International Journal of Innovative Solutions in Engineering
2025, Vol. 1 No. 2 (pages 54–64)
DOI: 10.47960/3029-3200.2025.1.2.54

Research Article

OPEN ACCESS

Toward Integrated Compliance with GDPR and the EU AI Act Based on Empirical Findings

Tonći Kaleb[1], Ivan Markić[2]

[1]ISACA Croatia Chapter, Croatia
[2]Faculty of Mechanical Engineering, Computing and Electrical Engineering, University of Mostar, Bosnia and Herzegovina

Abstract

This paper explores how the European Union is shaping rules for data and artificial intelligence (AI) through two key regulations: the General Data Protection Regulation (GDPR) and the EU Artificial Intelligence Act (AI Act). Those two regulations cover data topics, focusing on different aspects, both bringing challenges for organizations and individuals. This paper includes a survey conducted among data protection professionals to better understand how organizations deal with these challenges in practice. The results show that many organizations still have areas for improvement, especially when combining privacy and AI responsibilities. Based on this, the paper offers a simple and practical framework that helps organizations follow the GDPR and the AI Act in a transparent and integrated way. The goal is to support better decision-making, reduce legal and technical risks, and help with the responsible and trusted use of data and AI in the EU.

Article history
Received: 14. 05. 2025.
Revised: 18. 06. 2025.
Accepted: 30. 06. 2025.

Keywords
GDPR,
AI Act,
Data Governance,
Risk Management,
Privacy,
Compliance,
EU Regulation.

1 Introduction

The volume, utilization, and value of data are growing, supported by digital technologies. In response to evolving digital threats and privacy concerns, the European Union is intensifying its regulatory initiatives in cybersecurity and data management. The focus is on how personal data and artificial intelligence (AI) systems are used and protected. The EU's General Data Protection Regulation (GDPR) has been enforced since May 25, 2018, becoming the global standard for protecting personal data and privacy rights. The EU Artificial Intelligence Act (AI Act), which will come into effect in 2024, sets up a risk-based approach to create, use, and control AI systems in all EU countries. This research also includes findings from a survey conducted among data protection professionals to support the author's thesis. The goal was to better understand how organizations are currently positioned regarding compliance, what roles are involved (such as data protection officers), and the level of readiness to respond to AI-related obligations. Based on the comparative review and the survey results, this paper proposes a practical framework for integrated compliance with GDPR and the AI Act [1], [2].

The EU has placed several important digital rules in addition to the GDPR and AI Act. These rules create a larger legal framework for data governance. The EU Data Strategy, implemented in 2020, aims to create a unified European data market where data can move freely across sectors and countries. This would help new ideas and preserve people's rights. The EU Data Act clarifies who can get and use data from the EU, including non-personal and industrial data. The EU Data Governance Act also encourages safe and open data sharing through data spaces and markets. The Digital Services Act (DSA) makes online platforms more responsible and protects users better. At the same time, the Digital Markets Act (DMA) focuses on big digital platforms to ensure fair competition and that the market is not abused. These acts complement the GDPR and the AI Act to preserve fundamental rights in the digital economy, deal with data access, significant tech duties, and innovation [3].

Contact Tonći Kaleb, tonci.kaleb@isaca.hr, ISACA Chapter, Croatia.

This article discusses how the GDPR and the EU AI Act have regulated data and changed data governance together. It examines the legal, risk, and technical aspects of defined rules and the skills needed to deal with new challenges. The article is centered on two primary questions: what are the differences between the two regulations, and where do they overlap? Also, what skills do professionals need to keep up with and promote innovation in today's fast-changing digital world? A study of professionals in privacy, information security, and risk management was done to learn more about the fundamental duties, skills, and status of Data Protection Officers (DPOs) in enterprises. Most of the people who answered are members of the ISACA community in Croatia or professionals who work directly with DPOs. The survey aimed to learn more about DPOs' role and limitations, such as their level of authority in organizations, their professional background, how multidisciplinary their function/role is, and whether organizations support implementing personal data protection. The authors compare regulatory frameworks (GDPR and AI Act). The conclusions serve as the basis for suggesting a new way to govern (personal) data and AI together [4], [5], [6], [7].

2 Literature review

Recent research has shown how the GDPR and the AI Act work together and complement each other within the EU's system of rules. A study made by the European Parliament in 2020 explored how the GDPR contributes to AI systems' protection, primarily through data minimization. However, it also said that exercising some rights, e.g., transparency and explainability, can be challenging to achieve in complex AI systems [8].

Legal comparison shows that the GDPR and the AI Act regulate different aspects of data use. The GDPR covers the processing of personal data, while the AI Act covers how AI systems work with any form of data. However, both regulations have the same goals, such as reducing risk, ensuring clear accountability, and implementing technical and organizational measures (safeguards). This is especially clear when comparing Articles 25 and 32 of the GDPR to Articles 9 and 26 of the AI Act [5], [6].

Furthermore, the literature implies that the GDPR and AI Act cover some of the same topics, such as transparency, permissions, consent, documentation, and accountability. Professional evaluations, such as those from the IAPP, say that the AI Act mentions the GDPR more than thirty times, primarily when AI systems deal with personal data. However, their goals, scope, and enforcement mechanisms are very different. Because of this, many academics suggest that compliance should be practically achieved in an integrated way. This could include combined risk assessments (like DPIA and Fundamental Rights Impact Assessments), ongoing monitoring, and the creation of hybrid professional roles that combine legal, technical, and data governance knowledge. There is ongoing discussion about implementing the technical "right to explanation" from the AI Act, in addition to the rights already existing under the GDPR [5], [6].

3 Comparative Analysis: Legal, Risk, and Technological Perspectives

This section compares essential parts of the GDPR and the AI Act, concentrating on the legal obligations, risk management, and technological constraints that affect handling data and building AI systems. The General Data Protection Regulation (GDPR) is based on the principle that individuals, whether citizens or residents of the European Union, should be able to keep control of their data. This fundamental right applies to any processing [4], [9].

Key privacy concepts of the GDPR are a solid legal basis, transparency, purpose limitation, data minimization, accuracy, storage limitation, confidentiality, integrity, and accountability. To comply, businesses must have an apparent legal basis and a valid reason for processing personal data. They must respect the data subject's rights, which include the right to access, rectify, erase personal data, limit processing, object to processing, and be excluded from automated decision-making. Individuals also have the right to ask the national Data Protection Authorities (DPAs) for protection if their rights are being abused [10].

In a regular life, handling personal data comes with risks. For instance, if a company uses someone's data without a proper legal basis or does not keep it safe, that company could cause harm to the person and (consequently) face legal action. Organizations employ risk assessment techniques like Data Protection Impact Assessments (DPIAs), Legitimate Interest Assessments (LIAs), and Transfer Impact Assessments (TIAs) to find and deal with privacy-related risks. These assessments should lead to real steps to reduce risk. It is essential to distinguish these privacy risk evaluations from the overall audit of compliance with GDPR requirements [10].

Enforced since May 25, 2018, the GDPR has become the world's standard for privacy laws. Many laws outside the EU have been affected by its concepts, such as the Personal Data Protection Law (PDPL) in Saudi Arabia and the new Law on the Protection of Personal Data in Bosnia and Herzegovina. Because of this, the GDPR has become the gold standard for personal data protection worldwide. The European Data Protection Board (EDPB) is an independent EU agency that helps ensure that GDPR requirements are consistently understood. It provides guidelines about transferring personal data across borders, using pseudonymization, and applying GDPR to new technologies like blockchain and generative AI [10].

While GDPR is focused on individuals, their data, and rights, the EU Artificial Intelligence Act (AI Act) sets rules for how AI systems are made and used. The Act sends a strong message to businesses. It aims to ensure that AI technologies are safe, protect human rights (including privacy), and help the EU's responsible innovation. The Act establishes a risk-based approach that divides AI systems into three risk tiers: unacceptable, high-risk, and minimal-risk (*NOTE: some authors interpret that limited- and minimal-compliance levels are two risk tiers in the EU AI Act*) [5].

There are strict requirements for high-risk AI systems, such as those used in human resources management, law enforcement, healthcare, and critical infrastructure. The requirements include rules for managing risk, ensuring data accuracy, protecting against cyberattacks, being open and honest, keeping documentation and records of activities, having human oversight (HITL), and monitoring AI systems throughout the lifecycle [11].

3.1 Legal and Risk Management Aspects

Most EU member states have transposed the General Data Protection Regulation (GDPR) into their legal frameworks – e.g., Croatia does this through the Law on Implementing the GDPR. These national laws define specific details, e.g., empower national data protection authorities and define exceptions [12].

Data controllers and processors, mainly legal entities (businesses), are responsible for compliance with GDPR (more precisely, with requirements of national privacy laws). To handle these duties adequately, they need a privacy expert (*specialist, champion*). GDPR introduces the role of Data Protection Officer (DPO) [13].

Companies that do not follow GDPR rules could face several consequences, including fines. The fine amount depends on several factors, including the type of violation, its severity, whether it was intentional or repeated, the size of the business, and the organization's role. There are two levels of GDPR infractions. Fines for Tier 1 violations may reach up to €10 million or 2% of the company's global annual turnover, whichever is greater. Tier 2 violations are more severe and can result in penalties of up to €20 million or 4% of worldwide annual turnover [6].

The EU Artificial Intelligence Act covers all AI systems sold or used in the EU, no matter where they were made. This means that companies that sell AI systems to people in the EU must follow the Act's rules, even if they are based outside the EU. The Act emphasizes rules for high-risk AI systems. These include systems utilized in healthcare, education, law enforcement, employment, and managing essential infrastructure. Once used, high-risk systems must meet high standards for risk management, documentation, data quality and security, human oversight, and continuous monitoring [5], [6].

Companies not complying with the AI Act may also be penalized. Financial fines depend on the kind of infraction and its severity. The worst violations, such as applying prohibited AI systems, can result in penalties of up to 35 million euros or 7% of global annual sales. Fines of up to 15 million euros or 3 percent of revenue may be given for other infractions, like those involving high-risk AI systems or general-purpose AI models. Giving regulators false or misleading information can lead to fines of up to 7.5 million euros or 1% of global turnover. An overview of noncompliance scenarios and associated fines under the AI Act is presented in Table 1 [4].

Table 1 Overview of AI Act noncompliance cases and corresponding financial penalties

Noncompliance case	**Proposed fine**
Breach of AI Act prohibitions	Fines up to €35 million or 7% of total worldwide annual turnover (revenue), whichever is higher
Noncompliance with the obligations set out for providers of high-risk AI systems or GPAI models, authorized representatives, importers, distributors, users, or notified bodies	Fines up to €15 million or 3% of total worldwide annual turnover (revenue), whichever is higher
Supply of incorrect or misleading information to the notified bodies or national competent authorities in reply to a request	Fines up to €7.5 million or 1.5% of total worldwide annual turnover (revenue), whichever is higher

The AI Act lays out rules for people who build AI and people who use or run AI systems. It provides special regulations for general-purpose AI (GPAI) models, which are becoming more common in many applications. The law went into effect on August 1, 2024, and its rules will be implemented over the next 36 months, depending on the system's kind and level of risk [5].

The GDPR is focused on risks to individuals. Mechanisms include Data Protection Impact Assessments (DPIAs) for processing that may impact the rights and freedoms of individuals, security standards under Article 32, and privacy principles that are built in and set by default. GDPR requires special attention (*risk assessments*) when sensitive data is involved or when processing (*data actions*) is considered high risk [6].

The AI Act focuses more on risks to enterprises, with rules depending on how the AI system could impact people and communities. High-risk AI systems must adhere to a defined, strict risk management procedure, undergo constant monitoring, and be subject to robust human control. This approach ensures that AI technologies are safe, reliable, and in line with fundamental rights. Table 2 provides a structured overview of how AI systems are classified under the EU AI Act based on risk level, along with their respective compliance obligations and typical use case examples [4], [6].

When AI systems handle personal data, companies must implement risk management protocols that deal with privacy issues and AI-specific risks like bias, hallucinations, and the lack of explainability. Regarding AI, privacy-related issues comprise much of the entire risk landscape, especially when personal data is involved. Companies that use these systems must follow the GDPR and the AI Act, ensuring they meet their requirements under both regulations (transposed to national laws) [6].

There is an increasing use of Privacy-Enhancing Technologies (PETs), which allow safe AI/ML and personal data processing without compromising privacy. Examples of PETs are federated learning, homomorphic encryption, and the use of synthetic data. PETs help to comply with GDPR's privacy and the AI Act's risk-managing requirements. [14], [15].

The AI Act also has rules about building AI systems, especially high-risk ones. These systems require technical features that ensure they are open, allow users to explain their outputs, and maintain oversight of users by the AI system. Companies are using automation in compliance processes. AI fact sheets, traceability frameworks, and real-time dashboards aid with continual monitoring and organized documentation. They enable enterprises to align their privacy and AI governance processes better. However, it is crucial to avoid the checkbox-compliance approach and make adequate assessments followed by competent decisions [4].

Table 2 Classification of AI systems by risk level and corresponding compliance requirements under the EU AI Act

Classification (Risk-based tier)	**Description**	**Compliance level**	**Use case examples**
Prohibited AI systems	Prohibited: Because they pose an unacceptable risk to people's safety, security, and fundamental rights.	Prohibited	This includes using AI for social scoring, which could lead to detrimental treatment, emotional recognition systems in the workplace, biometric categorization to infer sensitive data, and predictive policing of individuals, among other uses. Some exemptions will apply.
High-risk AI systems	Permitted: Subject to compliance with the requirements of the AI Act (including conformity assessments before being placed on the market).	Significant	Includes use of AI in: • Recruitment • Biometric identification and surveillance systems • Safety components of systems covered by harmonized legislation (e.g., medical devices, automotive) • Access to essential private and public services (e.g., creditworthiness, benefits, health and life insurance) • Safety of critical infrastructure (e.g., energy, transport)
Minimal risk AI systems	Permitted: Subject to specific transparency and disclosure obligations where uses pose a limited risk.	Limited	Specific AI systems that interact directly with people (e.g., chatbots), and visual or audio "deepfake" content that an AI system has created for manipulation.
	Permitted: With no additional AI Act requirements where uses pose minimal risk.	Minimal	By default, all other AI systems that do not fall into the above categories (e.g., photo-editing software, product-recommender systems, spam filtering software, scheduling software)

4 Professional Competencies for Data and AI Governance

Aspiring experts require diverse skills and knowledge to effectively address privacy and AI issues. Understanding the laws' requirements coming from other parts of the world became paramount. Significant aspects of privacy and AI management include risk assessment, data governance, the use of advanced technologies, decision transparency, prioritization, effective communication, project management, and resource allocation. Is it realistic to expect that a single individual can excel across all these disciplines? Where might one find an individual possessing such a diverse skillset? The role of Data Protection Officer is a good example to evaluate these needs and possible consequences of (*non*-)finding an adequate solution (*skilled person*) [4].

4.1 Data Protection Officer Role

A Data Protection Officer (DPO) should understand the GDPR, the ePrivacy Directive, and other relevant data protection regulations at the national and EU levels. However, just knowing the law is not enough. The skillset needed to be a DPO, as shown in Figure 1. demands knowledge of risk management, technology, and computer systems, and the ability to communicate with different stakeholders. The DPO role is in the second line of defense and gives advice based on facts and legal interpretation. Independence (*lack of conflict of interest*) is necessary in both day-to-day operations and in organizational structure and reporting [4], [6].

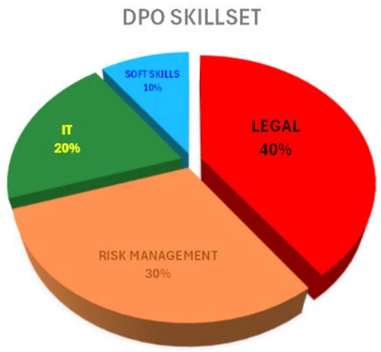


Figure 1 Data Protection Officer's (DPO) skillset

The work also entails knowing the rules for diverse fields, such as healthcare, finance, or education, understanding legal duties, and writing compliance documentation. It also involves learning about regulations outside of a country, since many data privacy legislations, such as the GDPR, govern data transfers between people from the EU and non-EU countries [4].

Privacy risk management differs from the usual approach. Privacy risk comes not just from external threats, but also from how data controllers and processors operate, which can violate people's rights and freedoms. Common harms include loss of dignity, discrimination, financial loss, or rights. To manage these kinds of risks, it is necessary to do assessments like Data Protection Impact Assessment (DPIA), Legitimate Interest Assessment (LIA), and Transfer Impact Assessment (TIA). Privacy risks require continuous monitoring, reviewing, and reassessment following changes in business, technology, or legal framework[4].

A good understanding of technology is fundamental. To meet many GDPR criteria, like data minimization, access control, encryption, and de-identification, adequate technological and organizational measures must be in place. Differential privacy, homomorphic encryption, and federated learning are all privacy-enhancing technologies that add extra layers of protection to help with secure and compliant data processing. It is essential to work with cybersecurity experts, especially while responding to an incident when personal data may be involved (data privacy breach), and there may be legal ramifications [4].

Strong soft skills are just as critical. Privacy programs usually involve multiple projects and must be coordinated among legal, technical, and risk teams. Communication, problem-solving, and time management are essential. Privacy training begins with onboarding, followed by annual refreshers and updates in response to primary processes or technological changes. This helps raise awareness and develop the organization's compliance culture [6].

4.2 AI Officer Role (or equivalent AI role)

Compared to privacy, artificial intelligence presents a broader and more complex challenge. This complexity is not only technological but also legal and risk-related. Professionals responsible for AI governance must go beyond understanding personal data protection and develop expertise in multiple domains that intersect with AI. The skillset needed for the AI Officer Role is estimated in Figure 2 [5].

AI officers should know the legal aspects of the EU AI Act and how these rules are transposed into national law. This includes understanding, using, and monitoring compliance in various industries, especially healthcare and finance. Knowing international AI regulations is also mandatory. [5].

AI governance goes beyond privacy, addressing bias, ethical concerns, and trust in automated decisions. Tools like impact and conformity assessments help manage risks, while technical challenges such as cyber threats and data quality remain. Ensuring ethical AI requires responsible development and human involvement through approaches like Human in the Loop (HITL) [5].

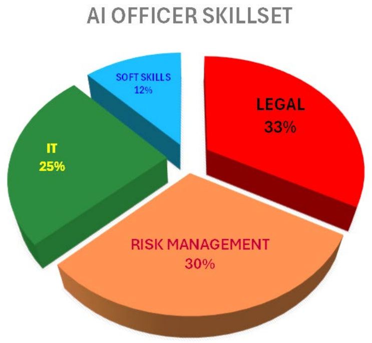


Figure 2 Artificial Intelligence Officer's (AIO) skillset

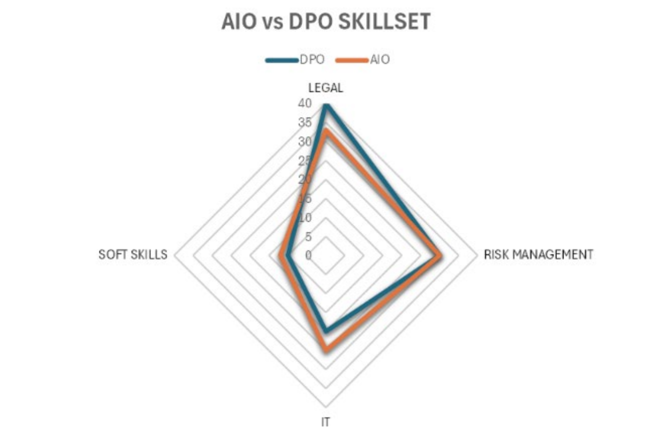


Figure 3 AIO vs DPO skillset

This role requires solid technical knowledge, as AI systems depend on quality data, computing power, and the ability to manage bias and explain outcomes. As these systems introduce new security risks, it's vital to ensure that data, models, and interfaces remain trustworthy. Managing AI projects also requires strong communication and coordination skills. With the growing use of large language models (LLMs), understanding how they work and how to write effective prompts is becoming increasingly important [5].

žWhen considering the skills required by data protection officers (DPOs) and new AI governance jobs, it becomes clear that the DPO role focuses on legal aspects. In contrast, the AI officer role demands a deeper understanding of technology. The difference (*skills drift*) between a DPO and an AI Officer is shown in Figure 3 [4], [6].

5 Personal Data and AI Governance

The GDPR and the EU AI Act call for a broad, interdisciplinary strategy that includes legal, risk, and technical perspectives. Good governance frameworks must allow for collaboration across various areas, which is made possible by excellent communication skills and continual professional growth. However, several problems make this process more difficult, such as complicated regulations, operational needs, and the fast rate of AI technology development. These need adaptable plans and constant communication with regulators and other interested parties [5].

In this situation, there is an approach to combine the jobs of Data Protection Officer and AI Officer. Even if this merger has some benefits, it raises many red flags. In EU companies, the DPO position is typically set at lower levels of the corporate hierarchy (such as B-3 or B-4), which means they do not have much power or visibility to the Board. Because of this, privacy is still a secondary issue unless something like an external audit, a legal or regulatory inquiry, or a personal data breach brings it up [4].

The DPO's main job is dealing with legal and privacy problems, while AI governance also involves covering ethical, operational, and business-related issues. AI is not only bringing regulatory matters, but also a chance to boost innovation, efficiency, and competitiveness. This is why organizations need to make the AI Officer's role of overseeing AI compliance more visible, with a more substantial impact on decision-making [5].

Authors support the separation of the two jobs/roles. By creating a dedicated position for AI governance, companies can better deal with AI's problems and opportunities. This approach avoids the structural issues associated with being a DPO and keeping both roles focused on meeting (personal) data protection requirements.

6 Methodology

The study combines empirical data with legal and regulatory analysis, focusing on the DPO role, position, and skills, as well as organizational readiness for the EU Artificial Intelligence Act (AI Act). The working hypothesis is that the DPO has a multidisciplinary role, including legal, risk, technical, and advisory functions, so there is a need for interdisciplinary competencies (Figure 1). A secondary hypothesis suggests that DPOs and emerging roles like AI Officers (Figure 2) should be positioned higher in the organization's hierarchy to ensure greater impact on decision-making. Figure 3 compares the key competencies of both roles. These hypotheses are examined within the specific context of Croatian organizations, potentially informing broader comparative studies across the EU [7].

An online survey was conducted among privacy, information security, and risk management professionals, primarily ISACA Croatia Chapter members. Most respondents were DPOs or worked closely with them. The questionnaire included 13 structured and one open-ended question, addressing DPO responsibilities, organizational hierarchy, involvement in decision-making, and the multidisciplinary scope of their roles. It also explored institutional support for data protection and readiness for AI-related regulatory obligations.

The article compares the GDPR and the AI Act, focusing on legal obligations, risk management, technical requirements, and operational practices. While the regulations share common goals, they differ in key areas such as documentation, accountability, transparency, and risk assessment. The article highlights challenges like the need for multidisciplinary skills and new roles, and proposes integrating compliance efforts across both frameworks. It links the survey's empirical findings with regulatory requirements and explores the competencies organizations need for effective and compliant implementation.

7 Survey Results and Analysis

A survey was conducted to examine the skills and organizational role of Data Protection Officers (DPOs). The questionnaire included 13 questions and an optional comment section. It focused on typical DPOs' background (whether legal, risk, or IT), required competencies, influence on decision-making, and the implementation of privacy practices. Respondents were primarily professionals in data protection, cybersecurity, and IT audit, mostly members of the ISACA Croatia Chapter, also including active DPOs working in Croatian companies.

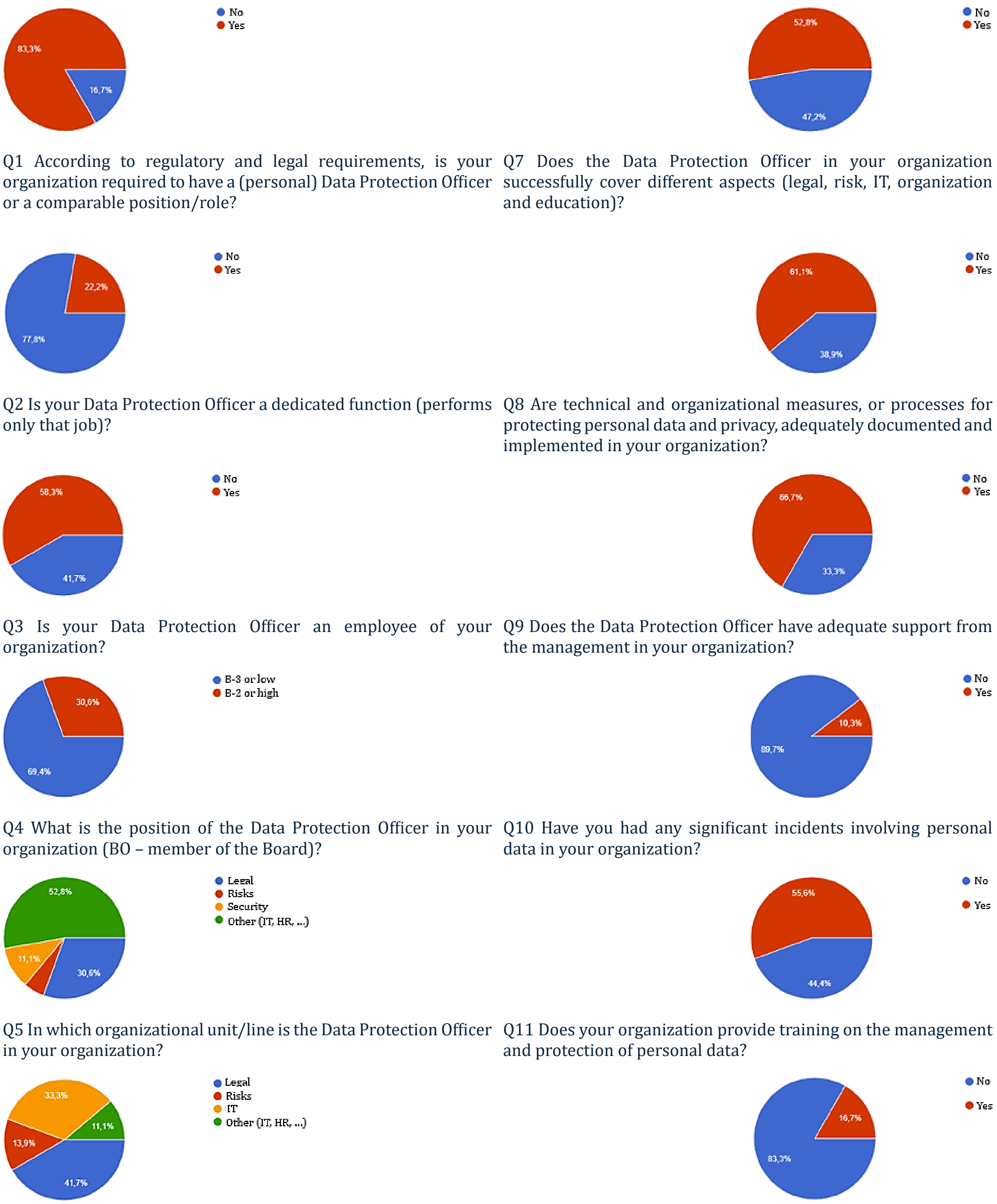
An online questionnaire was conducted among 36 Croatian professionals working in privacy, data protection, information security, and IT risk, to assess the role and position of Data Protection Officers (DPOs) in organizations. Given the limited sample size and national focus, the survey should be viewed as an exploratory case study. While the findings offer valuable insights into local practices, they are not statistically generalizable to the broader EU context but may serve as a foundation for further comparative research. The structure and results of the questionnaire are available in Figure 4.

Most respondents (83.3%) know that appointing a DPO is a regulatory obligation under certain conditions (Figure 4 Q1). In most cases, the role is not a dedicated function; 77.8% of DPOs also perform other duties (Figure 4 Q2). 58.3% of DPOs are internal employees of the organization (Figure 4 Q3).

When looking at the organizational level, most DPOs don't have a management position in the hierarchy (69.4% are at B-3 or below), which may reduce their visibility and influence on decision-making processes (Figure 4 Q4). The DPO function is typically placed within the legal department (30.6%) or security management (11.1%, Figure 4 Q5). As expected, the professional background of DPOs is highly diverse, with a dominant legal background of 41.7% and some risk of 13.9%. Surprisingly, other professions such as IT, HR, finance, and business cover 44.4% (Figure 4 Q6).

According to Figure 4 Q7, just about half of the respondents (52.8%) think that DPO successfully covers all necessary topics, including technical, legal, and risk management elements. However, 61.1% of respondents believe that privacy protection documents and processes are adequate (Figure 4 Q8). Also, two-thirds (66.7%) of respondents think that DPO has adequate executives' support (Figure 4 Q9), which may indicate the maturity of the privacy process or a false sense of accomplishment.

Regarding incident experience, most respondents (89.7%) reported that their organizations did not suffer serious privacy-related breaches (Figure 4 Q10). However, awareness and training appear limited, as only 55.6% of participants confirm that privacy training is conducted systematically (Figure 4 Q11). Finally, most participants (83.3%) think that the DPO will not participate in AI-related matters (Figure 4 Q12), indicating expectations that the new AI GRC role will go beyond the DPO's scope (privacy)



Q1 According to regulatory and legal requirements, is your organization required to have a (personal) Data Protection Officer or a comparable position/role?

Q2 Is your Data Protection Officer a dedicated function (performs only that job)?

Q3 Is your Data Protection Officer an employee of your organization?

Q4 What is the position of the Data Protection Officer in your organization (BO – member of the Board)?

Q5 In which organizational unit/line is the Data Protection Officer in your organization?

Q6 What is the professional profile (background) of your organization's Data Protection Officer?

Q7 Does the Data Protection Officer in your organization successfully cover different aspects (legal, risk, IT, organization and education)?

Q8 Are technical and organizational measures, or processes for protecting personal data and privacy, adequately documented and implemented in your organization?

Q9 Does the Data Protection Officer have adequate support from the management in your organization?

Q10 Have you had any significant incidents involving personal data in your organization?

Q11 Does your organization provide training on the management and protection of personal data?

Q12 Will the Data Protection Officer also be responsible for non-technical aspects of AI in the organization?

Figure 4 Questionnaire on the position and role of the DPO

8 Regulatory Trends and Future Challenges

Recently, the European Union has made efforts to make its necessary digital data regulations, including GDPR, Data Act, and AI Act, easier to understand and implement. An example of measures is the European Commission's proposal to simplify record-keeping obligations for small and medium-sized businesses. Still, it raises serious questions about whether these changes could weaken data protection and raise new privacy concerns for the EU's economic ecosystem [16].

On the other hand, enforcing the AI Act seems to be taking longer than expected. The European Commission was considering putting some parts of the Act on hold until technological standards were entirely created. "Big Tech" AI companies advocated and urged the Commission to delay the AI Act rollout. Several member states also want small enterprises to have more exemptions, and less complicated AI systems to have fewer duties. These unclear rules and the lack of unified standards make it harder to understand the regulation, transpose it to the national law(s), and implement it in practice. However, the Commission decided on July 4, 2025, to end the speculation regarding a potential delay on AI rules and holds firm on the AI Act implementation timeline (*"there is no stop the clock, there is no grace period, there is no pause"*).

Moreover, the EU has officially abandoned the long-stalled ePrivacy Regulation, likely due to the influence/pressure of powerful lobbying from "Big Tech" companies. This withdrawal underscores the impact of industry pressure and shifting legislative priorities toward competitiveness and data access for AI, rather than the protection of privacy. Similarly, the AI Liability Directive (AILD), which aimed to harmonize rules for civil liability related to AI-caused harm across the EU, has been officially withdrawn by the European Commission as of February 2025. The primary reasons for this withdrawal were a lack of agreement among EU Member States, calls for regulatory simplification, and concerns about overlapping with other EU directives [17].

Weakening or delaying fundamental rights' protections, whether through exemptions, delays in the process, or giving up on reforms, could have a negative impact on public trust, put EU citizens at greater risk, and eventually harm the EU's goal of a safe, innovative digital future that respects fundamental rights. European Union is committed to responsible innovation – enhancing efficiency and competitiveness without compromising fundamental rights, trust, or ethical principles [18].

9 Conclusion

The evolution of EU data governance and regulations, particularly through the GDPR and AI Act, demonstrates a shift toward risk-based, accountable, and transparent use of data and technologies. Research findings support the initial hypothesis within the specific context of the Croatian professional landscape and privacy practices, particularly among the ISACA Croatia Chapter community. These findings should be considered indicative, not conclusive, and should call for further validation across the EU. Effective compliance with GDPR and AI Act requires not just legal, but also strong risk management, plus technical expertise and soft skills. Also, the need for new AI skills, roles, and timely preparations for AI regulations' requirements is paramount. Future research should examine case studies for specific sectors, the impact of emerging technologies (e.g., quantum computing, agentic AI), and steps toward creating an integrated compliance framework.

Conflicts of Interest: The author(s) report no competing interests to declare.

References

[1] M. Veale and F. Z. Borgesius, "Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach," *Computer Law Review International*, vol. 22, no. 4, pp. 97–112, Aug. 2021, doi: 10.9785/CRI-2021-220402.

[2] S. Wachter, B. Mittelstadt, and L. Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation," *International Data Privacy Law*, vol. 7, no. 2, pp. 76–99, May 2017, doi: 10.1093/IDPL/IPX005.

[3] D. Clifford, M. Richardson, and N. Witzleb, "Artificial intelligence and sensitive inferences: new challenges for data protection laws in: Regulatory Insights on Artificial Intelligence," 2022. doi: https://doi.org/10.4337/9781800880788.00008.

[4] "Guidelines European Data Protection Board." Accessed: Mar. 23, 2025. [Online]. Available: https://www.edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_en

[5] "Regulation - EU - 2024/1689 - EN - EUR-Lex." Accessed: Mar. 23, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

[6] "Regulation - 2016/679 - EN - gdpr - EUR-Lex." Accessed: Mar. 23, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[7] "State of Privacy 2025 Report ISACA." Accessed: Jun. 23, 2025. [Online]. Available: https://www.isaca.org/resources/reports/state-of-privacy-2025

[8] A. D. Selbst and S. Barocas, "The Intuitive Appeal of Explainable Machines," *Fordham Law Rev*, vol. 87, no. 3, pp. 1085–1139, 2018, doi: 10.2139/SSRN.3126971.

[9] M. E. Kaminski, "Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability," *South Calif Law Rev*, Jan. 2019, [Online]. Available: https://scholar.law.colorado.edu/faculty-articles/1265

[10] R. Knyrim, "Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers," *International Data Privacy Law*, vol. 5, no. 2, pp. 156–157, May 2015, doi: 10.1093/IDPL/IPV002.

[11] A. Mantelero and M. S. Esposito, "An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems," *Computer Law & Security Review*, vol. 41, p. 105561, Jul. 2021, doi: 10.1016/J.CLSR.2021.105561.

[12] H. Hijmans, "The European Union as Guardian of Internet Privacy," vol. 31, 2016, doi: 10.1007/978-3-319-34090-6.

[13] G. González Fuster, "The Emergence of Personal Data Protection as a Fundamental Right of the EU," vol. 16, 2014, doi: 10.1007/978-3-319-05023-2.

[14] N. Rieke *et al.*, "The future of digital health with federated learning," *NPJ Digit Med*, vol. 3, no. 1, pp. 1–7, Dec. 2020, doi: 10.1038/S41746-020-00323-1.

[15] C. Troncoso, M. Isaakidis, G. Danezis, and H. Halpin, "Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments," *Proceedings on Privacy Enhancing Technologies*, vol. 2017, no. 4, pp. 404–426, Jun. 2017, doi: 10.1515/popets-2017-0056.

[16] D. Hartmann, J. R. L. de Pereira, C. Streitbörger, and B. Berendt, "Addressing the regulatory gap: moving towards an EU AI audit ecosystem beyond the AI Act by including civil society," *AI and Ethics*, Aug. 2024, doi: 10.1007/S43681-024-00595-3.

[17] R. N. Nwabueze and M. White, "Privacy law and the dead – a reappraisal," *Journal of Media Law*, vol. 16, no. 2, pp. 468–502, Jul. 2024, doi: 10.1080/17577632.2024.2438395.

[18] M. M. Maas, "AI, Governance Displacement, and the (De)Fragmentation of International Law," in *ISA Annual Convention*, Mar. 2021. [Online]. Available: https://papers.ssrn.com/abstract=3806624