdrawal, achievement of processing purposes, or expiration of the time period for which consent was granted. However, the law notably lacks an explicit right to be forgotten comparable to GDPR Article 17, right to data portability, and comprehensive right to object to automated decision-making including profiling.

The GDPR provides a comprehensive suite of data subject rights under Articles 12-22, including the right of access, right to rectification, right to erasure (right to be forgotten), right to restriction of processing, right to data portability, right to object, and rights related to automated individual decision-making. Article 17 specifically provides that data subjects may request erasure where data is no longer necessary for original purposes, consent is withdrawn, the subject objects to processing, data was unlawfully processed, or erasure is required for legal compliance. The right to data portability under Article 20 enables individuals to receive their data in a structured, commonly used, machine-readable format and transmit it to another controller.

Under HIPAA, patients have the right to access their medical records, request amendments, and receive an accounting of disclosures, request restrictions on uses and disclosures, and request confidential communications. However, HIPAA does not include a right to be forgotten or data portability in the GDPR sense. The CCPA/CPRA grants California residents the right to know what personal information is collected, the right to delete personal information, the right to correct inaccurate information, the right to opt-out of sale or sharing of personal information, the right to limit use of sensitive personal information, and the right to non-discrimination for exercising privacy rights.

IV. Discussion

The comparative analysis reveals both strengths and significant gaps in Uzbekistan's current framework for protecting special personal data. While the Law on Personal Data represents a commendable first step in establishing comprehensive data protection in Uzbekistan, several areas require legislative attention to align with international best practices and effectively protect citizens in the digital age.

The absence of an explicit right to be forgotten in Uzbekistan’s legislation represents a significant gap. The European enforcement experience, particularly the Google Spain case and subsequent GDPR Article 17 implementation, demonstrates that this right is essential for protecting individuals from the indefinite persistence of outdated or irrelevant personal information in the digital environment. While Uzbekistan’s law provides for data destruction upon consent withdrawal or purpose achievement, it lacks the proactive erasure right that enables individuals to request removal of their data from publicly accessible sources, particularly online platforms and search engines. Given Uzbekistan’s increasing digitalization and the growing online presence of its citizens, introducing this right would provide crucial protection against reputational harm and privacy violations stemming from historical information that is no longer relevant.

Uzbekistan’s current framework lacks comprehensive mandatory data breach notification requirements comparable to those in GDPR Article 33-34 or HIPAA’s Breach Notification Rule. The European cases examined, including the Dedalus Biologie breach affecting 500,000 individuals, highlight how delayed notification can

exacerbate harm to affected individuals. The GDPR requires notification to supervisory authorities within 72 hours and to affected individuals without undue delay when breaches pose high risks to their rights. Uzbekistan should consider implementing similar requirements, particularly for breaches involving special categories of data where the potential for harm is substantially elevated.

The penalty structure under Uzbekistan's current legislation appears insufficient to deter violations effectively. The European enforcement tracker reveals that since GDPR's implementation, data protection authorities across 27 countries have imposed 237 fines totaling approximately €22.8 million specifically in the healthcare sector, with average fines for technical and organizational measure failures reaching €203,423 in 2024. The GDPR's maximum penalties of €20 million or 4% of global annual turnover for severe violations create meaningful deterrence for large organizations. Uzbekistan should consider strengthening its penalty framework to ensure that the potential cost of non-compliance outweighs the cost of implementing adequate protection measures.

The enforcement mechanism and resources of Uzbekistan's authorized body - the State Personalization Center under the Cabinet of Ministers - merit examination. The European experience demonstrates that effective data protection requires well-resourced independent supervisory authorities with robust investigative and enforcement powers. The Portuguese hospital case, where the violation was discovered through media reports rather than proactive oversight, illustrates the importance of both responsive investigation capacity and systematic compliance monitoring.

The sectoral approach of the United States, while providing strong protection in specific domains such as health information through HIPAA, creates gaps in coverage for data processed by entities outside covered sectors. Uzbekistan's comprehensive approach is preferable in this regard, though the country could benefit from developing sector-specific guidance for high-risk areas such as healthcare, financial services, and telecommunications where special category data is frequently processed.

A. Recommendations for Legislative Reform

Based on the foregoing analysis, four specific recommendations are proposed for strengthening Uzbekistan's legislation on the protection of special personal data: The introduction of the right to be forgotten (right to erasure) should be a legislative priority (Kelly, Furey, & Curran, 2021). This right should enable data subjects to request erasure of their personal data from controllers and, importantly, obligate controllers who have made personal data public to take reasonable steps to inform other controllers processing the data of the erasure request. This is particularly relevant for online platforms, search engines, and social media services operating in Uzbekistan. The right should be subject to appropriate exceptions, including for exercising freedom of expression, compliance with legal obligations, public health

purposes, archiving in the public interest, and establishment or defense of legal claims.

Mandatory data breach notification requirements should be established, requiring owners and operators to notify the authorized body within 72 hours of becoming aware of breaches involving special categories of personal data, and to notify affected individuals without undue delay when breaches pose high risks to their rights and freedoms. The notification should include the nature of the breach, categories and approximate number of individuals affected, likely consequences, and measures taken or proposed to address the breach. This requirement would align Uzbekistan's framework with international standards and ensure timely response to data security incidents (Pattanasri, 2019).

The penalty framework should be substantially strengthened to create effective deterrence. Administrative fines should be calibrated to the severity of violations, the sensitivity of data involved, and the economic capacity of the violator (Violon, 2025). For violations involving special categories of personal data, fines should be significantly higher than for ordinary personal data violations, reflecting the enhanced potential for harm. The legislation should establish tiered penalty structures with maximum fines proportionate to the turnover of large enterprises, similar to the GDPR approach, while ensuring that penalties for smaller organizations remain meaningful without being disproportionately burdensome.

The right to data portability should be introduced, enabling data subjects to receive their personal data in a structured, commonly used, and machine-readable format, and to transmit that data to another controller. This right promotes competition, prevents vendor lock-in, and empowers individuals to exercise greater control over their personal information. The right should apply where processing is based on consent or contract and is carried out by automated means. Implementation guidelines should specify technical standards for data formats to ensure interoperability between service providers operating in Uzbekistan (Kuebler-Wachendorff et al., 2021).

Conclusion

This comparative analysis of special personal data protection frameworks in Uzbekistan, the European Union, and the United States reveals that while Uzbekistan's Law on Personal Data provides a solid foundation, significant enhancements are needed to ensure adequate protection of sensitive information in the digital era. The examination of European enforcement cases, the Portuguese hospital access control violations, and the landmark Google Spain right to be forgotten decision, demonstrates the practical importance of robust legal frameworks, effective supervisory authorities, and meaningful penalties in deterring violations and protecting data subjects.

The research has identified four critical areas requiring legislative attention: the absence of the right to be forgotten, the lack of mandatory data breach notification requirements, insufficient penalty structures, and the need for data portability rights.

Each of these gaps exposes Uzbek citizens to risks that are addressed in more mature data protection regimes. The recommendations proposed in this article provide a roadmap for legislative reform that would significantly enhance protection while remaining proportionate to Uzbekistan's economic and institutional context.

Implementation of these recommendations would not only strengthen the protection of special personal data in Uzbekistan but also facilitate the country's integration into the global digital economy by demonstrating commitment to international data protection standards. As cross-border data flows continue to increase and digital services become increasingly central to economic and social life, robust data protection is not merely a legal obligation but a fundamental prerequisite for sustainable digital development, international business partnerships, and the maintenance of citizen trust in digital government services. The time for legislative action is now, while Uzbekistan's digital transformation is still in its formative stages and foundational legal frameworks can be strengthened to meet the challenges of the digital age.

Bibliography

Kelly, M., Furey, E., & Curran, K. (2021). How to achieve compliance with GDPR Article 17 in a hybrid cloud environment. *Sci*, 3(1), 3. https://doi.org/10.3390/sci3010003

Kuebler-Wachendorff, S., Luzsa, R., Kranz, J., Mager, S., Syrmoudis, E., Mayr, S., & Grossklags, J. (2021). The right to data portability: Conception, status quo, and future directions. *Informatik Spektrum, 44*(1), 1-9. https://doi.org/10.1007/s00287-021-01372-w

Pattanasri, T. (2019). Mandatory data breach notification and hacking the smart home: A legal response to cybersecurity? *QUT Law Review*, *18*(2), 268. https://doi.org/10.5204/qutlr.v18i2.770

Paul, J., Ueno, A., Dennis, C., Alamanos, E., Curtis, L., Foroudi, P., Kacprzak, A., Kunz, W. H., Liu, J., Marvi, R., Nair, S. L. S., Ozdemir, O., Pantano, E., Papadopoulos, T., Petit, O., Tyagi, S., & Wirtz, J. (2024). Digital transformation: A multidisciplinary perspective and future research agenda. *International Journal of Consumer Studies*. Advance online publication. https://doi.org/10.1111/ijcs.13015

Violon, J. M. (2025). *Privacy at risk: Legal remedies and redress mechanisms for privacy breaches*. Eliva Press Global Ltd.