Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

European Union Law Working Papers

No. 153

Innovation under a Dual Regulatory Burden? The Interplay of the EU Artificial Intelligence Act and the General Data Protection Regulation: Regulatory Overlaps, Conflicts, and Compliance Challenges for AI Systems

Timo Tutschek

2026

European Union Law Working Papers

Editors: Siegfried Fina and Roland Vogl

About the European Union Law Working Papers

The European Union Law Working Paper Series presents research on the law and policy of the European Union. The objective of the European Union Law Working Paper Series is to share "works in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The working papers can be found at http://ttlf.stanford.edu.

The European Union Law Working Paper Series is a joint initiative of Stanford Law School and the University of Vienna School of Law's LLM Program in European and International Business Law.

If you should have any questions regarding the European Union Law Working Paper Series, please contact Professor Dr. Siegfried Fina, Jean Monnet Professor of European Union Law, or Dr. Roland Vogl, Executive Director of the Stanford Program in Law, Science and Technology, at:

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Timo Tutschek is an Austrian entrepreneur who works in public relations, marketing, and information technology, in fields in which AI-based tools have become an integral part of daily operations. He is pursuing a bachelor's degree in "International Legal Studies" at the University of Vienna's Faculty of Law. His first-hand experience with the increasing complexity and opacity of legal compliance in AI usage motivated the topic of this thesis.

General Note about the Content

The opinions expressed in this student paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum, or any of TTLF's partner institutions, or the other sponsors of this research project.

Suggested Citation

This European Union Law Working Paper should be cited as:
Timo Tutschek, Innovation under a Dual Regulatory Burden? The Interplay of the EU Artificial Intelligence Act and the General Data Protection Regulation: Regulatory Overlaps, Conflicts, and Compliance Challenges for AI Systems, Stanford-Vienna European Union Law Working Paper No. 153, http://ttlf.stanford.edu.

Copyright

© 2026 Timo Tutschek

Abstract

This thesis argues that applying the GDPR and the EU AI Act concurrently to AI systems creates a dual regulatory burden, but not irreconcilable conflicts often feared. Whenever an AI system processes personal data, both regimes apply: the GDPR as a rights-based data protection law and the AI Act as a risk-based product safety law. Since the AI Act leaves the GDPR unaffected, except for two narrow exceptions, and neither is a lex specialis, the two operate cumulatively and in parallel. Applying a conflict-of-norms framework that distinguishes between harmonious overlaps, pre-resolved tensions, actual tensions, and genuine conflicts, this thesis examines each point of contact between the two regimes. No genuine conflicts emerge: simultaneous compliance is always possible, and the residual friction takes the form of tensions, concentrated where the AI Act's acceptance of residual risk meets the GDPR's non-disposable rights. The available interface clauses and contractual tools make the burden manageable rather than prohibitive. However, many interpretational uncertainties remain unsolved.

Table of Content

List of Abbreviations 4

CHAPTER I: INTRODUCTION 6

CHAPTER II: THE REGULATORY BASIS 6

II.1. EU AI Act 6

II.2. General Data Protection Regulation 7

CHAPTER III: MAPPING THE OVERLAPS 7

III.1. Scope of Application 7

III.1.1. Territorial Scope 8

III.1.2. Temporal Scope 8

III.1.3. Material Scope 9

III.2. Role Actor Relation 15

III.3. Relation between the Regulations 16

III.4. Normative Overlaps 16

III.4.1. Transparency and Disclosure 16

III.4.2. Safeguards and Human Involvement 17

III.4.3. Data Quality and Governance 17

III.4.4. Accuracy 17

III.4.5. Documentation and Traceability 17

III.4.6. Risk Protection and Prevention by Design and by Default 18

III.4.7. Reporting Duties 18

III.4.8. Overview Table 19

III.5. Express Interface Clauses 19

III.5.1. Special Category Processing 20

III.5.2. Anti-Duplication Bridge 20

III.5.3. Compliance 21

III.5.4. Explanation of Decisions 21

III.6. Concurrently Applicable 22

III.6.1. Legal Basis and Lawfulness *23*

III.6.2. Data-Subject Rights *23*

III.6.3. International Transfers *24*

CHAPTER IV: TENSIONS AND CONFLICTS 24

IV.1. Analytical Framework 24

IV.2. AI Act Data Requirements vs GDPR Data-Processing Principles 26

IV.2.1. Purpose Limitation vs Model Re-Use and GPAI *26*

IV.2.2. Storage Limitation vs Retention and Logging *27*

IV.2.3. Accuracy and Erasure vs Trained Models *28*

IV.3. Art 10(5) AI Act vs Art 9 GDPR 30

IV.4. Automatic Decisions 31

IV.5. Transparency and Explanation 33

IV.6. Role Mismatch 35

IV.7. Enforcement 36

IV.8. Interim Conclusion 37

CHAPTER V: COMPLIANCE 38

V.1. The Double Regulatory Burden 38

V.2. Impact Assessments: DPIA and FRIA 38

V.3. Data Governance and Lawful Basis 39

V.4. Transparency and Explanation 40

V.5. Role Allocation and Contracts 41

V.6. Enforcement Exposure and Coordination 42

V.7. Takeaways 44

VI. CONCLUSION 44

BIBLIOGRAPHY 46

DISLCAIMER

Use of artificial intelligence. *In the course of preparing this thesis, AI-based tools were used as an aid for research, brainstorming, structuring of ideas, grammatical and linguistic correction, and stylistic enhancement. All AI-assisted output was critically examined, verified against the underlying primary and secondary sources, and revised by the author. The substance of this thesis — its analysis, arguments, and conclusions — is my own, and I assume full responsibility for the entire text, including any passages refined with the assistance of such tools.*

Gender-inclusive language. *For ease of reading, gender-specific terms are used in this thesis. Any such term is to be understood as referring to persons of all genders equally; where only one gender form is mentioned, all genders are addressed without distinction.*

List of Abbreviations

A

AI Artificial Intelligence

AI Act Artificial Intelligence Act (Regulation (EU) 2024/1689)

Art Article

B

BYIL British Yearbook of International Law

C

CFR Charter of Fundamental Rights of the European Union

CJEU Court of Justice of the European Union

D

DPA Data Protection Authority

DPIA Data Protection Impact Assessment

E

ECLI European Case Law Identifier

EDPB European Data Protection Board

EDPS European Data Protection Supervisor

EEA European Economic Area

eg for example

ELI European Economic Area

EU European Union

F

FRIA Fundamental Rights Impact Assessment

G

GDPR General Data Protection Regulation (Regulation (EU) 2016/679)

GPAI General-Purpose AI

I

ISO International Organization for Standardization

ie that is

IEC International Electrotechnical Commission

M

ML Machine Learning

O

OJ Official Journal of the European Union

T

TFEU Treaty on the Functioning of the European Union

Chapter I: Introduction

Artificial intelligence has become part of everyday economic and administrative life, and the systems behind it frequently rely on personal data. Where they do, two instruments apply at the same time: the GDPR and the AI Act. This raises the question to what extent the two regimes create regulatory overlaps and normative conflicts, and what compliance challenges arise from their concurrent application to AI systems. The following chapters address that question as a matter of Union law as it currently stands.

Chapter II: The Regulatory Basis

II.1. EU AI Act

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 2024/1689 ('AI Act'), was adopted in response to the rapid development of artificial intelligence and attendant risks, which called for a dedicated regulatory framework. The AI Act follows a product safety approach, broadly modelled on the EU's product safety legislation. Accordingly, it establishes distinct risk categories and calibrates the stringency of its requirements according to the risk category at issue. As yet, the AI Act does not apply in full. Its provisions become applicable in successive stages, with the general date of application on 2 August 2026, and the requirements for high-risk systems under Article 6(1) following on 2 August 2027 — the application milestone under Article 113. Certain transitional regimes extend further still: under Article 111, legacy high-risk systems used by public authorities must be brought into compliance by 2 August 2030, and AI components of the large-scale IT systems listed in Annex X by 31 December 2030.

II.2. General Data Protection Regulation

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 ('GDPR') is the central legislative instrument governing the protection of personal data at the Union level. It has been applied since 25 May 2018 and has since become an everyday consideration wherever personal data are processed, from collection and storage through retention and use. At its core, the GDPR is fundamental rights legislation: rooted in the right to the protection of personal data under Article 8 of the Charter and Article 16 TFEU, it seeks to safeguard the rights and freedoms of data subjects and adopts a rights-based approach that confers directly enforceable rights on individuals.

CHAPTER III: MAPPING THE OVERLAPS

III.1. Scope of Application

The two regimes are anchored in structurally different regulatory objects. The GDPR governs processing activity: it applies to the 'processing of personal data wholly or partly by automated means' and to non-automated processing forming part of a filing system.[1]

[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) .

By contrast, the AI Act governs a product, the 'AI system' or 'general-purpose AI model'. The definition in Art 3 (1) AI Act is open-textured, and in the absence of CJEU case law, its contours rest principally on the Commission's interpretive guidance.[2]

III.1.1. Territorial Scope

With respect to territorial application, both Regulations pursue a similar but not identical approach. While the GDPR connects either to the controller's or processor's establishment in the Union or to the processing of data subjects in the Union where the controller targets that market or monitors behaviour there, the AI Act relates to the placing on the market or putting into service within the Union, the establishment within the Union, the use of the output of an AI system within the Union by providers or deployers in third countries, and if persons are affected within the Union irrespective of where the system was deployed.[3] Therefore, the applicability depends on the place of the market or based on the impact of an AI system.[4]

The AI Acts' output-based extraterritorial trigger is therefore broader than that of the GDPR, since the latter requires either a targeted offer of goods or services or the monitoring of behaviour in the Union.[5]

III.1.2. Temporal Scope

The two regulations also differ in their temporal reach. The GDPR has been fully applicable since 25 May 2018.[6] By contrast, the AI Act applies in upcoming stages[7] During the transition window, data controllers therefore operate under a fully-

[2] European Commission, *Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act)*, 2025)
[3] Art 3(1) – (2) GDPR); Art 2(1) (a) – (c), (g) AI Act.
[4]Stefan Gutbrunner, 'AI Act – Anwendungsbereich in zeitlicher und räumlicher Hinsicht' (2026) <lexis360.at> accessed 19 May 2026.
[5] Art 3(2) GDPR.
[6] Art 99 GDPR.
[7] See Chapter II.1. above.

applicable data-protection regime and an only partly-applicable AI-specific regime, which itself produces a layer of compliance complexity that is examined in Chapter IV.

III.1.3. Material Scope

An overlap in material scope arises where the triggering conditions of both the AI Act and the GDPR are met. These conditions are, first, the qualification of a system as an AI system within the meaning of the AI Act and, second, the classification of the data processed as personal data under the GDPR. Parallel application is only possible when both conditions are satisfied.

III.1.3.1. Definition of AI System

The definition of an AI system delimits the entire scope of application, yet it is hard to draw and remains unclear. It is set out in Art 3(1) AI Act and comprises seven elements, deliberately imprecise so as to preserve flexibility:

AI system 'means a

1. **machine-based system** that is
2. designed to operate with varying levels of autonomy and
3. that may exhibit adaptiveness after deployment, and
4. that, for explicit or implicit objectives,
5. infers, from the input it receives,
6. how to generate outputs such as predictions, content, recommendations, or decisions
7. that can influence physical or virtual environments".[8]

[8] Art 3 (1)(f) AI Act.

Under Art 96(1) AI Act the Commission issued interpretative guidelines on 6 February 2025; they are a central aid but non-binding, so authentic interpretation still rests with the CJEU.[9]

The guidelines are detailed and presuppose both technical and legal understand, and Recitals 12 and 13 AI Act add only vague further guidance. No ruling yet addresses the definition directly; pending cases may not resolve it, as the CJEU may treat the elements as satisfied where uncontested or touch them only in *obiter*, though any judgement will at least indicate how it approaches the AI Act.

III.1.3.1.1 'Machine-based System'

'Machine-based' is broader than it sounds: the Commission treats it as any system providing computational capacity, so even biological or other on-traditional computing systems may qualify.[10]

Hardware (the infrastructure for computation, eg disks) is distinguished from software, which 'handles how the hardware processes data and performs tasks'.[11]

III.1.3.1.2. Autonomy

Autonomy is understood broadly and admits varying levels;[12] it requires at least some independence from human involvement. A system that merely executes a predetermined, exactly specified task is not autonomous, since it operates entirely as designed by humans — for instance a complex spreadsheet computing a value from set inputs.[13] Only systems operating with full human involvement are excluded.[14]

[9] Commission Guidelines (n 2): I.7.
[10] Commission Guidelines (n 2): II.1.
[11] Commission Guidelines (n 2): II.1.11.
[12] Recital 12 AI Act.
[13] Commission Guidelines (n 2): II.2.
[14] Commission Guidelines (n 2): II.2.17.

Autonomy is therefore established once any part of the system is not exactly specified by a human or produces output not fully controlled by human intervention; it is assessed materially, independently of the technique used, and the Commission's distinction between direct and indirect human involvement implies that even indirect involvement, through delegation or supervision, presupposes some autonomous output.[15]

III.1.3.1.3. Adaptiveness

Adaptiveness is the capacity for self-learning after deployment – automatic learning, discovering new patterns, or identifying relationships beyond the initial training set.[16] Following the ELI, the Commission distinguishes fixed models, fixed models with updates, and self-optimising models, the last marked by going beyond what the system was initially trained on;[17] the ELI further requires adaptation to be goal-oriented, the system using retained knowledge to improve itself toward a determined goal.[18] In practice the element carries little weight, since the 'may' in Art 3(1) AI Act makes adaptiveness merely indicative.

III.1.3.1.4. AI system objectives

An AI system must pursue one or more objectives, whether explicitly encoded by developers or implicitly deduced from its behaviour, training data, or interactions.[19] The distinction is largely one of perspective and of limited practical relevance: the wording makes clear that the Act applies even absent an explicit objective,[20] closing gaps that well-advised actors might otherwise exploit. The objective is internal and

[15] Ibid.
[16] Commission Guidelines (n 2): II.3.23.
[17] European Law Institute, *The concept of 'AI system' under the new AI Act: Arguing for a Three-Factor Approach*, 2024): III.3.b.
[18] ELI (n 17): III.3.a.
[19] Commission Guidelines (n 2): II.4.25.
[20] ELI (n 17): III.4.a.

need not equal the intended purpose;[21] under Art 3(12) AI Act the latter is 'the use for which an AI system is intended by the provider', ie external.[22]

Objectives are thus best read as algorithmic objectives, explicit or implicit. [23]

III.1.3.1.5. Inference

Inference is the hardest element to delimit. Merely generating output does not suffice where the rules are wholly defined by natural persons, even if the process is automated.[24] Were inference limited to deriving models from data, the AI Act would barely reach most ML systems, which cannot derive such model after deployment.[25]

The Commission therefore slits inference into a 'building phase', where models or algorithms are derived from input, an a 'use phase', where outputs are generated from input.[26] For 'input' it adopts the ISO/IEC 22989 notion of inference as 'reasoning by which conclusions are derived from known premises', premises being 'either a fact, a rule, a model, a feature, or raw data'.[27]

A system thus infers if, in development or after deployment, AI techniques let it derive models or algorithms from such premises and, at least in the use phase, generate outputs from inputs without rules exactly pre-specified by a person.[28] The relevant techniques — machine-learning and logic- and knowledge-based approaches — are both covered.[29] Inference may nonetheless fail where the system's capacity for

[21] AI Act Recital 12
[22] Commission Guidelines (n 2).
[23] ELI (n 17): III.4.c.
[24] Commission Guidelines (n 2): II.5.26.
[25] ELI (n 17): III.5.a.
[26] Commission Guidelines (n 2): II.5.27-28.
[27] Commission Guidelines (n 2): II.5.27; ISO/IEC 22989:2022.
[28] Commission Guidelines (n 17): II.5; ISO/IEC 22989:2022; ELI (n 17): III.5.
[29] Commission Guidelines (n 2): II.5.1.

autonomous analysis and output-adjustment is too limited, even if it can infer narrowly.[30]

III.1.3.1.6. Outputs that can influence physical or virtual environments

There are types of output where at least one of them must be generatable by the system to become an AI system. Another characteristic of these outputs is that the AI system can handle complex relationships and patterns that it learned while training or by using expert-defined rules, leading to more sophisticated reasoning within structured environments.[31]

III.1.3.1.7. Classification as High-Risk AI System

High-risk classification triggers numerous additional obligations. Art 6 AI Act sets the rules, combining the enumerated Annex III use-cases with exceptions, so that listing does not automatically entail high-risk status. Three overlap scenarios follow — no overlap, full overlap, and high-risk only overlap — and distinguishing them matters, since the applicable regime depends on the classification rather than on any single across-the-board rule. There are two routes to high-risk status: the Annex I route, for products or safety components covered by the Union harmonisation legislation listed in Annex I,[32] and the Annex III route, for the enumerated high-risk use-cases;[33] by derogation, an Annex III system falls outside the category where Art 6(3) AI Act is met, the provider then bearing documentation and registration duties.[34]

III.1.3.1.8. Interpretative Remarks

The Guidelines aid interpretation but leave much open. The imprecise wording is arguably necessary in a fast-moving field, where over-rigid interpretation would create

[30] Commission Guidelines (n 2): II.5.2.41.
[31] Commission Guidelines (n 2): II.5.2.59.
[32] Art 6(1) AI Act.
[33] Art 6(2) AI Act.
[34] Art 6 (4) AI Act.

regulatory gaps; the price is legal uncertainty, and until the CJEU rules on the point, the foregoing remains provisional.

III.1.3.2. Definition of Personal Data

Pursuant to Art 4 (1) GDPR 'personal data" is defined as

'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person'.

The definition of personal data under the GDPR pursues a broad understanding. The CJEU reads 'any information relating to an identified or identifiable natural person" expansively.[35] The CJEU confirmed that subjective personal data, such as opinions or assessments, may constitute personal data provided that they relate to the data subject by reason of content, purpose, or effect of the information.[36]

Identifiability is established as soon as there exist 'means reasonably likely to be used either by the controller or by another person"[37] to identify an individual.[38]

This does not mean that any additional information capable of enabling identification must be taken into account; rather, it suffices that the risk of identification appears, in practice, to be significant. It also follows that the same data may constitute personal data for one actor while falling outside the category for another — a situation that

[35]*Peter Nowak v Data Protection Commissioner* ECLI:EU:C:2017:994 (Court of Justice of the European Union).
[36]*European Data Protection Supervisor v Single Resolution Board* ECLI:EU:C:2025:645 (Court of Justice of the European Union);*Peter Nowak v Data Protection Commissioner*, paras 34–35.
[37]*Patrick Breyer v Bundesrepublik Deutschland* ECLI:EU:C:2016:779 (Court of Justice of the European Union), para 43.
[38]Ibid, para 42; Recital 26 Directive 95/46.

arises, in particular, where the data have been pseudonymised (asymmetry of data classification).[39]

The expansive understanding of personal data gives rise to significant difficulties in the context of training AI systems, as data that appear non-personal may in fact constitute personal data.[40]

III.2. Role Actor Relation

The GDPR's roles are functional and processing-centric; they attach to a specific processing operation and turn on who decides why and how personal data are processed: controller,[41] processor,[42] and joint controllers.[43]

The AI Act's roles are product safety and supply chain roles: they attach to the AI system's lifecycle position, regardless of whether personal data are involved — provider, deployer, importer, distributor, and authorised representative, with 'operator" as the umbrella term for all.

The mismatch that will be exploited later: an AI Act role attaches to the system, but a GDPR role attaches to each processing operation. Therefore, one legal person commonly wears two hats at once — different GDPR hats for different operations of the same system (eg, provider is the controller for training, and deployer is the controller for deployment). The AI Act expressly assumes this dual-hat reality rather than displacing it: Recital 10 states that the Act 'does not affect the obligations of providers and deployers of AI systems in their role as data controllers or processors,'

[39] Ibid, paras 45–46;*European Data Protection Supervisor v Single Resolution Board.*
[40]*European Data Protection Supervisor v Single Resolution Board.*
[41] Art 4(7) GDPR.
[42] Art 4(8) GDPR.
[43] Art 26 GDPR.

and Art 2(7) AI Act confirms that it 'shall not affect' the GDPR. Therefore, the two role sets run in parallel on the same actors.

This means that the GDPR and the AI Act allocate roles on different axes — processing function versus supply-chain position — so the same actor is typically a GDPR controller/processor and an AI Act operator simultaneously, which is the structural reason the substantive obligations overlap.

III.3. Relation between the Regulations

Under Article 2(7) AI Act, Union data-protection law applies to personal data processed in connection with the Regulation, and the AI Act 'shall not affect" the GDPR, save for Articles 10(5) and 59 AI Act.[44] It thus furnishes no general legal basis for processing, which must still be found in the GDPR.[45]

Neither instrument therefore operates as a general *lex specialis* displacing the other: the wo apply cumulatively and in parallel, giving rise to a double regulatory burden.[46]

III.4. Normative Overlaps

III.4.1. Transparency and Disclosure

Both regimes impose information obligations, but with different addressees. Article 13 of the AI Act requires high-risk AI systems to be sufficiently transparent for their deployers and to be accompanied by instructions for use directed at them, whereas Articles 13 and 14 of the GDPR require the controller to inform the data subject. The two sets of obligations stack rather than substitute for one another.

---

[44] Art 2(7), Recital 10 AI Act.
[45] Recital 140 AI Act; Hajo Michael Holtz and Jonas Ledendal, 'AI data governance – overlaps between the AI Act and the GDPR' (2026) 18 Law, Innovation and Technology 380: 387.
[46] Ibid; European Data Protection Board and European Data Protection Supervisor, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, 2021): para 15.

III.4.2. Safeguards and Human Involvement

The AI Act requires oversight of operations involving high-risk AI systems.

The primary overlap between Article 14 of the AI Act and Article 22 of the GDPR lies in their shared mandate for meaningful human involvement and intervention in automated systems.

III.4.3. Data Quality and Governance

Article 10 of the AI Act and Article 5 of the GDPR establish parallel and cumulative duties regarding data quality and governance, meaning that both frameworks apply simultaneously and reinforce each other.

III.4.4. Accuracy

The overlaps between Article 15 of the AI Act and Articles 5 and 32 of the GDPR centre on three fundamental pillars: accuracy, resilience, and cybersecurity or security of processing. Both frameworks establish complementary obligations to ensure that systems and the data within them remain correct, secure, and available.

III.4.5. Documentation and Traceability

The AI Act requires high-risk AI systems to record events automatically (logging) throughout their lifetime[47] and obliges providers and deployers to retain those automatically generated logs for a defined period,[48] with providers additionally preparing technical documentation.[49] Under the GDPR, the controller is separately

[47] Art 12 AI Act.
[48] Arts 19 and 26(6) AI Act.
[49] Art 11 AI Act.

required to maintain records of its processing activities and,[50] under the accountability principle, to be able to demonstrate compliance.[51]

The AI Act's logging requirement serves traceability: it captures how the system operated and when, so that its functioning can subsequently be reconstructed and monitored.

III.4.6. Risk Protection and Prevention by Design and by Default

Both regimes impose extensive obligations directed at risk prevention by design and default.

On the GDPR side, this is reflected in the requirement of data protection by design and by default and in the obligation to conduct a data protection impact assessment for high-risk processing.[52] The AI Act lays down corresponding duties for high-risk AI systems through its risk-management system,[53] data and data-governance requirements[54] and human-oversight obligations.[55]

III.4.7. Reporting Duties

Each regime imposes reporting obligations for incidents that may pose a threat. Under the AI Act, providers of high-risk AI systems must report serious incidents to competent market surveillance authorities.[56]

[50] Art 30 GDPR.
[51] Art 5(2) GDPR.
[52] Arts 25 and 35 GDPR.
[53] Art 9 AI Act.
[54] Art 10 AI Act.
[55] Art 14 AI Act.
[56] Art 73 AI Act.

Under the GDPR, a personal data breach must be notified to the supervisory authority and,[57] where it is likely to result in a high risk to the rights and freedoms of natural persons, be communicated to the affected data subjects.[58]

III.4.8. Overview Table

Transparency and Disclosure	Art 13 AI Act
	Arts 13 and 14 GDPR
Safeguards and Human Involvement	Art 14 AI Act
	Art 22 GDPR
Data Quality and Governance	Art 10 AI Act
	Art 5 GDPR
Accuracy	Art 15 AI Act
	Arts 5 and 32 GDPR
Documentation and Traceability	Arts 11, 12, 19, 26(6) AI Act
	Arts 5(2) and 30 GDPR
Risk Protection and Prevention by Design and by Default	Arts 9, 10, 14 AI Act
	Arts 25 and 35 GDPR
Reporting Duties	Art 73 AI Act
	Arts 33 and 34 GDPR

III.5. Express Interface Clauses

A number of clauses within the AI Act expressly bridge the GDPR. Since the GDPR remains unaffected by the AI Act — subject to only two exceptions — these interface

[57] Art 33 GDPR.
[58] Art 34 GDPR.

clauses serve to underline that the GDPR continues to apply in full and must be respected.

III.5.1. Special Category Processing

Art 10(5) AI Act permits providers of high-risk AI systems to process special categories of personal data within the meaning of Art 9(1) GDPR, to the extent strictly necessary for bias detection and correction, and subject to appropriate safeguards.

The provision applies expressly 'in addition to' the GDPR: it supplements, rather than displaces, Art 9 regime. Such processing therefore remains governed by the GDPR, which requires a legal basis[59] and an exception[60].

Recital 70 of the AI Act expressly characterises this processing as 'a matter of substantial public interest within the meaning of Article 9(2)(g)' GDPR. Whether Art 10(5) AI Act thereby itself constitutes a sufficient legal basis within the meaning of Art 9(2)(g) GDPR, or merely presupposes an exception to be found elsewhere, is contested; the question is examined in Chapter IV, so that both regimes govern the same processing in parallel.

III.5.2. Anti-Duplication Bridge

The AI Act mandates a fundamental rights impact assessment,[61] while the GDPR requires a data protection impact assessment.[62] To prevent the duplication of overlapping obligations, Article 27(4) of the AI Act provides that, where an obligation under Article 27 of the AI Act is already met through a data protection impact

[59] Art 6(1) GDPR.
[60] Art 9(2) GDPR.
[61] Art 27 AI Act.
[62] Art 35 GDPR.

assessment conducted pursuant to Article 35 GDPR, the fundamental rights impact assessment shall complement that assessment.

The two instruments are thereby coordinated rather than merged: the fundamental rights impact assessment complements and does not replace the data protection impact assessment.

Its focus is nonetheless wider, addressing the specific risks to the fundamental rights of the persons and groups affected by a high-risk AI system,[63] whereas the data protection impact assessment concerns the risks to rights and freedoms arising from the processing of personal data.[64]

III.5.3. Compliance

The transparency obligations set out in Art 50(1)–(4) AI Act apply, pursuant to Art 50(6) AI Act, 'without prejudice to other transparency obligations laid down in Union or national law for deployers of AI systems'; therefore, they do not override the GDPR's information obligations under Arts 12–14 GDPR, but operate alongside them. Art 50(3) AI Act makes this explicit for one case, providing that deployers of emotion recognition or biometric categorisation systems must inform the natural persons exposed and process their personal data in accordance with the GDPR.

III.5.4. Explanation of Decisions

Both regimes confer rights related to the explanation of the decisions. Under the GDPR, a data subject who is subject to a decision based solely on automated processing

[63] Art 27(1), Recital 96 AI Act.
[64] Arts 35(1) and (7) GDPR.

may obtain human intervention, express their views, and contest the decision,[65] and may access meaningful information about the logic involved.[66]

The AI Act grants an affected person the right to obtain from the deployer a clear and meaningful explanation of the role of the AI system and the main elements of a decision taken on the basis of a high-risk AI system listed in Annex III that produces legal or similarly significant adverse effects.[67]

III.6. Concurrently Applicable

Where a system is at once an 'AI system' under the AI Act and an operation processing personal data under the GDPR, both regimes apply concurrently to the same activity. This section maps, provision by provision, how that concurrency operates.

Two constellations must be distinguished. Where both instruments regulate the same subject matter, their norms genuinely overlap, applying either in parallel or through the express interface clauses by which the AI Act coordinates with the GDPR. By contrast, where both regimes remain applicable but only the GDPR supplies a rule and the AI Act is silent, no genuine overlap of norms arises, and the matter is governed by the GDPR alone.

The converse constellation does not occur: every AI Act obligation that bears on the processing of personal data has a counterpart in the GDPR, whereas the provisions unique to the AI Act concern product safety rather than data protection. The AI Act therefore never displaces the GDPR on the data-protection terrain — it only adds to it or leaves it to govern, which is the structural expression of the without-prejudice relationship established in Art 2(7) AI Act.

[65] Art 22(3) GDPR.
[66] Art 15(1)(h) GDPR.
[67] Art 86(1) AI Act.

III.6.1. Legal Basis and Lawfulness

Every processing operation in the development, training, or deployment of an AI system requires a legal basis under Art 6 GDPR. Where the data fall within the special categories of Art 9(1) GDPR — health, biometric, or ethnicity data, which large training datasets frequently contain — processing is in principle prohibited unless one of the exhaustive exceptions in Art 9(2) GDPR applies.

The AI Act supplies no such basis and expressly leaves the question to data-protection law,[68] the only qualifications being the narrow facilitations in Art 10(5) and Art 59 AI Act.

III.6.2. Data-Subject Rights

The GDPR equips an individual with a catalogue of enforceable rights — access,[69] rectification,[70] erasure,[71] restriction,[72] portability,[73] and objection[74] — which continue to apply unchanged where personal data are processed by an AI system.

The AI Act creates no equivalent individual entitlements; its remedies the complaint[75] and the explanation[76] supplement rather than replace them. The exception is Art 22 GDPR on solely automated decision-making, which — unlike the other rights — does have AI Act counterparts[77] and is accordingly treated under the overlap.

[68] Recital 10 AI Act.
[69] Art 15 GDPR.
[70] Art 16 GDPR.
[71] Art 17 GDPR.
[72] Art 18 GDPR.
[73] Art 20 GDPR.
[74] Art 21 GDPR.
[75] Art 85 AI Act.
[76] Art 86 AI Act.
[77] Arts 14 and 86 AI Act.

III.6.3. International Transfers

Where personal data processed by or for an AI system leave the EEA, what is a common occurrence given globally distributed training data and cloud infrastructure, the GDPR permits the transfer only on the basis of an adequacy decision,[78] appropriate safeguards,[79] or one of the derogations in Art 49 GDPR.

The AI Act does not contain a transfer regime and does not affect these requirements.

CHAPTER IV: TENSIONS AND CONFLICTS

IV.1. Analytical Framework

As discussed in Chapter III, Art 2(7) of the AI Act prevents formal collisions but not substantive friction. Since cumulative application is the rule wherever personal data is involved, the question shifts from 'which norm prevails?" to 'can both be satisfied, and at what cost?' Therefore, the test pursued here, therefore, analyses substantive friction within cumulative applications.

The analytical method used in this chapter distinguishes among harmonious overlaps, pre-resolved tensions, tensions, and conflicts. This distinction draws on the international law doctrine of conflict of norms.[80]

An overlap arises as soon as both regimes apply to the same conduct; every tension or conflict presupposes such an overlap. Such an overlap is harmonious when both sets of norms can be complied with frictionlessly.

[78] Art 45 GDPR.
[79] Art 46 GDPR.
[80] Wilfred Jenks, 'The Conflict of Law Making Treaties' (1953) 30 BYIL 401, 426.

Tension arises where simultaneous compliance is possible, but the norms pull in opposite directions or are grounded in contradictory rationales.

A pre-resolved tension is a tension the legislator has already resolved through an interface clause;[81] this category is not borrowed from doctrine but added for the purpose of this thesis. Finally, a conflict arises only where simultaneous compliance is impossible.[82]

The deeper cause of the friction lies in the conceptual divergence between the two regimes. The GDPR contains risk-based elements,[83] but these merely calibrate how obligations are to be performed; they do not determine whether the rights of data subjects apply.[84]

In contrast, under the AI Act, risk determines the applicability and intensity of the obligations, and the provider may tolerate residual risk provided it is 'judged to be acceptable.'[85] A controller cannot, in the same way, 'risk-accept" its way out of a data subject's rights. The EDPB and the EDPS flagged tis misalignment as early as 2021.[86]

In the following sections, the test is applied to each overlap identified in Chapter III, and a classification verdict (harmonious, pre-resolved, tension, or conflict) is rendered. The results are consolidated in the concluding section of this chapter.

[81] eg Arts 19(1), 27(4) and 50(6) AI Act.
[82] Wilfred Jenks (n 80).
[83] Arts 24, 25 and 35 GDPR; Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach' (2018) 9 European Journal of Risk Regulation 502: 504-506, 509.
[84] Article 29 Working Party, *Statement on the role of a risk-based approach in data protection legal frameworks*, 2014).
[85] Art 9(5) AI Act.
[86] European Data Protection Board and European Data Protection Supervisor, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).*

IV.2. AI Act Data Requirements vs GDPR Data-Processing Principles

Art 5(c) of the GDPR requires personal data to be processed 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed', thereby establishing the principle of data minimisation.

On the other hand, Art 10(3) AI Act requires 'training, validation, and testing data sets' to be 'sufficiently representative'.

The condition of representativeness is not an absolute concept and may vary depending on the 'sufficient levels.'[87] Frankly, the representativeness requires the datasets to pursue an *in concreto* appropriate and complete approach.

Therefore, the interplay requires the datasets to be limited to what is 'adequate, relevant, and necessary'[88] in order to be representative ('minimum necessary data').

However, the CJEU applies Art 5(c) GDPR strictly, emphasising that the 'indiscriminate use of all the personal data … irrespective of the level of sensitivity of the data' is not sufficient, while leaving open an exact determination of the minimum necessary data.[89]

IV.2.1. Purpose Limitation vs Model Re-Use and GPAI

The principle of purpose limitation does not prohibit further processing of personal data; it prohibits incompatible further processing. Its touchstone is predictability: the principle aims to ensure transparency, legal certainty, and the reasonable expectations of the data subject,[90] while the concept of compatible use deliberately preserves a degree of flexibility for controllers. Compatibility is assessed case by case against a set of key factors, with the consequence that further uses of data subjects that could not reasonably expect are the most likely to fail the test. Appropriate safeguards, such as

[87] Holtz and Ledendal, 'AI data governance – overlaps between the AI Act and the GDPR': 5.1.1.
[88] European Data Protection Board, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*, 2024): 64; *Maximilian Schrems v Meta Platforms Ireland Ltd* ECLI:EU:C:2024:834 (Court of Justice of the European Union): par 49 and the case law cited.
[89] *Maximilian Schrems v Meta Platforms Ireland Ltd*: para 64 and 65.
[90] Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, 2013). Although WP 203 interprets Art 6(1)(b) of Directive 95/46/EC, it remains the authoritative reference for Art 5(1)(b) GDPR, whose wording was carried over in substance; the EDPB continues to rely on it, see European Data Protection Board, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*: para 64, fn 48.

pseudonymisation or full or partial anonymisation, must be taken into account and may tip the assessment.[91]

The development of an AI model may itself constitute a valid purpose, provided it is sufficiently specified.[92] Yet, this merely shifts the problem to the deployment stage: general-purpose AI models, in particular, lack a delimitable purpose by definition, since Art 3(63) AI Act characterises them precisely by their 'significant generality' and capability to perform 'a wide range of distinct tasks."[93]

Measured against the test developed in Section IV.1, this overlap constitutes a tension, not a conflict: compliance with both regimes simultaneously is possible through stage-specific purpose specification, but the norms pull in opposite directions, and the decisive question of how specific the purpose of training and, above all, of deploying a general-purpose model must be remains unanswered. The CJEU requires a 'specific, logical and sufficiently close link" between the initial purpose and any further processing – a standard that the re-use of data for training a general-purpose model, whose deployment purposes are by definition open, will struggle to demonstrate.[94] Therefore, the tension is most acute for general-purpose AI models, and the resulting uncertainty is a compliance burden, examined in Chapter V.

IV.2.2. Storage Limitation vs Retention and Logging

Art 5(1)(e) GDPR permits storage for 'no longer than is necessary"; the AI Act, by contrast, requires logs to be retained for 'at least six months.'[95] A minimum-retention duty collides with a maximum-retention principle. This apparent conflict, however,

[91] Article 29 Working Party, *Opinion 03/2013 on purpose limitation*.
[92] European Data Protection Board, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*: para 64.
[93] Art 3(63) AI Act.
[94] *Digi Távközlési és Szolgáltató Kft v Nemzeti Adatvédelmi és Információszabadság Hatóság* ECLI:EU:C:2022:805 (Court of Justice of the European Union (First Chamber)): paras 31, 36-37.
[95] Arts 19(1) and 26(6) AI Act.

was expressly pre-resolved by the legislator in favour of the GDPR,[96] the first pre-resolved tension identified in this chapter. A second pairing remains: record-keeping under Art 12 AI Act itself generates personal data, since logging constitutes processing within the meaning of Art 4(2) GDPR. The full GDPR regime — legal basis, principles, and data-subject rights — therefore applies to the logs; the compliance measure of one regime creates regulated activity under the other. Moreover, retention is 'necessary" only while the AI Act obligation subsists once it lapses; the logs must be erased.[97] Measured against the test developed in Section IV.1, the retention-period pairing is pre-resolved, while the log-content pairing constitutes a tension.

IV.2.3. Accuracy and Erasure vs Trained Models

The GDPR requires personal data to be accurate and kept up to date,[98] and a data subject may demand rectification and erasure.[99] As shown in Chapter III, these rights apply unchanged when personal data are processed by an AI system.

The technical reality of the trained models raises two distinct problems. First, training data are absorbed into the model weights and distributed across the parameters; therefore, the selective removal of an individual's data–'machine unlearning "–is technically difficult or infeasible.[100]

Second, the model outputs are probabilistic: the system generates statistically most likely content, not verified facts, so hallucinations and mix-ups occur. Such outputs concerning real persons constitute personal data themselves, as they relate to an

[96] Art 19(1) AI Act: 'without prejudice to applicable Union or national law'.
[97] Digi (n 94): paras 53-54.
[98] Art 5(1)(d) GDPR.
[99] Arts 16, 17 GDPR.
[100] Eduard Fosch-Villaronga, Peter Kieseberg and Tiffany C Li, 'Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten' (2018) 34 Computer Law & Security Review 304: 3.2.

identified or identifiable person by reason of their content[101] and must therefore be accurate.[102]

The central question is whether the information embedded in a trained model itself remains personal data. According to the Hamburg DPA, it does not: the model stores tokens and embeddings rather than personal data, so data subject rights cannot relate to the model itself but are attached to the input and output of the AI system.[103]

The EDPB, by contrast, considers that models trained on personal data ' cannot, in all cases, be considered anonymous":[104] anonymity requires that both the likelihood of direct — including probabilistic — extraction of personal data and the likelihood of obtaining personal data from queries be insignificant, assessed case by case.[105] In any event, the 'probabilistic nature" of the system does not excuse inaccurate outputs: 'the principle of data accuracy must be complied with."[106]

Measured against the test developed in Section IV.1, no conflict between the two regimes exists because joint compliance is possible: no provision of the AI Act commands the retention of personal data contained in training data or model parameters, nor prevents their erasure. The log-retention duties of Arts 12 and 19 of the AI Act concern operational records, not the model's content, and are, in any event, expressly subordinated to Union data protection law.

[101] *Peter Nowak v Data Protection Commissioner*: paras 34-35.
[102] Art 5(1)(d) GDPR.
[103] The Hamburg Commissioner for Data Protection and Freedom of Information, *Discussion Paper: Large Language Models and Personal Data*, 2024).
[104] European Data Protection Board, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*: para 34.
[105] Ibid para 43.
[106] European Data Protection Board, *Report of the work undertaken by the ChatGPT Taskforce*, 2024): para 30.

IV.3. Art 10(5) AI Act vs Art 9 GDPR

The GDPR prohibits the processing of special categories of personal data unless an exception applies,[107] and the CJEU interprets these exceptions strictly.[108]

In contrast, the AI Act obliges providers of high-risk AI systems to take 'appropriate measures to detect, prevent and mitigate possible biases"[109] – a duty that, in practice, frequently requires precisely such data.

At first sight, this renders a conflict. The legislator, however, anticipated this: Art 10(5) AI Act is one of only two provisions expressly excepted from the rule that the AI Act leaves Union data protection law unaffected.[110] It permits providers of high-risk AI systems to 'exceptionally process special categories of personal data" where this is 'strictly necessary" for bias detection and correction, subject to 'appropriate safeguards" and the six cumulative conditions of Art 10(5)(a)–(f) AI Act.

The provision addresses a recognised pre-AI Act dilemma: debiasing was practically possible only on the basis of explicit consent, with the paradoxical result that AI could not be prevented from discriminating against the very rights data protection law seeks to protect.[111]

The question left open in Chapter III must therefore be answered here. Of the two readings identified there — that Art 10(5) AI Act is itself a sufficient basis under Art 9(2)(g) GDPR, or that it merely presupposes an exception to be found elsewhere — this thesis adopts the first.

---

[107] Art 9(1), (2) GDPR.
[108] *Maximilian Schrems v Meta Platforms Ireland Ltd*: paras 75-76.
[109] Art 10(2)(f)-(g) AI Act.
[110] Art 2(7) AI Act; see Chapter III above.
[111] Marvin van Bekkum and Frederik Zuiderveen Borgesius, 'Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?' (2023) 48 Computer Law & Security Review 105770.

Art 10(5) AI Act supplies the exception under Art 9(2)(g) GDPR: the substantial public interest — protection against discriminatory AI is identified by Recital 70 AI Act, while the conditions of Art 10(5)(a)-(f) constitute the suitable and specific safeguard measures that Art 9(2)(g) requires.[112]

Pursuant to the CJEU's case law, processing under an Art 9(2) GDPR exception must additionally satisfy one of the lawfulness conditions of Art 6(1) GDPR;[113] for bias correction, Art 6(1)(c) GDPR — the legal obligation arising from Art 10(2)(g) AI Act — or Art 6(1)(e) GDPR come into consideration.[114] The exception remains a needle's eye: it covers only providers of high-risk AI systems. The remainder of the GDPR applies 'in addition", and the data must be deleted once the bias has been corrected.[115] Art 59 AI Act repeats the same interface technique for regulatory sandboxes,[116] confirming a deliberate coordination method rather than an isolated fix.

This overlap constitutes pre-resolved tension: the legislator saw the collision between the debiasing duty and Art 9 prohibition and resolved it through an express interface clause. However, the narrow scope of the exception and its open interpretative questions are a source of compliance burden.

IV.4. Automatic Decisions

Art 22(1) GDPR lays down a prohibition principle, not a right that the data subject must invoke.[117] It applies under three cumulative conditions: a decision, based solely on automated processing, producing legal or similarly significant effects;[118] the

[112] Holtz and Ledendal, 'AI data governance – overlaps between the AI Act and the GDPR': 5.3.
[113] *ZQ v Medizinischer Dienst der Krankenversicherung Nordrhein* ECLI:EU:C:2023:1022 (Court of Justice of the European Union).
[114] Holtz and Ledendal, 'AI data governance – overlaps between the AI Act and the GDPR': 5.3.
[115] Art 10(5)(e) AI Act.
[116] Holtz and Ledendal, 'AI data governance – overlaps between the AI Act and the GDPR': 4.3.
[117] *OQ v Land Hessen (SCHUFA Holding (Scoring))* ECLI:EU:C:2023:957 (Court of Justice of the European Union): para 52.
[118] Ibid: para 43.

prohibition may be lifted only through an exception under Art 22(2), subject to the safeguards of Art 22(3) GDPR.[119]

The AI Act approaches the same phenomenon from the opposite end: Art 14(1) AI Act obliges providers to design high-risk systems so that they 'can be effectively overseen by natural persons," and Art 26(2) AI Act obliges deployers to assign oversight to persons with 'the necessary competence, training and authority." An ex-post prohibition attaching to the decision (the controller) thus meets an ex-ante design duty attaching to the system (provider and deployer).

At first sight, the two regimes reinforce one another. The capabilities requires by Art 14(4) AJ Act — to disregard, override or reverse the output[120] and to intervene in or halt the system through a stop button[121] — functionally echo the human intervention safeguard of Art 22(3) GDPR.

Compliance with the AI Act, however, does not automatically neutralise Art 22 GDPR because the regimes set their thresholds differently: the AI Act is satisfied by the existence of a competent overseer, whereas Art 22 GDPR asks whether the oversight genuinely determines the outcome — 'meaningful, rather than just a token gesture," by someone with 'authority and competence to change the decision".[122]

A deployer may satisfy Arts 14 and 26 AI Act on paper while the overseer merely rubber-stamps, leaving the prohibition applicable – a false sense of safety; conversely, the AI Act furnishes no authorisation under Art 22(2)(b) GDPR and no legal basis for the decision.[123]

---

[119] Ibid: paras53-55.
[120] Art 14(4)(d) AI Act.
[121] Art 14(4)(e) AI Act.
[122] Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 2018)
[123] Recital 10 AI Act; Chapter III.

SCHUFA widens the zone: scoring itself is an automated decision where a third party draws strongly on it,[124] so Art 22 GDPR bites upstream of any deployer, whose design decide addressee logic maps poorly onto a case law locating the decision wherever determinative influence lies.[125]

Concluding, the design-duty pairing is harmonious, but the meaningful-involvement interface is a tension, not a conflict.

IV.5. Transparency and Explanation

Both regimes impose information duties, but on different addressees, so they stack rather than collide: the AI Act makes high-risk systems transparent to their deployers[126] and obliges providers and deployers to disclose the artificial character of an interaction output or deepfake,[127] while the GDPR requires the controller to inform the data subjects.[128] Since the AI Act's duties apply 'without prejudice to" other transparency obligations under Union law,[129] they supplement the GDPR rather than displace it. Measured against the test developed in section IV.1, this overlap is harmonious.

The GDPR grants the data subject 'meaningful information about the logic involved" in automated decisions[130] and the right to contest them;[131] the AI Act gibes an affected person a 'clear and meaningful explanation" of decisions taken on the basis of an Annex III high-risk system.[132]

[124] *OQ v Land Hessen (SCHUFA Holding (Scoring))*: para 73.
[125] Ibid: paras 48, 50, 61-62.
[126] Art 13 AI Act.
[127] Art 50(1)-(4) AI Act.
[128] Arts 13-15 GDPR.
[129] Art 50(6) AI Act.
[130] Art 15(1)(h) GDPR.
[131] Art 22(3) GDPR.
[132] Art 86(1) AI Act.

What that GDPR entitlement actually requires was, however, long contested. On one reading the GDPR confers no binding right to an explanation of an individual decision, but only a narrower, ex ante right to information about a system's general functionality, the very phrase 'right to explanation" appearing in a recital rather than in the operative articles.[133]

On the competing reading, 'meaningful information about the logic involved" must be construed functionally, the test being 'pegged to some action the explanation enables in the data subject, such as the right to contest a decision",[134] up to a right to the 'legibility" of the decision.[135]

Both entitlements collide with the protection of trade secrets and intellectual property that each regime also secures.[136]

The CJEU held that meaningful information means 'the procedure and principles actually applied', not the algorithm or formula,[137] and that asserted trade secrets must be placed before the supervisory authority or court to be balanced, blanket statutory exclusions being precluded.[138]

Even so, an explanation right is, taken alone, a limited remedy — a likely 'transparency fallacy", given that data subject are typically too 'time-poor, resource-poor, and lacking in the necessary expertise" to use it — which is why the AI Act does not rely on it,

[133] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76.
[134] Andrew D Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 International Data Privacy Law 233.
[135] Gianclaudio Malgieri and Giovanni Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, 2017): 3.5.
[136] Art 78, Recital 167 AI Act; Art 23(1)(i) GDPR.
[137] *CK v Magistrat der Stadt Wien (Dun & Bradstreet Austria)* ECLI:EU:C:2025:117 (Court of Justice of the European Union): paras 58-59.
[138] Ibid: paras 70, 74-75.

supplementing the data subject's entitlements with systemic transparency and human-oversight duties addressed to providers and deployers.[139]

Measured against the test developed in Section IV.1, this is a tension, not a conflict: joint compliance is possible, yet the norms pull in opposite directions, and the explainability of opaque or general-purpose models remains open.

IV.6. Role Mismatch

As established in Chapter III, the two regimes allocate roles on different axes; the AI Act to the system, the GDPR to the processing operation. The consequence pursued here is that the controller accountable to the data subject need not be the actor that shaped the system under the AI Act.

The controller is whoever determines the purpose and means of an operation,[140] a functional, fact-based question;[141] the processor merely acts on its behalf.[142] A party is not the controller for an operation whose purpose and means it does not determine.[143] It follows that the provider may not be the controller despite having supplied the system, while the deployer becomes the controller once it determines an operation's purpose and means.

Controllership turn on determination, not on control over the data themselves: joint controllership can arise even where a party has no access to the raw data, since only the joint determination of purposes and means counts.[144]

---

[139] 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 : 18, 67.
[140] Art 4(7) GDPR.
[141] European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 2021): paras 12, 21.
[142] Art 4(8) GDPR.
[143] *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV* ECLI:EU:C:2019:629 (Court of Justice of the European Union): paras 74, 84-85.
[144] *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* ECLI:EU:C:2018:388 (Court of Justice of the European Union).

Across one lifecycle the GDPR therefore redistributes controllership among actors and stages while the provider and deployer roles stay fixed, and the rift widens under the value-chain rules: where a deployer distributor or importer is re-labelled a provider on affixing its name, substantial modification, or rep-purposing into high-risk,[145] GDPR controllership does not follow, and the re-labelled provider does not become the controller for the initial training.

Simultaneous compliance is possible and this is a tension as compliance is possible only through deliberate contractual allocation — joint-controller arrangements and processor terms (so called data processing agreement), [146] read against the AI Act's value-chain cooperation duty pursuant to Art 25(2) AI Act.

IV.7. Enforcement

The overlap is also institutional. The AI Act is enforced by market surveillance authorities under the Market Surveillance Regulation[147] and the GDPR by independent supervisory authorities,[148] each with its own fining regime.[149] The two partly converge — for biometrics in law enforcement, border management and justice, and Annex III points 6-8, the market surveillance authority must be the data-protection authority[150] — yet elsewhere two authorities with different mandates police one system, with no binding cross-regime consistency mechanism.

[145] Art 25(1)(a)-(c) AI Act.
[146] Arts 26 and 28 GDPR.
[147]Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 ; Arts 70, 74 AI Act.
[148] Art 51 GDPR.
[149] Art 99 AI Act; Art 83 GDPR.
[150] Art 74(8) AI Act.

The same conduct may thus attract both a GDPR fine[151] and an AI Act penalty,[152] raising a *ne bis in idem* concern under Art 50 CFR, which covers punitive administrative fines. The regimes' different objectives do not defuse it: after *bpost*, idem turns on the same offender and the same facts, the protected legal interest being irrelevant,[153] while Art 83(3) GDPR caps fines only within the GDPR. Duplication may nonetheless be justified under Art 52(1) Charter where the regimes pursue complementary aims directed at different aspects of the same conduct,[154] provided three conditions are met: foreseeable rules, coordinated proceedings, and penalties limited to what is strictly necessary.[155] Absent any express cross-regime clause, these safeguards fall to authorities and courts – the enforcement gap.

Measured against the Section IV.1 test, this constitutes a tension, not a conflict.

IV.8. Interim Conclusion

Applying the Section IV.1 test to each overlap yields a clear pattern: in no case does a genuine conflict arise, since simultaneous compliance always remains possible. That result is earned, not an artefact of the test: the retention clash and the Art 9 GDPR – Art 10(5) AI Act pairing each appeared *prima facie* irreconcilable, yielding only to an express interface clause without which a true conflict would have arisen. The relationship instead spans a spectrum – from harmonious overlap, through the two pre-resolved tensions, to a series of genuine tensions concentrated where the AI Act's risk-logic meets the GDPR's non-disposable, rights-based guarantees. The without-prejudice architecture[156] thus averts formal collision but at substantive cost: the

[151] Art 83 GDPR.
[152] Art 99 AI Act.
[153] *bpost SA v Autorité belge de la concurrence* ECLI:EU:C:2022:202 (Court of Justice of the European Union): paras 33-37.
[154] Ibid: para 49.
[155] Ibid: para 51.
[156] Art 2(7) AI Act.

friction is displaced onto compliance practice and onto questions of reform, for which the express interface clause of Art 10(5) AI Act offers the *de lege ferenda* template.

CHAPTER V: COMPLIANCE

V.1. The Double Regulatory Burden

For the reason of cumulative application, no conflict but tensions arise causing a doubling of compliance work, especially where the risk-vs-rights asymmetry bites. Although the legislator provided some express interface clauses, but they are only partial and leave many aspects disregarded.

V.2. Impact Assessments: DPIA and FRIA

A high-risk AI system may trigger both a data protection impact assessment[157] and a fundamental rights impact assessment.[158] The two overlap but are not identical: the FRIA is wider, reaching all CFR rights even where no personal data are processed.

Two interface mechanism coordinate them. Where any of the FRIA's obligations is already met through an Art 35 DPIA, the FRIA need only complement it;[159] and deployers must, 'where applicable", use the provider's instructions for use to perform that DPIA.[160]

Ultimately the duty remains cumulative: the two stay distinct instruments, and although overlapping content need to be assessed only once, every element unique to either must still be caried out – the FRIA adds to, rather than replaces the DPIA.

[157] Art 35(1), (3) GDPR.
[158] Art 27(1) AI Act.
[159] Art 27(4) AI Act.
[160] Art 26(9 AI Act.

V.3. Data Governance and Lawful Basis

The same dataset attracts cumulative duties. The AI Act's quality and data-governance requirements for high-risk training, validation and testing data[161] apply alongside the GDPR's processing principles[162] and its data-protection-by-design duty.[163] The result is that the AI Act's call for representative datasets must be harmonised both with the data minimisation and with purpose specification, the tension identified in Section IV.2, a challenge that is not easily lifted. As the AI Act supplies no legal basis of its own,[164] every operation still requires one under the GDPR.[165]

In practice both regimes are addressed through a single, combined data-governance process covering provenance, bias testing, minimisation, pseudonymisation, accuracy checks, retention and documentation, designed once to satisfy each, with the AI Act's records feeding GDPR accountability.[166] The lawful basis is drawn from the GDPR, the AI Act adding only two narrow facilitations: the processing of special category data for bias detection and correction,[167] and the further-processing route within regulatory sandboxes. [168] At least de-biasing is thereby expressly interfaced through Art 10(5) AI Act, while the EDPB has begun to map how legitimate interest and model anonymity operate at the training stage.[169]

The burden is mitigated, not removed: the duty stays cumulative. The threshold of data that is at once minimal and 'sufficiently representative" remains unsettled, and Art

[161] Art 10 AI Act.
[162] Art 5 GDPR.
[163] Art 25 GDPR.
[164] Recital 10 AI Act.
[165] Arts 6, 9 GDPR.
[166] Art 5(2) GDPR; Art 11 AI Act.
[167] Art 10(5) AI Act.
[168] Art 50 AI Act.
[169] European Data Protection Board, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*: 34, 43, 50ff.

10(5) AI Act is a needle's eye, open only to providers of high-risk systems and requiring deletion once the bias is corrected.[170]

Data-protection-by-design therefore reconciles the duties *in concreto* rather than guaranteeing that both are fully met.[171]

V.4. Transparency and Explanation

Transparency duties stack rather than collide. The same system owes layered information: provider to deployer,[172] provider or deployer to the exposed person,[173] and the controller to data subject.[174] AS the AI Act's duties apply without prejudice to other transparency obligations and preserve the AI Act's Chapter III requirements,[175] compliance means serving each addressee its layer from the same documentation; the burden is volume, not friction.

Explanation is hard. The data subject's right to meaningful information about the logic involved in an automated decision[176] and the affected person's right to an explanation of an AI Act Annex III decision[177] meet the trade-secret and IP protection both regimes secure.[178]

The CJEU ruled that the controller must explain the procedure and principles actually applied, not the algorithm or formula, and where a trade secret is genuinely engaged must place the protected material before the supervisory authority or court for

[170] Art 10(5)(e) AI Act.
[171] Art 25 GDPR.
[172] Art 13 AI Act.
[173] Art 50 AI Act.
[174] Arts 12-14 GDPR.
[175] Art 50(6) AI Act.
[176] Arts 15(1)(h), Art 22(3) GDPR.
[177] Art 86 AI Act.
[178] Art 78, Recital 167 AI Act; Art 23(1)(i) GDPR.

balancing, a blanket exclusion being precluded.[179] One layered explanation can thus satisfy both Art 15(1)(h) GDPR and Art 86 AI Act.

Data subject's rights raise a law-technology gap. Access, rectification and erasure[180] are hard to honour against a trained model, since selective removal ('machine unlearning") is often infeasible[181] and probabilistic outputs about real persons may themselves be inaccurate personal data.[182] In practice the rights are exercised at input and output level (filtering, correction, retaining where feasible), the accuracy duty still binding the output despite the model's probabilistic nature.[183] Whether they reach the model itself turns on whether it is anonymous, assessed case by case,[184] against the view that the model stores no personal data so the rights attach only to input and output.[185]

The burden is mitigated, not removed: transparency stacks without conflict and explanation is workable through the procedure-and-principles standard, but the explainability of opaque models, the infeasibility of machine unlearning, and the divergence over whether a trained model is itself personal data leave a residual uncertainty carried to the conclusions as a question for reform.

V.5. Role Allocation and Contracts

AS Section IV.6 found, the GDPR's controller and processor roles do not map onto the AI Act's provider and deployer roles, and the AI Act supplies no statutory mapping. The reconciliation therefore falls to the parties, through contract.

---

[179] *CK v Magistrat der Stadt Wien (Dun & Bradstreet Austria).*
[180] Arts 15-17 GDPR.
[181] Fosch-Villaronga, Kieseberg and Li, 'Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten'.
[182] Art 5(1)(d) GDPR.
[183] European Data Protection Board, *Report of the work undertaken by the ChatGPT Taskforce*: para 30.
[184] European Data Protection Board, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*: paras 34, 43.
[185] The Hamburg Commissioner for Data Protection and Freedom of Information, *Discussion Paper: Large Language Models and Personal Data*.

Three instruments do the work. Where two actors jointly determine the purposes and means, they must transparently allocate their respective responsibilities, in particular for data subject rights and the information duties under the GDPR,[186] by an arrangement whose essence is made available to the data subject.[187] Where one processes on another's behalf, a binding contract must govern the processing and contain the mandatory clauses of Art 28(3) GDPR. Alongside these, the initial provider of a re-labelled system must cooperate and supply the necessary information and technical access.[188]

Two limits keep this a tension rather than a fix: contracts allocate internal responsibility bit cannot cause external liability. Irrespective of the arrangement, the data subject may exercise its rights against each controller.[189] And labels cannot override the facts: the controller/processor question is functional and fact-based,[190] so a party styled a processor that in fact determines the purpose and means remains a controller, and mis-designation is itself a compliance risk.

The contractual toolkit thus manages the mismatch without dissolving it: the parties bear the burden of allocating correctly, and of re-allocation after any Art 25 AI Act re-labelling, while an error exposes liability under both regimes. Whether the two role taxonomies should be aligned is left to the conclusions as a question of reform.

V.6. Enforcement Exposure and Coordination

As Section IV.7 found, the same system is policed by two authority systems, the market surveillance authorities under the AI Act and the supervisory authorities under the

[186] Art 13, 14 GDPR.
[187] Art 26(1), (2) GDPR.
[188] Art 25(2) AI Act.
[189] Art 26(3) GDPR.
[190] European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*: paras 12,21.

GDPR, raising the risk of divergent interpretation and of double punishment for the same conduct. The following *de lege lata* mechanisms try to temper this.

First, optional statutory convergence: in defined Annex III areas, Member States must designate as market surveillance authority either the data protection authority or another authority meeting the same conditions under Arts 41 to 44 of the Directive (EU) 2016/680.[191] Where a Member State chooses the data protection authority, a single body enforces both regimes; where it does not, the two authorities remain distinct.

The EDPB has recommended that Member States make the former choice, so that the DPA serves as the single point of contract and coordination is improved.[192]

Second, the risk of double punishment is constrained by the prohibition of ne bis in idem.[193] The same conduct may attract both an AI Act penalty and a GDPR fine,[194] yet such double fining is permissible only on the conditions set out in *bpost*, as established in Section IV.7. Within the GDPR, cumulative fines are in any event capped at the gravest infringement, but no equivalent cap operates across the two regimes.[195]

These mechanisms temper the exposure without resolving it. Coordination of supervision rests on soft duties: Member States must facilitate cooperation between market surveillance authorities and other relevant national authorities, including the DPAs,[196] but the detailed procedures still fall to be developed.[197]

[191] Art 74(8) AI Act.
[192] European Data Protection Board, *Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework*, 2024): paras 9-10.
[193] Art 50 CFR.
[194] Art 99 AI Act; Art 83 GDPR.
[195] Art 83(3) GDPR.
[196] Art 74(10) AI Act.
[197] European Data Protection Board, *Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework*: para 11.

There is, moreover, no cross-regime ne bis in idem rule, so the proportionality of a second penalty is left to the *bpost* framework applied base by case. Coherence therefore depends on authority practice and case-by-case judicial control, and whether a binding coordination mechanism should be created is left to the Conclusions.

V.7. Takeaways

Taken together, the chapter shows that the AI Act's express interface clauses, from the special-category and sandbox bases[198] to the assessment and information bridges[199] and the transparency savings clause,[200] together with the GDPR's contractual and coordination tools, form a genuine but only partial mitigation toolkit. They remove redundancy and supply legal bases, yet the underlying obligations remain cumulative, and the residual friction is concentrated where the AI Act's risk logic meets the GDPR's non-disposable, rights-based guarantees, the asymmetry identified in Section IV.1. The double regulatory burden is therefore managed rather than dissolved, and the open questions of reform are taken up in the Conclusions.

VI. Conclusion

This thesis asked to what extent the AI Act and the GDPR create regulatory overlaps and normative conflicts, and what compliance challenges follow from their concurrent application. On the first question, Chapters III and IV show that the two regimes overlap extensively and apply parallel wherever an AI system processes personal data, yet produce no genuine conflict: measured against the test in Section IV.1, every overlap resolves as a harmonious overlap, pre-resolved tension , or a tension, the

[198] Arts 10(5), 59 AI Act.
[199] Arts 26(9), 27(4) AI Act.
[200] Art 50(6) AI Act.

friction concentrating where the AI Act's risk logic meets the GDPR's non-disposable rights.[201]

On the second question, Chapter V shows that this cumulative application produces a real double regulatory burden that the AI Act's interface clauses and the GDPR's contractual and coordination tools mitigate but do not dissolve. The burden is therefore manageable rather than prohibitive: the concurrent regimes constrain innovation without blocking it.

Several questions, by design, are left open rather than resolved here: whether Art 10(5) AI Act should be broadened[202], whether the controller-processor and provider-deployer taxonomies should be aligned,[203] whether a binding cross-regime coordination and ne bis in idem mechanism should be created,[204] and whether a trained model is itself personal data given the infeasibility of machine unlearning.[205] Their resolution awaits interpretation by the CHEU and, where appropriate, targeted legislative coordination; pending that, coherence rests on interpretation and compliance practice rather than in the removal of the double burden.

[201] See Section IV.8.
[202] See Section V.3.
[203] See section V.5.
[204] See Section V.6.
[205] See Section V.4.

BIBLIOGRAPHY

Journal Articles

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

Fosch-Villaronga E, Kieseberg P and Li TC, 'Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten' (2018) 34 Computer Law & Security Review 304

Holtz HM and Ledendal J, 'AI data governance – overlaps between the AI Act and the GDPR' (2026) 18 Law, Innovation and Technology 380

Jenks W, 'The Conflict of Law Making Treaties' (1953) 30 BYIL 401

Quelle C, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach' (2018) 9 European Journal of Risk Regulation 502

Selbst AD and Powles J, 'Meaningful Information and the Right to Explanation' (2017) 7 International Data Privacy Law 233

van Bekkum M and Zuiderveen Borgesius F, 'Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?' (2023) 48 Computer Law & Security Review 105770

Wachter S, Mittelstadt B and Floridi L, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76

Statutes

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)

Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011

Cases

Patrick Breyer v Bundesrepublik Deutschland ECLI:EU:C:2016:779 (Court of Justice of the European Union)

Peter Nowak v Data Protection Commissioner ECLI:EU:C:2017:994 (Court of Justice of the European Union)

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH ECLI:EU:C:2018:388 (Court of Justice of the European Union)

Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV ECLI:EU:C:2019:629 (Court of Justice of the European Union)

bpost SA v Autorité belge de la concurrence ECLI:EU:C:2022:202 (Court of Justice of the European Union)

Digi Távközlési és Szolgáltató Kft v Nemzeti Adatvédelmi és Információszabadság Hatóság ECLI:EU:C:2022:805 (Court of Justice of the European Union (First Chamber))

OQ v Land Hessen (SCHUFA Holding (Scoring)) ECLI:EU:C:2023:957 (Court of Justice of the European Union)

ZQ v Medizinischer Dienst der Krankenversicherung Nordrhein ECLI:EU:C:2023:1022 (Court of Justice of the European Union)

Maximilian Schrems v Meta Platforms Ireland Ltd ECLI:EU:C:2024:834 (Court of Justice of the European Union)

CK v Magistrat der Stadt Wien (Dun & Bradstreet Austria) ECLI:EU:C:2025:117 (Court of Justice of the European Union)

European Data Protection Supervisor v Single Resolution Board ECLI:EU:C:2025:645 (Court of Justice of the European Union)

Reports

Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, 2013)

Article 29 Working Party, *Statement on the role of a risk-based approach in data protection legal frameworks*, 2014)

Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 2018)

European Commission, *Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act)*, 2025)

European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 2021)

European Data Protection Board, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*, 2024)

European Data Protection Board, *Report of the work undertaken by the ChatGPT Taskforce*, 2024)

European Data Protection Board, *Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework*, 2024)

European Data Protection Board and European Data Protection Supervisor, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, 2021)

European Law Institute, *The concept of 'AI system' under the new AI Act: Arguing for a Three-Factor Approach*, 2024)

Malgieri G and Comandé G, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, 2017)

The Hamburg Commissioner for Data Protection and Freedom of Information, *Discussion Paper: Large Language Models and Personal Data*, 2024)

Web Pages

Gutbrunner S, 'AI Act – Anwendungsbereich in zeitlicher und räumlicher Hinsicht' (2026) <lexis360.at> accessed 19 May 2026