16 years ESJ
Special edition

Personal Data Security in Comparative Perspective: Legal Frameworks and Protections

Mariam Zarkua, PhD Student of Law
Grigol Robakidze University, Georgia

Doi:10.19044/esj.2026.v22n38p454

Submitted: 15 December 2025
Accepted: 25 February 2026
Published: 23 March 2026

Cite As:
Zarkua, M. (2026). *Personal Data Security in Comparative Perspective: Legal Frameworks and Protections.* European Scientific Journal, ESJ, 22 (38), 454.
https://doi.org/10.19044/esj.2026.v22n38p454

Abstract

The paper presents the general concept of personal data protection, its legal approaches in the European Union, the United States, Japan and Georgia and its main purpose is to study different legal frameworks and approaches that underlie the formation and development of general data protection policies. The present study examines the primary legislative instruments, including the GDPR and the CCPA, which are discussed below, as well as Japanese and Georgian legal regulations. The study's objective is to assess the legal standards of these states with a particular focus on the extent to which they balance and protect the confidentiality of individuals' personal data, while considering commercial interests and state needs. The study utilizes doctrinal and comparative legal methodologies to illuminate the primary regulatory mechanisms governing personal data, restrictions and the individual's right to access personal information. The conclusions presented herein underscore the challenges inherent in the establishment of a unified approach to personal data in the future. The study underscores that the foundation for effective personal data governance in the digital age is a hybrid approach, integrating flexible legal regulations that readily adapt to technological advancements. The document synthesizes fundamental information and methodologies concerning personal data, which are likely to be of interest to both personal data protection policymakers and legal professionals in general, as well as individuals with non-legal educational backgrounds. The protection of

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
20-21 November 2025, Tbilisi, Georgia

personal information and confidentiality is a matter of concern for each individual.

Keywords: Personal data, sensitive personal information, privacy, data processing

Introduction

The notion of data protection was conceptualized four decades ago with the initial objective being to impede the illicit utilization of information pertaining to individuals. The objective of this initiative was to dispel the pervasive belief that advancements in technology would compromise the safeguarding of fundamental human rights and interests in this domain (Hustinx, 2014). Conversely, this does not imply a total prohibition on the processing of personal data. Instead, it signifies the establishment of specific legal constraints for personal data owners within which they will process the data (De Hert, Gutwirth, 2009). The advent of modernity has rendered the collection and utilization of personal information an inextricable facet of quotidian existence. In many cases, personal data is used to provide customized services, enhance the experience for users, and encourage commercial innovations in various sectors. Concurrently, empirical evidence has demonstrated that many users are reluctant to disclose comprehensive personal information, despite recent research findings indicating that even "privacy-conscious" users may unintentionally divulge confidential information (Ngong et al., 2025). This phenomenon can be attributed to the tendency of users to furnish personal data unconsciously, a practice that frequently exposes them to the risk of subsequent misuse (Hendrickx et al., 2021). It is important to note that privacy-related problems have emerged in conjunction with the development of artificial intelligence (AI). This is due to the fact that individuals, in addition to formal documents and personal identifiers, share sensitive information that directly relates to their private lives. Recent findings suggest that any type of information provided by individuals to artificial intelligence (AI) can be utilized for various purposes. It must be noted that this does not imply a refusal of the aforementioned technological offer. However, the international regulations discussed in this paper thoroughly provide the main directions, existing challenges and main emphases on the policy of personal data protection, which are of fundamental importance to consider. It is evident that this information is of interest to individuals and entities involved in the fields of artificial intelligence and data security. It is imperative that public awareness and information sources regarding personal data protection be augmented to mitigate the exacerbation of existing problems. Consequently, it is imperative that each state, along with its respective bodies or private sectors, undertakes the collection, processing

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
20-21 November 2025, Tbilisi, Georgia

and storage of individual data in accordance with stringent legal standards. This is a fundamental prerequisite for a democratic society.

Literature Review

The Philosophical and Legal Origins of Privacy

The notion of personal data and its implications has been a subject of discourse even prior to the advent of contemporary technological advancements. The 1890 article "The Right to Privacy" by Samuel D. Warren and Louis D. Brandeis was instrumental in the development of the modern concept of privacy. The authors of the article contend that each individual has the right to determine how much of their thoughts, feelings and emotions should be communicated with others. It is incumbent upon the individual to determine whether to disseminate information without coercion and to establish the limits of publicity. The authors contend that such interference in people's lives undermines their personal dignity, as individuals possess the right to "be let alone." This approach played a significant role in the development of this issue and the formulation of specific approaches on a global scale, particularly in the United States (Warren, Brandeis, 1890).

In his book „Privacy and Freedom“, Westin defined the concept of privacy as both an infringement of external interference and a claim or right. This implies an individual's ability to determine when, how and to what extent information about them is transmitted to others. The right to control information is the primary principle that underlies nearly all contemporary data protection regulations, including the GDPR (Westin, 1968). In this regard, Daniel J. Solove's article, "Taxonomy of Privacy" is a seminal piece of scholarship that provides a comprehensive analysis of privacy and its various components. The author developed a taxonomy of privacy-related harms, which are divided into categories such as information collection, processing, dissemination, and intrusion. The categorization of these concepts is of paramount importance, particularly in the context of harm analysis in the era of rapid technological development (Solove, 2006).

This issue will be discussed in detail subsequently. It is also noteworthy to mention the American case, wherein data protection was predominantly situated within the ambit of consumer protection and market regulation. The European approach diverges significantly from this, as it prioritizes the legal regulation of data protection for the purpose of safeguarding human rights and interests. In this regard, Article 8 of the European Convention on Human Rights (ECHR, 1950) (European Court of Human Rights, 1950) should be noted first of all, as it concerns the right to respect for private and family life. Convention 108 of the Council of Europe (1981) represented a significant turning point in the realm of personal data protection, as it was legally binding. These principles are predicated on tenets

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
20-21 November 2025, Tbilisi, Georgia

of fairness, purpose limitation, proportionality and the protection of individuals' rights over their data. In fact, the Convention once again established that personal data, once collected and processed, directly affects the autonomy, identity and freedom of the individual. The Convention underwent an update in 1985, which included the addition of a section addressing the relationship between personal data and artificial intelligence. Subsequently, in 2018, the Council of Europe modernized it. This included the obligation to notify in the event of a personal data breach, additional accountability for data controllers and new rights to algorithmic decision-making (Council of Europe, 2018). It is important to acknowledge the impact of this initiative and the specific recommendations and requirements established by the Advisory Committee regarding the development of artificial intelligence. As the Committee stated in the report prepared by Alessandro Mantellero, personal data is increasingly becoming both the source and the target of artificial intelligence applications. This process is unregulated and largely disregards fundamental human rights. The Council of Europe has adopted a legal framework with the objective of developing technologies based on these rights (Council of Europe, 2019).

This approach to personal data was subsequently reinforced by the Charter of Fundamental Rights of the European Union, which established the protection of personal data as an independent right, alongside privacy in Article 8. The Charter underscored the notion that data protection is not merely an extension of privacy; rather, it constitutes an independent guarantee in the digital age. This assertion reflects the pervasive role of personal data in shaping social, economic and political life (European Union, 2000).

The General Data Protection Regulation (GDPR, 2018) was eventually adopted and it is now the main and most comprehensive instrument. A salient aspect of the GDPR is its balanced approach to technological innovation with a concomitant emphasis on respect for human dignity and autonomy. The European model, which is founded on human rights principles, stands in stark contrast to the U.S. model, which is characterized by its market-oriented approach and fragmentation.

The American model, in most cases, considers privacy to be a matter of user choice and contractual relations. In contrast, the European approach establishes data protection as a fundamental human right, recognizing that control over personal data and its supervision through appropriate regulations are essential not only for the private lives of individuals, but also for the implementation of freedom and democracy in the state. In this regard, the rapid development of technologies represents a significant challenge, underscoring the necessity for their legal regulation to occur in a manner consistent with technological advancement.

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
20-21 November 2025, Tbilisi, Georgia

General principles of personal data protection under the GDPR

Article 5 of the General Data Protection Regulation (GDPR) delineates the fundamental principles that govern the processing of personal data. These principles encompass lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality. All extant and prospective EU data protection legislation must comply with the listed principles (Council of Europe, 2018; European Union, 2016; European Union Agency for Fundamental Rights & Council of Europe, 2018). In the absence of such a basis, exceptional approaches must be justified by a legitimate aim and must constitute a necessary and proportionate measure in a democratic society.

According to the data protection legislation of the European Union and the Council of Europe, lawful processing necessitates the consent of the data subject or an alternative basis stipulated by law. In addition to lawful processing, the data protection legislation of the European Union and the Council of Europe stipulates the equitable handling of personal data, a principle that governs the relationship between the controller and the data subject. It is imperative that data subjects be cognizant of the lawful and transparent processing of their data and possess the capability to verify the compliance of processing operations with the GDPR. It is imperative that the data processing process be transparent and that data subjects be informed of any potential risks. In accordance with the principle of transparency, it is incumbent upon the controller to ensure that data subjects are informed about the utilization of their data. This term may refer to information provided to the subject prior to the initiation of data processing, as well as information to which data subjects have access after requesting access to their personal data. This stipulation signifies that the specific purpose of the processing of personal data must be known to the data subject at the time of their collection. It is imperative that the purpose of the data processing be determined prior to the initiation of processing. Accordingly, data may not be processed in a way that is incompatible with its original, specified purpose. However, the General Data Protection Regulation provides for exceptions to this rule for archiving purposes in the public interest, scientific or historical research purposes and statistical purposes. The principle of purpose limitation stipulates that the processing of personal data must be confined to specific, well-defined objectives. The principle of proportionality constitutes a foundational tenet within the framework of European data protection legislation, exhibiting a close correlation with the concepts of transparency and user control. The rationale underpinning this correlation is that when the objective of data processing is adequately delineated, individuals possess the requisite awareness concerning the anticipated consequences. Concurrently, it is imperative to ensure that data subjects can effectively exercise their rights,

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
20-21 November 2025, Tbilisi, Georgia

including the right to object to processing (Article 29 Data Protection Working Party, 2013). In addition to the aforementioned points, it is imperative to minimize data collection to the greatest extent possible. This entails the processing of personal data exclusively in circumstances where the purpose of the processing cannot be achieved through alternative means. It is imperative to ensure that the controller adheres to the principle of data accuracy at every stage of the operation. Inaccurate data should be erased or rectified without delay, which may require regular checks and updates of the data collected.

Article 5(1)(e) of the GDPR and similarly, Article 5(4)(e) of the modernized Convention 108 stipulate that personal data be stored in a manner that permits identification of data subjects for no longer than the time for which the data is processed. Consequently, the data must be eradicated or rendered anonymous once the stipulated objectives have been accomplished. To this end, temporal constraints for eradication or periodic review should be established to ensure that the data is not retained indefinitely. In the case of S. and Marper, the European Court of Human Rights determined that the fundamental principles of the relevant Council of Europe instruments and the law and practice of other contracting parties require that data retention be proportionate to the purpose pursued and limited in time, particularly in the police sector (Marper v. the United Kingdom, 2008).

In order to guarantee the confidentiality and security of personal data, measures of a technical or organizational nature may be implemented. In accordance with this principle, the sufficiency of security measures must be assessed on a case-by-case basis. When implementing such measures, the controller and the processor must take into account the state of the art, the costs of implementation, the scope, the context and the purpose. The accountability principle dictates that controllers and processors must proactively and consistently implement measures to ensure the promotion and protection of data protection in their processing activities. This is due to the fact that they are accountable for ensuring that their processing operations comply with data protection law and their respective obligations. It is imperative that controllers demonstrate unwavering commitment to adhering to data protection provisions. This obligation is not merely a matter of internal compliance; rather, it is a public responsibility that must be consistently upheld in the presence of data subjects, the general public and supervisory authorities. Additionally, processors are obligated to adhere to specific requirements concerning accountability, such as maintaining records of processing operations and appointing a data protection officer (Council of Europe, 2018, Art. According to the most recent data available, the European Union (2016) and the European Union Agency for Fundamental Rights (2018) are the primary sources for this information.

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
20-21 November 2025, Tbilisi, Georgia

U.S. and Asian Approaches

In the case of the United States, as previously mentioned, the system is markedly distinct. The country's privacy law is a combination of state and local regulations, which vary by state. The United States is currently lacking a single, comprehensive national privacy law. Notwithstanding this fact, the United States boasts a robust framework of privacy and data security legislation at both the state and federal levels. Initiated in 2018 by the state of California, the adoption of privacy legislation by other states has also commenced. Concurrently, numerous businesses operating within the United States are obligated to adhere to both federal law and individual state regulations. For instance, California has enacted over 25 state privacy and data security laws, including the comprehensive CCPA, which provides specific definitions and broad individual rights. The CCPA imposes requirements and restrictions on the collection, use, disclosure and processing of personal information of California residents. The document's distinguishing characteristic is the breadth of its protection, which extends beyond the realm of personal consumer information to encompass human resources and business-to-business contexts. The definition of personal data is subject to variation depending on the specific legal and regulatory framework in place. Certain laws, such as data breach and security laws are applicable to sensitive personal information, including financial account information, passwords, biometric data, health insurance or medical information and other information. Conversely, under a multitude of state and federal regulations, personal information is defined as any type of information that identifies or is associated with or can reasonably be linked to an individual. In the state of California, for instance, the CCPA defines personal information as any information that identifies, relates to, describes or can reasonably be linked directly or indirectly to a specific individual or household. The definition encompasses a wide range of personal information, including names, nicknames, contact information, government-issued identification documents, genetic data, location data, account numbers, educational history and purchase history, among others. The landscape of U.S. privacy laws and self-regulatory principles is characterized by significant variations. However, a common thread that emerges is the fundamental requirement that individuals or entities must be apprised of the company's collection, use and disclosure practices prior to the collection of information. In the context of sensitive data, including health information, credit reports, financial information, personal information about children, biometric data, geolocation data, and telecommunications usage information, explicit consent is mandatory for the collection, use and disclosure of such data. With the exception of California, Florida, Iowa and Utah, all states that have enacted comprehensive privacy laws require businesses to obtain consent from consumers before collecting their data. The

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
20-21 November 2025, Tbilisi, Georgia

state of California mandates that businesses grant individuals the capacity to restrict the utilization of their data. In Iowa, individuals must be informed of the potential use of their data and afforded the opportunity to opt out of sensitive data processing. Utah, on the other hand, requires that individuals be informed of the potential use of their data and be given the right to opt out of sensitive data collection. The Children's Online Privacy Protection Act (COPPA) stipulates that parental consent must be obtained prior to the collection, use, or disclosure of any personal information from children under the age of 13. As of 2025, COPPA will also require separate, specific parental consent before companies can use children's data for targeted advertising or disclose it to third parties (Lucente et al., 2025).

Japan's approach is noteworthy as well. The nation's legislation includes the Personal Information Protection Act ("APPI"), which governs privacy issues within Japan. The Personal Information Protection Commission ("PPC"), a central agency, functions as the government's oversight body for privacy matters. The APPI was originally enacted in 2003, but has undergone several amendments that have been in effect since May 30, 2017. On June 5, 2020, the Japanese Diet passed a bill to further amend the APPI, also known as the "Amended APPI." A distinct data protection law was applicable to the public sector. However, the Public Sector Data Protection Law was integrated into the APPI and entered into force on April 1, 2022. In Japan, personal information is defined as any information about a living person that can be used to identify a specific person by name, date of birth or other description that contains such information. Personal information is defined as any information that can be used to identify a specific person. With regard to sensitive information, this encompasses details such as an individual's race, religion, social status, medical history, criminal record and any victimization records. Additionally, any other information that could potentially lead to discrimination against the individual is considered sensitive. The acquisition of sensitive information generally necessitates the consent of the data subject. This principle is equally applicable to the transfer of information about the individual to a third party. According to the APPI, the transfer of information to third parties located in foreign countries requires the prior consent of the data subjects with the indication of the receiving country, unless the foreign country is not whitelisted under the APPI rules or the third party receiving the personal information does not have established similar adequate standards of privacy protection as specified in the APPI rules. Presently, the whitelist comprises the United Kingdom and the Member States of the European Union. According to the Guidelines on Offshore Transfers, one example of an acceptable international framework is the APEC CBPR system. With regard to the transfer of personal information to foreign countries, the revised APPI stipulates that business operators, upon obtaining consent, are obligated to

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
20-21 November 2025, Tbilisi, Georgia

provide data subjects with specific information. This includes the name of the country where the recipient party is domiciled, the data protection legal system in the country, and the data protection measures implemented by the recipient party. Furthermore, the business operator is obligated to implement the requisite measures to ensure that the recipient of such personal information consistently employs appropriate measures to process the personal information in a manner that aligns with the stipulated requirements of the APPI (Fujikouge, 2025).

Georgian Approach

Georgia's recently enacted Law on Personal Data Protection took effect on March 1, 2024. The document stipulates the rights of data subjects and imposes obligations on data controllers and processors, closely replicating the General Data Protection Regulation (GDPR) legal framework previously mentioned. The primary provisions of the GDPR include the establishment of the role of a data protection officer, the enhancement of internal accountability among controllers and the redefinition of the framework for international data transfers. The GDPR's alignment with Georgia's accession criteria to the EU is indicative of Georgia's commitment to adhere to European Union (EU) standards. Furthermore, the Civil Code of Georgia confers upon individuals the right to access their personal data and records that pertain directly to them, their financial affairs and their personal matters. Individuals may obtain copies of such data, except in cases where this right is restricted by Georgian legislation. According to the Georgian Law on Data Protection, personal data is defined as any information pertaining to an identified or identifiable natural person. An identifiable natural person is defined as an individual who can be identified, either directly or indirectly, through various means, including but not limited to: name, surname, identification number, location data, electronic communication identifiers and other pertinent information. With regard to special category data, this encompasses criteria such as racial or ethnic origin, political, religious, philosophical or other opinions, professional association memberships, health and sex life, among others. The national data protection authority is the Personal Data Protection Service, an independent state body that operates on the basis of law. The aforementioned body is guided by the Constitution of Georgia, international treaties ratified by Georgia, generally recognized principles and norms of international law, the Law on Data Protection and other relevant legal acts. The activities of this body are predicated on fundamental principles, including legality, the protection of human rights and freedom, independence and political neutrality, objectivity and impartiality, professionalism, the maintenance of secrecy and confidentiality. Public institutions, insurance organizations, commercial banks and medical institutions that actively process a significant amount of data on

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
20-21 November 2025, Tbilisi, Georgia

data subjects due to the specifics of their work and/or carry out systematic and large-scale monitoring of their behavior are obliged to appoint a personal data protection officer. This officer is then responsible for informing the controller, processor and their employees about the rules and regulations related to data protection. The officer is obligated to engage in such procedures as the formulation of internal regulations pertaining to data processing and a data protection impact assessment document, as well as the supervision of compliance with data processing legislation. The entity in question is also obligated to process applications and complaints received regarding data processing. Furthermore, it is required to receive consultations from the Personal Data Protection Office, serve as a representative in relations with the Personal Data Protection Office and address other procedural issues. It is imperative that data processing be carried out in accordance with the principles of legality, fairness and transparency with respect to the individual concerned by the data. Furthermore, it is imperative that data collection is conducted for legitimate purposes. The further processing of data and its subsequent utilization for alternative purposes is strictly prohibited. The further processing of data for other purposes that are incompatible with the initial purposes is strictly prohibited. Additionally, it is imperative to emphasize that data processing should be conducted solely to the extent necessary to achieve a specific and legitimate aim. Concurrently, data must be proportionate to the purpose for which it is processed. In the event that data is inaccurate, it is imperative that it be corrected, erased or destroyed without undue delay. Once the legitimate aim has been achieved, the data must be eradicated and destroyed, unless their retention is deemed necessary and proportionate in a democratic society. It is imperative to underscore that to ensure data security, it is essential to implement the requisite technical and organizational measures during data processing. The objective of this process is to ensure adequate security (Tchkuaseli, Kvartskhava, 2025).

Privacy in the age of artificial intelligence

The development of artificial intelligence (AI) has also given rise to concerns regarding privacy, prompting inquiries into the manner in which technology governs and utilizes personal data. Consequently, the capacity of artificial intelligence (AI) to amass, assess, and employ data has precipitated a profound transformation in numerous individuals' daily lives. The proper functioning of AI is contingent upon the presence of two key elements: high-performance algorithms and substantial personal data sets. Indeed, due to its functional operation, technology collects and uses sensitive information about individuals in ways that can violate their privacy, often without their knowledge or consent. Consequently, individuals in the legal field are attempting to regulate AI in a manner that maximizes individual rights.

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
20-21 November 2025, Tbilisi, Georgia

In her book Privacy in the Age of Artificial Intelligence, Fereniki Panagopoulos discusses the legal challenges posed by the rapid development of AI with respect to privacy. As previously stated, the development of artificial intelligence necessitates the utilization of substantial personal data to achieve its intended objectives. As posited by Panagopoulos, this attitude toward personal data is paradoxical. On the one hand, data enhances the accuracy of artificial intelligence systems; on the other hand, it increases the risk of violations. It has been observed that certain individuals have been found to employ manipulative tactics on artificial intelligence systems for the purpose of achieving their own objectives. These tactics have been documented as encompassing targeted information, disinformation, manipulation, surveillance, harassment and deception, among other methods. Managing such a substantial volume of data presents significant challenges and it is imperative to mitigate the risk of threats.

Furthermore, Panagopoulou posits that, while legal frameworks such as the General Data Protection Regulation (GDPR) and the European Union (EU) laws on privacy and security of personal data may necessitate revisions to mitigate complexity and address specific concerns posed by AI, the author proposes methodologies to address these issues, including the establishment of a supervisory authority for data protection and other domains such as information, research and intellectual property. (Panagopoulou, 2024).

In their publication, "The Right to Privacy and the Growing Scale of Artificial Intelligence," the authors Syed Raza Shah Gilani, Ali Mohammed Al-Matroochi and Mohammad Haroon Khan, proceed to explore the expanding influence of AI technologies in the context of privacy rights. In their study, the authors note that artificial intelligence (AI)-based methods, including facial recognition, biometric identification, and predictive analytics, have posed a threat to privacy. Privacy is a right that people have and it allows them to control their information and protect their reputation. Privacy is therefore essential to maintaining trust between individuals and institutions. Privacy also serves to protect against the abuse of power by technology. As artificial intelligence (AI) becomes increasingly integrated into our lives, it is imperative to strike a harmonious balance between leveraging the benefits of AI-driven advancements and safeguarding individuals' fundamental privacy rights. The utilization of artificial intelligence systems for mass surveillance and unauthorized data collection constitutes a violation of international human rights law. For instance, Article 12 of the Universal Declaration of Human Rights (UDHR) stipulates that no individual shall be subjected to arbitrary interference with his privacy, family, home or correspondence. A significant number of these AI practices have the potential to compromise human rights as they are defined in International law (Gilani et al., 2023).

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
20-21 November 2025, Tbilisi, Georgia

Daniel J. Solove, in a manner similar to Gilani, Al-Matrooshi and Khan, provides a more thorough examination of the intersection of AI technologies and privacy concerns in his article, "Artificial Intelligence and Privacy." He underscores the privacy concerns that arise from AI's capacity to collect data and draw conclusions without explicit consent. The ability to infer information is of critical importance because AI employs patterns and predictions about individuals to predict data about that person that they have not shared. Solove (2025) contends that while AI exacerbates traditional privacy concerns, current laws are failing to address these challenges.

As technology continues to advance, it becomes imperative to address these issues and ensure that society remains informed. The establishment of institutions and legislation that ensure the protection of human rights and security is conducive to maintaining public trust in technology. In the absence of sufficient regulatory frameworks, trust is diminished, thereby underscoring the imperative for a cooperative approach among legislators. Ensuring a balance between fundamental rights and technological innovations is imperative for the establishment of a society where privacy is protected. This is particularly challenging in the current context, where individuals utilize technological developments not only for professional purposes but also in their personal and daily lives. This phenomenon is accompanied by the widespread sharing of personal information, the protection of which is currently suboptimal (Chloe, 2024).

Research Methodology

To provide a thorough and nuanced examination of personal data, the paper employs a range of research methods, including doctrinal, historical, comparative and systemic approaches. The amalgamation of these methodologies provides a comprehensive framework that delineates the prevailing directions and challenges in this field. The research in this paper is fundamentally based on the doctrinal method within the framework of which a systematic and critical analysis of the existing legal framework is discussed particularly national and international laws. The indicated methods determine the fundamental legal principles of personal data protection, specifically its collection, processing and storage, which are an essential part of further analysis on this topic. In addition to the aforementioned, the utilization of the historical research method is imperative in the context of legal development and contemporary innovations in personal data protection. This method enables the reader to present the main historical steps and challenges in this area chronologically, facilitating anticipation and interpretation of potential future restrictions imposed by the legislator. It is necessary to note the comparative research method, through which the paper discusses different legal systems, such as the systems of the United States, Georgia, Japan and the

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
20-21 November 2025, Tbilisi, Georgia

European Union. The study presents their main similarities, differences and potential best legal practices. This method presents a variety of approaches to the management and control of personal data and allows for a nuanced approach to data protection from a global perspective. Finally, the conclusions of the doctrinal, historical and comparative analysis are synthesized using a systems method. This final, integrative approach considers the issue of personal data as a complex system. This method captures the interaction between legal systems, including corporate policy, consumer behavior and government oversight. By using and analyzing these methods as interconnected parts, it becomes clear how personal data is managed and regulated in a real-world context.

Results

The study, employing the aforementioned doctrinal method, has determined that the legal protection of personal data is predicated on several pivotal principles, among which the most salient are the individual's consent and purpose limitation. A thorough examination of a pivotal legal framework, such as the General Data Protection Regulation (GDPR), illuminates a particular legal obligation for data controllers to procure explicit consent for data processing and to utilize data exclusively for the designated and legitimate purposes for which it was collected. Furthermore, the analysis validated the establishment of several fundamental rights of the data subject, including the right of access to information, the right to rectification of information and the right to erasure, as well as the right to data portability and the right to object to certain forms of processing, particularly automated decision-making. Moreover, an examination of historical precedent reveals that these legal principles did not emerge in a legal vacuum but rather within the context of an evolving regulatory environment. The findings indicate that significant legislative changes have largely been made in response to technological advances. While the evolution and development of data collection technologies by legislators has always been continuous, in many cases the development effort has been relatively lagging and insufficient, creating a structural imbalance between rapid technological innovation and comparatively slower normative adaptation. In light of the significant differences between jurisdictions identified through the comparative method, it should be emphasized that the EU General Data Protection Regulation (GDPR) operates on the basis of a comprehensive, human rights-based legal model and is broadly applicable to all sectors. Conversely, the United States has adopted a more fragmented, sectoral approach, with regulations frequently concentrated on specific industries, such as healthcare or finance. This comparison indicates that while both countries aim to protect personal data, their legal methodologies differ significantly, which has implications for how

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
20-21 November 2025, Tbilisi, Georgia

personal data is treated globally, particularly in cross-border data transfers and multinational corporate compliance strategies. A notable finding was the considerable discrepancy between the legal doctrine and its practical implementation. While the legislation stipulates consent, the analysis revealed that intricate and voluminous privacy policies frequently result in perfunctory decision-making by users, rather than informed choice. The corporate data collection practices that are driven by business models frequently operate within legal ambiguities or exploit the failure of foreign entities to comply with mandatory actions. This demonstrates that formal legal safeguards do not necessarily guarantee substantive protection, particularly in contexts where enforcement mechanisms are ineffective or regulatory oversight lacks adequate resources. These systemic findings illustrate the intricate web of relationships that exist beyond the formal legal text and highlight the challenges of effective enforcement and real data protection.

In summary, the research demonstrates that modern data protection systems are grounded in shared core principles such as consent, purpose limitation and accountability, while differing significantly in structural design, ranging from comprehensive rights-based models to sectoral approaches. This finding underscores the persistent discrepancy between formal legal standards and their practical enforcement, highlighting the need for legislative entities to align more closely with the rapid advancements in technology. These findings underscore the necessity for more robust enforcement mechanisms and more transparent consent practices to ensure effective data protection in the digital era. Furthermore, a comparative analysis reveals an emerging trend toward normative convergence across jurisdictions, despite clear structural divergence in regulatory design. While legal systems differ in their institutional frameworks and enforcement models, they increasingly reflect common foundational principles and shared concerns regarding individual autonomy, transparency and accountability. This tendency suggests that future regulatory development may require more coordinated and harmonized responses, particularly in light of the inherently transnational nature of data flows and the growing interdependence of digital markets.

Conclusions and recommendations

The findings of this study confirm the primary hypothesis of the paper, which posits that in the contemporary digital environment, users frequently prefer operational technological operations, characterized by a relatively limited privacy protection level. The extant results, which indicate a high aspiration of users to grant extensive rights and permissions related to their data in exchange for personalized, high-standard services and their smooth functioning, highlight an important psychological and behavioral trade-off. These circumstances suggest that current standards and approaches to data

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
20-21 November 2025, Tbilisi, Georgia

protection require re-evaluation. This re-evaluation is, in part, related to the high degree of user readiness and the desire to control and protect privacy.

The findings presented herein are derived from a comprehensive review of the extant literature and the pertinent information therein. The study presents the main approaches and rules that must be followed to protect the personal data of individuals. This phenomenon is particularly salient in circumstances where individuals frequently relinquish their data in an unconsidered manner, motivated by the pursuit of expeditious and accommodating services. Consequently, it is imperative to consider specific security measures. The issue concerning the digital environment is of an international nature, not being confined to any specific legal system. As has been repeatedly emphasized, the regulatory frameworks for this issue vary considerably from one another. Nevertheless, it is possible to identify common principles that underpin the regulation of data protection. In the context of discussing common principles, it is imperative to acknowledge the fundamental tenets of consent, fairness and transparency. In addition to the aforementioned points, conducting a comparative analysis of state systems across various cultural contexts will be highly advantageous in the future. This is due to the continuous development of technology, which is accompanied by the escalating challenges that characterize our contemporary era. In this vein, the development of experimental platforms on an international scale, wherein individuals can directly control and monitor the scope of data sharing, would be a fascinating area of research. Such platforms would further enhance public awareness of this issue.

In summary, the present study not only validates the hypothesis but also establishes a foundation for a more nuanced comprehension of the notion of personal data and the dynamics of its evolution. It is imperative to acknowledge the necessity of implementing not only more stringent legal frameworks governing data protection but also the development of digital platforms that empower individuals to exercise control over their personal information.

AI Usage Statement

ChatGPT (OpenAI) and DeepL were applied for translation purposes from Georgian to English.

Conflict of Interest: The author reported no conflict of interest.

Data Availability: All data are included in the content of the paper.

Funding Statement: The author did not obtain any funding for this research.

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
20-21 November 2025, Tbilisi, Georgia

References:

1. Article 29 Data Protection Working Party. (2013, April 2). Opinion 3/2013 on purpose limitation (WP 203). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf
2. Chloe. A, (2024). Artificial intelligence: Privacy concerns. CSULB College of Business. https://www.csulb.edu/college-of-business/legal-resource-center/article/artificial-intelligence-privacy-concerns
3. Council of Europe. (2018). Modernised Convention 108 for the protection of individuals with regard to the processing of personal data. https://rm.coe.int/16808b36da
4. Council of Europe. (2018, May 18). Convention for the protection of individuals with regard to the processing of personal data (Convention 108). 128th Session of the Committee of Ministers, Elsinore. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108
5. Council of Europe. (2019, January 30). New guidelines on artificial intelligence and data protection. https://www.coe.int/en/web/data-protection/-/new-guidelines-on-artificial-intelligence-and-personal-data-protection
6. De Hert, P., & Gutwirth, S. (2009). Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action. Springer. https://works.bepress.com/serge_gutwirth/10/
7. European Convention on Human Rights, European Court of Human Rights Council of Europe 67075 Strasbourg cedex France www.echr.coe.int
8. European Union. (2000). Charter of Fundamental Rights of the European Union (2000/C 364/01). Official Journal of the European Communities. https://shorturl.at/chhtP
9. European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
10. European Union Agency for Fundamental Rights & Council of Europe. (2018). Handbook on European data protection law. https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
20-21 November 2025, Tbilisi, Georgia

11. Fujikouge, T. (2025). Data protection laws of the world: Japan – Data protection laws of the world [Web page]. DLA Piper. p.: 2-10 https://www.dlapiperdataprotection.com/?c=US&t=law
12. Gilani, S., Al-Matrooshi, A., & Khan, M. (2023). Right of privacy and the growing scope of artificial intelligence. Current Trends in Law and Society, 3, 1–11.
13. Hendrickx et al. (2021): Hendrickx, I., van Waterschoot, J., Khan, A., ten Bosch, L., Cucchiarini, C., & Strik, H. (2021). Take Back Control: User Privacy and Transparency Concerns in Personalized Conversational Agents. In Joint Proceedings of the ACM IUI 2021 Workshops (Vol. 2903, pp. 6-11). CEUR-WS.org. https://ceur-ws.org/Vol-2903/IUI21WS-CUIIUI-6.PDF
14. Hustinx, P. (2014, September 15). EU data protection law: The review of Directive 95/46/EC and the proposed General Data Protection Regulation. Eurɔopean Data Protection Supervisor. https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en
15. Lucente, K., Serwin, A., & Kashatus, J. M. (2025). Data protection laws of the world: United States – Data protection laws of the world [Web page]. DLA Piper. P.2-10 https://www.dlapiperdataprotection.com/?c=US&t=law
16. Marper v. the United Kingdom, 2008 ECHR 3 (2008). European Court of Human Rights. https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22Marper%22]}
17. Ngong, I., Kadhe, S. R., Wang, H., Murugesan, K., Weisz, J., Dhurandhar, A., & Ramamurthy, K. N. (2025). Protecting users from themselves: Safeguarding contextual privacy in interactions with conversational agents. arXiv. 10 https://arxiv.org/abs/2502.18509
18. Panagopoulou, F. (2024). Privacy in the age of artificial intelligence. Biomedical Journal of Scientific & Technical Research, 55(5), 47429–47434. https://doi.org/10.26717/BJSTR.2024.55.008761
19. Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477–564. https://scholarship.law.upenn.edu/penn_law_review/vol154/iss3/1
20. Solove, D. J. (2025). Artificial intelligence and privacy. Florida Law Review, 77(1), 1–11. https://doi.org/10.2139/ssrn.4713111
21. Tchkuaseli, R., Kvartskhava, K. (2025). Data protection laws of the world: Georgia – Data protection laws of the world [Web page]. DLA Piper. P.2-10 https://www.dlapiperdataprotection.com/?c=US&t=law
22. Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193–220.

ISSN: 1857-7881 (Print) e - ISSN 1857-7431
20-21 November 2025, Tbilisi, Georgia

https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

23. Westin, A. F. (1968). Privacy and freedom. Washington and Lee Law Review, 25(1), 166–182. https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20