



Comparative Analysis of Personal Data Protection Laws: The Case of Azerbaijan and the European Union's General Data Protection Regulation (GDPR)

Firuz M. Abbasova, Kamran I. Khalilov

Baku State University, Baku, Azerbaijan



Corresponding Author — Kamran I. Khalilov

© F.M. Abbasova, K.I. Khalilov, 2026

Abstract: The paper is dedicated to the comparative analysis of legal regulations on the protection of personal data in the Republic of Azerbaijan, with reference to the European Union framework. The purpose of this research is to identify the gaps and shortcomings in the legislative framework of the Republic of Azerbaijan by comparatively analyzing the key concepts and principles in the field of personal data protection, the area of application of normative acts, the rights of data subjects, applicable administrative and legal sanctions for data protection breaches, and the effectiveness of institutional control mechanisms. For this purpose, formal legal and comparative analysis, as well as various scientific research methods, including the doctrinal method are used. The Constitution of the Republic of Azerbaijan, the Law of the Republic of Azerbaijan “On Personal Data” and other related normative documents have been analyzed. By using this approach, the research achieved its principal goal, specifically to conduct a comparative analysis between the two legal systems. Although the normative framework for the protection of personal data in Azerbaijan meets modern requirements, reforms are needed to increase data subjects’ rights, deepen legal compliance, tighten sanctions, and establish a central control mechanism to enhance regulatory coherence with reference to the GDPR as a comprehensive and functionally developed regulatory framework. In this context, the paper emphasizes the obligation to ensure full compli-

ance of the legislation on the protection of personal data in the Republic of Azerbaijan with the GDPR and presents recommendations and conclusions for its development by using the experience of the European Union. The proposals prepared based on the results obtained have practical importance for increasing the effectiveness of the personal data protection mechanism.

Keywords: personal data protection; GDPR; mechanism; Regulation; legislation; comparison

Cite as: Abbasova, F.M. and Khalilov, K.I., (2026). Comparative Analysis of Personal Data Protection Laws: The Case of Azerbaijan and the European Union's General Data Protection Regulation (GDPR). *Kutafin Law Review*, 13(2), pp. 296–333, doi: 10.17803/2713-0533.2026.2.36.296-333

Contents

I. Introduction	297
II. Materials and Methods	302
III. Substantive Legal Comparison between Azerbaijan's Law and the GDPR	303
III.1. Scope of Application	303
III.2. Conceptual Framework: Alignment of Key Definitions	306
III.3. Processing Principles and the Protection of Data Subject Rights	311
III.4. Legal Consequences and Penalties for Data Breaches	316
III.5. Institutional Governance and Oversight Mechanisms	318
IV. Discussion	323
V. Conclusion	328
References	330

I. Introduction

As a result of the rapid development of technological innovations and the integration of digitalization into daily life, the collection, processing, and sharing of personal data have increased significantly. From people's birth dates to marriage and divorce information, as well as records related to court, property, election, and other legal activities, and biometric indicators are collected and processed in real-time by various interested parties, especially government authorities. D.J. Solove and P.M. Schwartz (2024) write that it is almost impossible today

to live without any record being taken of us. This reality shows that personal data has become not only information, but also a tool for economic worth and social power. The mass surveillance of human behaviour by states and governments, and the collection of personal data for various purposes and its conversion into economic worth create serious risks. According to V.P. Shehu and V. Shehu (2023), in today's rapidly advancing digital technologies, the free flow of personal data globally raises serious concerns regarding human rights, and legal norms ensuring data confidentiality aim to both promote technology driven development and protect personal liberties. Normative documents regulating the use of personal data are considered one of the essential foundations of information security in modern societies. Such legislative acts identify the legal framework for the collection, processing, transfer, and protection of personal data. Their principal function is to grant certain rights to citizens, determine the legal obligations of data-processing institutions, and provide possible legal defences in case of law violations (Gstrein and Beaulieu, 2022).

Contemporary legal systems have established legal regulations at international, regional, and national levels, based on fundamental principles such as transparency, accountability, and individual consent in the processing of personal data over time. Although the Universal Declaration of Human Rights, adopted by the United Nations in 1948, does not explicitly recognize personal data protection as an autonomous right, Art. 12 establishes protection against arbitrary interference with privacy, family life, home, and correspondence.¹ The first international instrument specifically addressing personal data protection was the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data² adopted in 1980. These Guidelines established core principles aimed at facilitating the free cross-border movement of personal data while ensuring minimum standards of privacy protection. Despite their advisory nature, they played a foundational role in shaping a more systematic and coordinated international approach to personal data protection, emphasizing principles such as transparency and accountability (Anderson et al., 2021).

¹ Available at: <https://www.un.org/en/about-us/universal-declaration-of-human-rights> [Accessed 10.07.2025].

² Available at: <https://lnk.ink/btda4> [Accessed 29.07.2025].

The application that best regulates the security of personal data at the regional level belongs to the European Union. There is no doubt that A.L. Newman (2015) evaluates the European approach to personal data protection based on a unified, organized, integrated, consistent, and reliable doctrine, in comparison to the “fragmented” American approach based on a multitude of different rules without a regulator.

One of the first steps taken to meet the need for personal data protection within the framework of the European Union was the approval of Convention 108 in 1981.³ The Republic of Azerbaijan is a Party to Convention 108, having ratified the Convention in 2010.⁴ This document, the first legally binding international convention in the field of personal data protection, aimed to protect individuals from legal risks arising from the processing of personal data and to regulate cross-border data transfers between countries.

In 2018, a revised version of the Convention, known as “Convention 108+”, was adopted with the aim of enhancing transparency in personal data processing, granting additional rights to individuals, and strengthening the accountability and responsibilities of data processors. Consequently, the Convention has been adapted to the challenges of the digital era and control mechanisms have been further enhanced.⁵

Directive 95/47/EC of the European Parliament and of the Council, adopted in 1995, aimed to strengthen the protection of personal data while facilitating the free movement of such data within the European Union. As a directive, it required transposition into national law, which resulted in divergent national implementations and a fragmented

³ Council of Europe. (1981, January 28). Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Available at: https://www.edps.europa.eu/data-protection/our-work/publications/legislation/council-europe-convention-no-108-data-protection_en.

⁴ Law of the Republic of Azerbaijan No. 879-IIIQ “On the Ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data” (2009, September). Available at: <https://e-qanun.az/framework/18625> [Accessed 08.07.2025].

⁵ European Union Agency for Fundamental Rights, Council of Europe, and European Data Protection Supervisor, (2018). Handbook on European Data Protection Law. Publications Office of the European Union. Pp. 1–404. Available at: <https://book.coe.int/en/european-court-of-human-rights/10091-pdf-handbook-on-european-data-protection-law-2018-edition-czech-version.html> [Accessed 04.07.2025].

regulatory landscape across Member States. This structural limitation highlighted the need for a more uniform and directly applicable legal instrument at the EU level. In 2016, the European Parliament adopted Regulation 2016/679, known as the “General Data Protection Regulation (GDPR).”⁶ This regulation is considered one of the most significant legal reforms in the field of personal data protection on an international scale. The GDPR was established to ensure the inviolability of personal data and to propose specific legal requirements for parties involved in the processes of collecting, storing, and processing data. The GDPR was implemented in 2018, not only established the fundamental standard for data protection in the EU but also provided encouragement for other countries to review their privacy policies (Aljeraisly et al., 2021). Another reason for its acceptance is, naturally, the increasing need to effectively protect privacy in light of technological advancements. According to A. Wodi (2023), the GDPR has managed to become a crucial milestone in shaping data protection law worldwide since its implementation. The GDPR has been characterized by an enhancement in the level of user data protection and the effective application of administrative fines during the initial five years of its implementation.

According to K. Yeung and L.A. Bygrave (2022), the most important elements underlying the Regulation are the protection of transparency in personal data processing, goal alignment, and fundamental principles of law. It is not by chance that C. Labadie and C. Legner (2019) point out that the principles established within the GDPR shaped the structure of this legal regulation and its approach to the processing of personal data. However, for the principles to be functionally applicable, it is essential that they are comprehended accurately. One of the authors, R. Ducato (2020), emphasises that the principle of transparency should not only be a formal legal obligation but should also be applied in a way that is adapted to human behaviour. Furthermore, the information presented to the data subject must be provided through more user-focused and behaviour-based mechanisms.

S. Zuboff (2019) states that regulatory frameworks such as the GDPR are essential for protecting the rights and freedoms of individu-

⁶ Available at: <https://gdpr-info.eu/> [Accessed 20.08.2025].

als in democratic societies. In this context utilising the GDPR experience, especially when identifying deficiencies in national legislation, is one of the most effective ways to establish ideal standards for states in the field of personal data protection.

M. Nakashima (2022) presents a clear table based on a comparative analysis of how different legal systems regulate the right to personal data portability. The author analyzes the approaches in the GDPR and the U.S. legislation to highlight the deficiencies in Japanese law. This research shows that the legal framework not only identifies the existence of the right but also reveals how it can be integrated with technical standards and market policy.

S. Lim and J. Oh (2025) carried out a comparative study on how personal data protection is regulated globally in the modern digital era, using data from five different jurisdictions (EU, U.S., Japan, China, and South Korea). The authors have demonstrated that the historical, political, and cultural contexts of each country shape its legal framework for privacy. Their research identified similarities and differences in key areas such as consent mechanisms, cross-border applicability, the scope of rights, sanctions, and corporate responsibility, emphasizing deficiencies in current legal frameworks and opportunities for international harmonization. Their comparative analysis, evaluating the similarities and differences, identified key recommendations for how the current research can enhance Azerbaijan's personal data legislation. In this context, the study recognizes that the harmonization of national laws with international principles and standards such as the GDPR is an essential tool for establishing a more flexible and effective legal framework.

Consequently, the aim of this study is to analyse GDPR practices for the development of legislation in the Republic of Azerbaijan in the field of personal data protection. The research has identified the following tasks in order to achieve the defined objectives: 1) to examine GDPR and the legislation of the Republic of Azerbaijan; 2) to identify current legal deficiencies and shortcomings in Azerbaijan's law within the framework of a comparative analysis of both legal approaches; 3) to present specific suggestions and recommendations for amendments to the legislation in the field of personal data protection in Azerbaijan.

II. Materials and Methods

The research incorporated multiple forms of analysis to explore the topic from diverse perspectives. This study uses a comparative legal methodology to assess the level of convergence and divergence between the General Data Protection Regulation (GDPR) and the national legal framework of the Republic of Azerbaijan for personal data protection. A structured analysis of primary substantive and procedural components within both legal systems is made possible by the comparative method. These elements include the scope of application, some necessary definitions, fundamental principles, legal grounds for data processing, rights of data subjects (especially the right to erasure and the right to data portability), legal sanctions and role of supervisory authorities from each system. This comparative assessment seeks to explore how Azerbaijani's legal framework responds to the evolving challenges of personal data protection in the digital age and evaluates the degree to which it aligns with the advanced regulatory tools embedded in globally accepted standards, such as the GDPR.

Through the legal formal method, it became possible to examine how personal data protection norms are framed and structured within the legislative framework. Thus, the research focused in particular on GDPR (2018), Law of the Republic of Azerbaijan No. 998-IIIQ “On Personal Data” (2010),⁷ In addition, this core legislation, other relevant laws, such as Criminal Code of Azerbaijan (2000), Administrative Offences Code of Azerbaijan (2015),⁸ Civil Code of Azerbaijan (1999), the Law of the Republic of Azerbaijan No. 460-IQ “On Information, Informatization, and Protection of Information” (1998),⁹ the Law of the Republic of Azerbaijan No. 651-IIIQ “On Biometric Information” (2008),¹⁰ the Law of the Republic of Azerbaijan 1024-IIQ “On Obtaining Information” (2005),¹¹ Order of the Cabinet of Ministers of Azerbaijan No. 161 “Requirements for the protection of personal data” (2010).¹²

⁷ Available at: <https://e-qanun.az/framework/19675> [Accessed 01.07.2025].

⁸ Administrative Offences Code of the Republic of Azerbaijan (2015, December). Available at: <https://e-qanun.az/framework/46960> [Accessed 11.07.2025].

⁹ Available at: <https://e-qanun.az/framework/3525> [Accessed 14.07.2025].

¹⁰ Available at: <https://e-qanun.az/framework/15144> [Accessed 12.07.2025].

¹¹ Available at: <https://e-qanun.az/framework/11142> [Accessed 23.07.2025].

¹² Available at: <https://e-qanun.az/framework/20046> [Accessed 22.07.2025].

To ensure a structured comparison, the research adopts a functional comparative method that analyzes how each legal system addresses the same regulatory issues in practice. This allows the study to identify not only textual and conceptual differences but also divergences in regulatory approach and enforcement mechanisms. For example, the analysis contrasts the extraterritorial reach of the GDPR, as defined under Art. 3 of the Regulation, with the predominantly territorial scope of Azerbaijani data protection law, as well as the GDPR's clearly defined legal bases for data processing with the relatively underdeveloped and scattered provisions in Azerbaijani framework, within a functional comparative methodology.

In addition to textual and normative comparison, the study employs a critical legal analysis to evaluate the effectiveness and adequacy of Azerbaijani data protection framework in practice. This involves interpreting the substantive content of laws, examining their implementation potential, and reflecting on their alignment with international standards and best practices.

The doctrinal approach was adopted to examine the legal framework governing personal data protection, allowing for a structured interpretation of relevant legal provisions and facilitating an understanding of how core principles are interconnected within the system. Additionally, the analytical method is employed to evaluate the internal consistency, normative clarity, and effectiveness of each framework. Furthermore, attention is paid to address terminological contradictions and institutional differences, both of which have the potential to have an effect on the efficient implementation of data protection standards.

III. Substantive Legal Comparison between Azerbaijan's Law and the GDPR

III.1. Scope of Application

The Law of the Republic of Azerbaijan No. 998-IIIQ "On Personal Data" (2010) implemented the first comprehensive regulation on data protection in the country. Before this law, there was not a unified and specific normative framework for the protection of personal data in Azerbaijan. It is true that although laws such as the "On Biometric In-

formation” (2008) and the “On Information, Informatization, and Protection of Information” (1998) exist, the implemented legal norms had a scattered, unsystematic, and hard-to-control structure. The Law of the Republic of Azerbaijan No. 998-IIIQ (2010) determines the legal relationship related to the collecting, processing, and protection of personal data, as well as the rights and responsibilities of the state and other subjects in this area. Additionally, the law also encompasses issues such as controlling personal data at the national sphere and its cross-border transfer. The main goal of the law is not only to determine the current principles in the field of personal data regulation, the foundations of state control, and the rules for processing and transferring data in information systems, but also to guarantee the privacy of an individual’s private and family life legally as well as human and civil rights and freedoms. (Para. 1). Although both the GDPR and the Law of the Republic of Azerbaijan No. 998-IIIQ (2010) serve similar goals, some differences are observed regarding their rules and scope.

The first legal gap in the law is that, although its scope encompasses both legal entities and natural persons, it contains no provision regarding the representations or branches of foreign legal entities in the Republic of Azerbaijan. However, under Art. 53 of the Civil Code of the Republic of Azerbaijan¹³, representations and branches may act on behalf of a foreign legal entity. In this regard, it should be explicitly stated in this law or in future legislation that the scope of application should include representative offices and branches of foreign legal entities. When it comes to the natural persons, laws on data protection and data privacy equally apply to all the individuals whose personal data is collected, stored, processed, and used in the Republic of Azerbaijan and are applied both to the citizens of the Republic of Azerbaijan and citizens of foreign states. Unlike the GDPR, the norm is not provided for the protection of the personal data and the extraterritorial application of data privacy in Azerbaijan’s law. In the context of increasing cross-border data processing, the absence of explicit provisions on the extraterritorial application of personal data protection rules constitutes a

¹³ Civil Code of the Republic of Azerbaijan (1999, December). Available at: <https://e-qanun.az/framework/46944> [Accessed 24.08.2025].

significant gap in the current legal framework, because the rise of complex global challenges has increasingly called into question traditional objections to extraterritorial jurisdiction (Walsh, 2013). As a result, there are no direct or indirect norms presented regarding situations such as a “foreign operator” or the processing of Azerbaijani citizens’ data by a subject operating abroad. For example, if a foreign company collects data on Azerbaijani citizens from abroad, the power to influence this activity is weak with the existing legislation. In fact, norms governing the cross-border transfer of data are set out in Art. 14 of the Law of the Republic of Azerbaijan No. 998-IIIQ (2010). However, these norms primarily apply to local entities that transfer data, and they do not define specific requirements concerning the data processing activities of foreign entities or the security guarantees applicable to such activities.

However, the GDPR is a regional regulation, its scope extends beyond the borders of the EU (Voigt and Bussche, 2017). Thus, the GDPR carries global importance not only for EU member states but also for other countries wishing to create economic relations with the EU. In other words, Art. 3 of the GDPR determines its geographical scope and encompasses three major situations: 1) data processing activities carried out within the borders of the EU; 2) offering of goods and services to individuals located in the EU, regardless of whether they are processed within the EU, and 3) monitoring of their behaviour located in the EU. If a data controller and a person or organization that acts on their behalf operate within the EU, the norms of the GDPR apply. At this point, the most important condition is that the data subject is situated within the EU borders. Consequently, it does not matter whether this person is an EU citizen or not. For legal entities, the fundamental criterion is not where they are registered but where they operate. For instance, if a legal entity that is established and registered in Azerbaijan processes personal data within the framework of economic relations with Germany, this activity will fall under the jurisdiction of the GDPR, and as a result, the norms of the GDPR will apply in case of violations.

According to Art. 3(2)(b) of the GDPR, tracking internet users’ behaviour via cookies is considered “behavioural tracking.” If this tracking is applied to individuals who live in the European Union, the activity of data processing is encompassed by the scope of the GDPR. In the EU

region, the intention to offer goods and services of the data controller to individuals located in the EU is of particular importance for the application of the GDPR. If a company directs goods or services to these individuals, the norms of the GDPR must apply. At this point, clear expression of intention is very important. For example, using the English language on any website and providing an email address is not sufficient for application. But, using a widely spoken language in the EU and offering the euro or other currencies as payment choices is an obvious example of the existence of clear intention.

Based on this foundation, it is possible to say that even if located outside the EU, platforms operating within the EU, such as Amazon, Google, and Meta, must comply with requirements of the GDPR. The GDPR's extraterritorial reach allows it to exert influence globally, thereby challenging conventional notions of sovereign immunity and non-intervention. This approach to extraterritoriality differs from the stance taken in the *Lotus* case (1927), where the Permanent Court of International Justice held that states are free to determine their own domestic legal norms, provided that they do not contravene any explicit rule of international law.¹⁴

III.2. Conceptual Framework: Alignment of Key Definitions

An accurate legal definition of personal data in regulations is an important tool for the effectiveness of its subsequent implementation mechanisms. An analysis of some terms used in the national legislation shows that it is behind in comparison to the GDPR. For instance, in the Law of the Republic of Azerbaijan No. 998-IIIQ (2010), personal data is described as any information that can identify a person directly or indirectly, but it is not clearly mentioned which information is considered direct personal data and which is considered indirect personal data. Direct personal data typically includes identifiers such as a person's name, surname, identification number, and date of birth, whereas indirect personal data may encompass information such as IP addresses,

¹⁴ The PCIJ Judgement. The case of the S.S. "Lotus" (France v. Turkey), Judgment No. 9, 1927 PCIJ (ser. A) No. 10. (Sept. 7). (1927). Available at: https://www.worldcourts.com/pcij/eng/decisions/1927.09.07_lotus.htm [Accessed 18.06.2025].

mobile device IMEI codes, cookies, and patterns of user behaviour. In this regard, the definition mentioned does not fully and comprehensively explain the notion of personal data. On the other hand, according to Art. 3.0.2 of the Law of the Republic of Azerbaijan 1024-IIQ (2005), information about private and family life is equated with the notion of personal data. This approach shows that the national legislator interprets the notion of personal data in a wider framework and directly links the inviolability of private life with the protection of personal data. This naturally leads to confusion.

The notion of personal data is regulated more systematically and broadly through the GDPR and is now defined as any information relating to a specific or identifiable natural person (Art. 4.1). This individual can be determined directly or indirectly, especially based on their name, identification number, geographical location indicators, online identifiers, and physical, genetic, psychological, economic, cultural, or social characteristics. This definition can include both information that directly reveals a person's identity and other content that allows for the indirect identification of an individual. This definition can encompass both information that directly reveals an individual's identity and other content that allows for the indirect identification of an individual.

In contrast to the legislation of the Republic of Azerbaijan, the GDPR further broadens the scope of personal data to add genetic information (Art. 4.13), biometric information (Art. 4.14), and health-related information (Art. 4.15) of natural individuals. Nevertheless, the legislation of the Republic of Azerbaijan adopts a general approach to this area, recognizing the individual's fingerprints, facial image, eye retina, voice recording, DNA analysis results, body measurements, handwriting, and signature as defining characteristics of personal data.¹⁵ Regulating this concept not in the primary data protection law, "On Personal Data," but instead in a separate and more general statute, "On Biometric Information," creates legal uncertainty and undermines the consistency of the regulatory framework, particularly given the heightened sensitivity of biometric data.

¹⁵ Law of the Republic of Azerbaijan No. 651-IIIQ "On Biometric Information." Art. 35.1.

In general, the legislation of the Republic of Azerbaijan recognizes four groups of subjects as the primary participants in the field of personal data protection: the subject of personal data, the data owner, the operator, and the user. In the GDPR, these are primarily defined as the data subject, controller, processor, recipient, and the third party. Regarding the data subject, the Law of the Republic of Azerbaijan No. 998-IIIQ (2010), proceeding from the same position as the GDPR, considers the natural person whose personal data is collected, processed, and protected, and who is identified or identifiable as the subject of personal data (Art. 2.1.2). In Azerbaijan's law, the term "owner" refers to a state or local self-government body, or a legal or natural person who holds the rights of ownership, use, and control over a personal data information system or resource, and determines the purposes of personal data processing (Art. 2.1.9). The term "controller" used in the GDPR considers a natural and legal entity, public authority, agency or any other body that, independently or collaboratively with others, determines the goals and means of processing personal data (Art. 4.7). Although the terms are similar in the general context, a minor difference is noticeable in the terms of legal interpretation. Consequently, the owner is legally and technically responsible for the information system. Thus, its institutional function is highlighted at the core of its ownership. Nevertheless, the notion of a controller in the GDPR does not have such a technical nature. The controller determines the goals and means of data processing. However, this does not mean technical ownership of the information system, instead who has the authority to make decisions regarding the data.

The next term that is used in the legislation of the Republic of Azerbaijan is "operator." The operator is considered the owner of personal data, responsible for its collection, processing, and protection or the state or local government body or legal or natural person to whom these functions are assigned to a certain degree and under specific conditions. Two problematic issues arise in the legislative approach. First, the operator is equated with the owner of the personal data. More precisely, the operator is understood as the person who both makes decisions in accordance with the data subject's wishes and carries out the given instructions. Second, the idea that the operator's power can be

transferred “to a certain extent and under certain conditions...” is an excessively abstract notion because the extent and conditions of the authority that will be granted are not specified.

The term “operator” partially aligns with the term “processor” in the GDPR. Therefore, according to the GDPR, a processor is a natural or legal entity, state body, agency or any other body that processes personal data on behalf of the controller (Art. 4.8). Thus, the notion of a processor appears to be limited solely to execution functions. There is clearly a significant need for clarification, as the approach adopted by Azerbaijani law is multifaceted and broad. By contrast, the legal boundaries between the concepts of “processor” and “controller” are clearly defined in the GDPR.

The other participant acts as the user of the personal data. According to the Law of the Republic of Azerbaijan No. 998-IIIQ (2010), the user is a state or local government body, a legal or natural entity who has the right to use personal data within their authority and in the manner and scope identified by the data subject, only for the aim of acquiring information essential for their needs (Art. 2.1.11). In the GDPR, the term “recipient” is used, which aligns with this notion. The recipient may be any natural or legal entity, government body or any other organization to whom personal data is transferred or revealed (Art. 4.9). The main difference is that in the legislation of Azerbaijan, the user obtaining information is limited by the phrase “...in the manner and scope determined by the owner...”. Furthermore, the information acquired by the user should only be what is essential for them. However, there are no limiting requirements established for the recipient regarding the scope and purpose of such information. Additionally, when a state making an inquiry under the GDPR is notified, this situation is regulated by specific rules. However, no such exception is provided for the user in the Law of the Republic of Azerbaijan No. 998-IIIQ (2010). Consequently, the GDPR approach is more comprehensive and flexible in nature.

Finally, the term “third party” as defined by the GDPR (Art. 4.10) is generally not provided for in the legislation of Azerbaijan.

The term “pseudonymization” is also used in the GDPR as a new notion (Art. 4.5). This notion is a technique used to guarantee that personal data is not known to belong to a particular person. In this case,

supplementary information identifying the data owner is stored separately and protected by specific technical and organizational measures. Consequently, without the additional information, the fundamental data can no longer be linked to a specific person independently (Art. 4.5). Thus, data that has been modified in this manner is still considered personal data and is subject to the GDPR rules (GDPR, Recital 26) because this data along with additional information can be related to a particular person and their identity can be determined. It should be noted that the notion of “pseudonymisation” is not used in any normative document of Azerbaijan’s personal data legislation. In this regard, it is essential for this concept to be normatively defined separately in national legislation and for the legal framework to be established.

However, the Law of the Republic of Azerbaijan No. 998-IIIQ (2010) characterizes the notion of anonymization and defines it as bringing personal data in a state that does not allow for the identification of the data subject (Art. 2.1.15). The concept of anonymization, achieved through randomization and generalization,¹⁶ aligns with the regulatory approaches of Azerbaijan and the GDPR (GDPR, Art. 5(1) (e)). For comparison, it should be noted that, unlike pseudonymized data, anonymized data is information that no longer permits the identification of the data subject; therefore, it is regarded as data whose ownership cannot be determined. Consequently, the GDPR does not apply a specific protection regime for anonymized data (GDPR, Recital 26).

The comparisons conducted show that the legal status, functions, and mutual relationships of entities engaged in personal data processing under Azerbaijani legislation have not been fully clarified or addressed in a systematic manner. Therefore, it is essential to align current concepts with the level of technological advancement and international and European standards, to clearly identify functions, and to allocate responsibility precisely. All of these will significantly enhance the quality of work by data owners, as well as government and local institutions engaged in this domain.

¹⁶ Art. 29 Data Protection Working Party (A29WP) (2014). Opinion 05.2014 on Anonymization Techniques, 0829.14.EN, WP216. Brussels, pp. 1–37. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf [Accessed 24.08.2025].

III.3. Processing Principles and the Protection of Data Subject Rights

The processing, collection, storage, use, and transfer of personal data must be carried out in accordance with the law. A valid legal basis is the primary requirement for lawful processing. Otherwise, the processing of personal data is considered unlawful and may give rise to legal liability. In this regard, the consent of the data subject is indicated as the main legal tool for the collection of personal data in Art. 8.1 of the Law of the Republic of Azerbaijan No. 998-IIIQ (2010). Furthermore, the legislation provides for certain situations related to the protection of state and public interests (Art. 9). However, other alternative legal bases, such as the performance of a contract, are either only partially regulated or not mentioned at all. By contrast, the GDPR specifies six essential legal bases for the processing of personal data (Art. 6), which form a more comprehensive and coherent regulatory framework compared to Azerbaijani law.

In the Law of the Republic of Azerbaijan No. 998-IIIQ (2010), the fundamental principles for the collection, processing, and protection of personal data are specified, including those provided for in the Constitution, specifically the principles of legality, confidentiality, and the reconciliation of voluntariness with compulsion (Art. 4). Because of this approach being quite broad, it can reduce the practical effectiveness of principles during the protection of personal data.

The fundamental principles are specifically listed in Art. 5 of the GDPR. The first of these principles is “Lawfulness, Fairness and Transparency,” and only one of these, the principle of legality, is included in Azerbaijani legislation (Art. 4). Among the key principles, fairness stands out as one of the most debated yet least clearly defined concepts. Fairness is frequently reduced to compliance with procedural requirements. However, meeting formal conditions does not always guarantee that data processing outcomes are fair. Therefore, additional elements such as good faith, non-discrimination, the prevention of harmful effects, and respect for individual autonomy should be taken into account when interpreting this principle (Häuselmann and Custers, 2024).

Subsequently, “Purpose limitation” requires that data must only be collected only for predetermined clear and lawful purposes and should not be processed in a way that contradicts these purposes. Occasionally, the initial goal changes over time or may arise new purposes. In this case, if the processing is not based on new consent or another legal basis, the data controller must assess the compatibility of the new purpose with the original purpose based on the GDPR. Although the GDPR establishes a number of criteria for this, this principle is reflected incompletely in the Law of the Republic of Azerbaijan No. 998-IIIQ (2010). Specifically, while it is stated that personal data must be collected only for legal, predetermined and declared purposes and processed through methods suitable for those specified purposes (Art. 9.1) analogical verification criteria are not provided for in Azerbaijan’s law.

According to the principle of data minimization, personal data must be collected and utilized only to the extent necessary and adequate for processing purposes (GDPR, Art. 5.1(c)). It should be highlighted that while this principle is not explicitly stated as a separate principle in the Law of the Republic of Azerbaijan No. 998-IIIQ (2010), it is reflected within the framework of the conditions considered during the processing of personal data: *“The volume and nature of personal data collected and processed must align with declared purposes and the rights of the owners”* (Art. 9.2).

The subsequent principle, accuracy ensures that personal data is accurate and updated as needed. Regarding this principle, the approach of the GDPR (Art. 5.1(d)) and Azerbaijan’s law (Art. 9.3) is the same.

Nevertheless, it is difficult to say the same opinion when comparing the “Storage limitation.” This principle requires that personal data be kept only for as long as essential to achieve the purposes for which it was processed (GDPR, Art. 5.1(e)). Similarly, the Law of the Republic of Azerbaijan No. 998-IIIQ (2010) requires the immediate destruction of data when the goals of collecting and processing personal data are attained and the necessity for their retention has ceased (Art. 9.4). However, Azerbaijan’s law does not provide a clear mechanism for determining who is responsible for destroying the data and what procedure they should follow. Furthermore, there are no defined legal or technical criteria for evaluating the data retention period.

Finally, according to the principle of “integrity” and “confidentiality,” personal data must be safeguarded through appropriate technical and organizational measures against unauthorized or unlawful processing, as well as accidental loss, destruction, or damage (GDPR, Art. 5.1(f)). This principle aims to ensure both the integrity and the confidentiality of personal data. It is also closely linked to the concept of “security of processing” enshrined in Art. 32 of the Regulation, which requires a risk-based approach. In this regard, measures such as encryption, pseudonymization, audit mechanisms, and internal policy frameworks are recommended as practical safeguards. The Law of the Republic of Azerbaijan No. 998-IIIQ (2010), adopts a similar position (Art. 5.8), however, unlike the GDPR, it does not explicitly embrace a risk-based approach. Instead, the determination of appropriate technical and organizational measures is delegated to a separate normative act. Specifically, the Order of the Cabinet of Ministers of the Republic of Azerbaijan No. 161 (2010) stipulates concrete security obligations for information systems processing personal data (Art. 2). While this regulatory framework provides clarity in terms of technical safeguards, it lacks the flexibility and contextual adaptation inherent in the GDPR, where security measures are designed to correspond to the likelihood and severity of risks to individuals’ rights and freedoms.

Differences are observed between the GDPR and the Law of the Republic of Azerbaijan No. 998-IIIQ (2010), regarding the consent mechanism, which plays a crucial role in the processing of personal data. Under the GDPR, consent must be freely given, specific, informed, and unambiguous, and its withdrawal of consent must be as easy as giving it (Art. 4(11) and 7(3)). By contrast, the requirements for consent under the Law of Azerbaijan are less detailed, although they reflect efforts to approximate European standards. Article 8.1 of the Law of the Republic of Azerbaijan No. 998-IIIQ (2010) provides that consent may be granted in writing or by other means, including electronic signature. However, the specific components of consent enumerated by the GDPR are absent. Consequently, Azerbaijan’s framework is less practical, as it does not embody the requirement of explicit and clearly expressed consent by the individual regarding the processing of their personal data.

In the Law of the Republic of Azerbaijan No. 998-IIIQ (2010), the cases permitting the processing of personal data without the data subject's consent are strictly limited. These exceptions primarily include the protection of an individual's life and health, as well as the fulfilment of public interests defined by law. In contrast, the GDPR considerably broadens the scope of such exceptions by incorporating, *inter alia*, such grounds as the performance of contract, compliance with legal obligations, and the pursuit of legitimate interests (GDPR, Art. 6). Article 5 of the Law of the Republic of Azerbaijan No. 998-IIIQ (2010) distinguishes between two categories of personal data: open and confidential, with each category subject to different levels of protection. For instance, biometric data, health-related information, and data concerning religious or political beliefs are treated as confidential and may only be processed based on the explicit consent of the data subject, unless otherwise provided by law. By contrast, information such as an individual's name or surname, when disclosed by the data subject or officially made public by law, is considered more accessible. In addition, Art. 2.1.6 of the Law of the Republic of Azerbaijan No. 998-IIIQ (2010) introduces a third type of personal data referred to as "special category data." Notably, this provision stipulates that special categories be classified either as open data or as confidential data. This indicates that the legislation of the Republic of Azerbaijan adopts a more complex classification model, distinguishing personal data as open, confidential, or special category, whereas the GDPR does not establish such a division. Primarily, this model of data protection in the legislation of the Republic of Azerbaijan differs fundamentally from the GDPR's unified approach. This is because, under the GDPR approach, personal data are subject to the same level of protection regardless of whether they are of a public or private nature. In other words, personal data are defined in a uniform manner, with only certain categories (such as health data, religious or political beliefs, biometric data) subject to stricter safeguards under Art. 9.

Another significant distinction becomes evident in the comparative analysis of two legal frameworks, specifically concerning the right to be forgotten. This right, allowing individuals to manage their personal data and request its erasure when appropriate, was first formally established in the GDPR. It gained widespread public attention following the

landmark judgment of the Court of Justice of the EU (CJEU) in *Google Spain v. AEPD and Mario Costeja González*. In that decision, the Court clarified the essence of the right to be forgotten, granting it substantial legal recognition and laying the groundwork for its consolidation within the GDPR.¹⁷ The case involved a lawyer who objected to the fact that, when his name was searched via the Google search engine, results displayed newspaper articles from years earlier covering the sale of his property due to outstanding social security debts. He argued that such information was no longer relevant and violated Directive 95/46/EC. The CJEU concluded that if personal data published in connection with an individual's name has lost its relevance or purpose, and its processing is no longer practically necessary, such data must be erased. Thus, relying on the principles of respect for private life and the purpose of limitation of data processing, the CJEU recognized the legal foundation of the right to erasure.

By contrast, the Law of the Republic of Azerbaijan No. 998-IIIQ (2010) does not recognize the right to be forgotten as an autonomous legal concept. Although Art. 7 of Law of the Republic of Azerbaijan No. 998-IIIQ (2010) underscores the necessity of obtaining the data subject's consent for data processing, it does not address the withdrawal of such consent or the erasure of personal data. As a result, the right to be forgotten remains unrecognized within the national legal framework.

One of the key differentiating elements is the right to data portability that entitles data subjects to transfer their personal data to another data controller. This right, introduced for the first time under the GDPR, grants individuals the ability to obtain personal data collected about them under specific conditions and to transmit such data to another entity. Its primary objective is to enhance the individual's control over their personal data and to strengthen user autonomy within the digital environment by facilitating greater freedom of choice (GDPR, Art. 20.1). For instance, if a person uses a service provider, such as a social network or cloud storage, they should be able to transfer their

¹⁷ The CJEU Judgement (Grand Chamber). *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Case C-131/12 (2014). Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131> [Accessed 18.06.2025].

data to another provider without obstacles. This right also places technical obligations on data controllers. Therefore, they are required to collaborate on appropriate formats to facilitate such data transfers and to ensure that their systems operate in a mutually compatible manner (GDPR, Art. 20.2). However, the Law of the Republic of Azerbaijan No. 998-IIIQ (2010) does not provide for the right to data portability, leaving this crucial aspect of personal data protection unregulated.

III.4. Legal Consequences and Penalties for Data Breaches

When examining sanctions for breaches of persons' data confidentiality, it is evident that Azerbaijan's law and the GDPR adopt distinct frameworks. Firstly, the Regulation places responsibility for the lawful processing of personal data not only on the data controller but also on the data processor. Therefore, all participants in data processing activities are liable for any infringements of the law resulting from the processing of data. In this context, under the provisions of the Regulation (Art. 3.2), sanctions may also be imposed against cloud service providers that carry out processing activities outside the EU. Although the Law of the Republic of Azerbaijan No. 998-IIIQ (2010) provides certain obligations on persons engaged in the processing of personal data, its liability provisions are formulated in a rather general manner. Article 19 of the Law stipulates that individuals who commit violations in this area shall bear responsibility in accordance with the legislation of the Republic of Azerbaijan. However, the Law itself does not define the substance, scope, or specific types of sanctions, leaving such matters to be regulated mainly by the Criminal Code and the Administrative Offences Code of the Republic of Azerbaijan.

Thus, according to the Administrative Offences Code of the Republic of Azerbaijan, the collection or processing of personal data in an information system that is subject to state registration but has not been duly registered, as well as the failure of the owner or operator to ensure the protection of such data, or the failure to destroy or discontinue their transfer within the prescribed period, entails a fine ranging from 300 to 500 manats (approximately 150 to 250 EUR) (Art. 375). In addition,

under the Criminal Code of the Republic of Azerbaijan,¹⁸ the unlawful collection or disclosure of personal or family secrets is punishable by a fine ranging from 1,000 to 2,000 manats (approximately 500–1,000 EUR), or by community service from 240 to 480 hours, or by corrective labour for up to one year. In cases involving aggravating circumstances, imprisonment may be imposed (Art. 156). Furthermore, the creation of information systems of personal data without the required license, or the operation of such systems without authorization, may result in a fine of up to four times the amount of the unlawful income, or imprisonment for a term of up to seven years (Art. 192).

The GDPR empowers national supervisory authorities of the member states to impose various administrative sanctions in cases of non-compliance with the Regulation. This mechanism aims to ensure harmonization and legal certainty within the EU.¹⁹ Supervisory authorities under the GDPR may issue fines for non-compliance with fundamental principles of personal data processing, including consent requirements and data subjects' rights, as well as for unlawful international data transfers. For undertakings, penalties can reach up to 20 million euros or 4 % of the total global annual turnover, while less severe violations carry fines of up to 10 million euros or 2 % of global turnover (Art. 83.4-5).

The comparison indicates that, in terms of liability, legislation of the Republic of Azerbaijan exhibits three main gaps: 1) sanctions for personal data violations are not primarily included in the main law but in the Criminal Code and Administrative Offences Code; 2) the amounts of fines are considerably lower compared to the GDPR; 3) criminal liability sometimes arises not directly for violations of personal data but generally for infringements of personal privacy. In other words, criminal responsibility is applied indirectly with regard to personal data protection.

Addressing these issues would require the development of regulatory mechanisms aligned with EU standards, improvements to the ex-

¹⁸ Criminal Code of the Republic of Azerbaijan (2000, December). Available at: <https://e-qanun.az/framework/46947> [Accessed 17.07.2025].

¹⁹ European Union Agency for Fundamental Rights, Council of Europe, and European Data Protection Supervisor (2018). Handbook on European Data Protection Law, pp. 1–404.

isting infrastructure, and comprehensive legislative reforms. A key element in this process is the establishment of a centralized and unified normative framework dedicated to personal data protection.

III.5. Institutional Governance and Oversight Mechanisms

The collection and use of personal data for various purposes may ultimately lead to violations of individuals' rights and unwanted interferences. Although legal mechanisms have been established at the national, regional, and international levels to prevent such situations, the existence of independent and effective supervisory authorities remains of particular importance in ensuring compliance with these rules. The supervisory mechanism for personal data protection in the Republic of Azerbaijan is relatively fragmented and multi-layered. Although the Ministry of Digital Development and Transport is primarily responsible for overseeing the implementation of the Law of the Republic of Azerbaijan No. 998-IIIQ (2010), other state bodies also hold specific competencies in this area. According to the Order of the Cabinet of Ministers of the Republic of Azerbaijan No. 161 (2010), personal data protection is carried out by the Ministry of Digital Development and Transport, the State Security Service, the Ministry of Internal Affairs, the Ministry of Justice, the Foreign Intelligence Service, the Special Communication and Information Security State Service, and the Central Bank of the Republic of Azerbaijan. As evident, no centralized authority is instituted for personal data protection in Azerbaijan, instead each state body performs these functions within its own mandate and jurisdiction.

The Law of the Republic of Azerbaijan No. 1024-IIQ (2005) initially envisaged the creation of the position of an "Information Commissioner." However, the 2012 amendments to the Law No. 1024-IIQ assigned these functions to the Commissioner for Human Rights of the Republic of Azerbaijan (Art. 42). Although the Commissioner for Human Rights submits annual general reports, the specific issues of this sphere remain unaddressed. This gap directly undermines the effectiveness of oversight in the field. Moreover, while Azerbaijan has ratified the "Convention for the Protection of Individuals with regard to Automatic processing of personal data," it has not signed the "Additional Protocol to the Convention for the Protection of Individuals with

regard to supervisory authorities and transborder data flows” (2001). However, one of the key objectives of the Additional Protocol was to ensure that each party to the Convention establishes an independent supervisory authority responsible for safeguarding personal data protection (Art. 1).

Consequently, the Republic of Azerbaijan lacks a unified and specialized authority in the area of personal data protection. Instead, various state executive bodies perform their functions within their respective mandates. The absence of a coordinated framework results in institutional fragmentation, weak oversight, and delayed responses to breaches of personal data protection. Accordingly, the formation of a single, centralized regulatory authority through legislative amendments would offer a more reliable guarantee of adequate data protection standards in Azerbaijan.

Unlike Azerbaijan’s law, Art. 51 of the GDPR requires each member state to designate one or more supervisory authorities. In cases where a country establishes more than one supervisory authority, the responsibility for determining which authority (or authorities) shall represent that state in the European Data Protection Board (EDPB) lies exclusively with the respective member state. The designated supervisory authority (or authorities) is obliged to cooperate both with domestic institutions and with the institutions of the EU to ensure the effective implementation of the Regulation. Furthermore, Art. 57 of the GDPR imposes additional obligations on supervisory authorities, such as informing the public, issuing recommendations aimed at safeguarding fundamental rights and freedoms, and fostering cooperation with other supervisory bodies. In this respect, the principal duty of a supervisory authority is to oversee and secure compliance with the Regulation within its jurisdiction.

According to the Regulation, supervisory authorities must possess an independent status and remain free from both direct and indirect external influence (Art. 52(1–4)). The mandate of the members of the supervisory authority shall not be shorter than four years (Art. 54(1)), and each member must have sufficient adequate knowledge and professional expertise in the field of personal data protection (Art. 53(1–2)).

The GDPR stipulates that every data controller, in the event of a personal data breach, must notify the supervisory authority without

undue delay and, in any case, within 72 hours of becoming aware of the breach (Art. 33). Where data processing is likely to result in a high risk, the data controller is required to consult the supervisory authority prior to carrying out the operation (Art. 36). However, the legislation of Azerbaijan does not prescribe any specific timeframe for notifying the supervisory authority in the event of such a breach.

The regulation also provides for a complaint mechanism aimed at safeguarding the rights of individuals whose personal data has been unlawfully processed. Under its provisions, a data subject who has suffered harm as a result of unlawful processing may bring claims not only against the data controller but also against the data processor. However, both the controller and the processor may be exempted from liability if they are able to demonstrate that they are not responsible for the infringement (GDPR, Art. 82). Furthermore, an individual who believes that his or her personal data has been unlawfully processed is entitled to lodge a complaint with the supervisory authority in the EU member state where he or she resides, works, or where the alleged violation occurred (GDPR, Art. 77.1). In addition, the data subject may bring the matter before a court in cases where he or she remains dissatisfied with the decision of the supervisory authority or faces undue delays in the resolution of the complaint (GDPR, Art. 78–79).

A similar approach can be found in the Law of the Republic of Azerbaijan No. 998-IIIQ (2010). Pursuant to Art. 7.4 of the Law No. 998-IIIQ, a person whose rights have been infringed may also apply not only to the court but to other executive authorities specified in Order of the Cabinet of Ministers of the Republic of Azerbaijan No. 161 (2010). Since they are numerous, each of them considers complaints within the scope of its own competence.

One of the crucial factors is that two fundamental legal instruments introduced by the GDPR to regulate the supervision mechanism are absent in the legislation of Azerbaijan. Firstly, the GDPR requires the designation of a Data Protection Officer (DPO), who is responsible for providing guidance on personal data processing, ensuring cooperation with auditing authorities, and preparing relevant compliance reports (GDPR, Art. 37). Secondly, the Regulation stipulates the obligation to conduct a data protection impact assessment (DPIA). According

to Art. 35 of the GDPR, if a data controller determines that a planned processing activity may involve risks, it must carry out an assessment prior to commencing the processing. If the assessment indicates that the processing entails a high risk and could potentially violate the Regulation, the controller is obliged to consult the supervisory authority before proceeding. By contrast, the Law of the Republic of Azerbaijan No. 998-IIIQ (2010) or other legislative acts regarding personal data does not set out a specific legal framework for assessing potential risks in personal data processing, nor does it assign a supervisory authority responsible for overseeing the outcomes of such assessments.

Finally, it should be emphasized that supervisory authorities in the EU are mandated to prepare annual activity reports detailing the measures undertaken and violations identified. These reports must be submitted to national parliaments, governments, and other competent bodies of the member states, as well as made available to the public, the European Commission, and the EDPB (GDPR, Art. 59). In Azerbaijan, according to Order of the Cabinet of Ministers of the Republic of Azerbaijan No. 161 (2010), supervisory bodies are required to conduct monitoring at least once a year to ensure the proper organization of data protection within information systems (Art. 3). However, neither the Decision nor the Law of the Republic of Azerbaijan No. 998-IIIQ (2010) provides a normative framework regulating the procedures for such monitoring or the submission of reports on its results.

Thus, based on the foregoing analysis, the principal differences between the GDPR and the legislation of Azerbaijan can be summarized in the following table.

**A comparative assessment of data protection rules
between the EU and Azerbaijan**

Main criteria	European Union	Azerbaijan
Primary legal act	GDPR (2018)	The law of Azerbaijan “On Personal Data” (2010)
Conceptual framework	Personal data is defined broadly with technical and practical criteria	Definitions are general and lacks detailed technological references

Extraterritorial application	Applies extraterritorially to non-EU entities processing EU resident's data (GDPR, Art. 3)	No clear extraterritorial scope. Application limited to national territory
Consent to data processing	Consent is composed of four critical elements: freely given, specific, informed and unambiguous (GDPR, Art. 4.11)	Consent is governed by a flexible approach that does not enforce limiting conditions (Law, Art. 8.1)
Data subject's fundamental rights	Comprehensive, broad, and modern legal guarantees.	The approach aligned with the GDPR, though some rights remain limited: right to erasure and data portability (Law, Art. 7)
Penalties applicable to breaches	Maximum EUR 20 million or 4 % of yearly revenue (GDPR, Art. 83)	Maximum fine amounting to 2,000 AZN (roughly 1,000 EUR)
Effectiveness of control authorities	Supervisory authorities of other member states cooperate by applying procedures of collaboration, consistency, and urgency	Authority is divided among several state bodies: due to the lack of a centralized system, coordination efficiency falls short of standards
Term of supervisory members	No less than four years (GDPR, Art. 54.1)	No defined period exists
Reporting of data breaches	Notification deadline is set at 72 hours	No exact time limit has been determined
Existence of DPO	Statutorily required for particular organisations (GDPR, Art. 37)	Not stipulated

Source: Developed by the author of this analysis with reference to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27.04.2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016), the Law of Azerbaijan No. 998-IIIQ (2010), Criminal Code of Azerbaijan (2000)

As a result, the systematic comparison reveals that although the legislative frameworks of the Republic of Azerbaijan and the EU on personal data protection share certain common features in the general context, they differ significantly in terms of structure, conceptual definitions, legal mechanisms, and implementation tools. These differences

primarily concern the scope of legal mechanisms, the precision of definitions, the clarity of implementation procedures, and the functionality of supervisory structures. While Azerbaijan's law incorporates certain fundamental principles and modern regulatory provisions in the field of data protection, compared to EU standards, it still requires substantial reforms both in its normative framework and in the mechanisms of enforcement.

IV. Discussion

The terminological approach adopted by the GDPR in defining the concept of personal data is precise, comprehensive, and fully aligned with contemporary technological requirements (Art. 4(1)). As Purtova (2018) observes, the notion of an "identifiable person" under the GDPR is closely tied to the idea of the targetability within the information society, meaning that any form of connection enabling behaviourally driven targeting or decision-making regarding an individual is considered personal data. Thus, Purtova's analysis underscores that the GDPR frames the concept of personal data not merely as a legal formalism but as one that is functionally and technologically responsive. Drawing inspiration from this perspective, the present study points out the importance of normative reforms in the legislation of the Republic of Azerbaijan.

Unlike the GDPR, Azerbaijan's law does not explicitly address digital identifiers such as cookies, device IDs, or profile-based targeting tools, which are central to contemporary data-driven environments. Consequently, the legal framework should be reformed to accommodate the challenges of the digital era. This includes treating biometric, health-related, and digital identifiers within a unified legal framework, thereby redefining the concept of personal data in line with modern technological realities, an issue that ought to be taken into account in future amendments to the Law of the Republic of Azerbaijan No. 998-IIIQ (2010).

The current study illustrates that the extraterritorial application of the GDPR constitutes one of its key legal innovations. Kuner et al. (2021) argue that this approach challenges the very notion of legal sovereignty in the global digital economy and provides a modern instru-

ment for governing cross-border data flows. In comparison, the legislation of Azerbaijan remains confined to a local framework and displays clear legal gaps in regulating the responsibilities of international actors. The scope of application explicitly articulated in Art. 3 of the GDPR, with its extraterritorial reach, stands in stark contrast to the more limited and fragmented regulation under Azerbaijan's law. This finding reinforces Greenleaf's (2014) concept of the "comprehensiveness deficit." Greenleaf highlights that in several Asian jurisdictions, such as the Philippines and Thailand, privacy legislation is formally in place but suffers from serious shortcomings in terms of scope and enforcement mechanisms. In this regard, the results of the present study align with Greenleaf's observations, particularly in demonstrating the necessity of developing the scope application in Azerbaijan's data protection framework.

Moreover, while Azerbaijan's law employs terms such as owner, operator, and user, the GDPR makes use of the concepts of controller, processor, recipient, and third party, which determine normative functions and the boundaries of legal responsibility with greater precision. Bygrave (2002) highlights the importance of maintaining consistent terminology as a necessary condition for legal clarity and effective allocation of obligations. However, the research reveals that in the Law of the Republic of Azerbaijan No. 998-IIIQ (2010), the notion *operator* may encompass the functions of both a controller and a processor. In this context, Fuster (2013) notes that significance of terminological distinctions and their role in safeguarding individual rights, which directly corresponds with the core objectives of the current study.

The research on data subject rights has evidenced that, unlike the GDPR, Azerbaijan's law does not fully provide for such important rights as the right to erasure and the right to data portability. Nonetheless, these rights are considered one of the essential attributes of modern legal governance in ensuring the protection of digital identity. The Estonian experience, which can serve as a model in this regard, demonstrates that the integration of digital technologies with legal mechanisms in the field of personal data protection produces effective results. As emphasized in the study by Solvak and Vassil (2016), in Estonia, transparency, respect for data subjects' rights, and the robustness of

legal grounds in data exchange constitute fundamental principles of digital governance. This may serve as a reference point for Azerbaijan in terms of introducing more precise mechanisms within legislation.

In the field of sanctioning mechanisms, Greenleaf (2021) points out that the scope and severity of measures applied to strengthen effective personal data protection should be deterrent. Hert and Papakonstantinou (2012) assess the fines imposed under the GDPR for infringements as an effective and preventive sanctioning model. By conducting this comparative analysis, the research may serve as a driving force for amending the relevant provisions of the Criminal Code and Administrative Offences Code of the Republic of Azerbaijan concerning personal data protection.

Brown and Korff (2021) note that the effective operation of supervisory authorities is possible not only through legal independence but also through institutional and functional guarantees. This aspect, while meeting the requirements set out in Art. 52 of the GDPR, also provides an academic basis for comparative findings that reveal the gaps in Azerbaijan's supervisory mechanisms in relation to EU standards.

Greenleaf and Kaldani (2025) write that while several Central Asian countries have adopted regulatory frameworks resembling the GDPR, enforcement and implementation mechanisms remain underdeveloped. Their analysis demonstrates that in the absence of effective supervisory structures, the legal impact of regulatory instruments is considerably weakened. In Azerbaijan, the supervisory authorities lack a centralized institutional status and operational mechanisms, which in turn limits their capacity for effective communication and their ability to respond promptly to violations. This situation diverges significantly from the concept of independent supervisory authorities envisaged under the GDPR (Art. 52–59). Consequently, the findings of this study may also serve as a warning for Azerbaijan, emphasizing the urgent requirement for reform and further improvement of the regulatory framework.

Hajduk (2021) analyzes the powers of supervisory authorities under the GDPR as a basis for shaping personal data processing practices. It is argued that the independence endowed upon supervisory authorities under the Regulation enables them to exercise their full competencies, which in turn influences practice across regulated entities. Admin-

istrative penalties play a crucial role, as their imposition sets precedents that encourage other entities in similar circumstances to align their practices with the standards defined in such decisions. In addition, guidance such as opinions, recommendations, and field-specific codes issued by supervisory authority functions as a reference for administrators, thereby providing a notable preventive effect.

Kasirzadeh and Clifford (2021) critically examine the extent to which the principle of fairness is integrated into the requirement of conducting a Data Protection Impact Assessment (DPIA) under Art. 35 of the GDPR (730). Their findings indicate that the current regulatory guidance offers only limited clarification on the operational definition of fairness, leaving its practical interpretation largely to the discretion of data controllers. This regulatory gap not only generates technical and organizational challenges but also significantly undermines the effective implementation of fairness in practice. The author's insights are particularly relevant for the present study, since the legislation of the Republic of Azerbaijan does not currently provide for a DPIA mechanism. Consequently, legal and ethical risks associated with high-risk data processing activities cannot be adequately assessed in advance. In this context, the study offers practical implications for Azerbaijan, emphasizing the importance of establishing a risk-based governance framework and translating the fairness principle into actionable standards.

Similarly, Fenwick (Fenwick et al., 2017) writes that the rapid advancement of technology has consistently outpaced the modernization of legal frameworks, thereby limiting the law's capacity to effectively address emerging challenges. From this perspective, Azerbaijan should seek to adopt GDPR standards more comprehensively and set the objective of bringing its data protection regime in line with the highest international benchmarks in the near future.

Analyzing the sociological and normative philosophy of data protection law, Pichlak and Gaczol (2023) identify two core approaches to the implementation mechanisms of the GDPR: simple reflexivity and advanced reflexivity. According to them, simple reflexivity refers to a normative system that merely monitors its own functioning, whereas advanced reflexivity signifies a legal system that does not only react

but also operates as a preventive and adaptive learning mechanism. The study defines that at the level of advanced reflexivity, the GDPR introduces instruments such as risk-based approaches, Data Protection Impact Assessments (DPIAs), and data protection by design. These tools transform the GDPR into more than a legal act, turning it into a dynamic governance instrument. By contrast, when compared with these findings, Azerbaijan's legislative framework on personal data protection remains fragmented across multiple normative acts and currently operates at the level of simple reflexivity. As a result, the tools of characteristic of advanced reflexivity has not yet been fully integrated into the national legislation. Consequently, the enhancement of Azerbaijan's legal framework requires not only strengthening substantive provisions but also the institutional embedding of reflexive approaches in the application of the law.

According to Buckley et al. (2024), the future of the GDPR can be assessed through four main drivers: geopolitical dynamics, the effectiveness of enforcement structures, public trust, and the rapid pace of technological change. This framework is equally relevant for Azerbaijan's law, where data protection continues to display notable shortcomings. In particular, supervisory authorities face limitations in institutional capacity, cross-border data transfer mechanisms remain underdeveloped, and the legal system has yet to establish flexible tools to address emerging technological challenges. Against this backdrop, three reform priorities appear essential: a) strengthening supervisory bodies and clarifying the scope of their powers; b) aligning data transfer procedures with established international standards, and c) designing a responsive legal framework capable of adapting to rapid technological change.

According to B. Kinikoglu's (2023) comparative research on Türkiye's domestic data protection legislation and the GDPR offers several findings that are highly relevant to the current situation in Azerbaijan. The research notes that Türkiye's decision of a comprehensive data protection law through a rapid legislative process, carried out without sufficient public deliberation, has created considerable challenges for both societal and business adoption. As a result, Türkiye's legislation does not incorporate key rights such as the "right to erasure" and the "right

to data portability,” thereby limiting both the scope and effectiveness of data subject rights. Furthermore, in the context of cross-border data transfers, the Turkish law relies solely on the principles of explicit consent and adequacy, without providing alternative mechanisms such as “Standard Contractual Clauses” or “Binding Corporate Rules.” Similar findings in the existing literature indicate that Azerbaijan’s legislation likewise exhibits significant gaps regarding both the scope of data subject rights and the safeguards for cross-border data transfers. These observations underscore the importance of broad and comprehensive deliberations during legislative reforms in Azerbaijan, while also highlighting the need to ensure long-term alignment with GDPR standards in order to mitigate comparable risks.

V. Conclusion

Today, the rapid development of technological tools, particularly the emergence of platforms facilitating direct user participation, has resulted in the extensive collection and processing of personal data. In this context, the presence and efficacy of legal regulations regarding the protection of personal data are critically significant. The EU’s GDPR document is recognized as a widely accepted international normative framework that establishes legal standards. In this regard, the systematic approach proposed by the GDPR can be considered an exemplary model for the pertinent legislation of the Republic of Azerbaijan, in both theoretical and practical contexts. A systematic comparison between the GDPR and Azerbaijan’s law, specifically the Law of the Republic of Azerbaijan No. 998-IIIQ (2010) has shown that the GDPR provides a more comprehensive and systematic approach in terms of the scope of application of the legislation. EU law applies not only its territorial boundaries but also to entities that supply goods and services to EU citizens in general and monitor their behaviour. Azerbaijan’s law does not contain any norms regarding extraterritorial application within itself, and legal uncertainty is specifically observed in case of the representative offices and branches of legal entities in Azerbaijan.

Systematic comparison has demonstrated that the most important and modern concepts of personal data protection are based on legisla-

tion within both legal systems. Nevertheless, EU legislation has encompassed numerous discrepancies regarding terminological precision and the explicit determination of the definitional boundaries. Therefore, the GDPR distinctly separates legal responsibilities and functions through the use of concepts such as controller, processor, recipient, and third party. Azerbaijan's law uses terms such as "owner," "operator," and "user." While the term "owner" has a terminological meaning that is entirely distinct from these, it actually corresponds to a certain extent to the concept of a "controller." On the other hand, the term "operator" encompasses specific features of both "controller" and "processor" concepts in the GDPR; it poses some practical challenges. The term "user," while partially similar to "recipient" in the GDPR, is more constrained in both functional and normative contexts.

Regarding fundamental principles and rights, both legal systems also have different directions. The GDPR explicitly delineates principles and rights related to data processing, which are broadly acknowledged. Azerbaijan's law, while encompassing certain principles, possesses inadequate mechanisms for their implementation and protection. The Law of the Republic of Azerbaijan No. 998-IIIQ (2010) does not incorporate key GDPR requirements, including the need for consent to be freely given, specific, informed, and explicit (Art. 6), as well as the obligation to provide data subjects with comprehensive information regarding the conditions under which their data will be transferred (Art. 13–14).

The classification of data into public and private categories in the Law of the Republic of Azerbaijan No. 998-IIIQ (2010), along with the implementation of a dual protection framework and the lack of contemporary rights such as "right to erasure" and the "right to data portability," suggests that it is time for new changes to be made to the Law.

In the area of sanctions enforcement, the GDPR is more stringent and imposes substantial financial penalties. In the EU, penalties are determined as either a fixed amount or a percentage of the company's annual turnover, specifically 2 % or 4 %. In Azerbaijan's law's imposition of penalties up to approximately 1,000 EUR indicates that the sanctions are deficient in terms of scope, scale, and impact.

One of the crucial reforms needed in the Law of the Republic of Azerbaijan No. 998-IIIQ (2010) are related to the independence and

functionality of supervisory authorities. The GDPR requires that supervisory authorities function with total independence. This requirement is one of the important elements for the institutions involved to function more efficiently, flexibly, and sustainably. In Azerbaijan, there is no single, centralized audit institution. While the Law of the Republic of Azerbaijan No. 998-IIIQ (2010) imposes obligations for data “controller” and “processor,” it does not benefit from the “Data Protection Officer” (DPO) and data impact assessment obligations offered by the GDPR. In practice, even if the supervisory authority exists, the Law of the Republic of Azerbaijan No. 998-IIIQ (2010) must be updated immediately regarding the swift investigations of violations, the precision of audits to be conducted, accountability, and transparency. The ongoing and systematic implementation of legal reforms in Azerbaijan in the future, taking into account current practices and ensuring international standards, will enhance regulations regarding personal data protection.

References

Aljeraisy, A., Barati, M., Rana, O. and Perera, C., (2021). Privacy Laws and Privacy by Design Schemes for the Internet of Things. *Acm Computing Surveys*, 54(5), pp. 1–38, doi: 10.1145/3450965.

Anderson, C., Baskerville, R. and Kaul, M., (2021). The Travel of Privacy Standards and Regulations in Healthcare. *Proceedings of the 54th Hawaii International Conference on System Sciences (2021)*, pp. 3859–3868, doi: 10.24251/hicss.2021.467.

Brown, I. and Korff, D., (2021). *Exchanges of Personal Data After the Schrems II Judgment and the Role of DPAs*. Study for the LIBE Committee, European Parliament, pp. 1–119, doi: 10.2139/ssrn.3884896.

Buckley, G., Caulfield, T. and Becker, I., (2024). How might the GDPR evolve? A question of politics, pace and punishment. *Computer Law and Security Review*, 54(106033), pp. 1–14, doi: 10.1016/j.clsr.2024.106033.

Bygrave, L.A., (2002). *Data Protection Law: Approaching its Rationale, Logic and Limits*. The Hague, New York: Kluwer Law International.

De Hert, P. and Papakonstantinou, V., (2012). The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals. *Computer Law and Security Review*, 28(2), pp. 130–142, doi: 10.2139/ssrn.3447095.

Ducato, R., (2020). Data protection, scientific research, and the role of information. *Computer Law and Security Review*, 37(105412), pp. 1–16, doi: 10.1016/j.clsr.2020.105412.

Fenwick, D.M., Kaal, W.A. and Vermeulen, E.P.M., (2017). Regulation Tomorrow: What Happens When Technology is Faster than the Law? *American University Business Law Review*, 6(3), pp. 1–29, doi: 10.2139/ssrn.2834531.

Fuster, G., (2013). *The emergence of personal data protection as a fundamental right of the European Union*. PhD Thesis. Brussels: Vrije Universiteit Brussel.

Greenleaf, G. and Kaldani, T., (2025). Data Privacy Laws in Central Asia: Between ex-SSR and “Belt and Road”. *International Data Privacy Law*, 15(1), pp. 67–90, doi: 10.1093/idpl/ipaf001.

Greenleaf, G., (2021). *Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance*. 169 Privacy Laws and Business International Report, 1, 3–5, UNSW Law Research Paper No. 21-60, doi: 10.2139/ssrn.3836348.

Greenleaf, G., (2014). “The Philippines and Thailand — ASEAN’s Incomplete Comprehensive Laws,” *Asian Data Privacy Laws: Trade and Human Rights Perspectives*. UNSW Law Research Paper No. 17-47, doi: 10.2139/ssrn.3000766.

Gstrein, O.J. and Beaulieu, A., (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philosophy and Technology*, 35(1), p. 3, doi: 10.1007/s13347-022-00497-4.

Hajduk, P., (2021). The Powers of the Supervisory Body in the GDPR as a Basis for Shaping the Practices of Personal Data Processing. *Review of European and Comparative Law*, 45(2), pp. 57–75, doi: 10.31743/recl.10733.

Häuselmann, A. and Custers, B., (2024). Substantive fairness in the GDPR: Fairness elements for Article 5.1a GDPR. *Computer Law and Security Review*, 52(105942), pp. 1–12, doi: 10.1016/j.clsr.2024.105942.

Kasirzadeh, A. and Clifford, D., (2021). Fairness and Data Protection Impact Assessments. *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society (AIES'21)*, May 19–21, 2021, pp. 1–8, doi: 10.1145/3461702.3462528.

Kinikoglu, B., (2023). Implementing a new data protection law: lessons from the Turkey experience. *International Data Privacy Law*, 13(1), pp. 25–46, doi: 10.1093/idpl/ipado01.

Kuner, C.B., Bygrave, L., Docksey, C. and Drechsler, L., (eds), (2020). *Data Protection Regulation: A Commentary*. Brussels; Oslo: Oxford University Press. DOI: 10.2139/ssrn.3839645.

Labadie, C. and Legner, C., (2019). Understanding data protection regulations from a data management perspective: a capability-based approach to EU-GDPR. *Proceedings of the 14th International Conference on Wirtschaftsinformatik*, pp. 1–15. Siegen.

Lim, S. and Oh, J., (2025). Navigating Privacy: A Global Comparative Analysis of Data Protection Laws. *IET Information Security*, pp. 1–18, doi: 10.1049/ise2/5536763.

Nakashima, M., (2022). Comparison of Legal Systems for Data Portability in the EU, the U.S. and Japan and the Direction of Legislation in Japan. *Proceedings of 15th IFIP International Conference on Human Choice and Computers (HCC)*, pp. 159–169, doi: 10.1007/978-3-031-15688-5_14.

Newman, A.L., (2015). What the “Right to Be Forgotten” Means for Privacy in a Digital Age. *Science*, 347(6221), pp. 507–508, doi: 10.1126/science.aaa4603.

Pichlak, M. and Gaczol, K., (2023). Simple and advanced reflexivity in GDPR enforcement: empirical evidence from DPA activity. *International Data Privacy Law*, 13(4), pp. 267–283, doi: 10.1093/idpl/ipado18.

Purtova, N., (2022). From knowing by name to targeting: the meaning of identification under the GDPR. *International Data Privacy Law*, 12(3), pp. 163–183, doi: 10.1093/idpl/ipaco13.

Shehu, V.P. and Shehu, V., (2023). Human rights in the technology era — Protection of data rights. *European Journal of Economics, Law and Social Sciences*, 7(2), pp. 1–10, doi: 10.2478/ejels-2023-0001.

Solove, D.J. and Schwartz, P.M., (2024). *Information Privacy Law*. (8th Edition). Burlington: Aspen Publishing.

Solvak, M. and Vassil, K., (2016). *E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005–2015)*. Tallinn: Johan Skytte Institute of Political Studies, University of Tartu.

Voigt, P. and von dem Bussche, A., (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Heidelberg: Springer. DOI: 10.1007/978-3-319-57959-7.

Walsh, R., (2013). Extraterritorial confusion: The complex relationship between Bowman and Morrison and a revised approach to extraterritoriality. *Valparaiso University Law Review*, 47(2), p. 629. Available at: <https://scholar.valpo.edu/vulr/vol47/iss2/27/> [Accessed 20.06.2025].

Wodi, A., (2023). The EU General Data Protection Regulation (GDPR): Five Years After and the Future of Data Privacy Protection in Review. *SSRN Electronic Journal*, doi: 10.2139/ssrn.4601142.

Yeung, K. and Bygrave, L.A., (2022). Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. *Regulation and Governance*, 16(1), pp. 137–155, doi: 10.1111/rego.12401.

Zuboff, S., (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.

Information about the Authors

Firuz M. Abbasova, Doctor of Law, Professor, Department of Criminal Procedure, Faculty of Law, Baku State University, Baku, Azerbaijan
firuza.abbasova@gmail.com
ORCID: 0009-0004-5108-4889

Kamran I. Khalilov, PhD Student, Department of Criminal Procedure, Faculty of Law, Baku State University, Baku, Azerbaijan
xalilovkamran75@gmail.com (Corresponding Author)
ORCID: 0000-0002-0086-009X

Received 28.09.2025

Revised 09.01.2026

Accepted 21.01.2026