IE University IE International Policy Review (IPR)
Journal **6 Issue 1** (2025)
https://ipr.blogs.ie.edu/

To what extent can the legal basis, implementation, and enforcement of the Azerbaijani Data Protection Law be shaped by the model of the European Union's General Data Protection Regulation (GDPR)?

Alya Rezk

Department One, Institution One, City One, Country One
Department Two, Institution Two, City Two, Country Two

E-mail: amohamedabde.ieu2022@student.ie.edu

Published: 27th of January, 2025

Abstract

Data protection rules are vital in the contemporary digital era, as the collection, processing, and storage of personal data create substantial data privacy issues. The European Union's General Data Protection Regulation (GDPR), which enforces stringent data protection rules in all EU Member States, sets a global standard for data privacy. While not a Member State, Azerbaijan created the Law on Personal Data in 2010 to govern the use and security of personal data inside its borders. This article analyzes the two legal frameworks, emphasizing their legal foundation, enforcement methods, and operational effectiveness. By studying the contrasts and similarities between Azerbaijan's data protection standards and the GDPR, the study identifies gaps in implementation and areas where harmonization is possible, particularly in cross-border data exchanges affecting EU individuals, entities, and Member States. As more countries across the world enact data privacy laws and entities increasingly conduct business across borders with disparate legal requirements, it is imperative to comprehend these differences. This study aims to determine to what extent can the legal basis, implementation, and enforcement of the Azerbaijani Data Protection Law be shaped by the model of the European Union's General Data Protection Regulation. By answering this query, the study investigates whether Azerbaijan's framework may gain by conforming to the widely accepted methodology of the GDPR.

Keywords: term, term, term

1. Introduction

The Law of the Republic of Azerbaijan on Personal Data[1] passed on May 11, 2010, marked the first comprehensive regulation of data protection in the country. Before this law, Azerbaijan lacked specific legislation governing data privacy, though the Law on Biometric Data (2008)[2] did address the collection and use of biometric data, setting the stage for more formal data protection laws. The political climate leading to the passing of the law was influenced by growing awareness of privacy concerns amid digital advancements and international pressure to align with global standards in data protection.

The new law sought to address gaps in the protection of personal data by regulating its collection, use, storage, and transfer. Before the law, Azerbaijan relied on various regulations and decrees, such as the Law on Biometric Data, and sector-specific rules. However, these were fragmented and insufficient for a unified data protection framework. The 2010 law introduced a more holistic approach, recognizing individuals' rights to privacy and the need for organizations to safeguard personal data. Importantly, the law laid down clear requirements for consent and accountability for data processors, ensuring transparency and control for data subjects.

Some regulations that preceded the 2010 law, like those on biometric data, were retained and incorporated into the new law. However, the new legislation expanded the scope, integrating more detailed provisions on the processing of data across different sectors, including employment. Certain earlier decrees were scrapped in favor of a more modernized and comprehensive approach to data privacy, targeting a higher level of compliance with international standards.

As for the EU legal landscape, the GDPR[3] came into force on the 25th of May, 2018, but was not the first of its kind in the EU. In light of the global digital economy and the speed at which technology is developing, the GDPR was passed to address growing concerns about privacy and the security of personal data. Its main goals were to improve data processing openness, uphold individuals' right to privacy, and standardize data protection regulations throughout EU member states. The GDPR aimed to guarantee that companies treated personal data properly and that people had more control over their data in light of the expanding digitization and cross-border data flows. Additionally, by offering a uniform framework throughout the EU, it sought to make the regulatory environment easier for companies. The Directive 95/46/EC of the European Parliament and of the Council of the 24th

[1] Azerbaijan Data Protection Law. Law of the Republic of Azerbaijan on Personal Data. Accessed December 3, 2024. https://family.gov.az/store/media/NewFolder/Law%20of%20the%20Republic%20of%20Azerbaijan%20%20On%20personal%20data.doc

[2] "Azerbaijan Republic, Law No. 651-IIIG, 'On Biometric Information,' June 13, 2008, as amended by Law No. 584-VIQD, July 8, 2022, CIS Legislation, https://cis-legislation.com/document.fwx?rgn=24349."

[3] European Union. 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, GDPR). Official Journal of the European Union, L 119, May 4, 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj

October 1995[4] was the first Directive the EU saw about the protection of individuals concerning the processing of personal data and the free movement of such data. The main difference between Directive 95/46/EC and the GDPR which came and superseded it in 2018, is the GDPR's wider scope which allowed it to tackle the shortcomings of the previous Directive, enhanced adaptability to be more future-proof and up-to-date with the digital sphere, and the implementation further and explicit obligations such as the Data Protection Officer (DPO)[5] and Data Protection Impact Assessments (DPIA)[6], amongst several further commitments.[7] EU Member States are all bound by the GDPR, as the GDPR operates in every Member State on a national level, ensuring the harmonization and uniformity of data protection law across the Union, additionally with Member States having their own data protection agencies domestically, such as the Agencia Española de Protección de Datos[8] (AEPD) in Spain, who provide resolutions on matters and cases concerning data protection, guides on fulfillment/adherence to GDPR, recommendations and local translation of EU Directives or Regulations when necessary.

While both the GDPR and the Azerbaijani Law on Personal Data govern data protection, their rules and scope are very different. While Azerbaijan's law is national, the GDPR is applied consistently throughout the EU. Additionally, the GDPR adds extra requirements that aren't specifically mentioned in Azerbaijani law, like the appointment of DPOs and the completion of DPIAs. Although the GDPR has more stringent standards for cross-border data transfers and offers greater individual rights, like the right to be forgotten, both laws seek to protect personal data and privacy despite these distinctions.

II. Legal Bases of GDPR and Law on Personal Data in Azerbaijan

With some similarities and some significant differences, both the GDPR and Azerbaijan's Law on Personal Data provide explicit legal justifications for data collection and processing. According to the GDPR, personal information may be gathered with the consent of the individual, to carry out a contractual obligation, to comply with legal requirements under EU or national law, for tasks that are performed in the public interest under EU or national law, to safeguard an individual's vital interests or for legitimate organizational purposes, so long as these do not conflict with the rights and freedoms of individuals.

[4] European Union. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. Official Journal of the European Union, L 281, November 23, 1995. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046

[5] European Data Protection Supervisor. "Data Protection Officer (DPO)." Accessed December 3, 2024. https://www.edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

[6] GDPR.eu. "Data Protection Impact Assessment Template." Accessed December 3, 2024. https://gdpr.eu/data-protection-impact-assessment-template/

[7] Advisera. "EU GDPR vs European Data Protection Directive." Last modified November 17, 2023. https://advisera.com/articles/eu-gdpr-vs-european-data-protection-directive/#:~:text=While%20co%2Dopting%20most%20but,effects%20for%20noncompliance%20and%20negligence

[8] Agencia Española de Protección de Datos (AEPD). "Home." Accessed December 3, 2024. https://www.aepd.es.

The same is true in Azerbaijan, where data collecting is allowed with consent, to fulfill legal requirements under national laws, to safeguard the subject's life and health, or for scientific and statistical reasons as long as the data is depersonalized. While both frameworks place a strong emphasis on consent and legal obligations, the GDPR covers a slightly wider range of topics, including legitimate organizational purposes and the public interest. On the other hand, Azerbaijan's law focuses on depersonalization for research purposes and makes no grants for organizational needs or the public interest.

III. Differences in Application

Given that there are differences in the legal basis of which personal data is collected, stored, processed, and transferred in Azerbaijan and the EU, under their respective personal data legislation, there is inevitably a difference in the application of each of the legislations.

However, it must be noted that Azerbaijan, despite not being in the EU, is familiar with the GDPR, as there are Azerbaijani entities that operate in the EU and EU residents and citizens who work with Azerbaijani entities. According to the application scope of the GDPR, all EU residents and citizens are subject to the GDPR regardless of what territory they're in, and the GDPR will apply to a company that is controlling or processing the personal data of a resident or citizen of the EU.

Furthermore, the EU and Azerbaijan have made a partnership, 'European Union 4 Azerbaijan'[9], in which on their website 'EU 4 Azerbaijan', we can find that the data controller for the matters concerning this partnership is the 'Directorate-General for Neighbourhood and Enlargement Negotiations (DG NEAR) /Directorate A / Unit NEAR.A1 Inter-institutional Relations and Communication', operating under the EU. This furthers that there is an understanding and application of the GDPR by the Azerbaijani authorities and entities.

The Ministry of Digital Development and Transport of Azerbaijan[10] is in charge of monitoring adherence to data privacy laws and has imposed sanctions for infractions. For example, companies have faced financial penalties and damage to their reputations as a result of breaches with insufficient protections for personal data. Under the Law on Personal Data, owners and operators of personal data must register their information systems with the Ministry. Failure to do so can result in administrative penalties ranging from AZN 300 to AZN 500 (approximately $180 to $300).[11] Additionally, the formation of information systems of personal data without obtaining the necessary license may lead to criminal liability under Article 192 of the Criminal Code, including fines up to four times the revenue generated from such non-licensed activity and/or up to seven years of imprisonment. While specific cases of enforcement are not extensively documented publicly, the legal framework provides for penalties, including fines, for non-compliance. For instance, repeated violations in the

[9] "EU for Azerbaijan," EU4Azerbaijan, accessed December 20, 2024, https://eu4azerbaijan.eu/.

[10] Ministry of Digital Development and Transport of the Republic of Azerbaijan. "Home." Accessed December 3, 2024. https://mincom.gov.az/en

[11] "Azerbaijan - Data Protection Overview," OneTrust DataGuidance, accessed December 20, 2024, https://www.dataguidance.com/notes/azerbaijan-data-protection-overview

sphere of personal data protection can lead to severe penalties under the Code of Administrative Offenses.

Pseudonymization of Data

With regard to the differences in the application of Azerbaijan's and the EU's data protection legislation;

Firstly we can see that in Azerbaijan, the requirement for pseudonymization (what's referred to in Azerbaijani law as "depersonalization") of data is only required with regards to collecting, processing, and transferring data for scientific and/or statistical purposes, however in the EU pseudonymization of personal data, which is incentivized in the GDPR in whichever situation it may be possible, due to the principle of 'data minimization', as indicated in "To create incentives to apply pseudonymization when processing personal data..."[12]. However, it must be highlighted that the pseudonymization of data under most circumstances, is left to the discretion of the data controller and data processor, unless it's a matter of "...processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfill those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymization of the data). In the Law on Data Protection, it's explicitly stated that "Surname, given name and patronymic of a person shall be regarded as permanently available public personal data"[13] whereas this compulsory nature of this specific set of personal data does not exist in the GDPR.

Governing Entities

According to the EU Charter of Fundamental Rights, every EU Member State has the right to protect its data. Therefore, Member States have set up national bodies, following Article 8 (3) of the EU Charter of Fundamental Rights[14], responsible for the protection of personal data in their corresponding Member States. On an EU level, there is the EU Data Protection Board (EDPB), which is composed of representatives of the national data protection authorities of the EU/EEA countries and the European Data Protection Supervisor and has the responsibility of ensuring the consistent application of data protection rules throughout the EU. The EDPB is not a governor over the national bodies established in each country, rather it is tasked with providing general guidance on key concepts of the GDPR and advising the European Commission on issues related to the protection of personal data and new proposed legislation in the EU, and adopting binding decisions in disputes between national supervisory authorities. This means every Member States national body responsible for the protection of personal data is the

[12] 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, May 4, 2016, accessed December 20, 2024, https://eur-lex.europa.eu/eli/reg/2016/679/oj

[13] Law of the Republic of Azerbaijan on Personal Data, accessed December 20, 2024, https://family.gov.az/store/media/NewFolder/Law%20of%20the%20Republic%20of%20Azerbaijan%20%20On%20personal%20data.doc

[14] "Article 8: Protection of Personal Data," European Union Agency for Fundamental Rights, accessed December 20, 2024, https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data

decision-maker when it comes to dispute resolution, all the EDPB contributes to this process would be guidance in the interpretation of the GDPR, however, the EDPB does have the right to refer a matter to the Court of Justice (CJEU) and the EDPB may intervene in cases where it is relevant to their tasks, and this right, in practical application, is not limited to cases where personal data is being process by EU institutions or bodies, but also extends to protection of personal data on a Member State level.

In Azerbaijan, the existence of a national body responsible for the protection of personal data does not exist. The institution responsible for the protection of personal data, and for executing the Law on Personal Data is the Ministry of Digital Development and Transport, however, several other ministries have vested powers to enforce applicable data protection/privacy laws, within the scope of their competencies. Subsequently, this concept will be further elaborated on in the "Policy Suggestion" section.

Constitution in the legal sphere of data protection

In the Law on Personal Data it's stated "Legislation of the Republic of Azerbaijan in the sphere of personal data shall be composed of the Constitution of the Republic of Azerbaijan, ..."[15], whereas in the GDPR, it is not stated that the Constitution of any of the States subject to the GDPR, will be within the legislation regarding personal data in that respective country. Both approaches make sense, especially given that the EU cannot implement the Constitution into the sphere of legislation for data protection when every country in the EU has a different Constitution. For example, the CJEU invalidated the Data Retention Directive in the case of Digital Rights Ireland Ltd v Minister for Communications (Joined Cases C-293/12[16]), emphasizing that any interference with fundamental rights must be proportionate and respect the essence of those rights, as enshrined in both the EU Charter of Fundamental Rights and national constitutions.[17] This jurisprudence demonstrates that the GDPR does not supersede national constitutional safeguards, despite the fact that it establishes a uniform standard for data protection throughout the EU. Rather, it collaborates with them to guarantee that data protection measures adhere to the constitutional traditions of member states and EU law.

What should be noted is the legal order to be considered in case of a dispute; given that under Azerbaijani law, the Constitution is part of the legal sphere for data protection, alongside the Law on Personal Data, and other normative acts that are given rise from the Law on Personal Data, it must be noted that if a case related to data protection is to be examined, it shall first be examined through constitutional compliance, then normative legislative acts, pursuant to the principle of following the legal order. The

[15] Law of the Republic of Azerbaijan on Personal Data, accessed December 20, 2024, https://family.gov.az/store/media/NewFolder/Law%20of%20the%20Republic%20of%20Azerbaijan%20%20On%20personal%20data.doc

[16] Radu, Case C-293/12, ECLI:EU:C:2013:39, EUR-Lex, accessed December 20, 2024, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62012CJ0293

[17] "Data Retention Directive Out: Are National Laws Next?" European Policy Review, accessed December 20, 2024, https://policyreview.info/articles/news/data-retention-directive-out-are-national-laws-next/264

question arises as to whether the application of lex specialis would be more appropriate, on a case-by-case basis, given the niche and sensitive nature of personal data protection, despite the obvious disequilibrium in the legal order of the Constitution, and a normative legislative act.

IV. GDPR Application in Spain

Among the countries that have adopted the GDPR is Spain, with a readily accessible system to gain access to all the information needed by entities and individuals concerning data privacy.

In Spain, the application of the GDPR is as per the mandates set out in the GDPR, and by the EU, and has been implemented with the Organic Law 3/2018, 5th December, on the Protection of Personal Data and Guarantee of Digital Rights ('LOPDGDD')[18]. The regulatory/supervisory authority is the 'Agencia Española de Protección de Datos' ('AEPD')[19] which is tasked with ensuring the implementation and compliance with LOPDGDD by all data processors and controllers in the territory of Spain. The AEPD provides resolutions, guidance, recommendations, and publications regarding all topics and concerns about the protection of personal data. Furthermore, in case of a sanction procedure, triggered by an infringement of the data protection legislation or claims filed by data subjects, the AEPD examines these procedures and imposes fines on data controllers and/or processors in case of non-compliance. The AEPD requires data controllers to appoint a Data Protection Officer ('DPO')[20] even in specific examples where the GDPR does not mandate it. A DPO cannot be punished in any way unless they commit fraud or gross negligence in their work. DPOs can intervene when a complaint is lodged against a data controller or processor, to a supervisory authority. Before complaining, the DPO may also intervene and communicate to the complainer, the organization's response within two (2) months upon receipt of the complaint. The AEPD reserves the right to forward the complaint straight to the DPO before attending to it, in which case the DPO has one (1) month to submit a response.

It can be argued that one of the biggest challenges being faced by the AEPD is adequately responding to all the complaints lodged, and this is a problem but due to no fault of their own. This can be inferred from Spain's amount of fines imposed in comparison to the amount of complaints received; The amount of fines imposed in 2022 was sky-high compared to the rest of the EU, reaching 378, a 47% increase in the amount of fines from the prior year. To put things into perspective, 378 fines amount to 40% of the total amount of imposed fines in the EEA in 2022. These numbers don't see a significant improvement in 2023, with 367 fines imposed, a minuscule decrease from 2022, however, these fines amounted to a total of €30

[18] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, Boletín Oficial del Estado (BOE-A-2018-16673), December 6, 2018, accessed December 20, 2024, https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

[19] Agencia Española de Protección de Datos (AEPD), accessed December 20, 2024, https://www.aepd.es

[20] "Data Protection Officer (DPO)," European Data Protection Supervisor, accessed December 20, 2024, https://www.edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

million, 44% higher than in 2022, despite fewer sanctions imposed. However, despite imposing significantly higher fines than other countries subject to the GDPR, the AEPD also receives more complaints than any other national body responsible for protecting personal data in the EU. While in 2023 they imposed 367 sanctions, which was less than the previous year, they received more complaints (21,590) in 2023 by 43% from 2022 and 55% from 2021. Yet, the AEPD, despite imposing less fines than in 2022, has earned 44% more in fines than in 2022. This may suggest that the AEPD is focusing its efforts on cases of greater economic compensation and therefore, not adequately responding to all complaints lodged.[21]

V. Application of the Law on Data Protection in Azerbaijan

According to the Law, the processing of personal data must adhere to principles of legality, confidentiality, and data minimization, as defined in Article 4. Article 9 specifies that the purpose for collecting and processing data must be explicitly defined and that the data collected must be limited to what is strictly necessary to achieve this purpose. Additionally, data should be complete, accurate, and updated as required. Article 11 further reinforces this by requiring data controllers to collect only the data necessary for the stated purpose and to inform data subjects of the reason, scope, and legal basis for processing their data. This emphasis on data minimization and transparency mirrors similar principles in the GDPR, though Azerbaijan's law is unique in its prescriptive approach to processing limitations.

Azerbaijani law places a strong emphasis on obtaining the data subject's explicit consent for processing, which is mandated under Article 8, except in cases where legal exceptions apply. Consent is generally required in written form, with data subjects granted rights to access, request corrections, prohibit further collection, and object to the processing of their data as per Article 7. Exceptions to consent requirements are strictly defined, and unlike the GDPR's broader grounds for data processing, the Azerbaijani Law provides narrower exemptions for instances where processing is necessary. This includes cases of protecting an individual's life or health, or for the public interest, where such grounds are explicitly stated.

The Law categorizes personal data into confidential and public classifications, with each category subject to different levels of protection. Article 5 defines confidential data, which includes biometric data and sensitive information related to health, religious beliefs, or political affiliations, and places strict restrictions on its transfer and use, requiring the subject's consent unless otherwise mandated by law. Public data, which includes data voluntarily made public by the subject (e.g., names), is accessible to a broader extent. Azerbaijani law's dual treatment of data based on these classifications contrasts with the GDPR's more uniform data protection approach,

[21] "Spain: AEPD Highlights Current Key Challenges in Data Protection," OneTrust DataGuidance, accessed December 20, 2024, https://www.dataguidance.com/news/spain-aepd-highlights-current-key-challenges-data

where all personal data enjoys a consistent level of protection regardless of its public or private nature.

Azerbaijan's Law also imposes specific obligations on data owners and operators in Articles 10 and 11. Data "owners" (controllers) and "operators" (processors) are responsible for ensuring data protection and must maintain the integrity, accuracy, and security of the data they process. Article 10.1 specifies that data owners are liable for damages caused by unauthorized data processing or security breaches. Operators are further obligated to ensure confidentiality and to adopt the necessary technical and organizational measures to prevent unauthorized access, alteration, or loss of data. These obligations align with data protection best practices, although Azerbaijani law does not require a Data Protection Officer (DPO) under the GDPR, nor does it impose data impact assessment obligations.

The Law's provisions on cross-border data transfer, outlined in Article 14, require that personal data only be transferred abroad if the receiving country provides protection levels equivalent to Azerbaijani standards, or if it does not threaten Azerbaijan's national security. The transfer is otherwise permitted if the data subject consents or if it is necessary to protect the subject's life or health. This restriction reflects a cautious approach to international data exchange and differs from the GDPR's cross-border framework, which operates under an adequacy mechanism determined by the European Commission.

Azerbaijan's approach to data protection oversight is decentralized, as no singular data protection authority exists. Instead, regulatory enforcement falls under the Ministry of Digital Development and Transport and other relevant sectoral ministries. Article 17 grants these authorities the power to monitor compliance, issue directives to correct violations, and enforce penalties for breaches of data protection obligations. This multi-agency oversight model differs significantly from the GDPR's requirement for independent supervisory authorities in each EU Member State, resulting in an enforcement structure in Azerbaijan that may be more complex and less unified.

VI. Policy Suggestion

Similar to Spain's Agencia Española de Protección de Datos (AEPD), Azerbaijan should think about creating an independent regulatory body to supervise the protection of personal data as part of its continuous efforts to fortify its data protection system. This recommendation is a result of the difficulties that Azerbaijan is currently facing, as the Ministry of Digital Development and Transport enforces the Law on Personal Data. The effectiveness and consistency of data protection initiatives are jeopardized by the fragmented enforcement caused by the allocation of responsibilities among several ministries, even though the ministry is crucial to the law's implementation. Therefore, it is imperative to create a centralized, independent organization to guarantee that protecting personal data is a top priority and is carried out correctly.

An autonomous authority in Azerbaijan might be built on the AEPD model, which offers a tried-and-true method of data protection. The EU's General Data Protection Regulation (GDPR), which has emerged as the standard for data protection procedures worldwide, and Spain's domestic data protection rules have both been enforced in large part by the AEPD. As an independent agency, the AEPD has the power to look into data protection infractions, impose fines, and advise people and organizations on their rights and responsibilities with regard to processing personal data. With well-defined legislative frameworks and consistent enforcement procedures, this structure guarantees that data protection is handled with a high degree of consistency.

For the Law on Personal Data to be implemented successfully, Azerbaijan would need an independent organization akin to the AEPD. A strong data protection authority is crucial given the speed at which technology is developing and the growing dependence on digital platforms for both personal and professional purposes. The AEPD model would give Azerbaijan the legal foundation it needs to protect the privacy of its people by providing unambiguous control over the processing, storing, and transfer of personal data. In order to hold people accountable for breaking the law, such a regulatory agency would be able to investigate data breaches, keep an eye on whether data protection regulations are being followed, and take enforcement action against non-compliant firms.

Azerbaijan's compliance with international norms would also be guaranteed by the creation of a specialized national data protection authority. To monitor the implementation of data protection regulations, member states are required by the General Data Protection Regulation (GDPR), which went into force in the European Union in 2018. Despite not being a member of the EU, Azerbaijan has a stake in adhering to these international norms, particularly as cross-border data flows become more prevalent in the digital economy. Azerbaijan would strengthen its domestic data protection regulations and improve its reputation in the international community by establishing an independent organization akin to the AEPD. This would build confidence with foreign organizations and individuals who are worried about the security of their personal data.

In Azerbaijan, a specialized data protection authority might serve a number of vital functions. The new authority might be charged with informing the public and organizations about their rights and responsibilities regarding the processing of personal data, in addition to making sure that the Law on Personal Data is properly enforced. Campaigns to raise public awareness are crucial for enabling people to make knowledgeable decisions about the handling of their data and for making sure that businesses are aware of their legal obligations. To keep legislation current and responsive to new technological problems, such as the application of artificial intelligence

and big data analytics, the new body might also actively advise lawmakers on changes to data protection laws.

A specialized regulatory body could provide useful solutions for companies looking to adhere to the Law on Personal Data in addition to directing legislative revisions. For instance, the AEPD offers extensive resources, such as thorough guidelines and templates, to assist enterprises in navigating the intricacies of data protection. This strategy guarantees that the law is applied consistently and equitably while also assisting businesses in meeting legal obligations. Establishing a comparable framework in Azerbaijan would encourage companies to embrace best practices in data management and assist promote a culture of compliance where privacy issues are proactively addressed.

Furthermore, a separate body would boost public confidence in the nation's data security initiatives. People's confidence would be bolstered by the institution's transparency and capacity to hold the public and private sectors responsible for their data practices. This would encourage people to feel more secure while using digital services. Since people are more inclined to reveal their personal information when they are certain that their privacy is being actively protected, public trust is crucial to the success of any data protection scheme.

This proposal is not merely a regulatory modification; it is a dedication to the protection of individual privacy and security in a world that is becoming more digital. An independent data protection organization would increase openness, foster public confidence, and strengthen Azerbaijan's standing as a reliable player in the global digital economy. Adopting this policy will enhance Azerbaijan's internal data protection landscape while also aligning it with international best practices, guaranteeing long-term resilience in the face of growing technological threats.

Bibliography

1. Advisera. "EU GDPR vs European Data Protection Directive." Last modified November 17, 2023. https://advisera.com/articles/eu-gdpr-vs-european-data-protection-directive/#:~:text=While%20co%2Dopting%20most%20but,effects%20for%20noncompliance%20and%20negligence
2. Agencia Española de Protección de Datos (AEPD). "Home." Accessed December 3, 2024. https://www.aepd.es
3. Article 8: Protection of Personal Data. European Union Agency for Fundamental Rights. Accessed December 20, 2024. https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data
4. Azerbaijan Republic. Law No. 651-IIIG, "On Biometric Information," June 13, 2008, as amended by Law No. 584-VIQD, July 8, 2022. CIS Legislation. https://cis-legislation.com/document.fwx?rgn=24349
5. Azerbaijan - Data Protection Overview. OneTrust DataGuidance. Accessed December 20, 2024. https://legacy.dataguidance.com/notes/azerbaijan-data-protection-overview
6. Caspian Legal Center. "Personal Data in Azerbaijan." Last modified February 12, 2021. https://www.caspianlegalcenter.az/insights/more/personal-data-azerbaijan
7. Data Retention Directive Out: Are National Laws Next? European Policy Review. Accessed December 20, 2024. https://policyreview.info/articles/news/data-retention-directive-out-are-national-laws-next/264
8. European Commission. "Data Protection in the EU." Last modified December 1, 2024. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en
9. European Commission. "EU Steps up Renewable Energy Cooperation with Azerbaijan." Last modified March 4, 2024. https://energy.ec.europa.eu/news/eu-steps-renewable-energy-cooperation-azerbaijan-2024-03-04_en
10. European Data Protection Board. "Processing Personal Data Lawfully." Last modified March 2021. https://www.edpb.europa.eu/sme-data-protection-guide/process-personal-data-lawfully_en
11. European Data Protection Supervisor. "Case Law and Guidance." https://www.edps.europa.eu/data-protection/data-protection/case-law-and-guidance_en
12. European Data Protection Supervisor. "Data Protection Officer (DPO)." Accessed December 3, 2024. https://www.edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en
13. European Data Protection Supervisor. "History of the General Data Protection Regulation." Last

modified March 15, 2023. https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

14. European Union. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. Official Journal of the European Union, L 281, November 23, 1995. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046
15. European Union. 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, GDPR). Official Journal of the European Union, L 119, May 4, 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj
16. "EU for Azerbaijan." EU4Azerbaijan. https://eu4azerbaijan.eu/
17. Free Group. "The European Union and State Secrets: A Fully Evolving Institutional Framework." Last modified July 30, 2010. https://free-group.eu/2010/07/30/the-european-union-and-state-secrets-a-fully-evolving-institutional-framework/
18. GDPR.eu. "Data Protection Impact Assessment Template." Accessed December 3, 2024. https://gdpr.eu/data-protection-impact-assessment-template/
19. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado (BOE-A-2018-16673), December 6, 2018. Accessed December 20, 2024. https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673
20. Ministry of Digital Development and Transport of the Republic of Azerbaijan. "Home." Accessed December 3, 2024. https://mincom.gov.az/en.
21. "Spain: AEPD Highlights Current Key Challenges in Data Protection." OneTrust DataGuidance. Accessed December 20, 2024. https://www.dataguidance.com/news/spain-aepd-highlights-current-key-challenges-data
22. The Republic of Azerbaijan. Law of the Republic of Azerbaijan on Personal Data. Accessed December 3, 2024. https://family.gov.az/store/media/NewFolder/Law%20of%20the%20Republic%20of%20Azerbaijan%20%20On%20personal%20data.doc