ITS INSTITUTE FOR TECHNOLOGY AND SOCIETY

Research Report

CHALLENGES AND REGULATORY OBLIGATIONS FOR LARGE DATA PROCESSORS

November 2024

Publisher: Institute for Technology and Society (ITS)

Author: Donika Çeta

Editor: Adison Gara and Lirim Bllaca

Financed by: HumanRightivism project, implemented by the Community Development Fund (CDF) and supported by the Embassy of Sweden in Pristina

Prishtina, 2024

Supported by:

Institute for Technology and Society
Str. Zenel Salihu no. 28 Prishtina
https://institutets.com/

Contents

Acronyms

GDPR	General Data Protection 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, and repealing Directive 95/46/EC
IPA	Information and Privacy Agency
LPPD	Law no. 06/L-082 on the Protection of Personal Data
DPO	Data Protection Officer
DPIA	Data Protection Impact Assessment
ICT	Information and Communication Technology
IoT	Internet of things
IHIS	Integrated Health Information System
BHIS	Basic Health Information System
GG	Government Gateway
KCSS	Kosovar Center for Security Studies
SME	Small and Medium-sized Enterprises

Executive Summary

Kosovo is working towards establishing strong data protection practices, driven by its rapid digitalization. Despite recent advances in legislative frameworks, such as the alignment with the EU's General Data Protection Regulation (GDPR) through the Law on Protection of Personal Data (LPPD), Kosovo faces significant challenges in practical implementation. These challenges are also present among large data processors, where the consequences of potential breaches are the greatest. This paper evaluates the current data protection landscape, focusing on the compliance of major sectors—telecommunications, finance, public administration and utilities, health, and education—with the LPPD, and highlights the challenges and opportunities for improving data protection in Kosovo.

The paper identifies a range of issues including inconsistent enforcement of the data protection law, gaps in public awareness, and insufficient internal capacities within organizations, particularly in public institutions. Moreover, large data processors such as telecommunications companies and financial institutions process significant amounts of personal data, but their compliance with data protection regulations remains inconsistent. The paper presents case studies, including the Kosovo Electricity Supply Company (KESCO) and the Municipality of Gjakova, to illustrate data protection challenges and enforcement issues.

Survey results from public and private sector entities indicate a disparity in the implementation of data protection practices. While larger institutions are making strides in aligning with the LPPD, smaller organizations struggle with resource and capacity constraints, leading to inadequate protection measures. Notably, there is a clear need for enhanced staff training, regular audits, and increased awareness of data protection rights.

Kosovo's progress toward establishing a secure data protection environment presents opportunities for both public and private sectors to collaborate on best practices, improve compliance, and build public trust in digital services. By addressing the identified challenges, Kosovo can advance toward a more secure and privacy-conscious digital landscape, positioning itself to benefit from its growing integration into the global digital economy.

Key Findings & Recommendations

Key Findings

1. Kosovo's data protection framework aligns with the GDPR, but enforcement is inconsistent. Limited resources, technical constraints, and low public awareness hinder compliance, especially among large data processors.
2. Key sectors, including telecommunications, finance, and public administration, face unique challenges. Large data processors struggle with managing compliance due to rapid data growth and technological demands.
3. The private sector demonstrates better compliance through more frequent data protection training and resource allocation, while the public sector shows less frequent updates to privacy policies and limited employee training.

4. Case studies, such as KESCO and the Municipality of Gjakova, illustrate failures in protecting personal data, resulting in high-profile fines and highlighting the need for improved compliance.
5. Many organizations lack regular updates to data protection policies and Data Protection Impact Assessments (DPIAs), indicating a reactive approach rather than integrating privacy measures into operations.

Key Recommendations:

1. Enhance the resources and capacity of the Information and Privacy Agency (IPA) to enable more frequent inspections, audits, and follow-up actions to ensure data protection compliance across sectors.
2. Establish ongoing data protection training, especially for public sector employees, to build a robust understanding of data protection practices, focusing on aligning public and private sector standards.
3. Encourage organizations to integrate Privacy by Design principles into system development to safeguard data proactively, complemented by regular DPIAs and policy updates.
4. Implement campaigns to educate the public on their data protection rights, empowering them to hold institutions accountable and increasing overall demand for compliance.
5. Develop standardized data protection guidelines through partnerships between public and private sectors to ensure consistent compliance and build a culture of data security across all sectors.

Chapter I: Introduction

In today's world, large processors, meaning entities that process personal data for and on behalf of *data controllers*, hold significant control over personal information. In data protection terminology, *a data controller* is an entity that determines the purposes and means of processing personal data, while *a data processor* carries out the actual processing on behalf of the controller. Data processors handle personal information in sectors such as telecommunications, finance, healthcare, education, and public administration, playing a vital role in maintaining data privacy and compliance with data protection laws.

Many processors use this data to improve their business processes or obtain a competitive edge, perhaps going beyond the bounds of the law or taking advantage of gaps in data protection laws. Particularly when data is utilized extensively without enough supervision, this may result in privacy violations.

Every day data is produced extensively in many forms and from different sources. The total data created is expected to grow to more than 180 zettabytes by 2025.[1] To put this in perspective, a 2-hour 4K movie is around 1 gigabyte. With 180 zettabytes, approximately 180 trillion 4K movies could be stored. That's enough for you to watch over 1,000,000,000,000 (one trillion) movies![2] Companies use technological advancement and analyze the vast amount of data from different sources to gain a more comprehensive understanding of customer behavior.[3]

In Kosovo, where digitization is progressing quickly, safeguarding personal information is both a challenge and an opportunity. The alignment with the EU's GDPR through Kosovo's LPPD was a critical step in safeguarding citizens' privacy. However, enforcement and practical execution are still difficult, and compliance is frequently hampered by poor public awareness, variable adherence, and resource constraints. As recent findings from our questionnaire indicate, while many organizations understand the importance of data protection, there are critical gaps in practice. For instance, although most public and private institutions have privacy policies in place, they often update these policies on a reactive, rather than proactive, basis. Additionally, only 42.9% of private and 33% of public institutions reported conducting DPIAs, underscoring a need for broader and more consistent application of risk management strategies.

Additionally, according to the results of the questionnaire, different sectors differ greatly in their preparedness to handle data breaches; 71.4% of private firms lack an incident response strategy, while 50% of public sector organizations do the same. This disparity highlights the essential need for increased readiness, especially given the ongoing evolution of digital threats. Responses to the survey also indicated a lack of ongoing education about data protection, particularly in governmental institutions.

---

[1] Amount of data created, consumed, and stored 2010-2020, with forecasts to 2025, published by Petroc Tazlylor, Statista, https://www.statista.com/statistics/871513/worldwide-data-created/

[2] Blog, What's the real story behind the explosive growth of data, https://www.red-gate.com/blog/database-development/whats-the-real-story-behind-the-explosive-growth-of-data

[3] Emerging Trends in Information Management for 2024: Navigating the Future Data, Khan Abdullah, 2024.

It should be understood the fact that digital transformation is changing our daily lives. Therefore, it is impossible to overestimate the significance of strong data protection at a time when data has turned into a vital resource for both governments and corporations. Managing sensitive and personal data has become increasingly important as digitization picks up speed in every industry. Kosovo is a country that is quickly joining the global digital economy, and data protection is both an opportunity and a concern. Large-scale data processors are crucial to the economy, therefore strong data security procedures are necessary not only for compliance but also to uphold public confidence and promote long-term growth. Moreover, the Government of Kosovo through its eGovernment Strategy 2023-2027 has set forth clear priorities towards digitalization.[4]

Beyond compliance, data protection is essential for building public confidence in Kosovo's digital economy. In addition to protecting individual privacy, effective data protection boosts the nation's competitiveness in a global economy that is becoming more and more reliant on data. This presents both a difficulty and an opportunity for Kosovo. Ensuring compliance can open the door to further integration with the European Union while strengthening data protection safeguards can increase residents' trust and encourage them to use digital services.

This study examines Kosovo's present data protection environment with an emphasis on big data processors. It aims to evaluate the efficacy of current data protection regulations and procedures, emphasize major obstacles, and draw attention to areas in need of development. The research question that directs this study are:

- How effective are the current data protection laws and practices in Kosovo, and what are the key challenges and opportunities for enhancing data protection to benefit society?

- How do large data processors comply with applicable legal and regulatory requirement?

This study examines Kosovo’s data protection landscape across several key sections:

- **Data Protection Landscape in Kosovo and Data Processors**: This chapter provides an overview of Kosovo’s data protection framework and the evolving legal landscape, highlighting the roles of data processors and controllers.

- **Big Data Processors in Kosovo**: Focusing on major data processors, this section explores the role of industries like telecommunications, finance, and healthcare in shaping Kosovo’s data ecosystem.

- **Challenges of Big Data Processors**: This chapter identifies the main obstacles data processors face, including technological constraints, regulatory complexities, and limited organizational capacities.

[4] eGovernment Strategy Kosovo 2023-2027, https://mpb.rks-gov.net/Uploads/Documents/Pdf/EN/2700/e-Government%20Strategy%20Kosovo%202023-2027.pdf

- **Case Studies**: By examining real-world cases, such as KESCO and the Municipality of Gjakova, this section illustrates the practical challenges of data protection compliance and enforcement in Kosovo.

- **Results of the Questionnaire**: This chapter presents the findings from a questionnaire distributed to public and private sector entities, providing quantitative insights into compliance practices and gaps.

- **Conclusion**: The final section synthesizes findings and offers recommendations for strengthening Kosovo's data protection framework, ensuring compliance, and building public trust in digital services.

1.1. Methodology

This paper's methodology combines qualitative and quantitative research approaches to assess the effectiveness of data protection practices in Kosovo, particularly among large data processors. The research included a comprehensive analysis of existing literature on data protection laws, such as the GDPR and LPPD. This review provided historical context for data protection in Kosovo and offered insights into international best practices. Key sources included legal texts, government reports, and relevant academic articles, which helped shape the framework for analyzing compliance in Kosovo.

This study was designed around key questions that frame the central issues in Kosovo's data protection landscape, focusing specifically on large data processors. These questions include: assessing the effectiveness of current data protection laws and practices, identifying the primary challenges and opportunities for enhancing data protection, and examining the compliance of large data processors with the LPPD.

Moreover, two key case studies were developed to illustrate the practical challenges and consequences of data protection enforcement in Kosovo. One case focused on KESCO (Kosovo Electricity Supply Company), a large data processor in the public utilities sector, whose practices were scrutinized by the Information and Privacy Agency (IPA) after data protection violations. The second case examined the Municipality of Gjakova, a public administration entity fined for the unlawful processing and public disclosure of personal data. This case provided insight into the public sector's challenges in handling sensitive data. These case studies were selected based on the availability of detailed information regarding their non-compliance and the regulatory actions taken, offering real-world examples of how data protection issues are handled in Kosovo.

This paper also gathered information through a questionnaire designed and distributed to Kosovo public and private sector organizations to gather data on their data protection practices, awareness of legal requirements, and challenges they face in complying with the LPPD. The survey focused on several key areas, including the presence of Data Protection Officers (DPOs), the existence and regular updating of data protection policies, the use of technical safeguards, such as encryption and firewalls, incident response plans for managing data breaches, and the integration of Privacy by Design principles into their systems.

Responses were collected from several organizations across sectors, including telecommunications, finance, health, education, and public administration. This data provided quantitative insights into the level of compliance and the gaps in data protection practices across different sectors.

This paper also involved a comparative analysis of data protection practices in Kosovo with other countries in the region and within the European Union, especially focusing on the challenges of aligning with GDPR standards. This comparison highlighted areas where Kosovo lags in enforcement and where improvements can be made by learning from international examples.

In the end, the data collected through the survey and interviews was analyzed using both descriptive statistics and thematic analysis. Survey results were categorized and compared across sectors to identify patterns in compliance, common challenges, and areas where regulatory support is needed. Thematic analysis of interviews and case studies provided qualitative insights into the real-world implications of Kosovo's data protection framework.

Chapter II: Data Protection Landscape in Kosovo and Data Processors

1. Definition, Importance and Historical Context

The establishment of modern data protection in Europe began in 1990 when the European Commission presented a comprehensive package of proposals aimed at defending personal data, marking a critical step towards the adoption of Community legislation on data protection.[5] This foundational exertion set the organization for the continuous advancement of data protection inside the European Union, which has progressed through a complex interaction of lawful concepts. Terms such as 'privacy', 'private life', and 'personal data protection' have at times been treated as particular and isolated, and at other times as identical, reflecting the nature of EU law in defining and forming the basic right to data protection.[6] The development of technologies and more and more services being developed in the digital realm led also to several incidents, these high-profile incidents served as reminders that linked to data acquisition and misuse.[7] For example, the incident with the 2018 Marriott International data breach where approximately 500 million guest records were compromised.[8] Therefore, ensuring a balance between data protection and data utilization is necessary, and to achieve it a mechanism shall be built which encourages and ensures effective protection.[9]

The EU data rules had a large impact across the world. It is worth mentioning that approximately 67 countries outside the EU have adopted the GDPR framework, from East Asian nations such as Japan and South Korea to Latin American countries.[10] However, as technology evolves the regulations may also change and, therefore, we cannot assume that the rules are in unison. It is worth mentioning that the GDPR data protection rules are also adopted in Kosovo through the Law on Protection of Personal Data.[11]

In Kosovo, according to the LPPD, "*data protection*" is the protection of personal data and the privacy of individuals, setting out rights, responsibilities, and principles to ensure personal data is processed lawfully and securely. It is a basic right that is protected by both international agreements and local laws, demonstrating the increasing understanding that privacy is a necessary component of autonomy and human dignity. The growing reliance on digital technology in Kosovo has highlighted the significance of data protection and the need for strong regulations to secure personal data.

Verifiably, the advancement of information assurance in Kosovo has been affected by its political and legitimate move, especially within the post-independence time, where endeavors have been made to adjust to European benchmarks. Kosovo's commitment to data protection

[5] The Emergence of Personal Data Protection as a Fundamental Right of the EU, Gloria González Fuster Law, Science, Technology and Society (LSTS) Vrije Universiteit Brussel (VUB), 2014.
[6] Ibid, pg. 254.
[7] Balancing Data Protection and Data Utilization: Global Perspectives and Trends, Yishi Wu, April 2024.
[8] Ibid.
[9] Data Rights Law 3.0: The Legislative Prospekt, edited by Yuming Lian, Peter Lang Ltd. International Academic Publishers, 2021.
[10] Balancing Data Protection and Data Utilization: Global Perspectives and Trends, Yishi Wu, April 2024.
[11] Law no. 06/L-082 on Protection of Personal Data, https://gzk.rks-gov.net/ActDetail.aspx?ActID=18616

is clear in its lawful system, which has been dynamically created to meet the challenges posed by the advanced age.

The Assembly of Kosovo approved the Constitution of Kosovo in 2008, which recognized the right to privacy, stating that "every person enjoys the right of protection of personal data. Collection, preservation, access, correction, and use of personal data are regulated by law."[12] This constitutional provision presents Kosovo's commitment to harmonize its legal framework with international data protection measures, guaranteeing that data protection is a principal right inside the country's legal framework.

The first law to advance regulate the provisions outlined in Article 36 of the Constitution of the Republic of Kosovo was Law no. 03/L-172 on the Protection of Personal Data. This law gave the rights, duties, standards, and measures to ensure data protection in harmony with the EU Directive 95/46/EC.[13] Through this law, it was established the National Agency for the Protection of Personal Data as an agency in charge of supervising the implementation of data protection rules with the obligation to report to the Kosovo Assembly.[14] The Agency had several duties, such as giving advice to public and private bodies on data protection questions, to decide on complaints of the data subjects, to carry out inspections and audits, to inform the public about issues and developments in the field of data protection, and to promote the fundamental right of data protection.[15]

In 2019, a new law on the protection of personal data was adopted. Law no 06/L-082 on Protection of Personal Data (LPPD) was adopted following the adoption of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons to the processing of personal data and on the free movement of such data (GDPR).[16]

2. Data Protection Regulation Landscape

Law No. 06/L-082 on Protection of Personal Data in Kosovo (LPPD) fundamentally represents the legal framework for data protection in Kosovo.[17] This law, which was adopted to align with the European Union's General Data Protection Regulation (GDPR), builds up comprehensive directions concerning the collection, processing, storage, and transfer of personal data within Kosovo. The law emphasizes the assurance of individual privacy rights while advancing transparency and accountability among data controllers and processors.

[12] Constitution of the Republic of Kosovo, Assembly of the Republic of Kosovo, published: 09.04.2008, art. 36.
[13] Law no. 06/L-082 on Protection of Personal Data, Assembly of the Republic of Kosovo, published on: 31.05.2010.
[14] Ibid Art. 29.
[15] Ibid.
[16] Law no. 06/L-082 on Protection of Personal Data, Assembly of the Republic of Kosovo. Published: 25.02.2019.
[17] Ibid.

The LPPD closely reflects the GDPR, by showing the commitment of Kosovo to harmonize its data protection regulation with those of the European Union. The Kosovo Country Report of 2019 found that the new LPPD constitutes significant progress in the area of data protection.[18]

Similar to the rights foreseen in the GDPR, the LPPD recognizes the right of data subjects to access, rectify, and erase their personal data, as well as the right to data portability and the right to object data processing. Also, it recognizes the principle of consent, meaning that the data subject gives their consent to the processing of their data based on one or more specific purposes. The LPPD defines the consent of the data subject as any freely given, specific, informed and unambiguous indication of the data subjects' wishes by a statement that signifies agreement to the processing of personal data relating to him or her.[19]

In addition, the LPPD imposes obligations on data controllers and processors. It requires them to implement suitable technical and organizational measures to ensure data security and compliance with data protection standards.[20] Moreover, regarding cross-border data transfers, the LPPD also sets rules and conditions for the transfer of personal data outside Kosovo. It requires that this kind of transfer guarantee an adequate level of data protection, which is similar to the requirements of the GDPR.[21]

The LPPD establishes the **IPA** is the independent authority responsible for supervising the implementation and enforcement of data protection laws in Kosovo. IPA is obliged with several duties, including reviewing complaints from persons, conducting investigations into potential breaches, giving opinions on data protection best practices, and guaranteeing that both the public and private sectors operate in compliance with data protection laws. The IPA is mandated to enforce sanctions for non-compliance, also propose administrative changes and work in collaboration with international data protection bodies. This comprehensive legal framework underscores Kosovo's commitment to guaranteeing data protection and adjusting its data protection measures with worldwide standards, especially those set by the European Union.[22]

Several bylaws derive from LPPD, which regulate for example the procedures of inspection, the case management system of the Ministry for Communities and Returns for the protection of personal data, for determining the criteria and procedures for the issuance of the personal data processing certificate, for processing of personal data obtained from drone use and so on.[23]

Until this date, there has not been an ex-post evaluation of the LPPD. However, it is evident that the number of cases brought before the IPA has grown. According to the Annual Report

[18] Kosovo Country Report, European Commission, 2019, https://neighbourhood-enlargement.ec.europa.eu/document/download/85bb4cd1-fbe1-47b3-8914-7f606f1ede37_en?filename=20190529-kosovo-report.pdf

[19] Law no. 06/L-082 on Protection of Personal Data, Assembly of the Republic of Kosovo, article 3, paragraph 1.17.

[20] Ibid.

[21] Ibid, Chapter XI.

[22] Ibid, Artc. 92.

[23] Bylaws that derive from Law on Protection of Personal Data, https://gzk.rks-gov.net/ActDetail.aspx?ActID=18616&langid=2.

of the IPA published in 2024 for the year 2023[24], they received 121 complaints. In the year 2022, they received 145 complaints and for six months in 2021, the IPA received 45 complaints.[25] This trend may indicate that more citizens are willing to exercise their rights under the LPPD, which could reflect growing confidence in the mechanisms for addressing data protection issues. Additionally, these reports reveal an increase in the number of inspections conducted, suggesting enhanced oversight by the IPA.

From the information gathered through the questionnaire, it can be emphasized that numerous companies, particularly larger enterprises and public institutions have made significant efforts to adjust their practices to the requirements of LPPD. Conversely, smaller enterprises and less-resourced organizations often struggle to meet these requirements. The impact of the GDPR is more pronounced within the compliance efforts of organizations that engage in cross-border data processing or aim to build trust with international partners.

Despite these efforts, a considerable number of organizations, especially within the private sector, stay uninformed of or insufficiently equipped to comply with the complete extent of the data protection requirements. Common areas of non-compliance incorporate insufficient data security measures, insufficient methods for obtaining and managing consent, and the lack of essential documentation and records of processing activities. Moreover, the appointment of Data Protection Officers (DPOs) isn't consistently observed, especially in organizations that are dubious about whether they fall within the thresholds that require such an arrangement.[26]

Since 2021, we have witnessed positive changes. The Bi-annual Report of the IPA showed that in the reporting period January – June 2021 the Agency received 63 complaints from public and private institutions and 15 were transferred from 2023. From the total number of 78 complaints, 53 cases are completed while the other 25 are still in process.[27] According to the published statistics, the nature of submitted complaints is mainly for camera surveillance to be followed by direct marketing, unauthorized publication of personal data, misuse of data, and so on.[28]

Moreover, it is worth mentioning that the IPA has established safeguards to support the effective implementation of the Law on Protection of Personal Data, offering guidelines and resources to help organizations and individuals adhere to data protection standards.[29] These measures include providing comprehensive guidelines on data handling, conducting regular inspections to ensure compliance, and offering educational resources to raise awareness about data privacy rights. By implementing these safeguards, the IPA plays a critical role in fostering

[24] Annual Working Report, Information and Privacy Agency, 2024, https://aip.rks-gov.net/download/raport-vjetor-i-performances-per-vitin-2023/?wpdmdl=6119&refresh=66c89a203ca4f1724422688

[25] Annual Working Report, Information and Privacy Agency, 2023, https://aip.rks-gov.net/download/raport-vjetor-i-punes-per-vitin-2022/?wpdmdl=6122&refresh=66ee19fa5a96d1726880250

[26] Information gathered from the questionnaire.

[27] Bi-annual Report 2024 of the Information and Privacy Agency, July 2024, https://aip.rks-gov.net/download/raporti-gjashtemujor-aip-2024/?wpdmdl=6222&refresh=66c89a2037fad1724422688

[28] Ibid, page 3.

[29] List of Safeguards available in the website of the IPA, https://aip.rks-gov.net/mbrojtja-e-te-dhenave-personale/mbrojtja-e-te-dhenave-personale/

a culture of accountability and responsibility in data processing across both the public and private sectors.

3. Challenges and Gaps in Enforcement Mechanisms

Implementing data protection laws in Kosovo presents numerous technical, political, organizational, and legal challenges. To begin with, the IPA is authorized to oversee compliance but faces limitations in terms of assets and capacity. This hampers its capacity to conduct thorough inspections, reviews, and follow-up actions. One of the significant legal challenges the IPA has experienced is the delayed recruitment procedures, which have resulted in an overburdened existing staff, thereby postponing the implementation of certain processes.

Moreover, the need for clear regulations for collecting fines forced on public institutions has constrained the IPA to rely on enforcement procedures, leading to extra costs for Kosovo's budget.[30] Whereas the AIP has the authority to impose fines and other punishments, the real enforcement of these measures sometimes faces procedural delays, due to the complexity of cases, and sometimes the lack of cooperation from organizations.

One of the key gaps in enforcement is the moderately low level of public awareness concerning data protection rights. This lack of awareness comes about in fewer complaints being filed by individuals whose rights have been damaged, reducing the overall pressure on organizations to comply with the law. Furthermore, the advancing nature of digital technologies poses a persistent challenge for the administrative system, as new forms of data processing arise that are not completely addressed by existing laws and regulations.

Another critical challenge is the absence of a strong system for cross-border cooperation on data protection matters. Given Kosovo's aspirations for closer integration with the European Union, there's a pressing need to upgrade mechanisms for international collaboration, especially in cases including multinational organizations or cross-border data flows.

To progress compliance and enforcement, it is vital to strengthen the institutional capacities of the AIP, improve public awareness campaigns, and guarantee that organizations are provided with clear rules and support to meet their data protection obligations. In addition, updating the legal framework to address rising technologies and fostering international participation will be fundamental steps toward guaranteeing strong data protection in Kosovo.

4. Big Data Processors

According to the GDPR, the term *Processor* is defined as “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”.[31] *Big Data,* as defined in the EU Digital Strategy refers to a “large amount of data produced very quickly by a high number of diverse sources.[32] Therefore, we will combine these definitions and use a working definition for this report that defines the term *Big Data Processors* as public

[30] Annual Report of the IPA for 2023, https://aip.rks-gov.net/download/raport-vjetor-i-performances-per-vitin-2023/?wpdmdl=6119&refresh=66c89a203ca4f1724422688

[31] GDPR, art. 3

[32] Digital Strategy: Shaping Europe’s digital future, 2024, https://digital-strategy.ec.europa.eu/en

or private entities that process large amounts of data that are produced very quickly by diverse sources.

Today, we are witnessing a switch to a data-driven business environment. Companies are leveraging big data and analytics to help them decide for their companies. For example, they use external data sources to provide additional context and insights, such as social media, market research reports, and government data.[33] These processors often face several challenges in processing data due to their volume and variety.

The large and unstructured dataset management and storage provide significant issues for Big Data Processors. These datasets include transactional data, social media feeds, sensor data from IoT devices, and more. For instance, to provide tailored experiences, businesses like Capital One and Amazon handle enormous amounts of client data in the retail and finance industries. To provide personalized marketing and product suggestions, they examine trends found in transactional data, consumer interactions, and purchase histories.[34]

To remain compliant with the GDPR, Big Data Processors must ensure that appropriate safeguards are in place to prevent unauthorized access, breaches, or misuse of data. The vast amount of personal and sensitive information processed can be a privacy concern. For example, medical institutions such as Memorial Sloan Kettering Cancer (MSKCC) manage a large amount of highly sensitive data and use big data analytics to tailor cancer treatments.[35] Therefore, such institutions should be very careful since breaches of this sensitive information can lead to major consequences.

Another issue for processors is obtaining and managing consent from individuals whose data is being processed. Since it is very difficult to explain the methods of data collection, individuals tend to unknowingly agree to process their data by third-party services. For instance, social media platforms, such as Facebook, have come under scrutiny for issues related to consent and transparency, particularly in the case of the Cambridge Analytica scandal, where millions of users' data was collected without their explicit consent.[36] In this case, Cambridge Analytica was a British-based political consulting firm which through, a quiz, harvested millions of Facebook profile data. It is believed that this was caused due to insufficient safeguards against data mining firms and inadequate supervision by Facebook.[37]

Another challenging issue is that Big Data Processors that operate internationally must comply with GDPR rules, including restrictions on cross-border data transfers. Managing global operations while adhering to regional data protection laws introduces added complexity. In the case of multinational companies (e.g., Amazon), they need to comply with various data

[33] Strategies for Leveraging Big Data and Analytics for Business Development: A Comprehensive Review Across Sectors, N. Adaobi Ochuba, et. Al., published: 9 March 2024.
[34] Ibid.
[35] Designing Data Spaces: The Ecosystem Approach to Competitive Advantage, edited by Boris Otto, et al., Springer International Publishing AG, 2022.
[36] Strategies for Leveraging Big Data and Analytics for Business Development: A Comprehensive Review Across Sectors, N. Adaobi Ochuba, et. Al., published: 9 March 2024.
[37] Facebook – Campridge Analytica data harvesting: What you need to know, Ikhlaq ur Rehman, University of Nebraska – Lincoln, 2019.

protection laws, such as the GDPR and the California Consumer Privacy Act (CCPA), which require constant monitoring and updating of their data processing practices.[38]

[38]Designing Data Spaces: The Ecosystem Approach to Competitive Advantage, edited by Boris Otto, et al., Springer International Publishing AG, 2022.

Chapter III: Big Data Processors in Kosovo

1. Big Data Processors and data protection

Big Data Processors play a significant role in processing and managing the personal data of the citizens of Kosovo, especially considering the high level of digitalization in Kosovo. These entities operate in various sectors, such as telecommunications, finance and healthcare, and can process vast amounts of information, some of which is sensitive. Therefore, it is crucial to assess whether these Big Data Processors act in compliance with the LPPD.

Across the world, we have witnessed major data breaches that exposed vulnerabilities within some of the largest data processors. Examples like the above-mentioned case of the Facebook-Cambridge Analytica scandal, also Equifax's breach of financial data, and Yahoo's massive user account breaches have shown the profound impact data misuse can have on individuals and public trust. These breaches highlight the global challenges in data protection and underscore the need for thorough compliance with legal frameworks.

In Kosovo, these concerns are becoming more significant due to the country being integrated deeply into the global digital economy. According to the Kosovo Digital Agenda 2030, Kosovo is an information society working in the direction of developing new technologies and services.[39] The main objectives that derive from this Agenda are:

- Fully Digitalized Atlas of Fixed Broadband Infrastructure;
- Gigabit Connectivity Available for all Public Institutions;
- Advanced National 5G Coverage; 80% of Kosovar Companies Using Cloud/AI/Big Data;
- 100% of Key Public Services Available Online;
- 90% of Kosovo Citizens Using Digital Identification;
- 100% of Medical Records Available in Digital Form Online; and so on.

Understanding that the focus of the Government of Kosovo is to advance and work towards these goals, this study will narrow its scope of research. In addition, since large financial institutions, telecommunications companies, and public sector organizations process substantial amounts of personal and transactional data daily this study will focus only on these fields. Furthermore, given their role in shaping Kosovo's data environment, it becomes essential to scrutinize their practices and ensure their compliance with the LPPD and GDPR-aligned data protection requirements.

Many prominent data processors significantly impact Kosovo's digital landscape, each playing a crucial role in the collection, organization, and management of personal data across various

[39] Kosovo Digital Agenda 2030: Strategic orientation for Kosovo transformation into a successful digital country, Government of Kosovo, 2023.

sectors. Key players include large retail businesses, financial institutions, public utilities, and telecommunications companies. These entities are central to the functioning of Kosovo's digital infrastructure, handling substantial volumes of personal and sensitive information daily. Given their influence, it is essential to evaluate their data protection practices to ensure they meet the standards set by the LPPD and align with GDPR requirements, thus safeguarding citizens' privacy in Kosovo's evolving digital economy.

2. Telecommunications Companies

According to the Country Commercial Guide from the International Trade Administration, Kosovo Telecom (Vala) holds a significant share of the telecommunications market, approximately 50%. Additionally, IPKO, another major player, competes in the mobile and broadband segments. These two companies are the main operators, and together they dominate much of the market.[40]

In Kosovo, telecommunications companies like Telecom (Vala) and IPKO play a critical role in the digital ecosystem. As primary providers of mobile and broadband services, they process vast amounts of personal data daily, ranging from user identification to traffic and location data. With the government's goals outlined in the Kosovo Digital Agenda 2030, telecommunications companies are expected to support key targets, such as providing advanced national 5G coverage, achieving gigabit connectivity for public institutions, and enabling comprehensive digital identification. These companies' role as large data processors makes them essential players in safeguarding personal data and upholding citizens' privacy rights.

Telecommunication companies around the globe, face unique opportunities to enhance their prospects in the market due to technological advancement. These companies process vast amounts of personal and transactional data, therefore, challenges related to data protection and compliance are inevitable. Recent studies show that *Big Data analysis* - the process of examining large and complex data sets—known as "big data"—to uncover patterns, trends, correlations, and insights that can inform business decisions - has transformed the telecommunications sector, enabling these companies to have a competitive advantage, particularly in identifying inefficiencies, optimally allocating resources, and improving processes.[41] This helps companies that use Big Data Analytics to stand out in a highly competitive market offering services tailored to the needs of consumers. Big Data Analytics enables telecommunication companies to analyze vast amounts of customer data in real-time, improving consumer satisfaction.

Also, in Kosovo companies like Telecom (Vala), Ipko, and Telcos are among the biggest data processors, processing enormous volumes of personal data. Through enhanced data analytics, they can better predict customer behavior, optimize service offerings, and address customer complaints promptly.

[40] International Trade Administration, Kosovo – Country Commercial Guide, https://www.trade.gov/country-commercial-guides/kosovo-telecommunications
[41] Impact of Big Data Analytics on Telecom Companies' Competitive Advantage, A. Alshawawreh, et.al., 2024.

Besides these advantages, the advancement mentioned raises privacy concerns. Telecom companies in Kosovo must ensure that data protection measures align with the LPPD. Ensuring compliance with the local law and addressing the growing risks of data breaches, especially with large datasets, is critical for these organizations to maintain customer trust.

For a comparison, Vodafone, one of the largest telecommunications providers in the EU, can be analyzed. Vodafone must comply with the GDPR. Vodafone states that it is important to seek to respect and protect the right to privacy to maintain the customer's rights. Vodafone ensures compliance with GDPR by implementing data protection policies, including appointing DPOs in all its European branches, enforcing the principle of "Privacy by Design," and allowing users to control their data through consent management systems.[42] Vodafone also takes steps to anonymize and encrypt data, minimizing the risk of breaches. Moreover, Vodafone publishes annual reports and privacy statements to inform its customers regarding compliance with GDPR.[43]

On the other side, **IPKO Telecommunications LLC**, one of Kosovo's largest telecom service providers, on its website has a section informing the public regarding their compliance with the existing Law on Personal Data Protection. It informs the public that the processing of the personal data of its electronic communications service users is performed by the LPPD.[44] IPKO's Privacy Policy states that the company gathers and uses personal data on a variety of legal bases, such as consent, legal requirements, contractual duties, and legitimate interests. Information about a person's identification, communication data, and data pertaining to using IPKO's services—such as location and traffic data—are among the data handled.[45]

Furthermore, IPKO's Privacy Policy highlights the several steps they take to guarantee data privacy, including having data protection procedures in place when handling personal data, determining if data processing is necessary, and enabling users to revoke their consent at any moment. Also, on its website, there is information and an email address on how to reach the Data Protection Officer of IPKO, for matters related to data protection.[46]

3. Financial Institutions

Financial institutions process a large amount of highly sensitive data. As banks and other financial service providers handle massive amounts of personal, transactional, and financial data daily, they play a pivotal role in the digital economy. The integration of Big Data analytics and artificial intelligence (AI) has significantly transformed the financial sector, providing institutions with tools to optimize their services, manage risks, and enhance customer experiences. Financial institutions by leveraging this asset can gain an understanding of markets, customers, products, regulations, and competitors that will enable them to better

[42] Privacy Centre, Vodafone, https://www.vodafone.com/about-vodafone/how-we-operate/consumer-privacy-and-cyber-security/privacy-centre
[43] Vodafone, Annual Report 2024, https://reports.investors.vodafone.com/view/197179846/47/#zoom=true
[44] IPKO Telecommunications LLC website, data protection section, https://www.ipko.com/en/private/data-protection/
[45] Ibid.
[46] Ibid.

compete.[47] This has proved to be efficient also in different areas such as fraud detection, credit scoring, and regulatory compliance. For instance, AI technologies and Big Data play a crucial role in helping financial institutions automate fraud detection by identifying patterns and anomalies in real time, preventing unauthorized transactions, and safeguarding consumer data.[48]However, these advantages come together with significant responsibilities concerning data privacy and security. Financial institutions are obliged to protect sensitive data from breaches and misuse, by implementing data protection rules.[49]

An example of an EU financial institution is Deutsche Bank. As one of the largest banks in Europe, Deutsche Bank has implemented measures to comply with the GDPR.[50] These include appointing a DPO responsible for overseeing compliance and acting as a liaison between the bank and regulatory authorities. Information regarding the DPO can be found on their website.[51] From the information provided by the Deutsche Bank, it is understood that the bank follows GDPR principles such as data minimization, only collecting necessary data for specific purposes, and purpose limitation, ensuring data is used solely for its intended purpose.

Additionally, Deutsche Bank provides clear privacy policies that outline customers' rights, including the right to access, rectify, delete, or transfer their data. To prevent data breaches, the bank employs strong cybersecurity measures such as encryption and regular audits. Employees are trained on GDPR requirements to ensure compliance across all levels of the organization. These efforts help Deutsche Bank maintain transparency, protect customer data, and avoid potential penalties under GDPR.

In Kosovo, the number of licensed and registered financial institutions in the Central Bank of the Republic of Kosovo is 154. This number includes licensed banks, micro-finance institutions, non-bank financial institutions, insurance companies, insurance brokers, independent brokers, and pension funds.[52] Generally speaking, financial institutions in Kosovo, especially Banks, have the most advanced mechanisms for compliance with data protection and other applicable requirements.

Raiffeisen Bank Kosovo and Banka Ekonomike are two examples of banks and financial service providers that play a crucial role in handling sensitive financial data. Because the data these organizations handle is so sensitive, they are subject to strict restrictions regarding data security and privacy. Their activities are a major contributor to Kosovo's digital economy since they use cutting-edge data processing technology to make safe transactions and financial administration easier.

---

[47] New Horizons for a Data-Driven Economy : A Roadmap for Usage and Exploitation of Big Data in Europe, edited by José María Cavanillas, et al., Springer International Publishing AG, 2016.
[48] Ibid.
[49] A Comprehensive Study on Integration of Big Data and AI in Financial Industry and AI in Financial Industry and its Effect on Present and Future Opportunities, S. Ahmadi, International Journal of Current Science Research and Review, 2024, 07 (01), pp.66-74. ff10.47191/ijcsrr/V7-i1-07ff. ffhal-04456267ff
[50] Deutsche Bank website, Privacy Notice, https://www.db.com/legal-resources/privacy-notice?language_id=1&kid=cookies.redirect-en.shortcut#show-content-of-cookies
[51] Data Protection Information under the EU General Data Protection Regulation for "natural persons", May 2018, https://www.deutsche-bank.de/dam/deutschebank/de/shared/pdf/GDPR_Datenschutzhinweis_f%C3%BCr%20Interessenten_EN.PDF.
[52] Financial Licensed and registered Institutions, Central Bank of the Republic of Kosovo, https://bqk-kos.org/wp-content/uploads/2024/08/Lista-e-institucioneve-financiare_12.02.2024-005.pdf.

As the local bank of Kosovo, Banka Ekonomike informs the public about data protection by posting explicit rules on its website. Customers are advised by the bank to send written requests to one specific email or to visit their offices if they have any concerns about how their personal data is processed through the website or wish to exercise their data protection rights.[53] Also, Banka Ekonomike mentions that to comply, its privacy notice may be amended regularly.[54]

Raiffeisen Bank in Kosovo has a lending market share of 20 percent by the end of June 2023 and is the largest bank in Kosovo.[55] Due to its size and influence in the financial landscape, Raiffeisen Bank emphasizes maintaining a robust infrastructure for personal data protection. The bank's privacy policies outline data protection principles and inform customers of their rights to access, rectify, or delete their personal information. In line with the LPPD, Raiffeisen Bank is committed to ensuring data security, implementing safeguards such as encryption, data minimization, and purpose limitation to protect customer information.

Other financial institutions in Kosovo, though varying in size and scope, are similarly bound by data protection obligations under the LPPD. These institutions must establish data protection mechanisms, appoint DPOs, and conduct regular audits to ensure compliance with both national and EU-aligned standards. As Kosovo's financial sector integrates more deeply into the global digital economy, ongoing efforts to strengthen data protection practices will be essential for maintaining compliance, safeguarding customer information, and fostering public trust in digital financial services.

4. Public Administration

Public administration in Kosovo plays a major role in the processing and management of substantial amounts of personal data. It is significantly important for public institutions to ensure data protection to maintain public trust and avoid damage to citizens. These institutions include ministries, agencies, regulatory bodies, and local government entities, which often manage sensitive information such as citizens' health, financial records, legal matters, and social services. To make sure that the data they process and have access to is secure, the LPPD applies to public institutions as well.

The eGovernment Strategy Kosovo 2023-2027 prioritizes the need for a more cohesive approach, focusing on eGovernment coordination, cybersecurity, and digital skills development. The Strategy encourages innovation, to reach its aim for Kosovo, to become a digitally modern country with an advanced digital economy and efficient public administration by 2030.[56] In 2023 the Government of Kosovo, approved the Digital Agenda 2030 where the main strategic priorities are the development of ICT infrastructure, the development of electronic content and services and the promotion of their use, and increasing the capacity of

[53] Banka Ekonomike website, https://bekonomike.com/sq/Mbrojtja-e-t%C3%AB-dh%C3%ABnave-personale-%7C-P%C3%ABrdorimi-i-Cookies
[54] Ibid.
[55] European Bank for Reconstruction and Development (EBRD), 2024 https://www.ebrd.com/news/2024/ebrd-teams-up-with-raiffeisen-to-boost-msme-lending-in-kosovo.html#:~:text=Raiffeisen%20Bank%20is%20the%20largest,than%20900%20employees%20across%20Kosovo.
[56] eGovernment Strategy Kosovo 2023-2027, https://mpb.rks-gov.net/Uploads/Documents/Pdf/EN/2700/e-Government%20Strategy%20Kosovo%202023-2027.pdf

Kosovo's residents to use ICT.[57] This means that the Government is working towards digitalization.

In Kosovo, the launch of eKosova Portal made it possible for citizens of Kosovo to interact with the Public Administration digitally. On this platform, there are services for citizens and businesses including services for civil status, education, taxes, police, health, and so on.[58] The usage of the platform has experienced considerable growth through the years.

The platform eKosova is considered to be one of the key reforms in Kosovo Public Administration where today are 155 online services in 22 categories offered by this portal.[59] However, a remaining challenge is that the technical management of the eKosova platform, along with other e-government services, depends heavily on external partners. This reliance on outside partners for critical technical functions—such as system infrastructure, cybersecurity, and ongoing maintenance—limits Kosovo's direct control over these platforms. This dependency could impact the long-term sustainability, security, and adaptability of eKosova and other digital government services.[60]

The increased use of Information and Communication Technology (ICT) in public administration also presents risks, particularly in ensuring the security of citizens' private data. According to a study on digitization, the use of ICT in Kosovo's public administration has enabled faster and more transparent service delivery but has also raised concerns about data breaches and the adequacy of legal protections.[61]

Civil Registration Agency is one of the biggest agencies that process personal data. In January 2024, Law no.08/L-240 on Civil Registration Agency was approved which established the Civil Registration Agency was approved which established the Civil Registration Agency and its duties and responsibilities at central and local levels.[62] The Agency has a vast amount of personal data. However, access is restricted to authorized officials within the Civil Registration Agency. Since 2018, the Agency has utilized the Interoperability Platform of Kosovo, based on Microsoft's Government Gateway (GG). The number of transactions processed through this platform has increased and in 2023 exceeded 16 million, marking a 26 percent increase from the previous year.[63]

[57] Kosovo Digital Agenda 2030: Strategic orientation for Kosovo transformation into a successful digital country, Government of Kosovo, 2023.
[58] eKosova Platform, https://ekosova.rks-gov.net/Services
[59] Kosovo 2024 Digital Public Administration Factsheet: Main developments in digital public administrations and interoperability, https://joinup.ec.europa.eu/sites/default/files/inline-files/NIFO_2024%20Supporting%20Document_Kosovo_vFinal_rev.pdf
[60] eGovernment Strategy Kosovo 2023-2027, https://mpb.rks-gov.net/Uploads/Documents/Pdf/EN/2700/e-Government%20Strategy%20Kosovo%202023-2027.pdf
[61] Digitalization of Administration and Legal Basis in Kosovo, K.Dërmaku, A.Emini, 2024.
[62] Law no.08/L-240 on Civil Registration Agency, https://gzk.rks-gov.net/ActDetail.aspx?ActID=85153
[63] Kosovo 2024 Digital Public Administration Factsheet: Main developments in digital public administrations and interoperability, https://joinup.ec.europa.eu/sites/default/files/inline-files/NIFO_2024%20Supporting%20Document_Kosovo_vFinal_rev.pdf

5. Public Utilities

Public utilities, such as Prishtina Parking and Kosovo Energy Corporation (KEK), play a vital role in Kosovo's digital economy, managing significant volumes of personal and operational data. These companies rely on ICT systems to optimize service delivery, monitor resource usage, and facilitate customer interactions. Similar to government institutions, public utility companies must also comply with data protection laws to safeguard personal information from unauthorized access or breaches.

As public services become more digital, utility companies are also integrating e-governance models to streamline processes and improve customer service. For instance, Prishtina Parking has adopted digital systems for managing parking services, making data protection a critical concern as they handle sensitive vehicle and payment information. The Law on the Information Society Government Bodies in Kosovo sets clear guidelines on the use of ICT for data management, ensuring that public utilities comply with national data protection regulations.

The general condition of the sector to data protection in Kosovo reveals a mixture of strengths and areas requiring improvement. While many companies, such as KESCO, have taken steps to publish privacy policies on their websites, there are often gaps in transparency and accessibility for customers seeking more detailed information. For instance, KESCO's Privacy Policy is accessible online, outlining the company's commitment to data protection; however, it lacks clear guidance on how customers can address data protection concerns or report potential breaches.[64]

This gap is not unique to KESCO. Across various sectors, data protection practices frequently fall short of fully meeting customer needs for transparency and accountability. Few companies provide specific contact information for data protection officers (DPOs) or a direct point of contact for privacy-related inquiries. Additionally, while policies may outline general data protection principles, actionable details—such as procedures for managing data breaches or handling customer requests to exercise their data rights—are often missing.

Strengthening data protection practices across sectors will require companies to not only comply with regulatory requirements like the LPPD but also adopt a proactive approach to making their data management processes transparent. Clear communication channels, dedicated data protection contacts, and detailed privacy policies can help build public trust and ensure compliance with both local and EU-aligned standards.

6. Health Sector

The health sector in Kosovo comprises a large network of public and private institutions handling substantial volumes of sensitive health data. According to the Kosovo Agency of Statistics, there are 2,095 licensed private health institutions in the country, including 29 hospitals and 2,066 other health facilities such as ambulances, polyclinics, and laboratories.[65] While Kosovo has taken steps to enhance data protection within healthcare, many institutions

[64] Privacy Policy, KESCO, 2020, https://www.kesco-energy.com/?pageId=74&language=2&isPreview=True
[65] Health Statistics 2022, Kosovo Agency of Statistics, https://ask.rks-gov.net/Releases/Details/7265

still face challenges in implementing comprehensive security measures due to limited resources and technical support.

Kosovo is in the process of developing an Integrated Health Information System (IHIS), which is considered very important to offer and improve the quality of care. This data can also be used by policymakers to contribute to these improvements.

Currently, only a Basic Health Information System (BHIS) is in place, and its functionality has recently expanded beyond simply registering patients to include tracking patients' medical histories. The BHIS communicates with some of the legacy systems (such as ePrescription, the Health Information Flow Information System, the Pharmaceutical Stock Management System, the Surveillance System and the Early Warning System).[66] Healthcare providers handle sensitive patient data, such as medical histories, diagnoses, and treatments, which makes the sector particularly vulnerable to data breaches.

According to international studies, if breaches of personal health data happen, it results in severe consequences, ranging from identity theft to insurance fraud.[67] A notorious example of this is the large-scale data breach in a U.S.-based health insurer where 78.8 million patient records were stolen, highlighting the severity of such incidents.[68] This breach resulted in widespread identity theft, where stolen personal and medical information was used to fraudulently obtain medical services and make insurance claims, affecting both patients' financial stability and their access to healthcare. Such incidents highlight the critical need for healthcare providers to implement strong security measures. In Kosovo, this emphasizes the importance for health institutions to adopt stringent protections to safeguard patient data from unauthorized access and misuse, thus preserving both patient privacy and trust in the healthcare system.

In Kosovo, data protection and privacy in the health sector are within the scope of the LPPD, which requires healthcare providers to implement technical and organizational measures to protect data. As digital health systems grow, these institutions must also invest in advanced data protection technologies, such as encryption and secure authentication methods, and provide regular staff training on privacy protocols. This is particularly important as the increasing use of telemedicine and remote patient care services introduces new risks. This is particularly important as the increasing use of telemedicine and remote patient care services introduces new risks.

The global health sector's experience provides a valuable lesson for Kosovo. It has been shown that healthcare organizations are more vulnerable to data breaches compared to other sectors, due to factors like the large number of individuals who have access to patient data, including clinicians, administrative staff, and third-party service providers.[69] To strengthen data protection, healthcare organizations in Kosovo should implement specific cybersecurity measures, such as conducting regular security audits, developing incident response plans, and

[66] Kosovo 2024 Digital Public Administration Factsheet: Main developments in digital public administrations and interoperability, https://joinup.ec.europa.eu/sites/default/files/inline-files/NIFO_2024%20Supporting%20Document_Kosovo_vFinal_rev.pdf
[67] A systematic analysis of failures in protecting personal health data: A scoping review, J. Pool, et. Al., 2023.
[68] Ibid.
[69] Ibid.

training staff to recognize potential security threats. By taking these proactive steps, they can better safeguard patient information, maintain compliance, and build lasting trust within the healthcare system.

By drawing from international practices, such as those implemented in the EU under the GDPR Kosovo's health sector can enhance its data protection strategies. For example, implementing Privacy by Design—which incorporates data protection into the development of new systems—can help prevent breaches. Additionally, maintaining transparency with patients about how their data is collected, processed, and stored is essential for building trust.[70]

7. Education Sector

The education sector in Kosovo handles sensitive personal information, including student records, attendance, health information, and disciplinary history. It plays another critical role in the collection and processing of personal data, particularly with the growing adoption of digital learning platforms and student management systems. Educational institutions, ranging from universities to primary schools, collect vast amounts of personal data on students, faculty, and staff, including sensitive information such as academic records, health information, and financial data related to tuition and scholarships. These institutions are also legally required to comply with the LPPD.

With the rise of e-learning platforms and remote education due to the COVID-19 pandemic, the amount of personal data processed has increased significantly, introducing new challenges for data protection in the education sector. Schools and universities must adopt robust cybersecurity measures to protect against data breaches that could expose student information. For example, many institutions are moving toward cloud-based systems for managing student records, which require strong encryption and secure access protocols to prevent unauthorized access.

These data are essential for managing academic programs and providing quality education services, their protection is critical to ensure student privacy. However, insights from the general questionnaire responses indicate varying levels of compliance and awareness around data protection requirements, suggesting that educational institutions in Kosovo may also face challenges in implementing consistent data protection practices.

Globally, breaches in the education sector have been on the rise. Recent international studies have shown that educational institutions are increasingly targeted by cyberattacks, often due to the sensitive personal and financial data they store.[71] In many cases, breaches result from vulnerabilities in outdated IT systems, insufficient training for staff on data protection, or insecure communication methods such as unencrypted emails.[72]

To ensure compliance with local regulations and global standards, educational institutions in Kosovo must focus on data minimization—only collecting the data necessary for educational purposes—and implementing privacy-by-design principles, where data protection is integrated

[70] Ibid.
[71] A systematic analysis of failures in protecting personal health data: A scoping review, J. Pool, et. Al., 2023.
[72] Ibid.

into the development and deployment of new digital tools. Additionally, schools and universities should provide regular training for staff on data privacy and security protocols, ensuring that everyone involved in handling personal data is aware of the risks and the importance of maintaining compliance with data protection laws.

One key finding from the questionnaire was a limited adoption of DPIAs across sectors, which is likely relevant for educational institutions as well. DPIAs are crucial in assessing risks before introducing new data processing systems, such as student information management systems. The limited use of DPIAs may indicate a need for greater awareness and resources in the education sector to evaluate data risks comprehensively.

Additionally, questionnaire responses highlighted that many organizations in Kosovo lack a formal incident response plan. This gap is particularly relevant for the education sector, where breaches of student data could have severe consequences, including unauthorized access to academic records or misuse of personal information. Developing incident response protocols and training staff on these procedures could significantly improve data protection in schools and universities.

The findings underscore the importance of targeted investments in advanced data protection technologies and organizational measures within the education sector. As Kosovo's digital transformation continues, establishing privacy protocols and ensuring transparent communication about data handling practices are critical steps in safeguarding student information.

Chapter IV: Challenges of Big Data Processors

1. Regulatory and Compliance Issues

Entities in Kosovo face challenges in following data protection laws due to different reasons. One of the essential difficulties is the complex and advancing nature of data protection regulations. Whereas Kosovo's data protection laws are generally aligned with the GDPR numerous organizations battle to completely comprehend and actualize these regulations. This is especially true for small and medium-sized enterprises (SMEs) which often lack the assets or skills to guarantee full compliance.

However, these challenges are present also in the EU countries, and even large enterprises face difficulties in complying with the GDPR. As an example in 2020, Vodafone, one of Europe's leading telecommunications companies, was fined over 12 million euros by Italy's Data Protection Authority (DPA) for violating GDPR rules. The fine was imposed due to aggressive telemarketing practices that disregarded customers' consent, including calls to individuals who had explicitly opted out.[73]

Moreover, during the investigation, the DPA found that there was a use of fake telephone numbers to place marketing calls. The DPA ordered Vodafone to implement systems and prove that processing for telemarketing will be done in compliance with consent requirements.[74] As a result, the company did not process data lawfully, and upon assessment, it was found that the data subjects could be re-identified through reasonable means. These challenges are not limited to telecommunication companies and in health sector; they extend to many sectors, including education, and finance. The case of Vodafone highlights the need for organizations to continuously monitor their data processing activities, implement robust compliance strategies, and ensure that customer consent is adequately respected across all operations.

Another recent case is the decision of 5th September 2024 of the French Supervisory Authority to issue CEGEDIM SANTÉ a fine of 800,000 Euros. The investigations started in 2021 and revealed that this company had processed non-anonymized health data without authorization. They have transmitted to their customers to carry out studies and produce statistics in the health sector.[75] These cases illustrate that even well-established companies struggle to fully comply with the strict regulations set forth by GDPR, especially in areas concerning data collection, consent management, and transparency.

Kosovo, with its LPPD, faces similar challenges, as local data processors strive to align their practices with both domestic regulations and international standards. This alignment becomes even more complex when considering the resource limitations, technological gaps, and evolving regulatory landscapes in the region.

[73] Aggressive telemarketing practices: Vodafone fined over 12 million Euro by Italian DPA, November 2020, https://www.edpb.europa.eu/news/national-news/2020/aggressive-telemarketing-practices-vodafone-fined-over-12-million-euro_en
[74] Ibid.
[75] Commercial prospecting: French SA fined CEGEDIM SANTÉ EUR 800 000, 17 September 2024, https://www.edpb.europa.eu/news/national-news/2024/commercial-prospecting-french-sa-fined-cegedim-sante-eur-800-000_en

2. Technological Challenges

Technological challenges show another noteworthy obstacle to compelling data protection in Kosovo. Cybersecurity dangers, such as hacking, phishing, and ransomware attacks are a consistent concern for organizations that handle huge volumes of personal data. Numerous organizations, particularly those within the public sector, depend on outdated or insufficiently secure technological frameworks, rendering their cybersecurity measures almost obsolete. Besides, the fast pace of innovative progression implies that organizations must persistently overhaul their frameworks to keep up with modern dangers, an errand that can be both expensive and resource-intensive.

The Kosovar Center for Security Studies (KCSS) reports that Kosovo has experienced a noteworthy increment in cyberattacks, including malware, social engineering, and ransomware, especially focusing on public institutions like Kosovo Telecom and e-Kosova.[76] These attacks misuse the outdated and insufficiently secure technological systems in place, which are common in numerous organizations, particularly inside the public sector.

Furthermore, despite recent improvements, Kosovo's cybersecurity infrastructure still falls behind that of more developed areas. These risks are made worse by a lack of qualified IT workers and restricted access to cutting-edge cybersecurity solutions, which makes it challenging for enterprises to properly manage and safeguard their data. The region's attempts to improve data protection are made more difficult by the constant requirement to update procedures and systems to stay ahead of changing threats.[77]

3. Awareness

A key concern in Kosovo is also the insufficient understanding of rights and duties regarding data privacy. A lack of awareness about the significance of data protection among many people and organizations can result in the negligent management of personal data and insufficient security measures. This problem is especially noticeable in SMEs and government organizations, where data security may not be given top priority or incorporated completely into daily operations.[78]

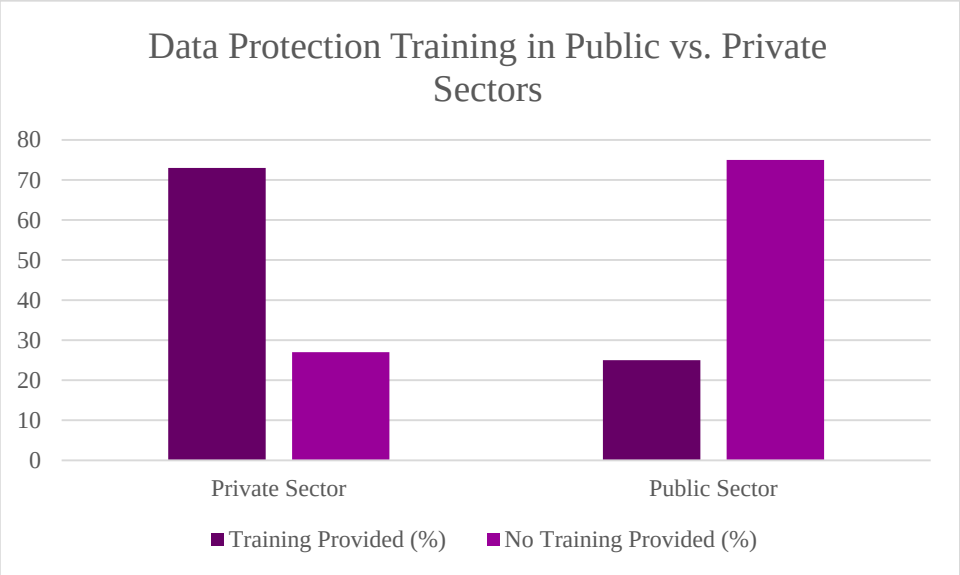
Furthermore, teaching stakeholders about data privacy laws and recommended practices is quite difficult. Even though some organizations have implemented awareness campaigns and trained their workers, these efforts are frequently insufficient. Due to the scarcity of comprehensive and successful teaching programs, many people are still not aware of their data protection rights.

The absence of awareness and proper training for data protection officers is a major issue that our survey results revealed. These officers find it difficult to successfully execute the rules and procedures required to protect data inside their businesses if they are not properly prepared.

[76] ROAD TO RESILIENCE: Governance and Capacity Building in Kosovo’s Cyber Defense and Critical Infrastructure, KCSS, March 2024, https://qkss.org/images/uploads/files/Road_to_Resilience.pdf.
[77] Ibid.
[78] Country Situation Report: Digital Rights in Kosovo, Open Data Kosovo, 2022.

Their capacity to guarantee adherence to data protection laws and preserve the integrity of personal information is directly impacted by this training gap.[79]

We discovered a sizable discrepancy in data protection training between the public and private sectors in our study. Of those surveyed in the private sector, 73% said their organizations regularly provide staff with training on data protection. By comparison, 75% of respondents from the public sector stated that their institutions do not offer this kind of training. This disparity emphasizes the necessity of emphasizing data protection education more, especially in public organizations where a lack of training may prevent data security measures from being implemented effectively.[80]



5. Key Questions for Assessing Data Protection Compliance in Kosovo

As Kosovo strengthens its legal framework for data protection under the LPPD, organizations need to assess their compliance with these standards. Our study was built around key questions that not only guide compliance but also serve as a valuable resource for entities aiming to enhance their data protection practices. These questions provide a structured framework that helps organizations identify specific areas for improvement and can support future assessments as data protection laws and risks continue to evolve.

Below are five critical questions designed to evaluate how well organizations align with the LPPD's standards. Addressing these questions can enable entities to protect personal data more effectively, reduce the risk of breaches, and ensure compliance with both local and international data protection standards:

1. Do you have a designated Data Protection Officer (DPO)?

[79] Information gathered from questionnaire on data protection in Kosovo.
[80] Information gathered from questionnaire on data protection in Kosovo.

Appointing a DPO is a critical requirement under data protection laws like GDPR and LPPD. The DPO is responsible for overseeing data protection strategies and ensuring that the organization complies with legal requirements. This role is pivotal for managing data security risks and acting as a point of contact for regulatory authorities. In the absence of a DPO, organizations may face significant gaps in compliance monitoring and risk management.

2. **Does your organization have a written and regularly updated data protection policy?**

A formal, written data protection policy is the cornerstone of compliance. It sets out the organization's approach to data protection, outlining protocols for data collection, processing, storage, and security. Regular updates to this policy ensure that the organization adapts to changes in regulations, technology, or the type of data processed. Without a policy, or with an outdated one, organizations are more vulnerable to regulatory breaches and penalties.

3. What security measures, such as encryption and firewalls, are in place to protect data?

In a digital age where data breaches are increasingly common, strong technical safeguards like encryption, firewalls, and access control systems are non-negotiable. These technologies protect personal data from unauthorized access, theft, or loss. Organizations that lack adequate security measures not only risk losing customer trust but also face hefty fines under the LPPD and GDPR for failure to protect sensitive data.

4. Do you have an incident response plan for managing data breaches?

Data breaches are not a matter of "if" but "when." A comprehensive incident response plan allows organizations to mitigate the damage caused by a breach. The plan should include steps for notifying affected individuals, reporting the breach to authorities, and remediating the cause of the breach. Without a plan, organizations may struggle to respond efficiently, resulting in higher penalties and damage to reputation.

5. Is Privacy by Design integrated into your systems and processes?

Privacy by Design refers to embedding privacy considerations into the development of systems, processes, and products from the outset. By incorporating privacy into the core design, organizations proactively protect data rather than reactively addressing issues after they arise. This approach not only ensures compliance with LPPD but also aligns with global best practices, such as those outlined in GDPR.

These questions not only serve as a framework for assessing compliance with the LPPD but also help entities identify areas where improvements can be made. By addressing these key aspects, organizations can better protect personal data, reduce the risk of breaches, and ensure they remain compliant with both local and international data protection standards. Key Question	Compliance Options	Compliance Rating (Low to High)	Recommended Measures
1. Do you have a designated DPO?	1. No DPO assigned	Low	Appoint a DPO; establish reporting to management; conduct regular reviews.
	2. Part-time DPO with limited scope	Medium	Assign full-time DPO with complete oversight of data protection activities.
	3. Full-time, trained DPO	High	Conduct regular DPO training; establish DPO as a point of contact with authorities.
2. Is there a written data protection policy?	1. No formal policy	Low	Develop a comprehensive data protection policy; ensure management approval.
	2. Policy exists but is outdated	Medium	Review and update the policy regularly (annually or as regulations evolve)
	3. Regularly updated policy	High	Publish policy internally and externally; incorporate it into employee training.
3. What security measures are in place?	1. Basic protection (passwords)	Low	Implement encryption, firewalls, and multi-factor authentication.

	2. Basic + encryption or firewall	Medium	Adopt advanced encryption protocols, regular software updates
	3. Full suite of security measures	High	Conduct security audits; use data masking for sensitive data
4. Is there an incident response plan?	1. No incident response plan	Low	Develop an incident response plan, outline response steps, and assign roles.
	2. Informal, ad-hoc responses	Medium	Formalize incident response, including regular updates and role assignments.
	3. Comprehensive, tested plan	High	Test the plan regularly; train employees on response protocols
5. Is Privacy by Design implemented?	1. No Privacy by Design measures	Low	Integrate privacy considerations into system development; conduct DPIAs
	2. Limited Privacy by Design practices	Medium	Apply Privacy by Design to new projects; regularly review design strategies.
	3. Fully embedded Privacy by Design	High	Regularly review and update Privacy by Design principles; conduct training.

Chapter V: Case Studies

1. Case Study 1: KESCO

Kosovo Electricity Supply Company (KESCO) serves as the universal electricity supplier in Kosovo, ensuring the delivery of electricity to customers throughout the country. This role involves not only delivering power to households and businesses but also managing services that support energy distribution, billing, and customer relations.[81] KESCO processes enormous volumes of personal data, including billing information and client identities, as a major data processor. Adherence to data protection standards is crucial, considering the delicate nature of the information involved.

KESCO, as mentioned earlier has published on its website the Privacy Policy.[82] This Privacy Policy is more regarding its internet website and explains how the client data will be used. It explains how the use of data will increase efficiency and offer better service and care for clients. Among others, in the Privacy Policy, it is written that: "The security of your data is important to us, but remember that no method of transmission over the Internet, or an electronic storage method is not 100% secure. While we try to use commercially acceptable means to protect your data and personal information, we cannot guarantee its absolute security."[83]

The Information and Privacy Agency (IPA) of Kosovo began investigating KESCO in 2024 for violating the Data Protection Law. The results of the examination showed that KESCO had not put in place sufficient safeguards for personal data, which might have put data breaches and illegal access at risk. The Law on Data Protection, which imposes stringent protections for the processing and storage of personal data, had many important sections that were broken by these errors.

Following these conclusions, KESCO was hit with one of the largest fines for data privacy violations in Kosovo—20,000 EUR—by the IPA.[84] This decision was taken after several complaints received by AIP. These complaints, submitted by data subjects, alleged that KESCO had delivered electricity bills openly, without envelopes, in semi-exposed mailboxes near doors in shared corridors and at house entrances, making them easily accessible to third parties.[85] AIP gave KESCO four months to improve this practice and act following the law. However, KESCO failed to protect its client data and therefore the AIP decided as described. This case acted as an example of caution for other significant data processors in the nation and emphasized the significance of abiding by data protection rules.

In August 2024, KESCO informed the public that they began distributing electricity bills in envelopes to over 700,000 customers across Kosovo. This shift follows a pilot project and was implemented in response to a decision by the Information and Privacy Agency to enhance the

[81] Kosovo Electricity Supply Company, KESCO, https://www.kesco-energy.com/eng/about-us/about-us/
[82] Privacy Policy of KESCO, https://www.kesco-energy.com/shq/legjislacioni/rregullat-dhe-procedurat/politikat-e-privatesise/
[83] Ibid.
[84] Decision of AIP, no. 182/2024, date 16 August 2024, https://aip.rks-gov.net/download/vendim_nr_182_-ndaj-kompanise-kosovare-per-furnizim-me-energji-elektrike-sh/?wpdmdl=6374&refresh=66cd969e170761724749470
[85] Ibid.

protection of personal data. Moreover, they informed the public that the company faced challenges, including the lack of mailboxes and address identifiers in rural areas, which slowed the process.[86]

The KESCO case serves as a reminder of the difficulties big businesses have in staying in compliance with data protection laws. It also highlights how important regulatory organizations like the IPA are to upholding these rules and safeguarding individuals' private information from exploitation. This event has probably prompted KESCO and other Kosovo-based businesses to review their data protection policies and make sure they are fully compliant with the law.

2. Case Study 2: Gjakova Municipality

In 2024, the Municipality of Gjakova was fined €20,000 by the Information and Privacy Agency (IPA) for unlawfully processing and publicly disclosing personal data. The municipality had published lists on its official website containing sensitive information such as names, birth years, personal identification numbers, medical diagnoses, and bank details of individuals who had applied for healthcare subsidies. This disclosure violated multiple provisions of the Law on Personal Data Protection, specifically regarding the inappropriate processing of sensitive data without proper legal basis or consent.[87]

The incident began when the IPA, acting on a report received in June 2024, investigated and found that Gjakova had inadvertently exposed the personal data of both subsidy recipients and non-recipients on its website. This information, accessible to the public, included sensitive medical records, personal identification numbers, and contact details. Despite being contacted by journalists about the breach, the municipality's initial response was inadequate, claiming the error was due to human oversight during publication.

Following a detailed inspection, the IPA concluded that the municipality’s actions posed a significant risk to the privacy and security of individuals, especially in an era of increasing digitalization. The IPA highlighted that such exposure to health-related data could severely affect the dignity and privacy of the individuals involved. The municipality was also criticized for failing to appoint a Data Protection Officer, a legal requirement that would have helped prevent such issues.[88]

Yet, the Gjakova Municipality website does not provide any clear information regarding the appointment of a Data Protection Officer (DPO). Despite the requirement under data protection laws for public institutions to have a designated officer responsible for ensuring compliance with data protection regulations, no contact details or specific information about a DPO can be found on the site.[89]

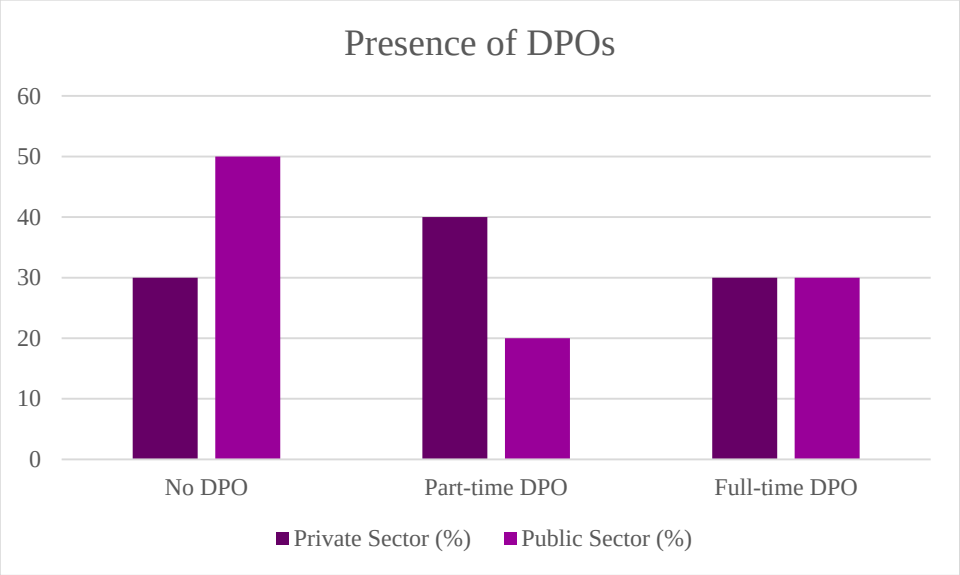
The case underscores the critical importance of safeguarding personal and sensitive data, particularly within public institutions. The fine and subsequent scrutiny emphasize the

[86] KESCO is distributing electricity bills in envelopes for over 700,000 customers, 28 August 2024, https://www.kesco-energy.com/shq/artikujt-e-fundit/kesco-po-shperndan-faturat-e-rrymes-ne-zarfe-521/
[87] Decision no.105/2024, date 14 June 2024, https://aip.rks-gov.net/download/vendim-nr-105-komuna-gjakoves/?wpdmdl=5672&refresh=66ff0f0adb97b1727991562
[88] Ibid.
[89] Gjakova Municipality website, https://kk.rks-gov.net/gjakove/?page_id=200000142

necessity of compliance with data protection laws to protect individuals' privacy in both the public and private sectors.

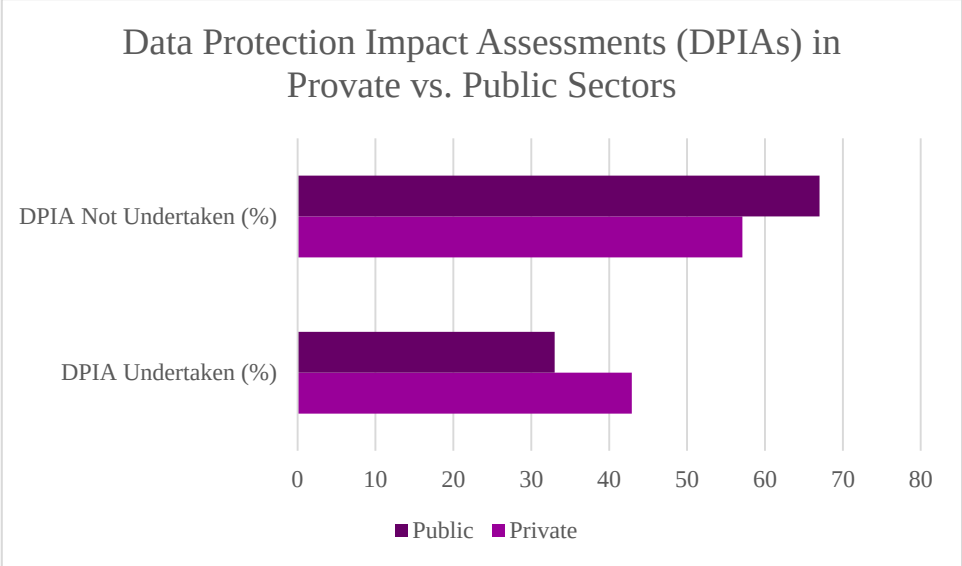
Chapter VI: Insights from the Data Protection Compliance Survey

Respondents' understanding of data protection was found to be generally strong, as indicated by the majority of respondents who gave their knowledge a grade of 4 out of 5. In the public sector, where the majority endorsed the appointment of a Data Protection Officer (DPO), this tendency was especially significant. While DPOs were reported by the private sector as well, the data shows a greater discrepancy in compliance than in the public sector.



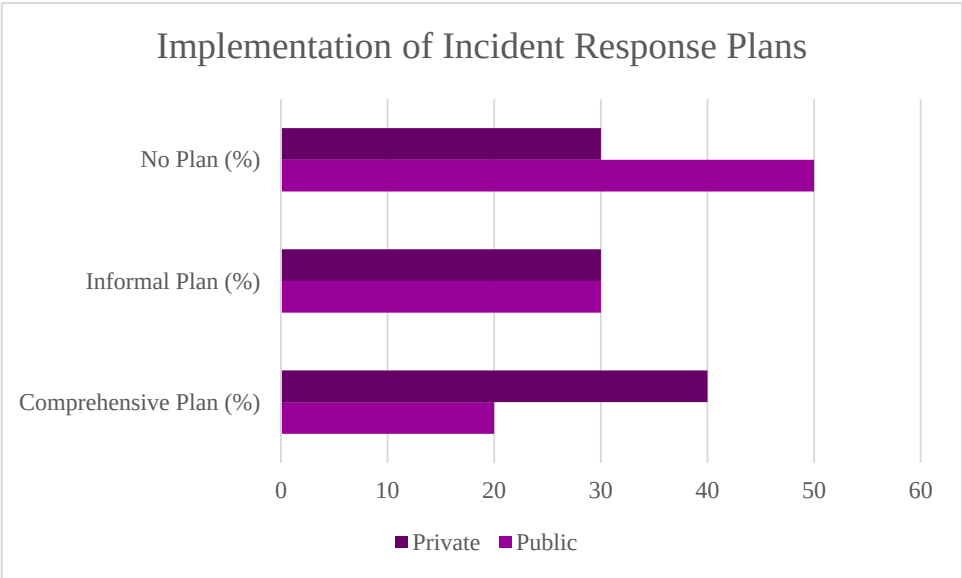
The majority of governmental and private institutions responded in the affirmative when asked if they have drafted privacy rules. Nonetheless, the most typical response from all sectors about the updating of these rules was that they are done "as needed," suggesting a reactive as opposed to a proactive strategy.

Only 42.9% of commercial sector respondents and 33% of public sector respondents reported undertaking DPIAs, which are essential before adopting new processing operations. This points to a clear need for development, particularly in light of the possible hazards connected to emerging technology.



Both sectors reported managing personal, financial, and health data in terms of data categories gathered and processed; however, marketing data was more common in the private sector. Technologies like data masking, access control systems, and firewalls are frequently employed to manage and safeguard this data.

Significant gaps existed in the commercial sector's readiness for data breaches; 71.4% of respondents said they lacked an incident response plan, whereas 50% of respondents in the public sector said they had. This disparity highlights the urgent need for the private sector to become more prepared.



The difficulties differed throughout industries. The main challenges in the public sector were a lack of knowledge and training, inadequate resources, and technical constraints. The private sector identified a lack of knowledge and burdensome regulations, in addition to technology limitations, as their primary problems.

The governmental sector claimed less frequent training, indicating a discrepancy in continuous education, whereas the commercial sector typically replied in the positive when asked if they often get data protection training. The public sector had differing opinions on the efficacy of present rules, while the private sector gave answers ranging from neutral to moderately effective when asked about the efficiency of current law enforcement measures.

The two sectors' public awareness campaigns were similar in that they mostly relied on their websites' privacy rules. But when asked about intentions to implement new technology to enhance data security, a sizable majority in both sectors—85% in the private and 75% in the public—said they had no such intentions.

It's interesting to note that neither industry reported any data breaches in the previous year. This might be due to either effective incident detection procedures or strict data security measures. There seems to be a lack of consistency in the verification of compliance with data protection rules, especially in the public sector where many have stated that no compliance checks are made. Practices in the private sector were somewhat better, and certain organizations conducted routine monitoring.

Requests from clients for access, modification, or deletion of their data are often handled by customer service departments in the private sector. On the other hand, the public sector often responds to these inquiries through written emails, while some organizations claim to have never received them.

Another area where governmental institutions differ from the private sector is in data sharing. The former typically reported not sharing personal data with other parties, while the latter does so under certain circumstances.

Lastly, the survey outlined the primary obstacles and chances for enhancing data security. The private sector has several obstacles, such as a shortage of skilled personnel, inadequate training, and resources, and the difficulty of keeping up with the quickly evolving legal landscape. The main issues facing the public sector were coming up with internal regulations, strictly executing the law, and getting over technology constraints. Regarding opportunities, both industries recognize the value of making technological investments, improving employee training, and creating thorough corporate policies to improve data security procedures.[90]

[90] Information gathered from questionnaire on data protection in Kosovo.

Chapter VII: Conclusion

Kosovo's data protection framework has made notable strides through alignment with the GDPR and the establishment of the Law on Protection of Personal Data (LPPD). However, our study highlights significant gaps between legislative advancements and practical implementation. The following recommendations aim to address these challenges and support Kosovo in creating a secure, privacy-conscious digital landscape:

1. **Strengthen the Resources and Capacity of the Information and Privacy Agency (IPA)**: To enable regular inspections, audits, and follow-ups, the IPA requires enhanced resources and skilled personnel. Strengthening IPA's capacity will allow more thorough oversight and better support organizations in understanding and meeting compliance requirements.

2. **Implement Regular Data Protection Training Across Sectors**: Our findings show a discrepancy in data protection training between the public and private sectors, with a notable lack of continuous education in public institutions. Regular, sector-specific training programs are essential to foster a data protection culture, ensuring that employees across all sectors understand and apply best practices in data handling.

3. **Mandate the Consistent Performance of DPIAs and Policy Updates**: Many institutions have yet to implement proactive data protection measures like regular policy reviews and DPIAs. Enforcing these requirements, especially in organizations handling large or sensitive datasets, can improve risk management and compliance, reducing vulnerabilities to breaches.

4. **Adopt Privacy by Design and Privacy by Default Principles**: Integrating data protection measures into the initial design stages of digital systems can enhance data security and compliance. This approach should be encouraged across sectors, particularly in organizations undergoing digital transformation, to ensure that privacy is embedded within operational processes.

5. **Develop and Enforce Standardized Data Protection Guidelines**: A collaborative effort between public and private sectors to establish uniform data protection practices can promote consistent compliance. Standardized guidelines would help align practices across sectors and address inconsistencies found in our survey.

6. **Launch Public Awareness Campaigns on Data Protection Rights**: Empowering citizens to understand and exercise their data protection rights is essential for accountability. Awareness campaigns and accessible guidelines can encourage individuals to demand better data practices, thereby reinforcing compliance and trust in digital services.

7. **Encourage the Development of Incident Response Plans**: Given the lack of formal incident response plans in many organizations, especially within the private sector, it is critical to encourage the establishment of structured procedures for managing data breaches. An effective incident response plan helps organizations respond swiftly, mitigating damage and enhancing customer trust.

By implementing these recommendations, Kosovo can address the practical challenges identified in this study and advance its data protection landscape. This approach not only aligns with international standards but also promotes a privacy-first culture, positioning Kosovo to benefit from its growing integration into the global digital economy.

ITS INSTITUTE FOR TECHNOLOGY AND SOCIETY