# Towards a European Data and AI Ecosystem: Convergences between the DGA, DA, AIA, and GDPR

Ignacio Miguel Rodríguez*, Jordi Castellà Roca*, Alexandre Viejo* M. Magdalena Payeras Capellà†
*Universitat Rovira i Virgili, Departament d'Enginyeria Informàtica i Matemàtiques, Tarragona, Spain
{ignacio.miguel, jordi.castella, alexandre.viejo}@urv.cat
†Universitat de les Illes Balears, Departament de Ciències Matemàtiques i Informàtica, Palma, Spain
mpayeras@uib.es

***Abstract*—The European Union has established a comprehensive and pioneering regulatory landscape to govern data protection, data sharing, and the deployment of artificial intelligence. Regulations such as the GDPR, DA, DGA, and AIA provide frameworks to safeguard individual rights, ensure data security and integrity, and promote trustworthy innovation. This paper presents a comparative overview of these regulatory instruments, highlighting their main objectives, actors, and responsibilities. Additionally, we analyze the opportunities they create for data-driven innovation and AI deployment, as well as the challenges associated with compliance, interoperability, transparency, and human oversight. The discussion emphasizes the EU's leading role in shaping global standards for ethical and responsible data and AI.**

***Index Terms*—GDPR, DGA, DA, AIA, Europe, Data, AI**

## I. Introduction

In today's digital era, data has become the driving force behind most services and innovations. To ensure the security and privacy of individuals whose data is being collected and processed, it is crucial to establish clear rules and regulatory frameworks. In this regard, the European Union (EU) has taken a leading role in shaping global standards for data governance—starting with the General Data Protection Regulation (GDPR) in 2018 and continuing with more recent initiatives such as the Data Governance Act (DGA), the Data Act (DA), and most notably, the Artificial Intelligence Act (AIA), reflecting the rapid progress of AI technologies in recent years.

Together, these regulations seek to prevent misuse of data, mitigate biases and unethical practices in AI systems, and safeguard individual rights by ensuring transparency, fairness, and user control. In particular, where processing is based on consent, the GDPR guarantees that individuals may freely give or withdraw it at any time, and the other instruments must be applied without prejudice to this right.

In this regulatory context, it is precise to define what is considered as personal and non-personal data, as they are treated differently. According to [1], *personal data* refers to any information relating to an identified or identifiable natural person, meaning one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, or an online identifier. Conversely, *non-personal data* refers to any information that does not relate to an identified or identifiable person, or that has been anonymized in such a way that individuals are no longer identifiable. The distinction is fundamental, as the GDPR applies specifically to personal data, whereas non-personal data are primarily governed by other regulatory instruments such as the DGA and the DA, which establish frameworks for data sharing and reuse across sectors within the EU. However, both the DGA and the DA may also encompass personal data under certain conditions, insofar as their provisions are fully consistent with the GDPR. In practice, this means that the GDPR remains the primary and prevailing legal basis for the protection and lawful processing of personal data. The DGA, the DA and the AI Act complement it by defining mechanisms for secure access, sharing, and reuse of data, but must be applied without prejudice to the GDPR. Consequently, data-subject rights, such as the right to withdraw consent at any time (Art. 7(3)), cannot be restricted by these instruments.

This paper provides an overview of the EU's current data-related regulatory landscape, identifying its main actors, their duties, and responsibilities. Furthermore, it explores the interconnections among these frameworks and offers a comparative analysis of their objectives, scope, and implications.

## II. Common actors

This section summarizes the common actors across all regulations, specifying their main obligations and responsibilities.

1) **Data Subjects**: Individuals whose personal data is processed and can be identified by any identifier directly or indirectly. This is a central concept in GDPR and relevant in other acts where personal data is involved.
2) **Data Holder**: An individual or entity that, while not being the data subject, possesses the authority to grant access to or share certain personal or non-personal data.
3) **Data Controllers**: Entities that determine the purposes and means of processing personal data. It is crucial under GDPR and may be relevant in other acts when data handling is involved.
4) **Data Processors**: Entities that process data on behalf of the data controller. Again, defined in GDPR but also relevant in the context of data processing in other acts.
5) **Users**: Individuals or entities that use digital services or products. This actor is relevant across all the mentioned legislations.
6) **Developers and Manufacturers (Providers)**: Companies involved in creating AI systems or digital products,

particularly relevant in the AIA and DA.

7) **Regulatory / Supervisory Authorities**: Bodies responsible for overseeing compliance with the legislation.

After conducting a comparative analysis of the four main European regulations (GDPR, AIA, DGA, and DA), we identified the key actors that appear consistently across these frameworks. Table I consolidates these common actors and summarizes their primary responsibilities and rights as defined by the respective regulations. The process involved mapping the provisions of each regulation to identify overlapping roles and extracting the most relevant obligations and entitlements for each actor. While this synthesis provides a unified perspective, it does not include some regulation-specific nuances or additional actors unique to individual frameworks. Note that throughout this document, references to Articles and Chapters are made directly, without explicitly restating the corresponding regulatory instrument.

## III. Regulations

Depending on the specific use case of an application, one or more regulations may apply. Figure 1 illustrates a decision workflow to determine the applicability of key European regulatory frameworks through a series of guiding questions. These regulations are cumulative, meaning that multiple frameworks can apply simultaneously. For instance, AI-driven apps that analyze biometric data from wearables to provide personalized health recommendations must comply with GDPR for sensitive data, AIA, as it is classified as high-risk, and DA, as it is a connected product that generates data. To verify whether an AI system qualifies as low-risk under the EU AI Act, organizations can consult the official questionnaire[1] provided by the European Union. Next, we provide a summary of the key aspects of each regulation.

### A. General Data Protection Regulation (GDPR)

The GDPR establishes a comprehensive regulatory framework, showcasing the European Union's pioneering role in setting global standards for personal data protection. According to [1], personal data refers to any information relating to an identifiable individual (data subject), including identification numbers, location data, genetic information, and similar attributes. The regulation empowers data subjects with control over how their data are collected, processed, and managed by service providers. Its main pillars include:

- **Right to access, rectification, and erasure (Right to be forgotten)** — Articles 15, 16, and 17.
- **Right to restriction of processing** — Article 18.
- **Right to data portability** — Article 20.
- **Right to object to processing** — Article 21.

These rights ensure that individuals maintain significant authority over their personal information, reinforcing transparency, accountability, and fairness in data processing activities.

[1]EU AI Risk Classifier and Compliance Checker: https://www.trail-ml.com/eu-ai-act-compliance-checker

### B. Data Act (DA)

The DA establishes a harmonized framework to ensure fair access to and use of data across the European Union, fostering a competitive and innovative data economy. It complements the Data Governance Act by focusing on the practical mechanisms of data access and sharing across sectors. According to [2], the regulation seeks to ensure that users, businesses, and public sector bodies can access and utilize data generated by connected devices (IoT) and related services under fair, reasonable, and non-discriminatory conditions.

Its main pillars include:

- **Right of access to data generated by IoT devices** (Chapter II).
- **Fairness in business-to-business (B2B) data sharing**: It establishes obligations to prevent unfair contractual terms and promote equitable data access among enterprises (Chapter IV).
- **Obligation of business-to-government (B2G) data sharing for the public interest**: The regulation enables public sector bodies to request access to privately held data in cases of exceptional need, such as public emergencies (Chapter V).
- **Right of change between data processing services**: The DA promotes cloud switching and interoperability between data processing services, aiming to reduce vendor lock-in and foster competition (Chapter VI). This objective aligns with the GDPR's Article 20 on data portability.
- **International data transfers and safeguards**: It ensures that non-personal data leaving the EU remain protected under conditions equivalent to EU standards, thereby safeguarding data sovereignty (Chapter VII).
- **Data interoperability**: Establishes requirements for data interoperability, including technical standards and mechanisms for secure data sharing, as well as the use of smart contracts to facilitate automated and transparent exchanges (Chapter VIII).

These provisions aim to create a fair and trustworthy data economy in which users retain control over the data they generate, businesses can innovate responsibly, and public authorities can leverage data for societal benefit.

### C. Data Governance Act (DGA)

The DGA focuses on promoting the reuse of data to enable data-driven solutions for both public and private entities. It also establishes the rules for data sharing and data altruism, introducing new certification schemes for enterprises that offer data intermediation services or engage in data altruism.

**Data intermediation services** (Chapter III) facilitate data sharing between multiple data subjects and data holders on one side and data users on the other side. These services build commercial relationships to share personal or non-personal data, while ensuring that data subjects can exercise their rights with respect to their personal data. These neutral figures are intended to foster trust in data sharing between individuals and enterprises. Currently, only a few companies are registered in the EU register of data intermediation services[2], with

[2]https://digital-strategy.ec.europa.eu/en/policies/data-intermediary-services Accessed in 2026

Table I
COMMON ACTORS ACROSS THE GDPR, AIA, DGA, AND DA: MAIN RESPONSIBILITIES AND RIGHTS

| Actor | Responsibilities / Obligations | Rights |
|---|---|---|
| **Data Subjects** | Provide accurate personal data; exercise their data protection rights; understand how their data are processed and used; cooperate with data controllers when required. | Right of access, rectification, erasure (right to be forgotten), restriction of processing, portability, and objection; right to transparent and lawful processing of their data. |
| **Data Holders** | Maintain and manage data securely; ensure that sharing or granting access complies with applicable laws and agreements; preserve data quality, confidentiality, and integrity. | Authorize access to or sharing of personal and non-personal data under defined conditions; retain control over how data are reused or accessed by third parties. |
| **Data Controllers** | Determine purposes and means of data processing; ensure compliance with legal frameworks; implement data protection, accountability, and transparency mechanisms; maintain documentation and conduct risk assessments. | Process data under lawful bases (e.g., consent, contractual necessity, legitimate interest); delegate processing under contractual safeguards. |
| **Data Processors** | Process data only on behalf of and under the instructions of the data controller; ensure data security, confidentiality, and technical compliance; assist controllers in fulfilling data subject rights. | Operate under lawful contracts; process data within the limits of the controller's mandate. |
| **Users** | Use digital or AI-based systems responsibly and in accordance with terms of service and applicable regulations; report misuse or unlawful content where relevant. | Access secure, transparent, and reliable digital and AI services; ask for correction for unlawful or harmful practices. |
| **Developers and Manufacturers (Providers)** | Design and develop AI systems, digital platforms, or products in compliance with regulatory standards; ensure robustness, transparency, and risk management; provide technical documentation and conformity assessments. | Commercialize compliant AI or digital products and services within the EU market; benefit from legal certainty and harmonized conformity frameworks. |
| **Regulatory / Supervisory Authorities** | Oversee implementation and enforcement of relevant acts; conduct audits, risk evaluations, and conformity assessments; handle complaints and impose corrective measures or sanctions. | Issue guidance and authorizations; supervise notified bodies; enforce penalties and ensure harmonized application of EU data and AI laws. |

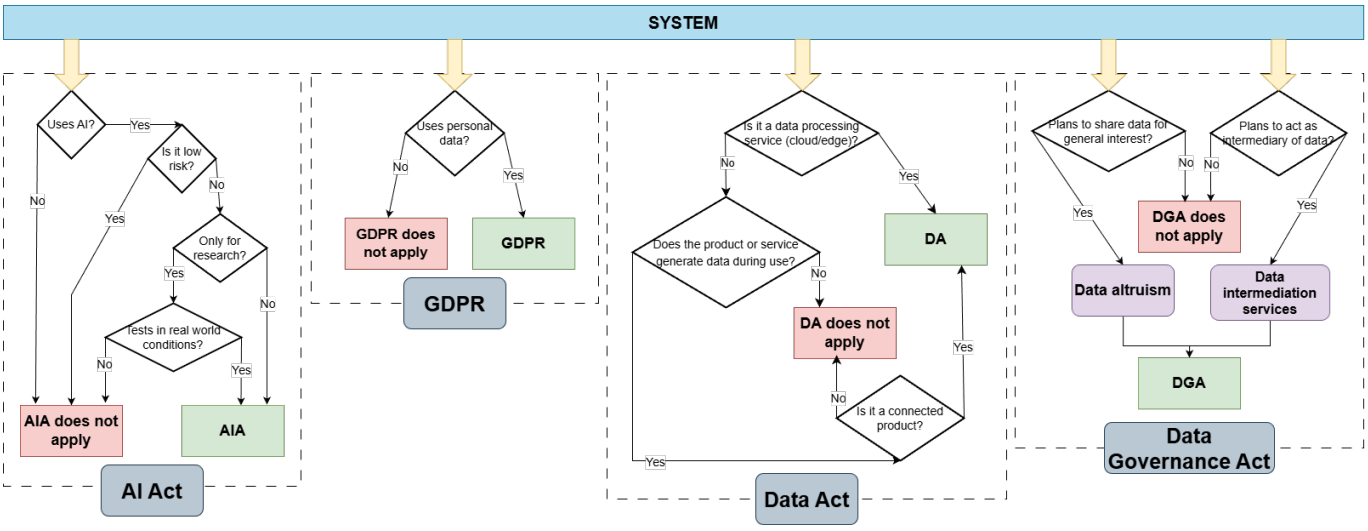



Figure 1. Workflow for assessing the applicability of European regulations.

registrations from countries including Austria, France and the Netherlands, among others. As of the beginning of 2026, 30 companies are listed, but this sector is expected to expand as more providers enter the market and as entities increasingly rely on the neutrality and practicality of these services.

The second main topic of DGA is **data altruism** (Chapter IV). Data altruism is understood as "*the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them [...] or non-personal data without seeking or receiving a reward [...] for objectives of general interest [...] such as healthcare, combating climate change, improving mobility [...]*" [3]. This concept is central to advancing scientific research and innovation within the EU, as free access to high-quality and diverse data is crucial for generating reliable and impactful results.

### *D. Artificial Intelligence Act (AIA)*

The European Union has taken significant steps in regulating the rapidly-growing field of artificial intelligence. This legislation aims to categorize AI systems based on the levels of risk they pose, ensuring safety and protecting human rights. It also establishes the regulations on general purpose AI systems such as ChatGPT [3].

This act establishes the pillars of AI systems' classification in several categories according to their risk (see Figure 2):

- **Unacceptable risk**: Systems that threaten safety, human lives, or human rights fall into this category and

[3]ChatGPT: https://chatgpt.com/

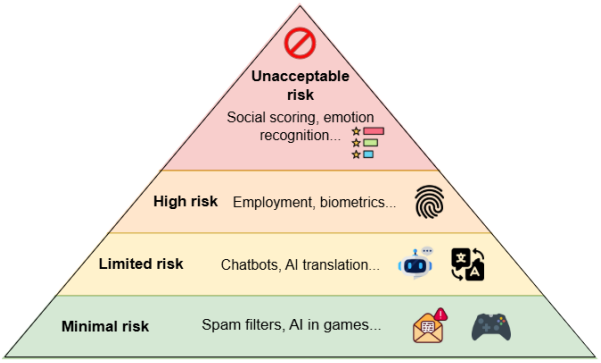



Figure 2. Categorization of AI systems according to their risk.

are strictly prohibited. Examples include social scoring, manipulation of individuals, and emotion recognition in sensitive environments like workplaces or schools.

- **High risk**: These systems are outlined in Annex III of the AIA [4] and are subject to ongoing evaluation. They require stringent oversight due to their potential impact on safety and fundamental rights. Examples include AI systems used in employment, education, access to essential services, and biometric identification.
- **Limited risk**: These applications require transparency to preserve trust (e.g., inform users that they are interacting with an AI system or tool) but do not pose any risk to the security or human rights. Examples include chatbots or translators.
- **Minimal risk**: Solutions that are not subject to any specific rules and cover most of the systems used in the EU, for instance spam filters or AI in video games.

In addition to system-level classification, the AIA regulates **general-purpose AI models (GPAI)**, including so-called *foundation models*, which can be adapted for a wide range of uses. Models that meet specific thresholds of computational power[4] or demonstrate capabilities with systemic impact are designated as **general-purpose AI models with systemic risk** (Article 51). These models are subject to enhanced obligations, including comprehensive risk assessments, evaluation of systemic impacts, documentation, and cybersecurity measures, as defined in Articles 53 and 55.

To encourage innovation, the AIA provides for the creation of **AI regulatory sandboxes** (Article 56). These controlled environments, supervised by national authorities, allow testing and validation of AI systems before market deployment. Additionally, the European Commission and the AI Office will promote the development of **codes of good practice** (Article 7), encouraging voluntary alignment with trustworthy and ethical AI principles beyond mere legal compliance.

The two principles of the AIA are:

- **Obligation and right of transparency**: The AIA explicitly regulates transparency obligations for both providers and users of AI systems, especially those considered high-risk or limited-risk. Article 13 establish that AI systems must be designed and developed to ensure that their operation is sufficiently transparent so that users can interpret and use them appropriately. Providers of high-risk AI systems must include clear instructions for use, describing the system's capabilities, limitations, performance metrics, and potential risks. In addition, limited-risk systems must inform users that they are interacting with an AI system and, when applicable, that content has been artificially generated or manipulated.
- **Obligation and right of reliability**: Although this term is not explicitly defined, the AIA addresses it through requirements for **robustness**, **accuracy**, **data quality**, and **cybersecurity**. Article 15 stipulates that high-risk AI systems must be technically robust, resilient to errors, and secure against manipulation or misuse. They must demonstrate consistent performance across their intended purposes and operate reliably under both expected and reasonably foreseeable conditions. Providers are further required to implement **risk management** (Article 9), **quality management** (Article 17), and **post-market monitoring** (Article 72) mechanisms to preserve reliability throughout the system's lifecycle.

[4]Floating-point operations greater than $10^{25}$

## IV. Discussion

The GDPR laid the groundwork for personal data processing within the European Union. However, the rapid evolution of AI technologies and the need to promote responsible data use and innovation made additional regulatory measures essential. New instruments such as the DGA, DA, and AIA build on the GDPR's principles. Although these frameworks share conceptual alignment, notable practical tensions emerge, as discussed below.

### A. GDPR vs. Data-Centric Frameworks: Points of Divergence

While the GDPR provides a robust framework for personal data protection, the introduction of DA and DGA incorporates new principles aimed at enhancing data sharing and reusability. These objectives, though complementary in theory, often create friction with GDPR's strict consent and purpose limitation requirements. This section examines the key areas where these regulations diverge and the implications for compliance and interoperability.

*1) **GDPR - DA**:* The DA imposes obligations on Data Holders to share or make data available, whereas the GDPR embraces the principle of data minimization (Art 5(1)(c)). The incentive to provide complete and diverse datasets clashes with GDPR's "privacy by design" principle, creating tension between data sharing and minimization.

*2) **GDPR - DGA**:* The DGA promotes altruistic data sharing, intended to support research and other public-interest purposes. However, GDPR provisions, such as the right to withdraw consent (Art. 7(3)) and, where applicable, the right to erasure (Art. 17), limit unrestricted data reuse. While the GDPR prevails and these rights remain fully enforceable whenever personal data are involved, this creates a significant operational challenge for data-altruism ecosystems, particularly regarding effective consent withdrawal and downstream data deletion in multi-actor settings.

Moreover, the GDPR mandates that Data Subjects receive clear and sufficient information about processing activities. In contrast, the DGA ecosystem involves multiple actors and potential future uses of data that are not yet defined,

complicating transparency obligations. This creates a tension between individual transparency and complex, evolving ecosystems.

### *B. From Data to AI: Interactions and Complementarity Between GDPR and AIA*

Next, we discuss how the GDPR and the AIA interact in practice and how their obligations largely converge when AI systems process personal data. Articles 13(2)(f), 14(2)(g), and 15(1)(h) of the GDPR require Data Controllers to provide Data Subjects with meaningful information about automated decision-making. The AIA complements this by imposing transparency and effective human-oversight obligations for high-risk systems (Art. 13–14), ensuring that AI outputs can be interpreted and supervised.

Likewise, the GDPR right not to be subject to a decision based solely on automated processing (Art. 22) is operationalized by the AIA through mandatory risk management and human control. Beyond transparency and oversight, both frameworks address a trade-off between data minimization and algorithmic fairness: larger and more diverse training datasets, including sensitive attributes when strictly necessary, can improve bias mitigation but also increase personal data processing, subject to strict GDPR safeguards. Notably, while the GDPR does not explicitly prohibit algorithmic discrimination, the AIA introduces concrete obligations to identify and mitigate discriminatory risks, illustrating their complementarity.

A remaining challenge concerns the practical enforcement of GDPR rights to erasure and consent withdrawal in AI training. Once personal data contribute to model learning, ensuring effective deletion or "unlearning" raises significant technical and economic difficulties, even though these rights remain fully applicable. Recent guidance from the EDPB (Opinion 28/2024)[5] further stresses the need to assess when AI-driven processing falls within the scope of GDPR Art. 22 and how newly generated AI data should be treated under data-protection law.

### *C. Opportunities and Compliance Burdens*

The introduction of the aforementioned regulatory instruments creates both opportunities and significant compliance challenges:

- **Data intermediation services**: This emerging niche market aims to foster trust and enable secure data sharing among individuals, organizations, and businesses. By acting as neutral intermediaries, they promote broader and more reliable data exchange.
- **Anonymization of data** (*data protection vs data utility*): In terms of the AIA, achieving strong privacy guarantees and high-utility datasets remains an open challenge [14]. To solve these issues, privacy-preserving techniques can be used. Among them, anonymization is one of the most widely adopted [15]. However, its use comes with additional complexities. For example, adding noise to personal data does not always ensure privacy, as aggregation or reconstruction techniques can potentially reverse these modifications, exposing sensitive information. Furthermore, as anonymization becomes more aggressive (e.g., through generalization), model accuracy deteriorates due to information loss, distorting underlying patterns and leading to biased or unreliable outputs [5]. This underscores the technical and ethical challenge of balancing data utility, privacy, and GDPR compliance when training AI systems.
- **Data lifecycle** (*data provenance and privacy*): A secure and well-documented lifecycle for training datasets is essential to demonstrate lawful sourcing and authorization. Measures that limit identifiability—together with strong governance—help maintain trust and regulatory conformity.
- **Dataset quality**: Dataset bias and misrepresentation are also critical concerns addressed in the AIA (Art. 10). Several initiatives aim to mitigate bias in datasets used for AI training. For instance, [10] introduces an open-source Python library offering dataset representations and algorithms for bias detection, mitigation, and metric explainability. This tool, along with others such as FiftyOne[6], has been proposed to support compliance with data governance requirements [11].
- **Compliance complexity** (*compliance automation*) : Although the AIA aims to encourage innovation within defined boundaries, some experts argue that its stringent requirements may have the opposite effect. According to Nizza [8], the regulatory burdens imposed by the AIA risk stifling innovation, particularly for small and medium-sized enterprises (SMEs). This concern is confirmed by the APPRAISE governance framework [9], which highlights the persistent tension between fostering innovation and ensuring compliance. The authors propose a structured approach to help organizations navigate these complexities, emphasizing auditing as a mechanism to prevent "creative compliance" and promote consistency. Their empirical study of 34 organizations in the Netherlands revealed generally low compliance levels, with SMEs performing worst due to assigning lower priority to regulatory conformity. To mitigate these challenges, the AIA offers facilitating measures for SMEs, including free access to regulatory sandboxes, proportional conformity assessment fees, simplified documentation templates, tailored training, and dedicated guidance channels. Penalties and obligations are also applied proportionally to organizational size.
- **Explainability and transparency** (*human understanding and interpretability*): The AIA does not impose a general duty of explainability but promotes it through transparency and documentation obligations, requiring that high-risk AI systems be sufficiently interpretable to enable effective human oversight (Art. 13), even where full algorithmic interpretability is technically infeasible. Despite progress, significant challenges remain, notably the lack of standardized explainability evaluation methods and the need for robust lifecycle monitoring and auditing of high-risk AI systems to ensure safety, accountability, and transparency. Current XAI tools involve

[5]https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en

[6]FiftyOne documentation: https://docs.voxel51.com/

trade-offs between fidelity, interpretability, and computational efficiency, and no universally accepted standard exists for evaluating explanation quality [6]. Moreover, AI reliability requires not only transparency but also data quality, bias mitigation, robustness, and stability [7]. Frameworks integrating these dimensions are therefore essential for trustworthy AI. Parlak's BAXDT approach [12] enhances transparency by recording explainable decision traces, but its reliance on a single technique may limit comprehensiveness; combining it with methods such as LIME [13] or other XAI strategies could support more holistic interpretability.

Ultimately, these challenges underscore the need for a practical compliance framework that is beneficial for all stakeholders—data subjects, enterprises, and regulators alike. Such a framework should harmonize GDPR principles with the operational requirements of the AIA, DA, and DGA, ensuring that privacy, transparency, and innovation can coexist without imposing disproportionate burdens.

## V. Conclusions

This study analyzed the interplay between the GDPR, the AIA, the DA, and the DGA, focusing on their points of convergence and interaction. We conducted a comparative analysis of these frameworks, identifying areas where principles align and where significant practical tensions arise (such as the tension between data altruism and consent withdrawal, or between data-sharing obligations and privacy-by-design requirements). While these regulations mark a significant step toward trustworthy AI by promoting transparency, accountability, and societal benefit, their effective implementation remains challenging.

Moreover, the parallel application of these frameworks implies the involvement of multiple supervisory authorities (data protection, data governance, and AI regulators), raising risks of regulatory overlap, fragmentation, and competence gaps.

Key issues include the gap between regulatory principles and practical feasibility, the difficulty of balancing privacy with data utility and model accuracy, and the complexity of ensuring consistent compliance across overlapping frameworks. Additionally, overcoming the opacity of "black-box" models remains critical: despite progress in explainability techniques, the lack of standardized methodologies and practitioner training limits their effectiveness.

## VI. Future Directions

Future work should focus on data provenance in AI training, effective consent management, and practical transparency and explainability mechanisms. It should also examine the interaction of the DA's international data-transfer regime and the AIA cybersecurity requirements with broader EU cyber-risk frameworks, including NIS2 and the Cyber Resilience Act, to ensure coherent and efficient compliance.

## Acknowledgments and Disclaimer

This research is supported by Project HERMES, funded by the European Union NextGenerationEU/PRTR via INCIBE; by Projects PID2021-125962OB-C32 "SECURING/DATA" and PID2024-156914OB-C42 "SAFE/DATA", funded by MCIN/AEI/ 10.13039/501100011033; and by Grant SGR2021-00115, funded by AGAUR, Generalitat de Catalunya. Ignacio Miguel Rodríguez is supported by the Generalitat of Catalonia under a FI-STEP grant (ref. 2025 STEP 00378).

## References

[1] European Parliament and Council, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)," *Official Journal of the European Union*, 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[2] European Parliament and Council, "Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)", *Official Journal of the European Union*, 2023.https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng

[3] European Parliament and Council, "Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)", *Official Journal of the European Union*, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng

[4] European Parliament and Council, "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence," *Official Journal of the European Union*, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

[5] H. Lee, S. Kim, J. W. Kim, and Y. D. Chung, "Utility-preserving anonymization for health data publishing," *BMC Medical Informatics and Decision Making*, vol. 17, no. 1, p. 104, Jul. 2017, doi: 10.1186/s12911-017-0499-0. [Online]. Available: https://doi.org/10.1186/s12911-017-0499-0

[6] H. I. Aysel, X. Cai, and A. Prugel-Bennett, "Explainable artificial intelligence: Advancements and limitations," *Applied Sciences*, vol. 15, no. 13, art. no. 7261, 2025, doi: 10.3390/app15137261. [Online]. Available: https://www.mdpi.com/2076-3417/15/13/7261

[7] S. T. H. Mortaji and M. E. Sadeghi, "Assessing the reliability of artificial intelligence systems: Challenges, metrics, and future directions," *IJIMES*, vol. 4, no. 2, pp. 1–13, Jun. 2024, doi: 10.59615/ijimes.4.2.1. [Online]. Available: https://doi.org/10.59615/ijimes.4.2.1

[8] U. Nizza, "Assessing the Impact of the European AI Act on Innovation Dynamics," *Transatlantic Technology Law Forum Working Paper*, no. 138, 2025. [Online]. Available: https://wwws.law.northwestern.edu/research-faculty/clbe/events/standardization/documents/nizza_assessing_impact_ai_act_innovation.pdf

[9] D. Dey and D. Bhaumik, "APPRAISE: a Governance Framework for Innovation with Artificial Intelligence Systems," *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, vol. 7, no. 1, pp. 328–340, Oct. 2024, doi: 10.1609/aies.v7i1.31640. [Online]. Available: https://ojs.aaai.org/index.php/AIES/article/view/31640

[10] R. K. E. Bellamy, K. Dey, M. Hind, S. C. Hoffman, S. Houde, K. Kannan, P. Lohia, J. Martino, S. Mehta, A. Mojsilovic, S. Nagar, K. N. Ramamurthy, J. Richards, D. Saha, P. Sattigeri, M. Singh, K. R. Varshney, and Y. Zhang, "AI Fairness 360: An Extensible Toolkit for Detecting, Understanding, and Mitigating Unwanted Algorithmic Bias," *arXiv preprint*, Oct. 2018. [Online]. Available: https://arxiv.org/abs/1810.01943

[11] A. Obradov and B. Pavković, "Ensuring Compliance of High-Risk AI Systems with the EU AI Act Using Open Source Libraries," *2025 IEEE Zooming Innovation in Consumer Technologies Conference (ZINC)*, pp. 54–59, 2025, doi: 10.1109/ZINC65316.2025.11103517.

[12] İ. E. Parlak, "Blockchain-assisted explainable decision traces (BAXDT): An approach for transparency and accountability in artificial intelligence systems," *Knowledge-Based Systems*, vol. 329, pp. 114402, 2025, doi: 10.1016/j.knosys.2025.114402. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0950705125014418

[13] M. T. Ribeiro, S. Singh, and C. Guestrin, "Why Should I Trust You?: Explaining the Predictions of Any Classifier," arXiv preprint arXiv:1602.04938, 2016. Available: https://arxiv.org/abs/1602.04938.

[14] H. Zhong and K. Bu, *Privacy-Utility Trade-Off*, arXiv:2204.12057, 2022. Available at: https://arxiv.org/abs/2204.12057.

[15] A. Majeed, *Attribute-Centric and Synthetic Data Based Privacy Preserving Methods: A Systematic Review*, *Journal of Cybersecurity and Privacy*, vol. 3, pp. 638–661, 2023. Available at: https://doi.org/10.3390/jcp3030030.