



SCHOOL OF
ECONOMICS AND
MANAGEMENT

Coordinating the GDPR and the AI Act

Overlaps, Conflicts and Gaps in High-Risk AI
Systems

Lei Nie and Yue Wang

DEPARTMENT OF BUSINESS LAW

Master's Thesis in European and International Trade Law

15 ECTS

HARN63

Spring 2026

Contents

Abstract	5
Abbreviations	6
1 Introduction	7
1.1 Background	7
1.2 Purpose and research questions	10
1.2.1 Purpose	10
1.2.2 Research Questions	10
1.3 Delimitations	11
1.4 Method and materials	11
1.5 Outline	13
2 Normative Framework and Legislative Logic of the GDPR and the AI Act	14
2.1 The GDPR: A Horizontal Framework for EU Data Protection	14
2.2 The AI Act: A Safety Framework for EU High-Risk AI Governance	15
2.3 Divergent Legislative Logics and the Normative Basis for Interaction	16
3 Overlaps, Conflicts and Normative Gaps	18
3.1 Introduction	18
3.2 Functional Overlaps: FRIA and DPIA	18
3.2.1 Conceptual and Procedural Convergence	18
3.2.2 Compliance Duplication and Practical Burdens	19
3.2.3 Strategic Coordination of Overlapping Assessment Requirements	19
3.3 Normative Conflicts in AI Training Data	21
3.3.1 Sensitive Data Processing and Bias Mitigation	21
3.3.2 Data Representativeness and Data minimization	22
3.3.3 Addressing the Conflicts: Practical and Interpretative Approaches	24
3.3.4 A Staged Approach to Data Collection and minimization	24
3.3.5 Integration of the DPIA and FRIA Processes	25
3.3.6 The Need for Regulatory Guidance and Coordinated Enforcement	25
3.4 Normative Gaps: The Inference Gap	27
3.5 Institutional Fragmentation and Enforcement Coordination	28
3.5.1 Divergent Mandates and Philosophies of DPAs and MSAs	28
3.5.2 Regulatory Cooperations and Interaction Mechanisms	30
4 Conclusion	32
4.1 Summary of Research Findings	32
4.2 Research Value	33

4.3 Research Limitations	33
4.4 Future Research Outlook	34
References	35

Abstract

This thesis explores the regulatory friction that surfaces when the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act) apply side by side to high-risk AI systems. It homes in on three connected problems. First, there is a procedural overlap between the Data Protection Impact Assessment (DPIA) and the Fundamental Rights Impact Assessment (FRIA). Second, a normative tension runs between the GDPR's data minimisation principle and the AI Act's demand for representative training data. Third, a regulatory gap surrounds AI-generated inferred data, and this is made worse by fragmented enforcement between Data Protection Authorities (DPAs) and Market Surveillance Authorities (MSAs).

The thesis adopts a legal dogmatic method, drawing on literal, systematic, and teleological interpretation. It analyses how the two frameworks interact, taking into account recent EU regulatory moves such as EDPB Opinion 28/2024 and the 2025 Digital Omnibus Proposal.

The findings show that running the DPIA and the FRIA in parallel leads to a good deal of duplication and makes coordination difficult. The study also flags ongoing legal uncertainty in several areas: the use of sensitive data for bias mitigation, how to strike a balance between representativeness and data minimisation, and the treatment of inferred data. To address these issues, the thesis suggests a more joined-up approach to compliance that combines DPIA and FRIA processes, along with stronger cooperation between DPAs and MSAs to boost consistency and legal certainty.

Keywords: Artificial Intelligence Act; General Data Protection Regulation (GDPR); high-risk AI systems; Fundamental Rights Impact Assessment (FRIA); Data Protection Impact Assessment (DPIA); inferred data

Abbreviations

AI	Artificial Intelligence
AI Act	Artificial Intelligence Act
CJEU	Court of Justice of the European Union
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EU	European Union
FRIA	Fundamental Rights Impact Assessment
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
MSA	Market Surveillance Authority
WTO	World Trade Organisation

1 Introduction

1.1 Background

The rapid evolution of Artificial Intelligence (AI) technologies has outpaced traditional legal frameworks, prompting the European Union to establish a dual regulatory model that seeks to balance technological innovation with the protection of fundamental rights. This model is anchored by two comprehensive legislative instruments: the General Data Protection Regulation (GDPR), which regulates the processing of personal data, and the newly enacted Artificial Intelligence Act (AI Act), which introduces a product-safety and risk-based framework for AI systems.¹ While both regimes share the overarching objective of protecting individuals within the digital ecosystem, their co-existence has created profound systemic frictions. The GDPR anchors its protection in the individual data subject and her rights, whereas the AI Act adopts a systemic, risk-management perspective centred on the safety of the AI system as a product.² As a result, when these two frameworks simultaneously apply to the same technological lifecycle, they generate an intricate web of legal interactions that threaten to undermine both legal certainty and regulatory compliance.

The GDPR sets up a horizontal, rights-based regime aimed at shielding personal data.³ It rests on core principles such as lawfulness, fairness and transparency, purpose limitation, and data minimization, and it imposes a strict ban on processing special categories of personal data under Article 9.⁴ Its procedural centerpiece is the Data Protection Impact Assessment (DPIA) under Article 35, which must be carried out by the data controller when processing is likely to result in high risks to individuals' rights.⁵

By contrast, the AI Act introduces a risk-based, product safety model focused on ensuring safe, lawful, and human-centric AI throughout the system lifecycle.⁶ It groups AI systems into four risk buckets, and subjects high-risk systems to tough obligations, including representative and unbiased training data under Article 10, and the Fundamental Rights Impact Assessment (FRIA) under Article 27.⁷ The DPIA obligation falls on the data controller, while the FRIA obligation rests with

¹ 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 (General Data Protection Regulation) [2016] OJ L119/1; Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain legislative acts (Artificial Intelligence Act) [2024] OJ L2024/1689.

² Hajo Michael Holtz and Jonas Ledendal, 'AI Data Governance – Overlaps between the AI Act and the GDPR' (2026) 17(1) *Law, Innovation and Technology* 1, 8.

³ GDPR (n 1), art 1.

⁴ Ibid arts 5–9.

⁵ Ibid art 35.

⁶ AI Act (n 1), recital 1.

⁷ Ibid arts 10, 27.

the deployer, and these actors will not always coincide, leaving the two assessments procedurally distinct and uncoordinated.⁸

This study examines the interaction between the GDPR and the AI Act through three connected types of regulatory interfaces: overlaps, conflicts, and gaps. These interfaces have been selected because they arise where both instruments simultaneously govern the same regulatory activity within the lifecycle of a high-risk AI system, including the deployment of the system, the processing of training data, and the generation of data-driven inferences about individuals. Although the GDPR and the AI Act apply to these activities from different regulatory perspectives, neither framework, nor the two read together, currently provides a fully coordinated mechanism for resolving the resulting tensions.

These interfaces emerge progressively through the parallel application of the Data Protection Impact Assessment (DPIA) under Article 35 GDPR and the Fundamental Rights Impact Assessment (FRIA) under Article 27 of the AI Act, both of which apply to the lifecycle of high-risk AI systems.⁹ The starting point is regulatory overlap. Because the GDPR and the AI Act simultaneously govern the deployment and operation of high-risk AI systems involving personal data processing, providers and deployers may be required to conduct parallel assessments addressing closely related legal and technical risks.¹⁰ From these overlaps, normative conflicts can surface where the two frameworks impose incompatible substantive requirements.¹¹ At the same time, the coexistence of the two frameworks does not guarantee complete coverage; certain risks remain insufficiently addressed by either regime, creating regulatory gaps.¹²

The GDPR and the AI Act touch on each other at many points, and the interactions examined in this thesis are not meant to be an exhaustive list. At the procedural level, the DPIA–FRIA overlap arises because a single deployment decision triggers both assessments. When the controller and deployer are same entities, this creates a coordination challenge across organisational boundaries, transforming what would be a double burden into an inter-institutional friction. Both assessments examine largely the same factual picture, only through different legal lenses. The EDPB has already pointed out that this interaction creates regulatory duplication and calls for coordination.¹³ For high-risk AI systems, this is not a legal conflict in the strict sense, but a structural inefficiency that drives up compliance costs.¹⁴ The GDPR builds a “rights firewall” through the DPIA, while the AI Act builds a “safety firewall” through the FRIA. To lawfully enter the EU internal market, both assessments must be satisfactorily completed.¹⁵

⁸ GDPR (n 1), art 35(1); AI Act (n 1), art 27(1).

⁹ GDPR (n 1) art 35; AI Act (n 1) art 27.

¹⁰ Holtz and Ledendal (n 2) 1, 13–14.

¹¹ European Data Protection Board, ‘Opinion 28/2024 on the Application of the GDPR to Artificial Intelligence Systems’ (17 December 2024) paras 38–45.

¹² Sandra Wachter and Brent Mittelstadt, ‘A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI’ (2019) 2 *Columbia Business Law Review* 494, 505–510.

¹³ EDPB, ‘Opinion 28/2024 on the Application of the GDPR to Artificial Intelligence Systems’ (n 11) para 52.

¹⁴ Przemysław (Shemy) Gruchała, Lucrezia Nicosia and Monika Zięciak, ‘Harmonising risk assessments for high-risk AI systems under the GDPR and the AI Act’ (2025) 7(4) *Journal of Data Protection & Privacy* 359.

¹⁵ EDPB Opinion 28/2024 (n 11), para 53.

At the substantive level, the training data conflict stems from a single technical activity. That activity is assembling and processing datasets for model training. It is governed by two sets of binding requirements that pull in opposite directions. The AI Act demands representativeness, and the GDPR demands minimization.¹⁶ The former emphasizes product safety and non-discrimination, while the latter emphasizes purpose limitation and proportionality; in operational terms, they pull in opposite directions. At the same time, the GDPR's blanket ban on sensitive data rubs up against the AI Act's permission to use such data for algorithmic fairness and bias mitigation.¹⁷ These are substantive legal cracks that directly shape the feasibility of technical design and lawful compliance.¹⁸ Although this normative tension exists independently of any procedural obligation, it is rendered practically unavoidable when the same operator must carry out both the DPIA and the FRIA. Because the two assessments force the same training-data practices to be defended under two evaluative frameworks that exert normative pressure in divergent directions.

On the enforcement side, the inferred-data gap stems from a structural mismatch. The same system output consists of inferences about individuals. It sits awkwardly between two regulatory focal points. The GDPR concentrates on input personal data, and the AI Act focuses on output system risks. This leaves those inferences in a grey zone.¹⁹ At the same time, Data Protection Authorities (DPAs) and Market Surveillance Authorities (MSAs) each work under their own distinct mandates, currently lacking the structured coordination procedures that would be needed.²⁰ Inferred data lies exactly where the two instruments' jurisdictional boundaries meet without overlapping, and regulatory guidance has repeatedly pointed to its ambiguous status as a protection gap that neither framework currently closes.²¹ This creates a functional protection vacuum: outputs produced by AI systems, such as risk scores and behavioral predictions, can have a serious impact on individuals, yet they do not clearly fit within the GDPR's safeguards for "personal data" or the AI Act's system-level risk management, leaving individual rights without a clear regulatory home.²² On the enforcement side, DPAs and MSAs apply different legal standards and currently lack binding joint procedures; the same high-risk system may be found compliant under the AI Act yet raise concerns under the GDPR.²³

Two recent regulatory developments have framed these tensions through a sequential reactive logic. EDPB Opinion 28/2024 (December 2024) first illuminated the practical friction of parallel application, warning that overlapping procedures may lead to inefficiency and duplication.²⁴ In response, the European Commission put forward the Digital Omnibus Proposal in November 2025 (still

¹⁶ EDPB Opinion 28/2024 (n 11), para 38.

¹⁷ AI Act (n 1) art 10(2); GDPR (n 1), art 9(1).

¹⁸ Michael Veale and Reuben Binns, 'Fairer Machine Learning in the Real World: Mitigating Discrimination Without Collecting Sensitive Data' (2017) 8 *Big Data & Society* 1, 3.

¹⁹ EDPB Opinion 28/2024 (n 11), paras 65–70.

²⁰ *Ibid.*

²¹ Sean Musch, Michael Charles Borrelli and Charles Kerrigan, 'Bridging Compliance and Innovation: A Comparative Analysis of the EU AI Act and GDPR for Enhanced Organisational Strategy' (2024) 7(1) *Journal of Data Protection & Privacy* 14, 20.

²² EDPB Opinion 28/2024 (n 11), paras 65–70.

²³ Holtz and Ledendal (n 2), 1, 14.

²⁴ EDPB Opinion 28/2024 (n 11), paras 45–60, 52.

being negotiated as of May 2026), introducing a new Article 4a that would permit the processing of special category data strictly necessary for detecting and mitigating bias, while mandating joint guidance aimed at bringing the AI Act more systematically into alignment with the GDPR.²⁵

Beneath all three structural frictions (procedural overlap, substantive conflict, and enforcement gap) lies a deeper tension between the protective philosophies of the two instruments. Each of them emerges where both frameworks regulate the same stage of the AI lifecycle while imposing competing or uncoordinated obligations, but without clearly explaining how those obligations should operate together. Three core issues thus stand out: first, the administrative overlap caused by parallel DPIA and FRIA procedures; second, the normative legal conflicts over training data and sensitive data processing; third, the regulatory gap around inferred data, made worse by fragmented institutional enforcement. Taken together, these overlapping requirements and regulatory blind spots chip away at legal certainty, complicate cross-Member State enforcement, and stand in the way of a balanced pursuit of AI innovation, system safety, and personal data protection.²⁶ Clarifying these layered challenges and establishing a coherent framework for the coordinated application of the GDPR and the AI Act has therefore become an urgent theoretical and practical challenge in EU data and AI governance.²⁷

1.2 Purpose and research questions

1.2.1 Purpose

This thesis conducts a legal-dogmatic analysis of the dual regulatory framework formed by the GDPR and the AI Act, focusing on high-risk AI systems. It examines three structural friction points from parallel application: the procedural overlap between the GDPR Article 35 DPIA and the AI Act Article 27 FRIA; the substantive normative conflict between the GDPR's data minimization principle and the AI Act's data representativeness requirement; and the regulatory gap concerning AI-generated inferred data, worsened by institutional fragmentation between DPAs and MSAs. These interconnected issues reflect a deeper tension between the GDPR's individual rights protection and the AI Act's systemic product safety logics. The overall aim is to provide clear interpretative guidance and practical compliance recommendations to reduce regulatory uncertainty and support consistent application of EU law.

1.2.2 Research Questions

- (1) What is the nature and extent of the procedural overlap between the Data Protection Impact Assessment under Article 35 of GDPR and the

²⁵ European Commission, Proposal for a Regulation amending Regulation (EU) 2024/1689 on Artificial Intelligence (Digital Omnibus Proposal) COM(2025) 836 final, art 4a.

²⁶ Sergey A Yablonsky, 'Multidimensional Data-Driven Artificial Intelligence Innovation' (2019) 9(12) Technology Innovation Management Review 16, 26.

²⁷ Bharath Kishore Gudepu and Rebecca Eichler, 'The Role of AI in Enhancing Data Governance Strategies' (2024) International Journal of Acta Informatica 169, 176.

Fundamental Rights Impact Assessment under Article 27 AI Act when applied to the same high-risk AI system?

- (2) To what extent does the normative tension between the data minimization principle under Article 5(1)(c) GDPR and the requirement of representative and unbiased training data under Article 10 of the AI Act constitute a genuine legal conflict rather than a mere regulatory divergence?
- (3) Under what circumstances do downstream inferences generated by high-risk AI systems escape the regulatory scope of Article 22 GDPR on automated decision-making while simultaneously falling outside the system-level risk management requirements of the AI Act?
- (4) How does the institutional split between Data Protection Authorities (Chapter VI GDPR) and Market Surveillance Authorities (Chapter V AI Act) deepen these regulatory gaps?

1.3 Delimitations

This thesis confines itself to a legal dogmatic analysis of the EU GDPR and the AI Act, and only looks into the normative clashes and coordination paths between the two when applied to high-risk AI systems. It does not reach into other EU digital regulations, such as the Digital Services Act and the Digital Markets Act, nor does it carry out empirical research or comparative studies with non-EU legal systems. The analysis stays at the normative level and does not dig into specific corporate compliance practices.

1.4 Method and materials

The main approach taken in this thesis is the legal dogmatic method. As Jan M. Smits notes, legal doctrine is all about systematically arranging and interpreting legal rules to present a coherent picture of the law.²⁸ This study applies this method to clarify the relationship between the AI Act and the GDPR. This study applies interpretative methods used in EU law, including literal, systematic, and teleological interpretation of the relevant provisions, as developed by the Court of Justice of the European Union and recognized in EU legal scholarship.²⁹ The purpose is to interpret the AI Act and the GDPR consistently with the broader objectives and structure of EU law.

The research draws on six categories of legally relevant sources, each described below:

²⁸ Jan M Smits, 'What is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research' in Rob van Gestel, Hans-W Micklitz and Edward L Rubin (eds), *Rethinking Legal Scholarship: A Transatlantic Dialogue* (Cambridge University Press 2017), 12.

²⁹ Koen Lenaerts and José A Gutiérrez-Fons, 'To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice' (2014) 20 *Columbia Journal of European Law* 3, 6.

- (1) EU Regulations (GDPR and AI Act)
Regulations such as the GDPR and the AI Act are binding and directly applicable legal acts of the European Union.³⁰ They constitute the primary legislative framework governing data protection and artificial intelligence and provide the binding normative basis for analysis. The 2025 Digital Omnibus Proposal amending the AI Act is also included as a key legislative source.³¹
- (2) CJEU Case Law
Case law from the Court of Justice of the European Union provides authoritative interpretations of EU law, including principles of data protection, automated decision-making, and fundamental rights. CJEU judgments clarify the scope and meaning of key provisions and ensure consistent application across Member States.
- (3) EDPB Opinions and Guidelines
The European Data Protection Board (EDPB) adopts non-binding but highly persuasive opinions and guidance concerning the practical application of the GDPR.³² Of particular importance is EDPB Opinion 28/2024, which addresses data protection aspects of personal data processing in AI systems and directly illuminates the interface between the GDPR and the AI Act.³³
- (4) Legal Doctrine (Academic Literature)
Academic scholarship offers critical analysis of the Overlaps, Conflicts, and Institutional Gaps between the AI Act and the GDPR. Legal doctrine contributes to the structural and normative understanding of the dual regulatory framework and supports coherent legal-dogmatic interpretation.
- (5) Travaux Préparatoires and Legislative Background
Preparatory documents, including commission proposals, recitals, and explanatory memoranda, assist in contextual and teleological interpretation. In EU law, such materials are increasingly important for clarifying the legislative intent behind regulations such as the AI Act and the GDPR.
However, the use of historical legislative materials in legal dogmatics requires justification. While some scholars have questioned the coherence of legislative intent as a concept, describing it as a “fiction”, this study does not rely on any notion of subjective legislative will.³⁴ Following the approach advocated by Lenaerts and Gutiérrez-Fons, it employs these materials strictly to ascertain the “objectives pursued by the legislation”, which is a key component of teleological interpretation.³⁵
Regarding the extent of their probative value, this study aligns with the case law of the Court of Justice of the European Union (CJEU). The CJEU has

³⁰ Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L 119/1; Regulation (EU) 2024/1689 (Artificial Intelligence Act) [2024] OJ L2024/1689.

³¹ European Commission, Proposal for a Digital Omnibus on AI Regulation, COM(2025) 836 final.

³² European Data Protection Board, Statement 3/2024 on Data Protection Authorities’ Role in the Artificial Intelligence Act Framework (16 July 2024).

³³ European Data Protection Board, Opinion 28/2024 on Personal Data Processing in AI Systems (2024).

³⁴ ‘Legislative Intent as a Fiction’ in Chiara Valentini and Teresa Marques (eds), *Collective Action, Philosophy and Law* (Routledge 2021) 115.

³⁵ Koen Lenaerts and José A Gutiérrez-Fons, ‘To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice’ (2014) 20 *Columbia Journal of European Law* 3, 28.

consistently held that while the wording of a provision is primary, recourse to preparatory documents is legitimate (and often necessary) to clarify ambiguous terminology or to define the context of a provision where the wording alone is insufficient.³⁶

Therefore, these documents will be used not to rewrite the law, but to illuminate the scope and meaning of contested provisions, particularly in the novel context of the interaction between the AI Act and the GDPR.

Taken together, these five categories of sources provide the foundation for the legal dogmatic analysis conducted in this thesis. EU regulations and CJEU case law establish the binding normative framework and its authoritative interpretation, while EDPB guidance, academic literature, and legislative materials contribute the analytical and contextual background necessary to clarify the scope and purpose of contested provisions within the evolving relationship between the GDPR and the AI Act.

1.5 Outline

The thesis is organized into four compact chapters to keep the analysis focused and the logic clear, while still digging into the dual impact assessment system made up of the FRIA and the DPIA.

Chapter 1 – Introduction sketches the background, pinpoints the core normative conflicts between the AI Act and the GDPR, lays out the research purpose and questions, clarifies what the study does not cover, and explains the legal dogmatic method and materials used.

Chapter 2 – Normative Framework and Legislative Logic of the GDPR and the AI Act: the two instruments’ regulatory architectures and their divergent legislative logics.

Chapter 3 – Overlaps, Conflicts and Normative Gaps: systematic examination of procedural overlap, substantive conflict inferred data gap and the institutional fragmentation.

Chapter 4 – Conclusion pulls together the key findings, answers the three research questions, reflects on the practical implications for legal practitioners and AI providers, and points out the study’s limitations as well as possible directions for future research.

³⁶ Georg Kofler and others (eds), *Tax Treaty Interpretation in Light of the Vienna Convention on the Law of Treaties* (Wolters Kluwer 2024) 102.

2 Normative Framework and Legislative Logic of the GDPR and the AI Act

Before examining the specific points of friction between the two instruments, it is necessary to understand their respective regulatory architectures. This chapter provides a concise overview of the GDPR and the AI Act, focusing on their legislative objectives, core obligations, and enforcement structures, and highlighting the structural differences that give rise to the overlaps, conflicts, and gaps analyzed in subsequent chapters.

2.1 The GDPR: A Horizontal Framework for EU Data Protection

The General Data Protection Regulation (GDPR, Regulation (EU) 2016/679), which entered into force in 2018, serves as the overarching horizontal framework for personal data protection in the European Union.³⁷ It unifies data protection rules across Member States, strengthens the fundamental rights of natural persons, and guarantees the free movement of personal data within the EU. Rooted in a rights-based logic, the GDPR establishes a compliance system covering the entire data lifecycle, with its core value lying in balancing data utilization with the protection of personal privacy and human dignity through stringent legal constraints.³⁸

From a normative perspective, the GDPR enshrines seven core principles: lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation, Integrity and confidentiality, and accountability (GDPR, art 5). Among these, the data minimization principle (Article 5(1)(c)) is central to the regulation, requiring personal data to be adequate, relevant and limited to what is necessary for the purposes for which they are processed.³⁹ It prohibits excessive collection, storage and use of data, essentially imposing an ex ante constraint on the processing of personal data. Additionally, Article 9 of the GDPR imposes a general ban on the processing of special categories of personal data, with exemptions set out exhaustively in Article 9(2), including explicit consent, employment and social security obligations, vital interests, and substantial public interest in the area of public health or scientific research.⁴⁰ This further strengthens protection for highly sensitive information such as racial or ethnic origin, religion, health and sexual orientation.

³⁷ 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 (General Data Protection Regulation) [2016] OJ L119/1. See generally Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020).

³⁸ Damiano A Tamburri, 'Design Principles for the General Data Protection Regulation (GDPR): A Formal Concept Analysis and Its Evaluation' (2020) 91 *Information Systems* 101469, 12.

³⁹ AJ Biega and M Finck, 'Reviving Purpose Limitation and Data minimization in Data-Driven Systems' (arXiv preprint, 2021) arXiv:2101.06203, 7.

⁴⁰ GDPR, (n 1) art 9.

At the procedural level, the Data Protection Impact Assessment (DPIA, Article 35) is the core risk management tool under the GDPR. It mandates data controllers to conduct an ex ante assessment when processing activities are likely to pose high risks to the rights and freedoms of natural persons, to identify risks, design mitigation measures and maintain records.⁴¹ Focused on risks arising from personal data processing, the DPIA operationalises the GDPR's rights-protective logic in high-risk scenarios. As subsequent chapters will examine, the DPIA's interaction with the Fundamental Rights Impact Assessment (FRIA) under the AI Act lies at the centre of the procedural coordination challenges between the two frameworks. Furthermore, the GDPR designates Data Protection Authorities (DPAs) as enforcement bodies, ensuring consistent EU-wide enforcement via the one-stop-shop mechanism and consistency procedures, forming a closed loop of legislation, compliance and enforcement.⁴²

2.2 The AI Act: A Safety Framework for EU High-Risk AI Governance

The Artificial Intelligence Act (AI Act, Regulation (EU) 2024/1689), adopted in 2024, is widely regarded as the first comprehensive horizontal legislation regulating AI systems globally.⁴³ Adopting a risk-based governance model, it classifies AI systems into four categories: unacceptable risk, high risk, limited risk and minimal risk, imposing strict mandatory obligations only on high-risk AI systems.⁴⁴ Its legislative logic centres on product safety, technical reliability and the protection of health, safety and fundamental rights, establishing a regulatory system covering the entire AI lifecycle.

High-risk AI systems lie at the heart of the AI Act's regulation, spanning critical sectors such as education, employment, healthcare, justice and public services, directly impacting the health, safety and fundamental rights of natural persons. Article 10 of the AI Act sets out training data governance obligations, requiring training datasets for high-risk AI systems to be relevant, representative, sufficiently complete, and free of errors and bias to the greatest extent feasible

(AI Act, art 10). This ensures systems operate fairly across diverse population groups and avoid algorithmic discrimination. Grounded in technical effectiveness and fairness, the provision imposes rigid requirements on data scale, diversity and representativeness from a product safety perspective.

For rights impact assessment, Article 27 of the AI Act introduces the Fundamental Rights Impact Assessment (FRIA), mandating an ex ante assessment prior to the

⁴¹ Katerina Demetrou, 'Data Protection Impact Assessment: A Tool for Accountability and the Unclarified Concept of "High Risk" in the General Data Protection Regulation' (2019) 35 *Computer Law & Security Review* 105342. See also Dariusz Kloza and others (eds), *Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework towards a More Robust Protection of Individuals* (VUBPress 2017).

⁴² Holtz and Ledendal (n 2), 14.

⁴³ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain legislative acts (Artificial Intelligence Act) [2024] OJ L2024/1689.

⁴⁴ Claudio Novelli and others, 'Taking AI Risks Seriously: A New Assessment Model for the AI Act' (2024) 39 *AI & Society* 2493.

deployment of high-risk AI systems to identify and mitigate risks to broad fundamental rights such as non-discrimination, human dignity, freedom of expression and access to essential services (AI Act, art 27).⁴⁵ Broader in scope than the DPIA, the FRIA extends beyond personal data protection to encompass the impact of system operation on the broader social order of rights. However, the two assessments are triggered under different legal bases, imposed on different actors — the data controller for the DPIA and the deployer for the FRIA — and designed to serve distinct regulatory purposes, a divergence that gives rise to significant procedural duplication and coordination challenges. Additionally, the AI Act designates Market Surveillance Authorities (MSAs) as enforcement bodies, leveraging the EU's product safety regulatory system to conduct market access reviews, compliance audits and post-market oversight for high-risk AI systems, forming a governance chain of technical compliance, market access and safety supervision.⁴⁶

2.3 Divergent Legislative Logics and the Normative Basis for Interaction

While both the GDPR and the AI Act are core instruments of EU digital governance, they differ fundamentally in regulatory philosophy. The GDPR is a horizontal, rights-based, data-centric statute anchored in the protection of the fundamental right to personal data protection; the AI Act is a vertical, safety-based, system-centric statute oriented towards ensuring AI technologies are safe, reliable and non-discriminatory.⁴⁷

These divergent orientations generate regulatory frictions at three distinct levels, which the following chapters examine in turn. At the procedural level, the GDPR's DPIA and the AI Act's FRIA impose parallel ex ante assessment obligations triggered by the same deployment activity, yet operate under different legal criteria and are imposed on different actors. At the substantive level, the GDPR's data minimization principle and its prohibition on processing special categories of data pull in the opposite direction from the AI Act's requirements for representative training data and the use of sensitive data for bias mitigation. At the enforcement level, the gap between the GDPR's focus on personal data and the AI Act's focus on system safety leaves certain AI-generated harms without a clear regulatory home, while the institutional fragmentation between Data Protection Authorities and Market Surveillance Authorities further compounds the resulting uncertainty.⁴⁸

Despite these tensions, the two instruments share a natural basis for interaction: both are anchored in the protection of fundamental rights, both deploy ex ante risk

⁴⁵ Alessandro Mantelero, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, Legal Obligations and Key Elements for a Model Template' (2024) 54 *Computer Law & Security Review* 106020.

⁴⁶ Claudio Novelli and others, 'A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities' (2024) 15 *European Journal of Risk Regulation* 597.

⁴⁷ Holtz and Ledendal (n 2), 1, 8; Paul De Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 *Computer Law & Security Review* 179, 182.

⁴⁸ Holtz and Ledendal (n 2), 13–14, 17, 20, 23–25; European Data Protection Board, 'Statement 3/2024 on Data Protection Authorities' Role in the Artificial Intelligence Act Framework' (16 July 2024) 2.

assessment mechanisms, and both govern high-risk digital activities. The challenge, as recent regulatory developments have acknowledged, is to coordinate their application without undermining their respective protective functions.⁴⁹

⁴⁹ European Commission, 'Proposal for a Regulation amending Regulation (EU) 2024/1689 on Artificial Intelligence (Digital Omnibus Proposal)' COM(2025) 836 final, 19 November 2025.

3 Overlaps, Conflicts and Normative Gaps

3.1 Introduction

The parallel application of the GDPR and the AI Act creates a structurally complex regulatory environment for providers, deployers, and data controllers involved in the development and deployment of high-risk AI systems. In this case, providers of high-risk AI systems must comply with two distinct, yet partially overlapping, legal regimes. While the GDPR establishes a horizontal, rights-based framework centred on the protection of personal data and individual autonomy, the AI Act introduces a vertical, risk-based regime primarily concerned with product safety, system reliability, and the protection of fundamental rights in a broader sense.⁵⁰

This chapter addresses Research Question 1-3 by identifying and analysing three types of legal interaction between the two instruments: (i) functional overlaps, particularly in the context of impact assessments; (ii) direct and indirect normative conflicts, especially in relation to training data and sensitive data processing; and (iii) regulatory gaps and institutional inconsistencies that generate legal uncertainty in practice. The analysis adopts a systematic and teleological approach in order to clarify how these tensions may be interpreted and, where possible, reconciled within EU law.

3.2 Functional Overlaps: FRIA and DPIA

3.2.1 Conceptual and Procedural Convergence

A primary area of overlap arises from the coexistence of the Data Protection Impact Assessment (DPIA) under Article 35 GDPR and the Fundamental Rights Impact Assessment (FRIA) under Article 27 of the AI Act.⁵¹ Both instruments operate as ex ante risk assessment mechanisms designed to identify and mitigate potential harms before deployment.⁵²

From a functional perspective, the DPIA focuses on risks to the “rights and freedoms” of natural persons resulting from personal data processing, whereas the FRIA extends this analysis to a broader set of fundamental rights, including non-discrimination, human dignity, and access to essential services.⁵³ Despite this difference in scope, the two assessments share core analytical elements, including

⁵⁰ Holtz and Ledendal (n 2), 8.

⁵¹ GDPR (n 1), art 27.

⁵² Holtz and Ledendal (n 2), 13.

⁵³ *ibid* 14.

the evaluation of necessity and proportionality, risk identification, and the design of mitigation measures.⁵⁴

The DPIA may be understood as a subset within the broader logic of the FRIA.⁵⁵ In practice, this creates a situation in which the same underlying activity that the development and deployment of high-risk AI systems involving personal data is assessed twice under partially overlapping frameworks.

3.2.2 Compliance Duplication and Practical Burdens

Despite their conceptual proximity, the parallel operation of DPIA and FRIA generates significant procedural duplication. Providers are required to produce separate documentation, even where the substantive assessment overlaps considerably.⁵⁶

The duplication undermines the effectiveness of both instruments. Instead of enhancing risk mitigation, it may incentivise formalistic compliance, where the focus shifts from substantive risk analysis to fulfilling parallel documentation requirements.

For example, providers of high-risk AI systems in sectors such as automated recruitment or credit scoring are often required to conduct both a Data Protection Impact Assessment (DPIA) and a Fundamental Rights Impact Assessment (FRIA) based on largely overlapping datasets and risk scenarios. In practice, this may lead to the reproduction of similar risk descriptions, mitigation measures, and proportionality assessments in two separate documents, rather than a deeper, integrated analysis of systemic risks.⁵⁷

3.2.3 Strategic Coordination of Overlapping Assessment Requirements

The coordination of the DPIA and the FRIA should begin from the legal connection between Article 27 of the AI Act and the GDPR, rather than from a general appeal to administrative efficiency. Article 27 AI Act requires deployers of certain high-risk AI systems to assess the system's impact on fundamental rights before deployment.⁵⁸ In many cases, these risks arise directly from the processing of personal data, particularly in systems used for recruitment, credit scoring, biometric identification, education, or access to public services. The assessment of discrimination, exclusion, unequal treatment, and adverse effects on individuals therefore often depends on compliance with GDPR rules on lawfulness, fairness, data minimization, special category data, automated decision-making, and impact assessment.⁵⁹

⁵⁴ European Data Protection Board, 'Statement 3/2024 on Data Protection Authorities' Role in the Artificial Intelligence Act Framework' (16 July 2024) 2.

⁵⁵ Holtz and Ledendal (n 2), 13.

⁵⁶ *ibid.*

⁵⁷ Holtz and Ledendal (n 2), 13–14.

⁵⁸ AI Act (n 1), art 27.

⁵⁹ GDPR (n 1), arts 5, 9, 22 and 35.

This connection becomes especially important where the deployer of the high-risk AI system is also the data controller within the meaning of Article 4(7) GDPR. In such cases, the same actor may need to carry out both a FRIA under Article 27 AI Act and a DPIA under Article 35 GDPR.⁶⁰ Although the two assessments pursue different objectives, they rely on substantially overlapping factual material, including the purpose of the system, the categories of data processed, affected persons, risks of discriminatory outcomes, human oversight, and mitigation measures. Treating them as entirely separate procedures may therefore reproduce the same legal and technical analysis without significantly improving substantive protection.

A more feasible approach is to construct DPIA as a data protection layer in a broader FRIA. DPIA should first clarify the processing activities, legal basis, personal data categories, the necessity and proportionality of processing, the possibility of using special categories of data, and the safeguards required by the GDPR.⁶¹ These findings provide a basis for a broader FRIA assessment under the framework of the Artificial Intelligence Act, including risks related to non-discrimination, access to basic services, human dignity, and effective human supervision. Such coordination will not combine these two obligations or lower the legal standards stipulated in any legal instrument, but will enable the service provider and the deployer to rely on a common evidence base.

The practical significance of this overlap can be seen in the artificial intelligence-assisted credit score system. In the SCHUFA Holding case, the CJEU examined a credit scoring system that predicts the possibility of individual debt repayment by generating probability scores.⁶² The Court held that automated scoring may fall within Article 22 GDPR where the score significantly influences the final decision-making process.⁶³ Similar systems may also fall into the high-risk categories stipulated in the Artificial Intelligence Act, which means that the same operational practice may generate both the obligations under the GDPR and the regulatory requirements under the Artificial Intelligence Act.

Inter-agency coordination is still essential because the GDPR and the AI Act are implemented through different regulatory systems. The DPAs is still responsible for enforcing the GDPR, while the competent authority of member states (MSAs) is responsible for overseeing compliance with the AI Act. The EDPB has emphasized the need for cooperation between data protection agencies and other competent authorities within the framework of the Artificial Intelligence Act.⁶⁴ Such a structure could reduce repetitive compliance obligations and facilitate more consistent review by supervisory authorities.

In practice, this may involve sharing report templates, consulting programs, or joint review mechanisms for high-risk artificial intelligence systems involving large-scale user portraits, biometric processing or access to basic services. Without such

⁶⁰ GDPR (n 1), art 35(1); AI Act (n 1), art 27(1).

⁶¹ GDPR (n 1), arts 5, 6, 9, 25 and 35.

⁶² Case C-634/21 SCHUFA Holding AG EU:C:2023:957, paras 23–31.

⁶³ *ibid* paras 46–52, 73.

⁶⁴ Alessandro Mantelero, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, Legal Obligations and Key Elements for a Model Template' (2024) 54 Computer Law & Security Review 106020.

coordination, the same system may be considered compliant under the AI Act, but at the same time raises concerns under the GDPR.

3.3 Normative Conflicts in AI Training Data

3.3.1 Sensitive Data Processing and Bias Mitigation

The parallel application of Article 9 GDPR and the AI Act's data governance obligations creates practical uncertainty for providers developing high-risk AI systems that require sensitive data for fairness testing. Article 9(1) GDPR prohibits the processing of special categories of personal data unless one of the exceptions in Article 9(2) applies.⁶⁵ At the same time, Article 10 AI Act requires providers of high-risk systems to use training, validation, and testing datasets that are sufficiently representative and capable of reducing discriminatory bias.⁶⁶ In practice, these requirements may point in different directions when providers attempt to evaluate whether an AI system produces systematically unequal outcomes across protected groups.

This difficulty is particularly visible in healthcare and biometric systems. For example, developers of AI-assisted diagnostic tools may need access to health data, ethnicity data, or sex-based medical information in order to test whether a system performs less accurately for certain demographic groups.⁶⁷ Similar concerns arise in facial recognition technologies, where researchers have repeatedly identified significantly higher error rates for women and persons with darker skin tones when datasets lack demographic diversity.⁶⁸ Without access to sensitive demographic information during testing, providers may struggle to identify whether the system embeds discriminatory patterns at the model-training stage.

Providers must still identify a lawful basis under Article 9(2) GDPR before sensitive data can be processed for fairness testing purposes. However, the GDPR does not expressly recognize bias detection as an independent legal ground for processing special category data.⁶⁹ As a result, providers are often left relying on fragmented interpretations of substantial public interest, scientific research, or explicit consent, none of which were originally designed specifically for AI bias mitigation.⁷⁰

The practical significance of this issue can be seen in *Ligue des droits humains*, where the Court of Justice examined the automated processing of Passenger Name

⁶⁵ GDPR (n 1), art 9.

⁶⁶ AI Act (n 1), art 10.

⁶⁷ Inioluwa Deborah Raji and Joy Buolamwini, 'Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products' (2019) *AAAI/ACM Conference on AI Ethics and Society*, 2-6.

⁶⁸ Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 *Proceedings of Machine Learning Research* 1, 8-12.

⁶⁹ Lee A Bygrave, 'Data Minimization and the Purpose Limitation Principle' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020) 118-123.

⁷⁰ Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014) 214-216.

Record data for risk assessment purposes in the context of terrorism prevention.⁷¹ Although the case did not concern AI fairness testing directly, the Court stressed that large-scale automated profiling systems may generate discriminatory effects where algorithmic assessment criteria are insufficiently reliable or representative.⁷² The judgment illustrates that automated systems frequently depend on statistical categorization and behavioral prediction, but the data necessary to evaluate discriminatory impact may itself fall within the GDPR's stricter protection regime.

The requirement of "strict necessity" further narrows the scope of permissible processing. EU data protection law requires providers to demonstrate not only that fairness testing is useful, but also that the processing of sensitive data is genuinely necessary and that less intrusive alternatives are unavailable.⁷³ In practice, this creates difficult operational choices. If providers limit dataset diversity too aggressively in order to comply with data minimization obligations, the resulting model may fail to identify discriminatory outcomes across different population groups. Conversely, broader demographic testing may expose providers to claims that they processed sensitive data beyond what was strictly necessary for the stated purpose.

3.3.2 Data Representativeness and Data minimization

A second challenge concerns the tension between the AI Act's data quality requirements and the GDPR's principle of data minimization. Under Article 10(3) of the AI Act, high-risk AI systems must be trained on datasets that are relevant, representative, sufficiently complete, and free of errors.⁷⁴ The purpose of this requirement is to ensure that AI systems perform reliably across different population groups and do not produce discriminatory outcomes caused by gaps or imbalances in training data.⁷⁵

The GDPR adopts a different approach. Article 5(1)(c) requires personal data to be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".⁷⁶ Data minimization reflects the principle that individuals should not be exposed to unnecessary processing risks without a specific and proportionate justification. As a result, broader data collection, even where technically useful for improving AI performance, may be unlawful if it cannot be shown to be necessary for the relevant processing purpose.⁷⁷

This divergence reflects the different objectives of the two instruments. The AI Act approaches training data from a product safety perspective, under which representativeness becomes both a technical and legal requirement because

⁷¹ Case C-817/19 *Ligue des droits humains* EU:C:2022:491, paras 169–177.

⁷² *ibid* paras 195–197.

⁷³ European Data Protection Supervisor, 'Opinion 4/2021 on the Proposal for a Regulation laying down harmonised rules on artificial intelligence' (2021) paras 69–72.

⁷⁴ AI Act (n 1), art 10(3).

⁷⁵ Holtz and Ledendal (n 2), 17.

⁷⁶ GDPR (n 1), art 5(1)(c).

⁷⁷ Article 29 Working Party, 'Opinion 03/2013 on Purpose Limitation' (WP 203, 2 April 2013) 19–21.

insufficiently diverse datasets may produce discriminatory or unreliable outputs.⁷⁸ The practical consequences of inadequate representativeness can be seen in facial recognition systems trained predominantly on lighter-skinned male faces, which produced significantly higher error rates for women and darker-skinned individuals.⁷⁹ Similar concerns have also been identified in healthcare AI systems trained on datasets derived from limited population groups.⁸⁰

By contrast, the GDPR approaches personal data processing from the perspective of individual rights and informational self-determination.⁸¹ The principle of data minimization reflects concerns relating to profiling, behavioral monitoring, exclusion, and loss of control over personal information.⁸² The GDPR therefore does not assume that broader data collection automatically becomes lawful merely because it improves predictive accuracy or statistical representativeness.⁸³

This creates a practical dilemma for providers of high-risk AI systems. A credit-scoring model designed to test demographic bias may require datasets reflecting the diversity of the affected population in order to verify that particular groups are not systematically disadvantaged. However, collecting or retaining broader demographic data may conflict with the GDPR's requirement that processing remain limited to what is necessary for a specific purpose.⁸⁴ Similar tensions arise in healthcare AI systems, where broader datasets may improve diagnostic reliability but exceed what would ordinarily be permitted under the GDPR.⁸⁵

The GDPR does not require the absolute minimum quantity of data in all circumstances, but rather that processing remain proportionate to its purpose. However, neither the GDPR nor the AI Act clearly explains how this balance should be assessed in the context of AI training.⁸⁶ The EDPB has emphasized that data minimization applies throughout the lifecycle of AI systems, including the design and training stages, and that improving model quality does not justify unlimited data collection.⁸⁷ At the same time, it has not provided a clear standard for assessing necessity where representativeness and bias mitigation are involved.⁸⁸

The absence of a coordinated framework therefore creates significant compliance uncertainty. Providers who prioritize strict minimization may fail to satisfy the AI

⁷⁸ Mireille Hildebrandt, 'The Artificial Intelligence Act and the GDPR: Twins or Distant Relatives?' (2022) *Technology and Regulation* 1, 5.

⁷⁹ Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 *Proceedings of Machine Learning Research* 1, 8–11.

⁸⁰ Obermeyer Z, Powers B, Vogeli C, Mullainathan S, 'Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations' (2019) 366 *Science* 447.

⁸¹ Paul De Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 *Computer Law & Security Review* 179, 181–183.

⁸² Lee A Bygrave, 'Data Minimization and the Purpose Limitation Principle' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020) 56–60.

⁸³ Paul De Hert and Vagelis Papakonstantinou (n 85) 182.

⁸⁴ Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI' (2021) 41 *Computer Law & Security Review* 105567, 8–10.

⁸⁵ Nils Groschädl and Oliver Jaros, 'Legal Perspectives on the Use of Health Data in AI Systems under the AI Act and GDPR' (2024) 12 *Journal of European Public Policy* 1, 6.

⁸⁶ European Data Protection Board, 'Opinion 28/2024 on Personal Data Processing in AI Systems' (2024) 7–9.

⁸⁷ *ibid* 5.

⁸⁸ *ibid* 8.

Act's representativeness requirements, while those relying on broader datasets to improve representativeness risk infringing the GDPR.⁸⁹

3.3.3 Addressing the Conflicts: Practical and Interpretative Approaches

The two normal conflicts pointed out above are, one is the conflict between Article 9 of the GDPR and the provisions on bias detection in the AI Act, and the other is the conflict between the principle of data minimization and the representative requirements. There is no simple legal solution to these conflicts at present. Neither of these two regulations has clearly resolved the contradictions between each other, and there is no binding guidance to clearly inform service providers how to deal with conflicts between the two frameworks. Nevertheless, there are still a number of practical methods to help service providers deal with these conflicts more effectively, some of which have begun to be developed at the regulatory level.⁹⁰

3.3.4 A Staged Approach to Data Collection and minimization

The conflict between data representativeness and data minimization is harder to resolve through interpretation alone, because it reflects a genuine difference in regulatory purpose rather than a misalignment of terminology. Nevertheless, a staged approach to data collection offers a practical way to manage the tension without abandoning either requirement.⁹¹

Under this approach, the provider begins by defining the specific purpose of the AI system and the particular risks it is intended to address. The system is then trained on an initial dataset that is limited to what is clearly necessary for that purpose. Further data is collected only where testing reveals specific gaps, such as, where the system performs significantly less well for particular demographic groups, or where bias testing shows that the existing dataset does not adequately represent the population the system will affect.⁹² Each stage of data expansion is documented, so that providers can demonstrate to both Data Protection Authorities and Market Surveillance Authorities that each addition to the dataset was justified by a specific and identified need.⁹³

Functional separation of datasets can complement this approach. A similar approach has been discussed in regulatory guidance on AI governance, particularly where sensitive demographic data is processed exclusively for auditing and bias-testing purposes rather than for operational deployment.⁹⁴ Restricting access to fairness-testing datasets and separating them from core training environments may reduce unnecessary exposure to sensitive data while still allowing providers to evaluate discriminatory outcomes across different demographic groups. Data used exclusively for bias testing or representativeness checks should be kept distinct

⁸⁹ Holtz and Ledendal (n 2), 20.

⁹⁰ European Commission, 'Proposal for a Regulation amending Regulation (EU) 2024/1689 (Digital Omnibus Proposal)' COM(2025) 836 final, Explanatory Memorandum, 9–11.

⁹¹ European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (20 October 2020) 21–23.

⁹² GDPR (n 1) arts 5(1)(b)–(c), 25.

⁹³ Information Commissioner's Office, AI and Data Protection (2023) 22–24.

⁹⁴ Information Commissioner's Office, *AI and Data Protection Risk Toolkit* (ICO 2023) 45–48.

from the datasets used for core model training. Access to this additional data should be restricted to the personnel directly involved in the testing process, and the data should be deleted or anonymised once the testing phase is complete. This kind of functional separation reduces the overall risk associated with broader datasets while still allowing providers to satisfy the AI Act's requirement that bias be actively tested and corrected.⁹⁵ Wachter, Mittelstadt and Russell have identified functional separation of this kind as one of the few technically feasible ways to conduct meaningful fairness testing while limiting exposure under data protection law.⁹⁶

3.3.5 Integration of the DPIA and FRIA Processes

A further practical approach concerns the relationship between the DPIA and the FRIA. As noted before, the two assessments share a significant amount of analytical content. Rather than treating them as entirely separate procedures, providers can structure their compliance work so that the DPIA forms a foundational layer within the broader FRIA exercise. The data-specific analysis carried out for the DPIA provides information that is directly relevant to the FRIA's assessment of risks to non-discrimination, human dignity, and other fundamental rights.⁹⁷

This integrated approach does not eliminate either obligation. Article 35 GDPR and Article 27 of the AI Act each impose their own procedural and substantive requirements, and providers must ensure that both are met. However, the two assessments can be conducted using a shared analytical framework that avoids the reproduction of identical risk descriptions and mitigation measures in two separate documents. Where the DPIA already identifies, for example, a risk of discrimination arising from automated decision-making, that finding can be carried through directly into the FRIA rather than being reassessed from scratch.⁹⁸

The EDPB has acknowledged the possibility of coordinating DPIA and FRIA requirements and has called for joint guidance from the Commission and the data protection authorities on how the two assessments should interact in practice.⁹⁹ The 2025 Digital Omnibus Proposal similarly provides for the Commission to issue joint guidance on the application of the AI Act alongside GDPR obligations, which could eventually offer clearer direction on how the two impact assessments should be structured and how their outputs should relate to each other.¹⁰⁰

3.3.6 The Need for Regulatory Guidance and Coordinated Enforcement

The practical approaches described above depend to a significant extent on clear and consistent regulatory guidance. At present, neither the GDPR nor the AI Act

⁹⁵ Michael Veale and Reuben Binns, 'Fairer Machine Learning in the Real World: Mitigating Discrimination Without Collecting Sensitive Data' (2017) 8 *Big Data & Society* 1, 3–6.

⁹⁶ *ibid* 15–16.

⁹⁷ GDPR (n 1) art 35; Holtz and Ledendal (n 2) 13–14.

⁹⁸ EDPS (n 74), 7.

⁹⁹ European Data Protection Board, 'Statement 3/2024 on Data Protection Authorities' Role in the Artificial Intelligence Act Framework' (16 July 2024) 3.

¹⁰⁰ Digital Omnibus Proposal (n 56), art 1(5).

provides the level of specificity that providers need in order to navigate the conflicts between the two frameworks with confidence. The question of how “strict necessity” applies to bias detection, how necessity and representativeness should be balanced in training data decisions, and how the DPIA and FRIA should be structured in relation to each other all remain areas of significant uncertainty.¹⁰¹

As envisaged by the Digital Omnibus Proposal, joint guidelines from the European Commission and the EDPB could address several of these gaps. Guidelines on the meaning of “strict necessity” in the context of bias detection, on what safeguards are required under Article 4a, and on how the DPIA and FRIA can be structured to complement rather than duplicate each other would give providers a reliable framework for compliance. Importantly, such guidance does not require legislative change and can be issued relatively quickly in response to practical difficulties that are already emerging as the AI Act’s obligations come into effect.¹⁰²

Collaborative law enforcement between data protection agencies and market regulators is also crucial. When the same artificial intelligence system is subject to the review of the GDPR and the AI Act at the same time, different regulatory authorities carry out parallel investigations based on different legal standards, which may lead to inconsistent results and increase compliance costs without improving the level of protection accordingly. The EDPB has pointed out that cooperation between data protection agencies and other competent authorities is crucial for effective law enforcement in this area.¹⁰³ Developing a common procedure for the joint review of high-risk AI systems and developing a standardized document format that can be used by the two regulatory bodies will help reduce the risk of inconsistency in decision-making and make it easier for service providers to manage compliance processes.¹⁰⁴

None of the above methods can resolve the fundamental conflict between these two regulatory frameworks. The conflict between the data quality requirements of the AI Act and the data minimization principle of the GDPR, as well as the contradiction between the GDPR’s ban on sensitive data processing and the AI Act’s demand for data to ensure fairness, ultimately stem from these two laws. The original intention of the design is different. To achieve more fundamental coordination, it is necessary to amend legislation or formulate binding explanatory documents to clarify how the two frameworks should be interpreted in combination.¹⁰⁵ For example, through the clear provisions on AI training data in the GDPR. Before the relevant regulations are officially introduced, service providers need to manage the risks arising from operating under two regulatory systems at the same time in combination with prudent legal interpretation, perfect

¹⁰¹ Holtz and Ledendal (n 45), 21.

¹⁰² European Commission, Proposal for a Regulation amending Regulation (EU) 2024/1689 on Artificial Intelligence (Digital Omnibus Proposal) COM(2025) 836 final, Explanatory Memorandum 9–11.

¹⁰³ EDPB (n 11), 2.

¹⁰⁴ Herwig Hofmann, Gerard Rowe and Alexander Türk, *Administrative Law and Policy of the European Union* (OUP 2011) 376–382.

¹⁰⁵ Orla Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015) 64–68.

internal governance mechanisms and close communication with regulatory authorities.¹⁰⁶

3.4 Normative Gaps: The Inference Gap

In fact, this problem is evident in AI systems used for user portraits and predictive analysis. For example, the credit score system may use basic personal data such as age, employment status and repayment records to infer a person's "creditworthiness" or risk level. Although the input data is obviously within the scope of application of the GDPR, the legal status of the inferred risk score is not very clear, especially when it is regarded as an independent output result rather than the personal data itself.¹⁰⁷

There are similar problems in the recruitment system. Artificial intelligence tools may analyze resumes and behavioral data to predict candidates' "suitability" or "future performance". These predictions are not directly provided by individuals, but derived from the data model. Even so, they may still have a significant impact, such as leading to the exclusion of certain candidates from follow-up consideration. In this case, it becomes difficult to determine whether the existing GDPR safeguards are sufficient, especially when the inference results are difficult to trace back to specific data points.¹⁰⁸

This uncertainty is partly addressed through Article 22 GDPR on automated decision-making, which provides certain protections where decisions produce legal or similarly significant effects. However, Article 22 focuses on the decision itself rather than on the underlying inference process.¹⁰⁹ As a result, situations may arise where the inference is influential but does not formally qualify as a decision, leaving individuals with limited protection.

The judgment in SCHUFA holding illustrates both the potential and the limits of Article 22 GDPR.¹¹⁰ In that case, the Court of Justice held that the automated establishment of a probability value concerning a person's ability to meet payment obligations could fall within Article 22 where a third party such as a bank, draws strongly on that score when deciding whether to establish or implement a contractual relationship with the individual. A similar case is *Ligue des droits humains*, the Court claimed that the use of passenger name record data for automated risk assessment in the context of serious crime and terrorism prevention.¹¹¹ Although the case did not concern Article 22 GDPR directly, it shows that algorithmic risk indicators can affect individuals before any final legal decision is taken, especially where automated pre-screening influences subsequent human assessment.

¹⁰⁶ European Commission, Better Regulation Toolbox (2023) 415-419.

¹⁰⁷ Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) 2 *Columbia Business Law Review* 517-518.

¹⁰⁸ Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For' (2017) 16 *Duke Law & Technology Review* 32-37.

¹⁰⁹ GDPR (n1), art 22.

¹¹⁰ *ibid* 73.

¹¹¹ Case C-203/22 *Dun & Bradstreet Austria GmbH* EU:C:2024:1025, paras 54-58.

The AI Act does not fully resolve this issue. Although it requires risk management and data governance for high-risk systems, it does not clearly define how inferred data should be treated from a data protection perspective. This creates a gap between system-level regulation and individual-level rights, especially in cases where harm arises from probabilistic predictions rather than direct data processing.¹¹²

3.5 Institutional Fragmentation and Enforcement Coordination

3.5.1 Divergent Mandates and Philosophies of DPAs and MSAs

There is another regulatory gap in the GDPR and the Artificial Intelligence Act in the structure of law enforcement agencies. GDPR mainly relies on data protection agencies (DPAs), which monitor compliance with principles such as legality, proportionality, transparency and data minimization through mechanisms such as “one-stop” mechanisms and consistency procedures.¹¹³ By contrast, the AI Act follows the logic of EU product safety regulation and places supervision of high-risk AI systems in the hands of Market Surveillance Authorities (MSAs).¹¹⁴ These institutions work according to different legal authorizations and pursue different regulatory goals. DPAs mainly focus on the protection of personal rights arising from the processing of personal data, while MSAs are mainly responsible for conformity assessment, technical standards, risk management systems and product safety obligations.

This difference in system may lead to the same set of AI systems being evaluated from a completely different regulatory perspective. For example, a set of biometric or behavioral analysis systems, although may meet the technical requirements of the AI Act in terms of accuracy, data set governance and manual supervision, may also raise issues of concern to the GDPR, including legal basis, proportional principle, large-scale relevant safeguards for data retention and sensitive data processing.¹¹⁵ In *Digital Rights Ireland*, the European Court of Justice reviewed the EU Data Retention Directive, which requires telecommunications service providers to retain a large amount of communication metadata for law enforcement purposes. The court believes that the inadequacy of safeguards and supervisory mechanisms, the indiscriminate and large-scale retention of personal data will pose a particularly serious risk to privacy rights and data protection rights.¹¹⁶ Similarly, in *La Quadrature du Net*, the Court examined French legislation permitting extensive retention and access to communications data for national security purposes, stressing that broad and continuous data processing measures must remain proportionate and subject to strict safeguards under EU law.¹¹⁷ Although these cases did not concern AI systems directly, they illustrate the broader concern

¹¹² European Data Protection Board, ‘Opinion 28/2024 on Personal Data Processing in AI Systems’ (2024) 12.

¹¹³ GDPR (n 1), arts 56–65.

¹¹⁴ AI Act (n 2), arts 70–74.

¹¹⁵ GDPR (n 1), arts 5, 6 and 9; AI Act, arts 9–15.

¹¹⁶ Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd* EU:C:2014:238, paras 26–28, 37–39, 54–55.

¹¹⁷ Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net* EU:C:2020:791, paras 130–133, 168.

within EU law regarding large-scale automated processing and insufficiently coordinated oversight structures.

The fragmented nature of AI enforcement has already become visible in several regulatory investigations involving AI-driven systems. In 2023, the Italian Data Protection Authority temporarily restricted ChatGPT on the basis of GDPR concerns relating to transparency obligations, lawful basis, and the accuracy of generated personal data outputs.¹¹⁸ The investigation focused primarily on personal data processing rather than on the broader systemic or technical risks associated with generative AI systems. At the same time, discussions at EU level increasingly approached generative AI through the perspective of systemic risk, model governance, and AI safety obligations.¹¹⁹ These parallel supervisory approaches demonstrate how the same AI system may simultaneously fall within multiple regulatory frameworks without a fully integrated enforcement structure.

Similar coordination difficulties have appeared in relation to facial recognition technologies. Several European DPAs imposed sanctions and enforcement measures against Clear view AI for unlawfully scraping and processing biometric data from publicly accessible online sources in order to build a facial recognition database.¹²⁰ These investigations concentrated mainly on GDPR principles such as lawfulness, purpose limitation, and data minimization. However, many of the broader concerns associated with facial recognition systems, including discriminatory error rates, mass surveillance risks, and insufficient human oversight, also correspond to the type of fundamental rights and safety risks addressed by the AI Act's high-risk framework.¹²¹ Providers may therefore face overlapping supervisory expectations from different authorities applying different legal standards to the same operational system. Regulatory fragmentation has consequently become a practical compliance challenge for providers operating across several legal regimes simultaneously, leading to redundant regulatory burdens and legal uncertainty.

The divergence is reinforced by the procedural architecture of the two regimes. The GDPR contains relatively developed coordination mechanisms between national supervisory authorities, particularly through Chapter VII GDPR and the role of the European Data Protection Board.¹²² The AI Act adopts a more decentralized market-surveillance structure derived from EU product safety law, where enforcement practices may vary depending on national supervisory capacity and technical expertise. This creates a risk that providers operating across several Member States may encounter inconsistent enforcement approaches even where the same AI system and deployment context are involved. The Court's reasoning in *Facebook Ireland* further illustrates the complexity of cross-border supervisory competence within EU data protection law. The case concerned the competence of

¹¹⁸ Garante per la protezione dei dati personali, 'Temporary Limitation of the Processing of Italian Users' Data by OpenAI' (30 March 2023).

¹¹⁹ European Parliament Research Service, *Generative AI and EU Governance* (2024) 18–22.

¹²⁰ Commission nationale de l'informatique et des libertés (CNIL), 'Clearview AI Formal Notice' (16 December 2021).

¹²¹ Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 *Proceedings of Machine Learning Research* 1-2, 7-12.

¹²² GDPR, ch VII ('Cooperation and consistency').

national supervisory authorities to initiate enforcement proceedings in cross-border processing situations involving Facebook's operations across several Member States.¹²³ The judgment demonstrates how questions of institutional competence and coordination may themselves become sources of legal uncertainty within complex digital regulatory frameworks.

3.5.2 Regulatory Cooperations and Interaction Mechanisms

In practice, providers of high-risk AI systems are not dealing with a single regulator. A system may be assessed under the AI Act by a Market Surveillance Authority, while at the same time being reviewed under the GDPR by a Data Protection Authority. These parallel processes do not always align, especially where the same system is evaluated from different legal perspectives.

This becomes particularly visible in areas such as biometric identification or credit scoring. A system may satisfy the data governance and risk management requirements under the AI Act, while still raising concerns under the GDPR due to issues such as lack of a valid legal basis or excessive data processing. The absence of a structured coordination mechanism increases the likelihood of inconsistent outcomes.

The need for closer cooperation has already been recognized at EU level. The European Data Protection Board has noted that the effective application of data protection law in the context of AI depends on cooperation between competent authorities.¹²⁴ It has also highlighted that overlapping competences may lead to uncertainty if coordination is not ensured.¹²⁵ Similar concerns appear in guidance from the European Commission, where the interaction between different regulatory regimes is identified as a key challenge in the implementation of digital legislation.¹²⁶

One possible response is to introduce joint review procedures for high-risk AI systems involving personal data. Instead of separate assessments, authorities could coordinate their analysis at an earlier stage. Comparable models already exist in EU administrative practice, where different authorities cooperate in areas involving shared competences.¹²⁷ While this does not remove the distinction between legal regimes, it reduces the risk that the same system is subject to conflicting evaluations.

Another area concerns documentation. If providers are required to present risk assessments in a format that can be used by both Data Protection Authorities and Market Surveillance Authorities, this can simplify the review process. Standardised documentation has been identified as a useful tool in improving consistency across

¹²³ Case C-645/19 *Facebook Ireland Ltd v Gegevensbeschermingsautoriteit* EU:C:2021:483, paras 37–45, 54–63.

¹²⁴ European Data Protection Board, Statement 3/2024 on Data Protection Authorities' *Role in the AI Act Framework* (2024) 2.

¹²⁵ *ibid* 3.

¹²⁶ European Commission, 'Shaping Europe's Digital Future' COM(2020) 67 final, 4–7.

¹²⁷ Paul Craig, *EU Administrative Law* (3rd edn, OUP 2018) 424–428.

regulatory frameworks.¹²⁸ It also makes it easier for authorities to compare findings and identify potential conflicts at an early stage.

Furthermore, the operational intersection over AI-generated outputs requires an institutional consensus. While the substantive gap of inferred data is analyzed in Section 3.4, the institutional challenge lies in how DPAs and MSAs handle these outputs administratively. Without institutional cooperation mechanisms, an MSA might clear a high-risk system's output risk profile based on technical documentation, while a DPA could simultaneously flag the resulting automated inferences as non-compliant with data subject rights. This procedural friction emphasizes that regulatory alignment cannot be achieved through legislative texts alone, but requires operational interplay.

Finally, coordination can be supported through joint interpretative guidance. Joint guidelines issued by the EDPB and the newly established AI Office or national MSAs can help clarify how the GDPR and the AI Act should be applied in parallel. This type of guidance has already been suggested as a way to address uncertainty in AI regulation. It does not require legislative change, but it can significantly influence how both authorities and providers approach compliance in practice, thereby bridging the institutional fragmentation.

¹²⁸ European Commission, Proposal for a Regulation on Artificial Intelligence COM(2021) 206 final, Explanatory Memorandum, 13.

4 Conclusion

4.1 Summary of Research Findings

This thesis has adopted a legal-dogmatic methodology to systematically examine the regulatory frictions arising from the parallel application of the GDPR and the AI Act to high-risk AI systems, and provided precise answers to the three core research questions.

In response to Research Question 1, this study confirms that the DPIA under Article 35 GDPR and the FRIA under Article 27 AI Act are functionally overlapping and hierarchically structured. The DPIA, which focuses on risks to personal data protection, constitutes a substantive subset of the broader FRIA, which covers a full spectrum of fundamental rights. This structural overlap results in significant procedural duplication, administrative inefficiency, and the risk of formalistic compliance, especially where the data controller and the deployer are separate legal entities. Although both assessments serve *ex ante* risk mitigation, their separate procedural requirements and responsible actors create unnecessary compliance burdens without enhancing protection.

In response to Research Question 2, the divergence between the data minimisation principle under Article 5(1)(c) GDPR and the requirement for representative, unbiased training data under Article 10 AI Act constitutes a genuine normative conflict, rather than a mere regulatory divergence. The two principles impose contradictory operational demands: the GDPR restricts data collection to what is strictly necessary, while the AI Act requires sufficiently diverse and complete datasets to ensure fairness and safety. A second normative conflict exists between the general ban on processing sensitive personal data under Article 9 GDPR and the functional need to use such data for bias mitigation under the AI Act. The 2025 Digital Omnibus Proposal introduces a limited exception in new Article 4a to alleviate this tension, but it does not provide a definitive and durable legal resolution.

In response to Research Question 3, addressing the normative gap of AI inferences, this thesis finds a functional protection vacuum in system outputs. AI-generated inferences, such as credit probability scores or behavioural risk predictions, frequently escape Article 22 GDPR when they only "significantly influence" rather than finalise decisions, while remaining unregulated by the AI Act's system-level mandate. This leaves individual data subjects vulnerable to automated algorithmic classifications without clear regulatory recourse.

In response to Research Question 4, splitting between DPAs and MSAs significantly deepens this regulatory vacuum. Because these authorities operate under divergent legislative mandates—rights-centric versus product-safety-centric—without binding joint procedures, a high-risk AI system faces the risk of inconsistent supervisory outcomes. To remedy this fragmentation, the thesis concludes that the institutional gap must be bridged through formal cooperation

mechanisms, such as joint review procedures, shared assessment templates, and unified regulatory guidance as foreshadowed by recent EU proposals.

Beyond direct responses to the research questions, this thesis reflects that the fundamental source of regulatory frictions lies in the divergent normative philosophies of the two frameworks: the GDPR adopts a rights-based, data-centric approach, whereas the AI Act follows a safety-centred, system-oriented governance model. Practical reconciliation demands an integrated FRIA-led assessment framework, a staged data collection strategy that reconciles representativeness and minimization, and enhanced inter-institutional cooperation through joint guidelines and coordinated enforcement. The 2025 Digital Omnibus Proposal, while marking a progressive step, ultimately represents a piecemeal solution; durable legal certainty requires not merely exceptions but a more fundamental, long-term legislative alignment of the two frameworks' core principles.

4.2 Research Value

This work speaks to an urgent gap, both in theory and in practice, within EU AI and data governance.

On the theoretical side, it puts together a coherent analytical picture of how the GDPR and the AI Act interact. It spells out the hierarchical logic of dual impact assessments, marks the core boundaries of normative conflicts, and digs into the root causes of institutional fragmentation. By doing so, it fills a hole in the literature where systematic studies on the GDPR-AI Act synergy are still thin, giving later research a solid base to build on when looking at EU AI regulatory coordination.

On the practical side, the thesis offers something concrete for AI providers, regulators, and policymakers. For providers, it suggests integrated DPIA-FRIA documentation strategies and staged data collection models that can lighten the compliance load while still meeting both sets of requirements. For regulators, it pushes for joint DPA-MSA coordination mechanisms and unified interpretative guidance – something the Digital Omnibus Proposal already points towards – which would help sweep away legal uncertainty and make enforcement smoother. For policymakers, it underlines why targeted legislative tweaks are needed to bring conflicting norms into alignment, backing the EU's wider goal of balancing AI innovation with fundamental rights protection.

4.3 Research Limitations

Even with its systematic approach, the thesis carries three main limitations.

First, the method is purely legal-dogmatic. There is no empirical data on what compliance actually costs. While the study spots administrative duplication and the risk of formalistic compliance, it does not put a number on the real-world burden

for high-risk AI providers in different sectors – healthcare, finance, and so on – which takes some weight out of the practical recommendations.

Second, the analysis sticks to the regulatory framework as it stands now, without mapping out what might shift after implementation. The 2025 Digital Omnibus Proposal is still being hammered out in trilogue negotiations; its final shape and how it will be enforced are still up in the air. The recommendations here are therefore based on draft texts and may need a rethink once the text is formally adopted.

Third, the study keeps its eyes only on the EU regulatory system. It does not bring in comparative analysis with other jurisdictions – for instance, the UK’s AI regime or the US AI Bill of Rights. That limits how far the findings can travel in global AI governance debates.

4.4 Future Research Outlook

Building on what this study has found and keeping its limitations in mind, future work could push forward in three main directions.

First, empirical compliance research would be valuable – putting numbers on the administrative drag caused by dual assessments and testing how well integrated compliance strategies work across different high-risk AI sectors. That sort of data-driven evidence could really anchor regulatory reform.

Second, following up on the implementation of the 2025 Digital Omnibus Proposal would be a natural next step. Researchers could dig into how the new Article 4a and the joint guidance provisions actually sort out the sensitive data conflicts and bring DPIA-FRIA requirements into line, and look at how enforcement coordination between DPAs and MSAs plays out on the ground.

Third, widening the lens to cross-jurisdictional comparisons on AI data governance would make sense. Putting the EU’s dual regulatory model side by side with other frameworks could pull out universal lessons on how to strike a balance between AI innovation and privacy protection on a global scale.

References

Official documents

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) [2016] OJ L119/1.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L2024/1689.

European Commission

European Commission, 'Proposal for a Regulation amending Regulation (EU) 2024/1689 on Artificial Intelligence (Digital Omnibus Proposal)' COM(2025) 836 final.

European Commission, Better Regulation Toolbox (2023).

European Commission, 'Shaping Europe's Digital Future' COM(2020) 67 final.

European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (20 October 2020).

European Data Protection Board and Article 29 Working Party

European Data Protection Board, Statement 3/2024 on Data Protection Authorities' Role in the Artificial Intelligence Act Framework (16 July 2024).

European Data Protection Board, Opinion 28/2024 on the Application of the GDPR to Artificial Intelligence Systems (17 December 2024).

European Data Protection Supervisor

European Data Protection Supervisor, Opinion 4/2021 on the Proposal for a Regulation laying down harmonised rules on artificial intelligence (2021).

Other official and institutional materials

Commission nationale de l'informatique et des libertés (CNIL), Clearview AI Formal Notice (16 December 2021).

Garante per la protezione dei dati personali, Temporary Limitation of the Processing of Italian Users' Data by OpenAI (30 March 2023).

Information Commissioner's Office, AI and Data Protection (2023).

European Parliament Research Service, Artificial Intelligence Act: Overview (2024).

Literature

Monographs

Craig P and De Búrca G, *EU Law: Text, Cases, and Materials* (5th edn, Oxford University Press 2011).

Fuster GG, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014).

Hofmann H, Rowe G and Türk A, *Administrative Law and Policy of the European Union* (OUP 2011).

Kofler G and others (eds), *Tax Treaty Interpretation in Light of the Vienna Convention on the Law of Treaties* (Wolters Kluwer 2024).

Lynskey O, *The Foundations of EU Data Protection Law* (OUP 2015).

Smits JM, 'What is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research' in Rob van Gestel, Hans-W Micklitz and Edward L Rubin (eds), *Rethinking Legal Scholarship: A Transatlantic Dialogue* (Cambridge University Press 2017).

Valentini C and Marques T (eds), *Collective Action, Philosophy and Law* (Routledge 2021).

Articles

Buolamwini J and Gebru T, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 *Proceedings of Machine Learning Research* 1.

Bygrave LA, 'Data Minimization and the Purpose Limitation Principle' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020).

De Hert P and Papakonstantinou V, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 *Computer Law & Security Review*.

Demetzou K, 'Data Protection Impact Assessment: A Tool for Accountability and the Unclear Concept of "High Risk" in the General Data Protection Regulation' (2019) 35 *Computer Law & Security Review*.

Edwards L and Veale M, 'Slave to the Algorithm? Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For' (2017) 16 *Duke Law & Technology Review*.

Groschädl N and Jaros O, 'Legal Perspectives on the Use of Health Data in AI Systems under the AI Act and GDPR' (2024) 12 *Journal of European Public Policy*.

Gruchala P, Nicosia L and Zięciak M, 'Harmonising Risk Assessments for High-Risk AI Systems under the GDPR and the AI Act' (2025) 7(4) *Journal of Data Protection & Privacy*.

Gudepu BK and Eichler R, 'The Role of AI in Enhancing Data Governance Strategies' (2024) *International Journal of Acta Informatica*.

Hildebrandt M, 'The Artificial Intelligence Act and the GDPR: Twins or Distant Relatives?' (2022) *Technology and Regulation*.

Holtz HM and Ledendal J, 'AI Data Governance – Overlaps between the AI Act and the GDPR' (2026) 17(1) *Law, Innovation and Technology*.

Kuner C and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020).

Lenaerts K and Gutiérrez-Fons JA, 'To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice' (2014) 20 *Columbia Journal of European Law*.

Mantelero A, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, Legal Obligations and Key Elements for a Model Template' (2024) 54 *Computer Law & Security Review*.

Musch S, Borrelli MC and Kerrigan C, 'Bridging Compliance and Innovation: A Comparative Analysis of the EU AI Act and GDPR for Enhanced Organizational Strategy' (2024) 7(1) *Journal of Data Protection & Privacy*.

Novelli C and others, 'A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities' (2024) 15 *European Journal of Risk Regulation*.

Novelli C and others, 'Taking AI Risks Seriously: A New Assessment Model for the AI Act' (2024) 39 *AI & Society*.

Raji ID and Buolamwini J, 'Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products' (2019) *AAAI/ACM Conference on AI Ethics and Society*.

Tamburri DA, 'Design Principles for the General Data Protection Regulation (GDPR): A Formal Concept Analysis and Its Evaluation' (2020) 91 *Information Systems*.

Veale M and Binns R, 'Fairer Machine Learning in the Real World: Mitigating Discrimination Without Collecting Sensitive Data' (2017) 8 *Big Data & Society*.

Wachter S and Mittelstadt B, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) 2 *Columbia Business Law Review*.

Wachter S, Mittelstadt B and Russell C, 'Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI' (2021) 41 *Computer Law & Security Review*.

Yablonsky SA, 'Multidimensional Data-Driven Artificial Intelligence Innovation' (2019) 9(12) *Technology Innovation Management Review*.

Case law

Case C-634/21 *SCHUFA Holding AG* EU:C:2023:957.

Case C-817/19 *Ligue des droits humains* EU:C:2022:491.

Case C-203/22 *Dun & Bradstreet Austria GmbH* EU:C:2024:1025.

Case C-645/19 *Facebook Ireland Ltd v Gegevensbeschermingsautoriteit* EU:C:2021:483.

Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd* EU:C:2014:238.

Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net* EU:C:2020:791.

Case C-300/21 *Österreichische Post* EU:C:2023:370.