E-ISSN 2520-0429
ISSN 2519-1284

European Journal of Economics, Law and Social Sciences

Vol.10 No.1
January, 2026

Research Article

Personal data protection and privacy

PhD (C.) Iris Shkelzen Berisha
University of Tirana, Albania

Assoc. Prof. Dr. Ela Podgorica Kerka
University of Tirana, Albania

Aigars Andersons
Vidzeme University of Applied Sciences, Valmiera, Latvia

DOI: https://doi.org/10.2478/ejels-2026-0009

Abstract

Protecting personal data has become a critical issue in the digital era, both in law and public policy. This paper examines the legal aspects of privacy and data protection in Albania by analyzing Law No. 124/2024, *On the Protection of Personal Data*, which represents a significant effort to align national legislation with the European Union's General Data Protection Regulation (GDPR). The recently enacted law introduces a more comprehensive approach to the processing of personal data, prioritizing the principles of lawfulness, transparency, purpose limitation, and data minimization. Particular emphasis is placed on the rights of data subjects, alongside the establishment of enhanced institutional mechanisms to monitor compliance and ensure effective implementation by competent authorities. The paper critically assesses the effectiveness of this updated legal framework in safeguarding fundamental rights within an increasingly technologically advanced environment, where the use of artificial intelligence (AI) is expanding and the risks of privacy infringement are intensifying.

Keywords: privacy, personal data protection, fundamental right, legal, ethical.

1. Introduction and Background

We live in an era in which personal data are collected, stored, and processed on an unprecedented scale. Rapid technological development, the pervasive digitalization

of everyday life, and increasingly data-driven business models mean that even routine activities—such as online shopping, registering for services, traveling, or visiting a physician—are now intrinsically linked to the disclosure of personal information. What once consisted of basic identifiers, such as a name or age, has evolved into extensive data profiles revealing preferences, habits, locations, and even predictive indicators of future behavior.

This expansive data environment raises significant legal, ethical, and social concerns. Individuals should be aware of the digital footprints they leave behind, while companies and public authorities bear responsibility for ensuring that collected data are processed in a transparent, secure, and fair manner. As a result, the protection of personal data and privacy has emerged as a fundamental right and a central policy challenge of the digital age, necessitating comprehensive regulation and responsible institutional conduct.

Although the scale and sophistication of data processing are relatively recent, the collection and use of personal data are not new phenomena. Historically, societies have gathered and stored information since ancient times. Early civilizations, such as the Sumerians and Chinese, recorded personal and administrative data on clay tablets, parchment, and registers, preserving them in manual archives and libraries. During the nineteenth and early twentieth centuries, data storage and processing relied on mechanical devices, including calculating machines and punch cards. The twentieth century marked a turning point with the advent of computers, enabling electronic data storage and processing, initially through magnetic tapes and disks and later through digital storage systems.

The proliferation of the internet and networked technologies further transformed data management practices. Information began to be stored on servers and in large-scale data centers, accompanied by the development of structured database systems such as SQL and NoSQL (Bentein, 2021). In contemporary society, the emergence of Big Data has enabled the storage and analysis of vast quantities of information in diverse formats, while cloud-based storage has become the dominant model due to its accessibility and scalability (Bentein, 2021). At the same time, advanced algorithms and intelligent systems increasingly facilitate the processing, analysis, and protection of data.

Data, however, acquire value only when they are structured in a manner that allows them to be read, interpreted, and effectively utilized, and—most importantly—when they are accessible to authorized users. This principle historically underpinned the establishment of libraries as repositories of knowledge. In modern organizational contexts, emerging technologies such as the Industrial Internet of Things (IIoT), Robotic Process Automation (RPA), and Business Process and Workflow Management (BPM) have generated entirely new streams of data, significantly expanding both the volume and complexity of information flows (Paul, 2020).

In today's digital society, information about individuals is continuously stored, processed, and exchanged. This development is a direct consequence of technological progress, digital integration across social and economic activities, and innovative business practices. It is increasingly difficult to imagine a time when purchasing

goods, registering for services, entering banking agreements, or accessing healthcare required only minimal personal information. Currently, nearly every digital interaction involves the provision of multiple data points, often extending well beyond what appears strictly necessary (Schneier, 2015). Consequently, personal data have acquired substantial economic and strategic value in the global marketplace.

Individuals disclose personal data either voluntarily or out of necessity in their daily interactions, thereby creating legal and ethical obligations not only for data controllers and processors but also for individuals themselves as data subjects. These obligations relate directly to the protection of personal data as a fundamental constitutional and human right. Whereas traditional interactions were largely conducted face-to-face, relying on paper records and cash transactions, the pervasive digitalization of modern life has fundamentally altered this paradigm, rendering personal data both omnipresent and indispensable.

2. International Legal Framework for Privacy and Information Security

At the international level, states have long acknowledged the risks associated with the misuse of personal information and have progressively developed legal frameworks to safeguard privacy and personal data (European Court of Human Rights [ECtHR], n.d.). These concerns have intensified alongside technological developments that facilitate large-scale data collection, processing, and dissemination. The right to privacy received formal international recognition with the adoption of the *Universal Declaration of Human Rights* (UDHR) in 1948. Article 12 of the UDHR affirms that no one shall be subjected to arbitrary interference with their privacy, family, home, or correspondence, nor to attacks upon their honor and reputation (Harris et al., 2018). This foundational principle laid the groundwork for subsequent international and regional legal instruments protecting privacy and personal data.

In the aftermath of the Second World War, the Council of Europe was established in 1949 with the objective of promoting democracy, the rule of law, and human rights across the continent (European Court of Human Rights, 1987). One of its most significant achievements was the adoption of the *European Convention on Human Rights* (ECHR) in 1950, which entered into force in 1953 (Lynskey, 2015). The ECHR constitutes a binding international treaty for its member states and has been incorporated, either directly or indirectly, into many national legal systems.

To ensure the effective protection of the rights enshrined in the Convention, the European Court of Human Rights was established in Strasbourg in 1959. The Court adjudicates alleged violations of the ECHR and is empowered to examine both individual applications under Article 34 and inter-state complaints under Article 33 (European Court of Human Rights, 2000). Importantly, applicants need not be nationals of a member state, provided that the alleged violation occurred within the jurisdiction of a contracting state.

Article 8 of the ECHR explicitly guarantees the right to respect for private and family life, home, and correspondence (Kuner, 2013). Any interference by public authorities

is permissible only when it is prescribed by law, pursues a legitimate aim—such as national security, public safety, or the protection of the rights and freedoms of others—and is necessary in a democratic society. This provision establishes a careful balance between individual rights and collective interests.

Through its extensive jurisprudence, the European Court of Human Rights has interpreted Article 8 broadly. The scope of protection now extends to issues such as state surveillance, interception of communications, mass monitoring programs, and the collection and processing of personal data by public authorities (HUDOC, n.d.). Significantly, the Court has clarified that Article 8 not only imposes negative obligations on states to refrain from unjustified interference but also creates positive obligations to adopt effective measures protecting individuals from privacy violations committed by third parties.

Parallel protections are enshrined in the *Charter of Fundamental Rights of the European Union*, which recognizes the protection of personal data as a distinct and autonomous fundamental right under Article 8 (European Union, 2012). While this right is not absolute, Article 52(1) of the Charter stipulates that any limitation must be provided for by law, respect the essence of the right, and comply with the principle of proportionality. Such limitations are permissible only where they are necessary and genuinely serve objectives of general interest or protect the rights and freedoms of others (Council of Europe, 1981).

3. Albania's efforts and challenges in strengthening personal data protection

In Albania, the adoption of effective measures for the protection of personal data has historically been delayed, resulting in significant vulnerabilities within national data protection systems. Albanian citizens' personal data have been—and continue to be—exposed to serious risks arising from cyberattacks targeting digital platforms used for the storage and processing of personal information (Council of Europe, 2024). These risks were starkly illustrated when sensitive personal data belonging to more than 690,000 Albanian citizens were unlawfully disseminated and circulated across mobile devices following a large-scale cyber incident (Council of Europe, 2024). Similarly, more than 1,200 public online services were temporarily blocked as a result of cyberattacks on government platforms, severely disrupting public administration (IDP, 2022). These incidents revealed substantial deficiencies in Albania's data protection framework, encompassing legislative gaps, inadequate technical safeguards, and insufficient physical and organizational security measures.

In response to rapid technological developments and in the context of Albania's European Union accession process, the Albanian legislature has undertaken a series of reform initiatives. One of the earliest steps was the approval and signing of the Second Additional Protocol to the Convention on Cybercrime, developed in Strasbourg, which aims to enhance international cooperation and facilitate the exchange of electronic evidence (Official Publishing Center, 2025). The ratification of this Protocol enables the establishment of joint investigative teams composed of Albanian and

European experts, supports cross-border criminal investigations, and requires the implementation of appropriate technological, physical, and organizational measures to safeguard personal data against unauthorized access, loss, or destruction.

Although the Protocol has not yet entered into force as a binding instrument, preparatory steps toward ratification are being implemented through the CyberSEE project (Council of Europe, 2024). Within this framework, Albania may transfer personal data to another state or international organization only upon prior authorization by the competent supervisory authority and only where reciprocal guarantees exist. This approach establishes a comprehensive legal structure governing cross-border data transfers for the purposes of prevention, detection, investigation, and prosecution of criminal offenses, while ensuring compliance with data protection standards.

Programs such as CyberSEE, jointly implemented by the European Union and the Council of Europe, have played a crucial role in aligning Albania's data protection framework with European standards. These initiatives aim to enhance institutional capacities, introduce advanced technical safeguards, and strengthen cross-border cooperation mechanisms, particularly in the context of cybercrime investigations and information security.

Under Albanian Law No. 124/2024, the international transfer of personal data is permitted only where the receiving country ensures an adequate level of protection, as determined by a formal decision of the national supervisory authority. Jurisdictions meeting this criterion include European Union member states, European Economic Area (EEA) countries, and parties to Convention 108+ (DLA Piper, 2019). Where adequate protection cannot be ensured, data transfers are permitted only under specific conditions, such as the implementation of additional safeguards or the granting of prior authorization by the competent authority.

This article focuses on the innovations introduced by Law No. 124/2024, *On the Protection of Personal Data* (hereinafter "the New Law"), adopted by the Albanian Parliament on 19 December 2024 and published in the Official Gazette No. 9 on 17 January 2025. The New Law consists of six parts, comprising 101 articles across 51 pages, organized into thematic chapters that comprehensively regulate personal data protection.

The first part, titled *General Provisions*, defines the object, purpose, scope, and key definitions of the law. The second part regulates the lawful processing of personal data and is divided into five chapters addressing data processing principles, data subject rights, obligations of controllers and processors, international data transfers, and processing for specific purposes. The third part governs the processing of personal data by competent authorities for public security and national security purposes, including crime prevention and prosecution, and sets out specific rules concerning data subject rights, controller obligations, and international transfers in this context.

The fourth part establishes the organization and functioning of the Commissioner for the Right to Information and Protection of Personal Data as the independent supervisory authority. The fifth part regulates legal remedies, liability, and sanctions for violations of the law, while the sixth part contains transitional and final provisions ensuring the effective implementation of the New Law.

The New Law entered into force on 31 January 2025, although certain provisions will be implemented gradually over the following two years. Upon Albania's accession to the European Union, the law will be partially repealed, with Parts III and IV remaining in force, along with any provisions cross-referenced therein. These sections will continue to regulate the processing of personal data by competent authorities for law enforcement, criminal prosecution, and national security purposes.

With the entry into force of Law No. 124/2024, the former Law No. 9887 of 10 March 2008 on the Protection of Personal Data was repealed. However, existing sub-legal acts and international agreements adopted under the previous legal framework remain applicable until new implementing measures are adopted, provided that they do not conflict with the provisions of the New Law.

The law also delegates significant rule-making responsibilities to executive and supervisory authorities. The Council of Ministers is required to adopt relevant sub-legal acts within three months of the law's entry into force, while the Commissioner for the Right to Information and Protection of Personal Data is tasked with approving additional implementing acts within the same timeframe to ensure the effective application of key provisions.

At the legislative level, Law No. 124/2024 represents the closest alignment Albania has achieved with European Union standards on personal data protection. While the law is highly technical and, in some instances, complex in its application, it retains core principles from the 2008 framework while introducing substantial reforms concerning data protection principles, data subject rights, and the obligations of controllers and processors. Overall, the New Law reflects the standards and principles of the EU General Data Protection Regulation (GDPR) and constitutes a significant advancement in Albania's legal framework, adapting national rules to technological developments and the realities of the digital age.

The enactment of this legislation was driven by two primary factors. First, the rapid digitalization of public administration and private sector services—particularly in banking and telecommunications—necessitated updated legal safeguards. Second, the adoption of the New Law fulfilled a key requirement within Albania's EU accession process, as compliance with EU data protection standards constitutes a prerequisite for the opening of further negotiation chapters (European Parliament & Council, 2016). The previous directive-based framework, originating in 1995, was no longer adequate to address contemporary technological challenges, underscoring the need for comprehensive legislative reform.

4. Data Protection Officer (DPO) and Sector-Specific Codes of Conduct

The institution of the Data Protection Officer (DPO) constitutes a core component of the contemporary normative framework for personal data protection, reflecting European standards and modern approaches to legal risk management in the digital environment. Albanian legislation, harmonized with the principles of the EU General Data Protection Regulation (GDPR), establishes mandatory circumstances

for the appointment of a DPO. These include public authorities and bodies (with the exception of courts acting in their judicial capacity), entities engaged in large-scale processing of sensitive or criminal data, and controllers or processors carrying out systematic monitoring of individuals.

DPOs are entrusted with a broad range of responsibilities, including advising and informing controllers and processors of their legal obligations; monitoring compliance with data protection legislation; participating in data protection impact assessments; raising awareness and training staff involved in processing activities; and cooperating with the supervisory authority, namely the Commissioner for the Right to Information and Protection of Personal Data. The law safeguards the functional independence of the DPO by prohibiting the issuance of instructions regarding the performance of their duties and by protecting them from dismissal or sanctions related to the exercise of their functions. Furthermore, DPOs are required to report directly to the highest management level of the organization. The promotion of a national network of DPOs further supports professionalization, institutional cooperation, and the exchange of best practices, strengthening administrative capacity and reinforcing the protection of privacy rights in an increasingly interconnected technological landscape.

Codes of conduct represent one of the most significant innovations introduced by Law No. 124/2024 *On the Protection of Personal Data*. These instruments of self-regulation complement public oversight mechanisms by allowing associations and representative bodies of controllers or processors to develop sector-specific rules governing the application of data protection principles. Such codes may address, inter alia, fair and transparent data collection, the protection of minors, public information practices, the exercise of data subject rights, breach notification procedures, organizational and technical safeguards, international data transfers, and dispute resolution mechanisms between controllers and data subjects. The Commissioner may approve these codes only after determining that they provide adequate safeguards. Their implementation is conditional upon the designation of an authorized monitoring body that demonstrates independence, technical expertise, and transparent procedures for handling complaints and assessing compliance.

In parallel, the law introduces certification mechanisms and data protection seals as voluntary tools to demonstrate compliance with legal requirements. Certification procedures are carried out by bodies accredited by the General Directorate of Accreditation, based on criteria established by the Commissioner. These bodies must be independent, competent, and equipped with written procedures for evaluating processing operations, as well as for suspending or withdrawing certification in cases of non-compliance. Data protection certifications and labels are valid for a maximum period of three years. This framework reflects a modern regulatory approach that combines self-regulation with institutional supervision, enhancing transparency, accountability, and trust in personal data processing without undermining the authority of the public supervisory body.

Law No. 124/2024 permits the international transfer of personal data only where an adequate level of protection is ensured in the receiving country or organization. Such adequacy is determined through a formal decision of the Commissioner, who

assesses factors including the existence of data protection legislation, respect for human rights, the functioning of independent supervisory authorities, and the international obligations of the recipient. In the absence of an adequacy decision, data transfers may take place on the basis of appropriate safeguards, such as legally binding instruments, standard contractual clauses, approved codes of conduct, or certification mechanisms. Exceptionally, transfers may also be authorized on the basis of the explicit consent of the data subject or for specific purposes, including the protection of vital interests, the establishment or exercise of legal claims, or overriding public interest considerations. The law further regulates binding corporate rules, requiring corporate groups to establish internal governance structures, training, auditing, reporting mechanisms, and cooperation with the supervisory authority. These rules apply to all group members, both within and outside Albania, and ensure enforceable rights for data subjects.

The law also provides balanced provisions reconciling personal data protection with freedom of expression and information. Limited and proportionate exemptions are permitted for journalistic, academic, artistic, and literary purposes, provided that processing remains strictly necessary for publication and serves the public interest while safeguarding the fundamental rights of data subjects, particularly children and victims. Personal data may also be processed for archiving in the public interest, scientific research, and statistical purposes, subject to safeguards such as data minimization, pseudonymization, and anonymization. Direct marketing is permitted on the basis of legitimate interest, while the processing of sensitive data requires explicit consent. In all cases, data subjects retain the right to object at any time, ensuring an appropriate balance between commercial communication and privacy protection.

Finally, the processing of personal data by competent authorities must strictly comply with legal principles and be limited to purposes explicitly defined by law, including crime prevention, investigation, prosecution, and the protection of national and public security. Data retention must be limited to what is necessary, with periodic reviews to assess the continued need for storage. Controllers are required to distinguish clearly between different categories of individuals involved in criminal proceedings—such as suspects, convicted persons, victims, witnesses, and collaborators—and to maintain separate records of personal assessments influencing processing decisions. These safeguards aim to ensure legality, proportionality, and accountability in the use of personal data by public authorities.

The Data Protection Commissioner plays a central role in ensuring that the processing of personal data is carried out in accordance with applicable legislation. This role includes extensive investigative powers, most commonly exercised in response to complaints submitted by individuals or other legal entities. The Commissioner is responsible for protecting and promoting the fundamental rights of data subjects, including the rights of access, rectification, and erasure, and for continuously informing and advising data subjects regarding the exercise of these rights.

In exercising investigative authority, the Commissioner may request and obtain any information or documentation from controllers and processors, conduct audits and on-site inspections, and verify the lawfulness of data processing activities, including

the validity of certifications. The Commissioner is vested with broad corrective powers, such as issuing warnings and compliance orders, requiring controllers or processors to satisfy data subject requests, restricting or suspending processing activities, revoking certifications, and imposing administrative sanctions in accordance with the law. Where violations involve elements of criminal liability, the Commissioner cooperates with the competent law-enforcement and prosecutorial authorities to ensure appropriate prosecution and enforcement.

At the international level, the Commissioner is empowered to develop and strengthen cooperation with counterpart supervisory authorities and international organizations, facilitating information exchange, joint investigations, and the harmonization of supervisory practices in the protection of personal data. The Commissioner represents the institution in both national and international engagements and maintains comprehensive registers of infringements and corrective measures adopted, thereby enhancing transparency and accountability. In addition, the Commissioner prepares detailed annual reports submitted to Parliament and may report upon request. Public authorities and private entities are legally obliged to cooperate with the Commissioner and to implement issued recommendations and binding decisions.

Under the personal data protection framework, every data subject has the right to lodge a complaint with the Commissioner in the event of an alleged violation. The Commissioner is required to examine such complaints in accordance with the Code of Administrative Procedure and to inform the parties of the progress and outcome of the proceedings, ensuring access to judicial review before the competent administrative court. During the examination of a complaint, controllers or processors may not substantially alter the contested processing operations without the prior authorization of the Commissioner. The Commissioner may reject manifestly unfounded or repetitive complaints in order to safeguard administrative efficiency. Individuals who consider that their rights or legitimate interests have been infringed by an act or omission of the Commissioner may seek judicial review before the administrative courts. In cases of unlawful data processing, controllers and processors may be held jointly and severally liable for civil damages, ensuring effective compensation for affected data subjects. Data subjects may also mandate public interest organizations to act on their behalf. Where there is an imminent and irreparable risk to the rights and freedoms of data subjects, the Commissioner is authorized to impose immediate interim measures, including restrictions on processing activities, pending the final resolution of the complaint.

Administrative sanctions imposed by the Commissioner for violations of personal data protection legislation are substantial and proportionate. The determination of penalties takes into account factors such as the nature, gravity, and duration of the infringement; the intentional or negligent character of the violation; the categories and volume of personal data affected; the extent of the damage suffered; and the degree of responsibility of the controller or processor. Mitigating factors include cooperation with the Commissioner, measures taken to reduce harm, the implementation of appropriate technical and organizational safeguards, and adherence to approved

codes of conduct or certification mechanisms. This sanctioning framework reinforces accountability and compliance while ensuring fairness and proportionality in enforcement.

5. Conclusion

In cases of serious infringements—such as violations of the fundamental principles of data processing, breaches of data subject rights, or unlawful transfers of personal data to third countries—administrative fines may reach up to two billion Albanian lek or 4% of the undertaking's total worldwide annual turnover, whichever is higher. For less severe violations, fines may amount to up to one billion lek or 2% of annual turnover. Decisions imposing administrative sanctions are subject to judicial review before the competent courts, while their enforcement follows the general rules governing administrative offenses, with collected fines allocated to the state budget. The Commissioner is further empowered to issue binding instructions establishing criteria for the assessment and calculation of sanctions, drawing upon guidelines and standards adopted by the European Data Protection Board, thereby ensuring that penalties are effective, proportionate, and dissuasive.

Beyond its regulatory function, the protection of personal data constitutes a foundational element of democratic governance and a core guarantee of respect for human dignity. Law No. 124/2024 represents a substantial advancement in aligning Albania's legal framework with European standards; however, its significance extends beyond formal compliance. The law provides an opportunity to foster a culture of accountability, transparency, and trust among public institutions, private entities, and citizens. In an era characterized by rapid technological change and the pervasive circulation of information, privacy should not be perceived as an impediment to innovation, but rather as an ethical compass guiding sustainable and human-centered development. Ultimately, the primary challenge lies not only in the effective enforcement of legal provisions, but in cultivating collective awareness that the protection of personal data is intrinsically linked to the preservation of individual freedom and democratic values.

References

Bentein, A. (2021, April 8). *Data is the new gold*. QAD Blog.
https://www.qad.com/blog/2021/04/data-is-the-new-gold
Council of Europe. (1950). *European Convention on Human Rights*.
https://www.coe.int/en/web/human-rights-convention
Council of Europe. (1981). *Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108)*.
https://www.coe.int/en/web/data-protection/convention108
Council of Europe. (2018). *Protocol amending the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108+)*.
https://www.coe.int/en/web/data-protection/convention108plus

Council of Europe. (2023, February 27). *Shqipëria bëhet shteti i 36-të që nënshkruan Protokollin e Dytë Shtesë të Konventës për krimin kibernetik*. Zyra e Këshillit të Evropës në Tiranë. https://www.coe.int/sq/web/tirana/-/shqip%C3%ABria-b%C3%ABhet-shteti-i-36-t%C3%AB-q%C3%AB-n%C3%ABnshkruan-protokollin-e-dyt%C3%AB-shtes%C3%AB-t%C3%AB-konvent%C3%ABs-p%C3%ABr-krimin-kibernetik

Council of Europe. (2024, November 13). *CyberSEE: Albania commences legislative reform for the ratification and effective implementation of the Second*
Additional Protocol to the Budapest Convention. Council of Europe Cybercrime. https://www.coe.int/en/web/cybercrime/-/cybersee-albania-commences-legislative-reform-for-the-ratification-and-effective-implementation-of-the-second-additional-protocol-to-the-budapest-convention

DLA Piper. (2019). *Global data protection laws of the world – World map*.
https://www.dlapiperdataprotection.com/

European Court of Human Rights. (1987). *Leander v. Sweden*
(Application No. 9248/81), Judgment of March 26, 1987.
https://hudoc.echr.coe.int/

European Court of Human Rights. (2000). *Rotaru v. Romania* (Application No. 28341/95), Judgment of May 4, 2000.
https://hudoc.echr.coe.int/

European Court of Human Rights. (n.d.). *Factsheet: Personal data protection*. https://www.echr.coe.int/documents/fs_data_protection_eng.pdf

European Parliament & Council. (1995). *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 Communities*, *L* 281, 31–50.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046

European Parliament & Council. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)*. *Official Journal of the European Union*, *L* 119, 1–88.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

European Union. (2012). *Charter of Fundamental Rights of the European Union* (2012/C 326/02). *Official Journal of the European Union*.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

Harris, D. J., O'Boyle, M., Bates, E. P., & Buckley, C. M. (2018). *Law of the European Convention on Human Rights* (4th ed.). Oxford University Press.

HUDOC – European Court of Human Rights. (n.d.). *HUDOC database*.
https://hudoc.echr.coe.int/

IDP. (2022). *International transfer of personal data: Albania and Kosovo mutual recognition as countries with an adequate level of data protection*.
https://idp.al/en/2025/05/05/international-transfer-of-personal-data-albania-and-kosovo-mutual-recognition-as-countries-with-an-adequate-level-of-data-protection/

Kuner, C. (2013). *Transborder data flows and data privacy law*. Oxford University Press.

Lynskey, O. (2015). *The foundations of EU data protection law*. Oxford University Press.

Official Publishing Center. (2025). *[Official publication title]*. Tirana, Albania: Qendra e Botimeve Zyrtare.

Paul, K. (2020, April 21). *Hundreds of Amazon warehouse workers to call in sick in coronavirus protest*. *The Guardian*.
https://www.theguardian.com/technology/2020/apr/20/amazon-warehouse-workers-sickout-coronavirus

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. W. W. Norton & Company.