STUDY

Requested by the ITRE committee

European Parliament

Interplay between the AI Act and the EU digital legislative framework

Policy Department for Transformation, Innovation and Health
Directorate-General for Economy, Transformation and Industry
Authors: Hans GRAUX, Krzysztof GARSTKA, Nayana MURALI, Jonathan CAVE, Maarten BOTTERMAN

PE 778.575 – October 2025

EN

Interplay between the AI Act and the EU digital legislative framework

Abstract

This study explores how the AI Act relates to various other crucial pieces of EU digital legislation, such as the GDPR, the Data Act and the Cyber Resilience Act. It assesses overlaps and gaps between these acts, and shows that, while each of them is individually well targeted, their interplay creates significant regulatory complexity. Finally, it also provides reflections and suggestions for possible evolutions of the AI Act, and of EU digital legislation as a whole, keeping in mind the objective of ensuring that Europe can establish a competitive AI industry.

This study was prepared at the request of the ITRE Committee.

This study was requested by the European Parliament's Committee on Industry, Research and Energy (ITRE).

AUTHORS
Hans GRAUX, Timelex
Krzysztof GARSTKA, Timelex
Nayana MURALI, Timelex
Jonathan CAVE, GNKS Consult
Maarten BOTTERMAN, GNKS Consult
Julie PELLEGRIN, CSIL (QA)

ADMINISTRATOR RESPONSIBLE
Matteo CIUCCI

EDITORIAL ASSISTANT
Irene VERNACOTOLA

LINGUISTIC VERSIONS
Original: EN

ABOUT THE EDITOR
Policy departments provide in-house and external expertise to support European Parliament committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for email alert updates, please write to:
Policy Department for Transformation, Innovation and Health
European Parliament
B-1047 Brussels
Email: ecti-poldep-b@europarl.europa.eu

Manuscript completed: September 2025
Date of publication: October 2025

This document is available on internet at:
http://www.europarl.europa.eu/supporting-analyses

DISCLAIMER AND COPYRIGHT

For citation purposes, the publication should be referenced as: Graux, H., Garstka, K., Murali, N., Cave, N., Botterman, M., *Interplay between the AI Act and the EU digital legislative framework*, publication for the Parliament's Committee on Industry, Research and Energy (ITRE), Policy Department for Transformation, Innovation and Health, European Parliament, Luxembourg.

CONTENT

LIST OF ABBREVIATIONS

AI	Artifical Intelligence
CPS	Core Platform Service
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
DA	Data Act
DMA	Digital Markets Act
DORA	Digital Operational Resilience Act
DPIA	Data Protection Impact Assessment
DSA	Digital Services Act
EDIB	European Data Innovation Board
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ENVI	Committee on the Environment, Climate and Food Safety
EUCC	European Union Certification Scheme for Common Criteria
EUCS	European Cybersecurity Certification Scheme for Cloud Services
FRAND	Fair, Reasonable and Non-Discriminatory
FRIA	Fundamental Rights Impact Assessment
GDPR	General Data Protection Regulation
GPAI	General Purpose AI
ITRE	Committee on Industry, Research and Energy

NIS	Network and Information Security
NIS2	Network and Information Security Directive 2
NLF	New Legislative Framework
PDE	Product with Digital Elements
SANT	Committee on Public Health
TFEU	Treaty on the Functioning of the European Union
VLOP	Very Large Online Platform
VLOSE	Very Large Online Search Engine

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Background

The Artificial Intelligence Act (AI Act), adopted by the European Union in June 2024, marks a pivotal milestone in global technology governance. As the first comprehensive regulatory framework for artificial intelligence, it sits at the heart of the EU's digital legislative corpus, which has in recent years expanded to include instruments such as the General Data Protection Regulation (GDPR), the Data Act, the Digital Services Act (DSA), the Digital Markets Act (DMA), the Cyber Resilience Act (CRA), and others. While each instrument pursues legitimate and targeted policy aims, questions are increasingly being raised about their combined impact on the competitiveness, coherence, and innovation capacity of the European AI ecosystem.

Aim

This report, commissioned by the European Parliament's Committee on Industry, Research and Energy (ITRE), explores the interplay between the AI Act and these surrounding legislative instruments. The study assesses whether the EU's digital legal framework operates as a coherent system or whether it instead introduces overlapping obligations, inconsistencies, or undue burdens that could fragment the internal market and undermine the development of a globally competitive European AI industry. In doing so, it offers short-, medium-, and long-term reflections aimed at reducing regulatory friction while maintaining the EU's commitment to rights, trust, and safety.

Key Findings

The Regulatory Logic and Structural Challenges of the AI Act

The AI Act is built upon a risk-based logic. It bans certain AI practices, imposes stringent duties on high-risk AI systems, requires transparency for specified use cases, and sets standalone obligations for general-purpose AI models (including those with systemic risk). The regulation draws substantially from the EU's product safety legislation model (under the New Legislative Framework), while layering on novel requirements related to fundamental rights impact assessments, traceability, and oversight.

Yet, several tensions are evident. Firstly, the Act stretches traditional product safety logic into less determinate domains such as human rights compliance, which may prove difficult to assess using conventional conformity mechanisms. Secondly, the regulation's applicability to both AI system providers and deployers imposes complex chains of responsibility that may be difficult to navigate, particularly for SMEs or non-specialist users. Thirdly, the definition and classification of high-risk systems rely on Annex-based lists and subjective assessments of harm potential, thereby introducing legal ambiguity. Finally, while the Act purports to promote innovation (through regulatory sandboxes, open-source exemptions, and lighter regimes for non-systemic GPAIs), the overall framework still largely centres on mitigating harms, often through prescriptive obligations.

Interactions with Other EU Digital Legislation

The AI Act does not operate in isolation. Its obligations frequently overlap with those in adjacent regulatory instruments. The report identifies a number of frictions and challenges in this interplay:

GDPR: The AI Act introduces requirements for fundamental rights impact assessments (FRIAs) in cases that often also trigger data protection impact assessments (DPIAs) under the GDPR. These instruments differ in scope, supervision, and procedural requirements, creating duplication and uncertainty. Transparency and logging obligations are also redundant across both regimes. Moreover, there is ambiguity over how controllers and providers should manage rights of access, rectification, and erasure when personal data becomes embedded in complex AI models;

Data Act: While the AI Act governs the design and deployment of AI systems, the Data Act ensures access to and portability of data generated by connected products and services. AI providers may be data holders under the Data Act and simultaneously subject to obligations under the AI Act. The cumulative compliance load is significant, especially in real-world testing or in contexts involving third-country data transfers;

Cybersecurity and the CRA: High-risk AI systems must meet certain cybersecurity standards. These may overlap with those imposed by the Cyber Resilience Act, which introduces mandatory cybersecurity requirements for all digital products. While the CRA provides for presumptions of AI Act compliance where its requirements are met, the partial alignment between the two frameworks leaves room for interpretative uncertainty;

DSA and DMA: Intermediary services (such as online platforms and search engines) that deploy or provide AI systems and models, e.g., in recommender systems or moderation tools, face increased transparency obligations that may overlap. Very large online platforms and search engines may face simultaneous risk-assessment obligations under the AI Act and the DSA, especially where general-purpose AI models are provided through the intermediary service. There is also a possibility of overlapping obligations related to AI-generated or manipulated content, both legal and illegal. The AI Act and DSA interplay may also impact intermediary liability and researchers' access to data. The DMA's provisions on data access, interoperability, and anti-self-preferencing could be relevant to AI APIs or foundation models offered by gatekeepers. However, AI systems are not yet designated as core platform services under the DMA, limiting the scope of these interactions in practice;

NIS2 Directive: Essential and important entities under NIS2 that develop or deploy AI systems must comply with both cybersecurity requirements and AI-specific risk management frameworks. The overlap is especially pronounced in incident reporting obligations and the governance of supply chain risks.

Governance and Institutional Complexity

The AI Act introduces a novel governance architecture centred around the European AI Office (AIO). While the AIO is mandated to supervise GPAIs, support regulatory sandboxes, and coordinate enforcement, its role overlaps with that of existing regulators such as data protection authorities, market surveillance bodies, and the European Data Protection Board.

The risk of regulatory fragmentation is non-trivial, particularly in areas where concurrent competences exist without robust coordination mechanisms. Moreover, the AIO's institutional position within the Commission raises concerns about its operational independence and capacity to fulfil its remit without a dedicated legal personality or ring-fenced resources.

Broader Strategic Considerations

The cumulative effect of the EU's digital legislation, although rooted in legitimate policy goals, risks burdening European AI innovators disproportionately. This is particularly concerning given the relative underperformance of the EU in AI investment and innovation metrics. While the AI Act sets out a vision for human-centric, trustworthy AI, its intersection with other digital laws is not always calibrated for agility, scalability, or global competitiveness.

The report notes that many of the obligations arising from this regulatory ensemble can be reasonably justified in isolation. However, their simultaneous application to the same actors and use cases often produces duplicative, inconsistent or unclear requirements that deter uptake, delay time to market, and introduce compliance asymmetries across Member States. These burdens may affect domestic SMEs and start-ups more acutely than multinational firms, many of which are headquartered outside the Union and better equipped to absorb compliance costs.

Recommendations

In light of the identified frictions, the study advances several reflections for future legislative and policy development:

Short-term: Encourage joint guidance and coordinated enforcement practices among supervisory bodies. Promote mutual recognition of assessments (e.g. DPIAs and FRIAs) and harmonised sandbox procedures across Member States;

Medium-term: Consider light-touch legislative amendments to clarify role definitions, streamline overlapping obligations (particularly in fundamental rights and cybersecurity domains), and enhance the executability of rights in AI contexts;

Long-term: Re-examine the EU's digital regulatory architecture with a view to consolidation, simplification, and strategic coherence. Foster an integrated approach that enables agile compliance for innovators without compromising the Union's fundamental rights and safety values.

By refining the interplay between digital legislative instruments, the EU can ensure that its regulatory model not only safeguards its constitutional values but also enables the emergence of a globally competitive and sovereign AI industry.

1. INTRODUCTION TO THIS STUDY

1.1. Background

On 13 June 2024, the Artificial Intelligence Act (AI Act or Act) was formally adopted in the European Union. This legislative milestone marked the culmination of nearly four years of arduous negotiation, following the European Commission's original proposal in April 2021[1]. The AI Act is widely regarded as the world's first comprehensive legal framework specifically aimed at regulating artificial intelligence technologies and forms a cornerstone of the EU's broader digital regulatory strategy.

The Regulation was published in the Official Journal on 12 July 2024 and entered into force on 1 August 2024. Its provisions become applicable in stages. The prohibitions of unacceptable-risk AI practices and AI-literacy obligations apply as of 2 February 2025. Obligations for general-purpose AI (GPAI) models and governance structures apply as of 2 August 2025. The general date of application covering most remaining provisions is 2 August 2026, with a small set of later-applying provisions beginning on 2 August 2027. The Commission is also due to issue practical implementation guidelines by 2 February 2026. Thus, the framework is expected to be fully effective by 2027, giving EU-facing businesses roughly three years to adapt governance and risk management practices.

The Regulation was published in the Official Journal on 12 July 2024 and entered into force on 1 August 2024. Its rules apply in stages: the bans on unacceptable-risk AI practices and the AI-literacy obligations apply from 2 February 2025; obligations for general-purpose AI (GPAI) models and the new governance framework apply from 2 August 2025; and most remaining provisions, including enforcement, apply from 2 August 2026. In practice, the framework is expected to be fully effective by 2027, giving the European-facing AI industry roughly a three-year window to adapt governance and risk-management practices.

Not unpredictably for such a transformative legal instrument with far-reaching ambitions for an emerging and rapidly evolving industry, **the AI Act has elicited a mixed response**. It has many clear merits: scholars and practitioners have at times commended its risk-based approach, its attempt to provide legal certainty and its alignment with fundamental rights standards[2]. Similarly, and equally predictably, however, concerns have also been raised notably regarding the potentially chilling effect of regulatory complexity and compliance costs for AI providers, particularly on SMEs and start-ups operating in the European AI ecosystem[3].

---

1 European Commission, 2021, *Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, COM(2021) 206 final.

2 Veale, M. et al., F., 2021, *Demystifying the Draft EU Artificial Intelligence Act*, Computer Law Review International, 22(4), pp. 97-112.

3 Smuha, N.A. et al., 2022, *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*, European Law Journal, 28(1), pp. 1-14.

Some commentators have questioned whether the AI Act's detailed and prescriptive nature, coupled with its broad extraterritorial reach, risks creating barriers to innovation and legal (or market) fragmentation across Member States[4] and forms a disproportionate barrier to international trade.

These tensions reflect a deeper structural challenge for European digital policymaking: how to facilitate the governance of emerging and rapidly evolving technologies in a manner that preserves public trust and democratic values without undermining Europe's global competitiveness in the AI sector?

Moreover, **the AI Act is not the sole regulatory change shaping the digital industry**. Beyond the AI Act, new legal frameworks include – but are certainly not limited to – the Data Act, the Digital Services Act, the Digital Markets Act, the Cyber Resilience Act, the NIS2 Directive and a broad range of other and more sector-specific initiatives. To mitigate some of the resulting complexities, the European Commission is advancing simplification packages, including the so-called 'Omnibus IV'[5], a package with draft measures to digitalise and align 'common specifications' in product legislation and extend certain SME mitigating measures to small mid-caps; and a forthcoming 'Digital Omnibus' to simplify how EU rules on data, cybersecurity and artificial intelligence are applied. All of these initiatives are regulatory responses to real societal problems but raise questions as to their interconnectedness and collective impacts.

The present study has been requested by the ITRE Committee of the European Parliament, not to evaluate the AI Act as such; but rather to examine a broader question: **how does the AI Act interact with other European digital legislation, and what options exist for optimising this interplay**, in light of the general objective of ensuring that the EU is capable of establishing and maintaining a competitive AI industry in a highly globalized market?

1.2. Scope and objectives of this study

1.2.1. Key research questions

This study aims to address three principal research questions:

- How do the **regulatory requirements and enforcement mechanisms of the Artificial Intelligence Act (AI Act) interact with those of horizontal and sector-specific EU digital legislation?** The analysis focuses on key legislation within ITRE's remit: energy, research and innovation, industry and SMEs, digital, telecoms and cybersecurity, as well as space policy, including topics such as sustainable prosperity, competitiveness, and European technological sovereignty.

  As a result, the legislation in scope is the GDPR, recent data legislation (the Data, Data Governance, Digital Services and Digital Markets Acts), recent information security legislation (the Cybersecurity Act, the Cyber Resilience Act and NIS2), as well as the New Legislative

[4] Sartor, G. et al., 2022, *Thirty years of Artificial Intelligence and Law: the second decade.* 2022, Artificial Intelligence and Law, Volume 30. pp. 521-557.

[5] European Commission proposals for an Omnibus IV Simplification Package.

Framework (NLF) on product quality assurance, taking into consideration the role of compliance certification mechanisms. Other digital legislation is out of scope of the present study, although other Committees have examined key topics – such as e.g. AI liability[6] – through separate initiatives.

- In what ways do the existing overlaps and inconsistencies between the AI Act and other EU digital regulations **impede industry development and the adoption of emerging AI technologies?** How are these barriers manifested across various sectors, and across the lifecycles of development, deployment and application?

- What **specific recommendations and policy actions** can be proposed to harmonise the AI Act with the broader EU digital legislative framework, reduce unnecessary and/or counterproductive regulatory burdens and foster a more conducive environment for the development and adoption of AI technologies across industries?

In this study, we thus examine the main overlapping, inconsistent and/or conflicting provisions between the AI Act and EU digital and sector-specific regulations, with particular attention to certification mechanisms and procedures entrusted to national law, which are likely to result in fragmentation. Ultimately, the study will provide recommendations, supported by quantitative key findings, to enhance the integration of AI technologies within the EU digital legislative framework, thereby fostering innovation while ensuring safety and trustworthiness.

The analysis is complemented by an Annex presenting a comparative table of the AI Act and other EU digital laws, indicating the type of interplay (overlap, gap, inconsistency), a short description, and suggested remedies where applicable.

1.2.2. Methodological challenges

The preparation of this study faces several methodological challenges. Firstly, **the AI Act is a very recent legislative initiative**, which makes it impossible to evaluate its overall effectiveness at this stage. Considerable uncertainty remains regarding its practical implications and long-term impacts on stakeholders across both the AI and the broader digital ecosystem.

Secondly, artificial intelligence is inherently a **global and general-purpose technology**, characterised by dynamic and rapid advancements and cross-border applications.

While this creates challenges when compared with other international regulatory frameworks, the EU's position as "regulatory first mover" provides a measure of regulatory certainty that can encourage investment and support medium- to long-term planning by AI providers.

[6] Bertolini, A., 2025, *Artificial Intelligence and Civil Liability – A European Perspective*, Publication for the Committee on Legal Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg.

Thirdly, the European Union's digital regulatory landscape is notably **intricate and multifaceted**, encompassing numerous layers of legislation that govern different aspects of technology and innovation.

This complexity can inadvertently hinder the competitive edge of EU-based companies in global markets. It is therefore essential to strike a balance between ensuring robust regulation and maintaining an environment conducive to technological growth and competitiveness.

However, it should also be recognised that each existing digital regulation established by the EU addresses specific policy needs that are pertinent to safeguarding the EU's values and ethical considerations, such as user safety, privacy and trustworthiness. The objective of this study is to determine whether the current regulatory terrain can be harmonised, streamlined, or simplified without undermining these fundamental policy goals. This requires a **balance between reducing regulatory burdens while maintaining robust protections** for all parties involved in and affected by AI development and deployment.

Ultimately, achieving a coherent and efficient regulatory approach depends on close cooperation among policymakers, industry experts and other key stakeholders.

1.3. Methodology and structure of the study

This study relies on legal analysis and a desk review of academic and policy literature. Findings were cross-checked to ensure accuracy and mitigate the challenges noted above. The study is structured to directly respond to the three research questions identified above.

Chapter 2 establishes the baseline of the assessment by setting out the roots, content, philosophy, global context, and challenges of the AI Act, providing a common understanding of the instrument before examining its interaction with other frameworks.

Chapter 3 analyses the interplay between the AI Act and other EU digital legislation, highlighting overlaps, inconsistencies and areas where obligations may be fragmented, duplicative, or burdensome in practice.

Chapter 4 examines EU-level governance and coordination mechanisms, including the role of the AI Office, which is central to addressing fragmentation risks.

Chapter 5 sets out recommendations for short-, medium-, and long-term policy actions to streamline the regulatory landscape, enhance coherence, and support innovation, competitiveness, trust, and safety.

In addition, the study includes an Annex presenting a comparative table of the AI Act and other EU digital laws, indicating the type of interplay (overlap, gap, inconsistency), a short description, and suggested remedies where applicable.

2. A DEEPER LOOK AT THE AI ACT

Before examining the interplay between the AI Act and other digital legislation in the EU, it is important to establish a **baseline for comparison**: how is the AI Act actually intended to work? What problems does it aim to solve and how? How are the various stakeholders affected?

The purpose of this chapter is not to provide a comprehensive overview of the AI Act's obligations; there are many authoritative sources[7] on this topic already. Rather, it aims to provide an accessible understanding of how the AI Act is designed to function. This baseline is necessary to support the subsequent assessment of its interplay with other digital legislation in Chapter 3.

2.1. Intervention logic of the AI Act – what problem does it set out to resolve?

The initial proposal for the AI Act was published in 2021, accompanied by an impact assessment[8], exploring the problems the Act sought to address. While the assessment related to the Commission's original proposal (and not to the ultimately adopted version), it is nonetheless instructive to examine the problems highlighted in that study. It identified the **following problems** in particular[9]:

Table 1: Problem identification of the AI Act

Main problems	Stakeholders concerned
1. Use of AI poses increased risks to safety and security of citizens	Citizens, consumers and other victims; affected businesses
2. Use of AI poses increased risk of violations of citizens' fundamental rights and Union values	Citizens, consumers and other victims; whole groups of society; users of AI systems liable for fundamental rights violations
3. Authorities do not have powers, procedural frameworks and resources to ensure and monitor compliance	National authorities responsible for compliance
4. Legal uncertainty and complexity dissuade development and use of AI systems	Businesses and other providers developing AI systems; businesses and other users
5. Mistrust in AI would slow down AI development in Europe and reduce the global competitiveness of the EU economy	Businesses and other users; citizens using AI systems or being affected by them
6. Fragmented measures create obstacles for a cross-border AI single market and threaten the Union's digital sovereignty	Businesses developing AI, mainly SMEs affected; users of the AI system, including consumers; businesses and public authorities

Source: European Commission, 2021, Impact Assessment SWD (2021) 84 final, 'Main problems', p. 13.

[7] Pehlivan, C. et al., 2024, *The EU Artificial Intelligence (AI) Act: A Commentary*, Wolters Kluwer; or Smuha, N. (ed.), 2025, *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, Cambridge University Press.

[8] European Commission, 2021, *Impact Assessment accompanying the Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, SWD (2021) 84 final (Parts 1/2 and 2/2).

[9] European Commission, 2021, SWD (2021) 84 final, p. 13.

Together, these problems underscored a central concern: AI technologies posed inherent risks for which no coherent legal framework or enforcement mechanism existed. Absent EU-level intervention, Member States might legislate independently, creating fragmentation and undermining trust. The impact assessment, therefore, treated AI primarily as a risky product category requiring harmonised EU rules to secure the internal market. By contrast, innovation and competitiveness were treated as incidental considerations, seen mainly as outcomes of restored trust rather than objectives in their own right. This framing decisively shaped the AI Act's design.

2.2. Objectives of the AI Act – what does it set out to achieve?

The purpose of the AI Act is spelled out in its first Article: it aims "*to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union and supporting innovation*".

Thus, the Act emphasises regulatory harmonisation to protect against harmful effects, while also introducing innovation as a distinct policy goal. Innovation was not included in the original objectives of the Commission's Impact Assessment[10]; it emerged later in the legislative negotiations as a separate political priority.

Thus, the Act serves **three interlinked objectives: harmonising the internal market, protecting against harmful effects and supporting innovation.**

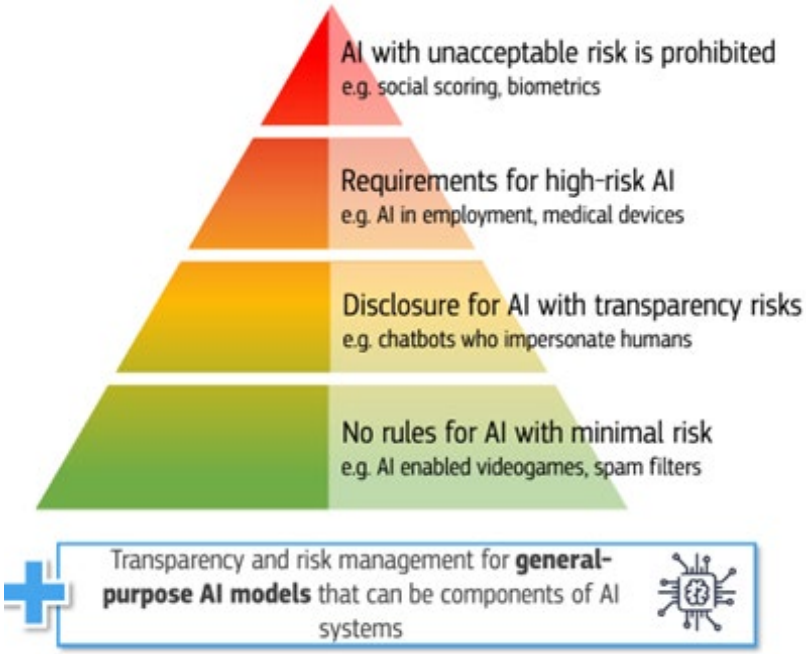
2.3. Regulatory philosophy of the AI Act – how does it aim to intervene?

2.3.1. Product legislation as the basic model

Based on the intervention logic and the objectives, it was reasonably foreseeable that the AI Act would largely follow the model of **European product legislation, supplemented with a risk-based approach and explicit human rights safeguards**. This approach was taken in the Commission's initial proposal and in the final AI Act.

[10] European Commission, 2021, SWD (2021) 84 final, p. 32.

Figure 1. Risk-based rules for AI systems



Source: European Commission, 2025, authors' own elaboration.

The AI Act places primary obligations on providers (developers), who must **assess and mitigate risks** linked to foreseeable uses of their systems:

- A short list of unacceptable risk[11] systems is banned entirely;
- Minimal-risk AI systems face no AI-Act-specific obligations (other EU laws, such as the GDPR, consumer law, or the DSA, can of course still apply);
- The Act imposes transparency obligations for certain use cases (e.g., chatbots, deepfakes), which do not pose a particularly high level of risk towards the users;
- Providers of high-risk AI systems are required to apply extensive measures, in line with those applied under the New Legislation Framework, as will be explored in Chapter 3 below.

[11] Namely those:

- deploying subliminal, manipulative, or deceptive techniques to distort behaviour and impair informed decision-making, causing significant harm.
- exploiting vulnerabilities related to age, disability, or socio-economic circumstances to distort behaviour, causing significant harm.
- containing biometric categorisation systems inferring sensitive attributes (race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation), except labelling or filtering of lawfully acquired biometric datasets or when law enforcement categorises biometric data.
- applying social scoring, i.e., evaluating or classifying individuals or groups based on social behaviour or personal traits, causing detrimental or unfavourable treatment of those people.
- assessing the risk of an individual committing criminal offenses solely based on profiling or personality traits, except when used to augment human assessments based on objective, verifiable facts directly linked to criminal activity.
- compiling facial recognition databases by untargeted scraping of facial images from the internet or CCTV footage.
- inferring emotions in workplaces or educational institutions, except for medical or safety reasons.
- applying 'real-time' remote biometric identification (RBI) in publicly accessible spaces for law enforcement, with certain exceptions.

Notably, they must:

- Establish a risk management system throughout the high-risk AI system's lifecycle;
- Conduct data governance, ensuring that training, validation and testing datasets are relevant, sufficiently representative and, to the best extent possible, free of errors and complete according to the intended purpose;
- Draw up technical documentation to demonstrate compliance and provide authorities with the information to assess that compliance;
- Design high-risk AI systems to enable them to automatically record events relevant to identifying national-level risks and substantial modifications throughout the system's lifecycle;
- Provide instructions for use to downstream deployers to enable the latter's compliance;
- Design high-risk AI systems to allow deployers to implement human oversight;
- Design high-risk AI systems to achieve appropriate accuracy, robustness, and cybersecurity;
- Establish a quality management system to ensure compliance;
- Draw up an EU declaration of conformity for each high-risk AI system and keep it at the disposal of the national competent authorities for 10 years after the high-risk AI system has been placed on the market or put into service; and
- Apply the CE marking to the system, to be affixed visibly, legibly and indelibly for high-risk AI systems.

The application of this traditional product legislation model poses particular challenges in the AI context. Firstly, the Act's broad definition of an "AI system" – "*a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*" – **creates legal uncertainty**. Because the definition relies on subjective criteria such as "varying autonomy" or "adaptiveness," it creates grey areas such that conventional algorithmic tools may fall within scope.

This ambiguity results in borderline situations where the distinction between AI systems and traditional digital tools becomes unclear, with significant compliance consequences. The Commission has issued specific guidance[12] on the notion of an AI system, but considerable uncertainty remains in practice.

Secondly, the **classification of 'high-risk' systems is complex and partly subjective in practice**.

[12] European Commission, 2025, *Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act)*, C(2025) 5053 final, Brussels.

An AI system is considered high risk if it is:

- used as a safety component or a product covered by EU laws in Annex I of the AI Act, and is required to undergo a third-party conformity assessment under those Annex I laws;
- or if it is listed under Annex III use cases, with a range of exceptions.

The dependence on cross-references to Annexes, which are partially based on objective legislation and partially on more subjective use cases that must be evaluated by the provider, makes it particularly complex in many instances to determine what is or is not a high-risk AI system. This burden is largely placed on the provider, who clearly has an incentive to downplay risks.

Thus, the AI Act applies a familiar EU product-safety model, but its broad definitions and complex classification rules significantly increase interpretive burdens, especially for providers.

2.3.2. Areas where the AI Act diverges from typical product legislation

While the core model of the AI Act is thus based on product legislation, it diverges from the standard template on a number of points. Since these are extremely relevant for the assessment of the interplay between the AI Act and other digital legislation in Europe, it is worth describing these briefly but explicitly.

a. Fundamental rights

Firstly, the AI Act has a **particular focus on fundamental rights**, including but not limited to data protection. This is, for instance, reflected in the high-risk classification rules: for Annex III use cases, an AI system is considered high risk in principle, except where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making. A provider that concludes an Annex III system does not present a significant risk must document that assessment before placing the system on the market or putting it into service.

Even more explicitly, Article 27 requires deployers of certain high-risk AI systems to conduct a fundamental rights impact assessment prior to their first deployment. This applies where the deployer is a body governed by public law, or a private entity providing public services, or another specified deployer of high-risk AI systems referred to in Annex III. The outcome of that assessment must be notified to the competent market surveillance authority. This obligation complements, but does not replace, any data protection impact assessment required under the GDPR, thereby creating a higher compliance threshold for fundamental rights than in other product categories.

Finally, Article 77 of the AI Act expands the powers of national authorities responsible for protecting fundamental rights, in relation to the use of high-risk AI systems referred to in Annex III, allowing them to demand the production of additional documentation from developers or deployers.

b. Application to deployers (users) of AI systems

A second difference between traditional product legislation and the AI Act is that the former focuses on the manufacturer and/or distributor of a product, whereas the AI Act extends (admittedly lighter) **obligations to users of AI systems** (referred to as 'deployers' in the AI Act, except where the AI system is used in a personal, non-professional context). The extent of these obligations depends primarily on the risk classification of the system. Deployers of general AI systems (i.e. those which are neither high risk nor prohibited) face transparency obligations: deployers must ensure that individuals are informed when they are interacting with an AI system, unless this is obvious from the context (Article 50).

By contrast, the AI Act imposes a significantly more **prescriptive set of obligations on deployers** of high-risk AI systems. These include obligations to ensure use of the AI system in accordance with the provider's instructions[13], assign human oversight to persons with necessary competence, training, and authority[14], ensure input data is relevant, sufficiently representative, and of appropriate quality where they control the data[15], monitor system operation and keep automatically generated logs[16], meet data governance obligations[17], conduct a fundamental rights impact assessment[18] where applicable, report incidents[19], and cooperate with competent authorities[20].

The distinction between general and high-risk AI systems is therefore crucial. While the former are subject mainly to transparency obligations, the latter trigger a substantial compliance burden that resembles the obligations of regulated actors under traditional product safety law. Importantly, these obligations are not merely procedural: the AI Act imposes substantive and continuous duties of diligence, transparency, and risk mitigation, which may necessitate significant internal organisational adjustments, especially for SMEs and non-specialist users. This asymmetry also raises concerns regarding legal uncertainty[21], especially in borderline cases where the classification of an AI system as 'high-risk' may not be straightforward.

c. GPAIs, systemic risk, and the Code of Practice

A third important consideration is that general-purpose AI systems (GPAIs) began to suddenly rise in popularity after the publication of the Commission's proposal for an AI Act in 2021. That proposal did not contain any specific rules in relation to GPAIs, and did not even mention them by name.

This gap was rectified during the trialogue negotiations, during which GPAI-specific rules were added as a parallel regulatory track in response to the emergence of powerful foundation models, alongside the general rules for AI systems.

---

13 Article 26(1), AI Act.

14 Article 26(2), AI Act.

15 Article 26(4), AI Act.

16 Article 26(5) and (6), AI Act.

17 Article 10, AI Act.

18 Article 27, AI Act.

19 Article 26(5) and 73, AI Act.

20 Article 26(12), AI Act.

21 Ebers, M. et al., 2022, *The European Artificial Intelligence Act: A Critical Assessment*, Law, Innovation and Technology, 14(1), pp. 1-44.

The need for this separate framework was driven by the challenge that GPAIs, by definition, are not bound to a specific use case and thus cannot be linked to a risk category. The application of the risk-based system was thus not possible.

As a result, an alternative model was created in Chapter V of the AI Act. Crucially, **GPAIs are not classified according to their risk level**. Instead, they are treated as a distinct functional category requiring upstream regulatory control, even before any specific application is built on top of them.

Under Chapter V, all providers of GPAI models must:

- Draw up and keep up to date technical documentation, including training and testing process and evaluation results;
- Draw up, keep up to date and make available information and documentation to supply to downstream providers intending to integrate the GPAI model into their own AI system, so that they understand the GPAI's capabilities and limitations;
- Establish policies to comply with Union law on copyright and related rights; and
- Publish a sufficiently detailed summary of the content used for training the GPAI model.

For GPAIs deemed to present "systemic risk"[22], further obligations apply, including adversarial testing, systemic-risk mitigation at the Union level, incident reporting, and cybersecurity safeguards[23]. Since these criteria are highly abstract, the AI Act also notes that a GPAI model shall be presumed to have high impact capabilities when the cumulative amount of computation used for its training, measured in floating-point operations, is greater than 10^{25} [24].

In practice, the computational threshold creates a presumption of systemic risk. Although arguably arbitrary and likely to become outdated, it reflects the legislator's view that – unlike general AI systems – GPAI risks correlate with the sophistication of training and must be addressed at the foundational layer of the AI value chain, rather than deferred until high-risk applications are deployed.

Providers meeting the quantitative threshold must notify the Commission and may attempt to rebut the presumption by demonstrating that their model does not present systemic risks.

In addition to having to satisfy the four general obligations above that apply to all GPAIs, providers of GPAI models with systemic risk must also:

- perform model evaluations in accordance with standardised protocols and tools reflecting the state of the art, including conducting and documenting adversarial testing of the model with a view to identifying and mitigating systemic risks;

[22] Article 51, AI Act.

[23] Article 55, AI Act.

[24] Article 51, AI Act.

- assess and mitigate possible systemic risks at the Union level, including their sources, that may stem from the development, the placing on the market, or the use of general-purpose AI models with systemic risk;
- keep track of, document, and report, without undue delay, to the AI Office and, as appropriate, to national competent authorities, relevant information about serious incidents and possible corrective measures to address them; and
- ensure an adequate level of cybersecurity protection for the GPAI model and the physical infrastructure of the model.

Since these are all fairly high-level obligations – both for general GPAI models and for those presenting systemic risks – GPAI model providers may demonstrate compliance with their obligations by voluntarily adhering to a Code of Practice, published by the AI Office. A final draft of this Code[25] was published in July 2025 and consists of three separately authored chapters: Transparency, Copyright, and Safety and Security. The first two chapters (Transparency and Copyright) apply to all GPAI providers[26], whereas the third Chapter (Safety and Security) applies only to providers of GPAIs with systemic risk[27]. On 1 August 2025, the Commission and the AI Board confirmed the Code of Practice as an adequate voluntary tool for demonstrating compliance. As of publication, more than 25 providers have elected to sign up to the Code of Practice, including major players such as Amazon, Anthropic, Google, IBM, Microsoft, Mistral AI, and OpenAI, signalling early uptake by major actors. The obligations pertaining to GPAIs also become applicable in a stages: as of August 2, GPAI providers must comply with transparency and copyright obligations when placing GPAI models on the EU market; models that were already on the market before 2 August 2025 must ensure compliance by 2 August 2027.

d. Innovation

As a fourth point where the AI Act diverges from the model of traditional product legislation, it **also aims to encourage innovation**.

The principal example is that the AI Act **does not apply to AI systems released under free and open-source licences**, unless they are placed on the market or put into service as high-risk AI systems, prohibited AI systems, or GPAIs[28].

This is justified in recital 102 of the AI Act by noting that such systems contribute to research and innovation, create growth opportunities for the Union economy, and inherently promote transparency and openness.

[25] European Commission, 2025, *General-Purpose AI Code of Practice*.

[26] Article 53, AI Act.

[27] Article 55, AI Act.

[28] Article 2(12), AI Act.

This philosophy **also lightens compliance obligations for downstream users of AI systems and models. Under Article 53(2) of the AI Act, providers** of certain AI models that are released under a free and open-source licence that allows for the access, usage, modification, and distribution of the model, are subject to lighter obligations than GPAI providers: they are not required to create technical documentation or provide information to support the integration of the GPAI model into their own AI system. A related exemption exists under Article 25(4), which relieves third parties making tools, services, processes, or components publicly available under free and open-source licences (other than GPAIs) from contractual obligations to provide information or assistance to high-risk AI providers.

Finally, one of the most innovation-oriented features of the AI Act is its **support for AI regulatory sandboxes**, defined as a controlled framework set up by a competent authority's supervision, allowing providers to develop, train, validate and test, where appropriate in real-world conditions, an innovative AI system, for a limited period under a sandbox plan[29].

These sandboxes are regulated in Articles 57-58 of the AI Act and have been promoted by EU institutions as tools for responsible experimentation and the support of SMEs and start-ups. Under Article 57(1) of the AI Act, the Member States must establish at least one regulatory sandbox at the national level by 2 August 2026. Their primary function is to enable AI system providers or deployers to develop and test AI systems in real-world conditions, without being subject to the full application of the AI Act's obligations, provided that adequate safeguards are in place. The AI Act also explicitly links the sandbox mechanism to SME participation, noting in Article 62 that SMEs should be granted priority access to the AI regulatory sandboxes by the Member States, and that Member States should provide them with advice and respond to queries about participation in AI regulatory sandboxes. This emphasis responds to widespread concern in the legal and policy literature that the compliance burden of the AI Act may disproportionately affect smaller actors, who often lack in-house legal or regulatory capacity[30].

By enabling temporary regulatory flexibility, AI sandboxes seek to lower the barriers to entry for novel AI systems, especially in sensitive or highly regulated sectors such as health, transport, and public administration. From an innovation policy perspective, sandboxes represent a "safe harbour" approach to a certain extent, balancing precaution with the need to stimulate European AI development. Comparative studies have noted that regulatory sandboxes can act as "learning laboratories" for both innovators and public authorities, as seen, e.g. in fintech and data protection contexts[31].

The sandboxing framework of the AI Act thus offers one of the few institutional mechanisms designed explicitly to reconcile innovation with regulation. While its scope is limited – particularly by the non-derogability of certain obligations – it nonetheless provides a structured avenue for safe and lawful experimentation.

[29] Article 57, AI Act.

[30] Smuha, N.A. et al., 2022, p. 8.

[31] OECD, 2023, *Regulatory Sandboxes in Artificial Intelligence*, OECD Digital Economy Papers, No. 356, OECD Publishing, Paris.

The effectiveness of this mechanism will ultimately depend on Member States' investment in competent authority and their willingness to interpret the sandbox provisions in a way that facilitates agile and iterative AI development within the bounds of EU law.

e. Mixed governance and enforcement

Finally, a fifth divergence from the traditional template of product legislation is the **mixed governance model of the AI Act**. Traditional EU product legislation relies on designated notifying authorities and market surveillance authorities, and accredited conformity assessment bodies. The AI Act incorporates these, but also introduces additional governance layers: the AI Office and the European AI Board at the EU level, the national GDPR supervisory bodies and the EDPS with respect to data protection issues, and more broadly, any national public authority or body responsible for supervising or enforcing fundamental rights obligations, including the right to non-discrimination. This produces a very broad and potentially overlapping set of competent national supervisory bodies[32], resulting in a particularly fragmented supervision and enforcement landscape for the AI Act.

2.4. Global Context and the EU position

2.4.1. AI in the global economy and the position of the EU

The AI Act represents the European Union's strategic response to the growing impact of artificial intelligence across sectors such as industry, healthcare, and public administration. The overarching challenge in this response is that, **while AI is a strategically indispensable component of modern technological advancement, the leadership in AI predominantly resides outside Europe**. The United States and China enjoy a particularly dominant position in the AI market and are largely unbound by the EU's fundamental values and unfettered by the AI Act. This raises doubts as to whether the AI Act alone can foster European digital leadership, or whether additional measures are required to bridge the gap between ambition and execution.

Globally, AI adoption is accelerating across all sectors. The 2025 AI Index Report by Stanford HAI[33] notes that US private AI investment in 2024 reached $109.1 billion, nearly 12 times China's $9.3 billion and 24 times the UK's $4.5 billion. AI business usage rose to 78% in 2024, up from 55% the year before, according to the same report.

Forbes projects global AI adoption will reach 378 million users in 2025, with the AI market valued at $244 billion[34] and expected to rise to $1 trillion by 2031. Additionally, 66% of people use AI regularly[35], making it an everyday reality for two-thirds of the planet's population.

---

[32] European Commission, 2025, *List of Fundamental Rights Protection Authorities under the AI Act*.

[33] Stanford University Human-Centered Artificial Intelligence, 2025, *Artificial Intelligence Index Report 2025*.

[34] Forbes, 2025, *AI 50 List*, dynamically updated online source.

[35] KPMG, 2025, *Trust, Attitudes and Use of Artificial Intelligence: A Global Study 2025 – Empowering Human-AI Collaboration for a Trusted Future*.

However, leading AI companies remain predominantly non-European. The aforementioned Forbes' 2025 AI 50 List contains only three EU companies (Deepl in Germany and Mistral and Photoroom in France), as opposed to 42 from the USA. Top players such as OpenAI, Anthropic and xAI are US-based, with OpenAI and Anthropic raising $81 billion in venture funding, more than half of the total $142.45 billion secured by companies on the AI 50 list. The Stanford AI Index further observed that U.S. institutions produced 40 notable AI models, compared to China's 15 and Europe's 3.

Concerns have also been raised within the European Parliament. A June 2025 ITRE Committee motion[36] noted that "*Weak investment and too much regulation are causing the EU to fall further behind on AI. In 2021, the Union accounted for only 7 % of global investment in AI, compared to 40 % for the USA and 32 % for China. In 2023, Europe invested approximately 5 billion euros in AI, compared to 20 billion euros for the USA. The US Stargate Project plans to invest 500 billion dollars over four years. The AI Action Summit in Paris showed that the EU was seen as a blocking factor because of its regulations*".

China is also rapidly closing the gap with the US. The recently established DeepSeek (founded in July 2023) disrupted the industry with its cost-efficient AI models, including its R1 model (released in January 2025), which matched Western models like GPT-4 at a fraction of the cost. Moreover, Chinese tech giants such as Alibaba, Baidu, ByteDance, Huawei and Tencent have all released their own AI products.

The relative dominance of non-European companies in the AI sector raises concerns about the alignment of these technologies with EU norms and values. AI solutions developed outside Europe are less likely to reflect EU regulations and ethical standards. The global nature of AI development and the fact that EU companies have thus far not been able to achieve a strong market position create concerns in relation to digital sovereignty: a critical technology is becoming increasingly central to the EU market, without certainty that it safeguards EU fundamental rights and values.

2.4.2. Regulatory approaches in the US and China

The AI Act represents the EU's adaptive, rights-based legislative response to AI, built to align with European values while remaining interoperable with global frameworks. The Act has been deliberately framed as adaptive legislation, leaving scope for future adjustment as technology evolves. This positioning becomes clearer when contrasted with the US and Chinese regulatory models.

The US and China are presently engaged in vigorous technological, economic and regulatory competition for dominance of the AI value chain[37]. Within this realm, the EU faces a decision as to whether it should contest dominance directly, align itself with one of the two powers, or seek to assert and sustain a comparative advantage in selected parts of the AI ecosystem. In making this choice, it must weigh competitive dynamics, citizen welfare and its regulatory, societal, digital and economic sovereignty.

---

[36] European Parliament, Committee on Industry, Research and Energy, 2025, *Report on European Technological Sovereignty and Digital Infrastructure – Motion for a European Parliament Resolution on European Technological Sovereignty and Digital Infrastructure*, 11 June 2025 (2025/2007(INI)).

[37] Chun et al., 2024, Comparative Global AI Regulation: Policy Perspectives from the EU, China, and the US. 2024.

The **EU's regulatory approach, through the AI Act,** is built around a coherent, universal, risk-based regulatory framework with strict and well-defined penalties. It has been praised for coherence but criticised for potentially stifling innovation, relying on ambiguous language and not anticipating the difficulties of implementing it consistently across use cases.

The **USA's AI regulatory approach** follows a decentralised, multi-stakeholder model. The Biden Administration's Executive Order on "Safe, Secure and Trustworthy Development and Use of Artificial Intelligence" delegated over one hundred tasks to more than fifty federal agencies across eight core policy areas (safety and security, innovation and competition, worker support, bias and civil rights, consumer protection, privacy, federal use of AI and international leadership). Additional initiatives have also emerged from the US Congress, individual states like California and even cities. This market-driven model has been criticised for over-reliance on self-regulation and the resulting risk of regulatory capture. In response, California (home to most leading AI companies) attempted to introduce stringent AI rules, but the proposals were ultimately vetoed[38], highlighting the tension between reliance on self-regulation and calls for stronger regulatory intervention.

China's AI regulatory approach combines the US approach of use-case-specific laws with general guidelines to produce a centralised and comprehensive registration, testing and monitoring framework. Innovation and economic growth are directly and indirectly supported by initiatives such as large-scale investment in thousands of SMEs and startups ('Little Dragons'), coupled with regulatory forbearance (lax enforcement). This hybrid approach has led to technological breakthroughs and economic successes, but risks criticism of capriciousness, given that regulations are not uniformly applied or enforced, which can impede investment and fall into the classic industrial policy trap of 'picking winners.'

More recently, growing trade tensions and technological and geopolitical competition between the US and China are bolstering arguments for AI regulation policies favouring faster innovation and technological independence aligned with industrial policy. The US, followed by China, has increased tariffs, coordinated international export bans and imposed sanctions on strategic technologies like EVs, advanced chips and semiconductor manufacturing equipment.

The present Trump administration has also floated the idea of an AI enforcement moratorium[39], which would limit the ability of individual states to legislate AI, a measure that is presented as pro-innovation.

These geopolitical tensions mean that the global regulatory landscape will continue to evolve as countries re-evaluate their stance towards risk alongside their desire to remain at the forefront of AI development.

[38] Associated Press (AP), 2023, *California governor vetoes proposed AI safety measures.*

[39] U.S. House Energy and Commerce Committee, *Proposal on Energy and Commerce*, 2025, notably Part 2—Artificial Intelligence And Information Technology Modernization, p.6.

2.5. Summary of the key challenges in the interpretation and application of the AI Act

The AI Act seeks simultaneously to function as product legislation, a fundamental rights instrument, and an innovation policy tool. This layering creates tensions that complicate its interpretation and application.

The main challenges can be summarised as follows:

Table 2: AI Act challenges

Tension	Description
Product legislation vs. fundamental rights	The AI Act adopts the model of product legislation (standardisation, CE marking, conformity assessment) but expands it to cover fundamental rights. This stretches a traditionally technical framework into areas requiring different expertise and methodologies.
Comprehensive legislation vs. fragmented approach	While framed as a horizontal regime, the AI Act coexists with other EU instruments (GDPR, copyright, and Data Act) with little to no carve-outs. Overlapping competences and governance across multiple authorities create risks of inconsistency or ambiguity in the interpretation and application of the AI Act
Static regulatory model vs. highly dynamic market reality	Although built on risk classification, the AI Act retains static features: systemic risk categorisation of GPAIs based on computational strength, reliance on conformity assessment and CE marking, and fixed (though amendable) lists in Annex I and Annex III. For high-risk AI and GPAIs with systemic risks, compliance burdens (documentation, evaluation, data governance) are significant and assumed to be continuous and permanent, requiring providers and deployers to re-evaluate risks as systems evolve. In practice, this combination of dynamic technology and a static framework may create uncertainty and incentivise risk acceptance over risk management.
Compliance burden vs. viable innovation	The AI Act seeks both to control a technology deemed highly likely to cause harm (thus requiring stricter rules than other ICT products) and to foster innovation. Reconciling these aims is difficult. In July 2025, 45 European companies (including Airbus, TotalEnergies, BNP Paribas, Carrefour, Siemens, Lufthansa, ASML, and AI startups such as Mistral AI and Pigment) sent an open letter (Stop the Clock)[40] to the European Commission requesting postponed enforcement and calling for "simplified and practical regulation". In their related report[41], they stated that the AI Act "*created market uncertainty through unclear risk categorisation, causing businesses to hesitate in AI adoption and potentially weakening Europe's global competitive position*"; and that there were "*insufficient guidelines for having*

[40] EU AI Champions Initiative. *Stop the Clock – Open Letter.*

[41] AI Champions, 2025, *An ambitious agenda for European AI,* February 2025, p. 42 and following.

Tension	Description
	different roles (e.g., as a provider or user), making it difficult to understand their obligations and liabilities". Simultaneously, 52 civil society organisations, experts and academics (including Amnesty International, BEUC, Bits of Freedom, Epicenter. works, European Digital Rights (EDRi), Statewatch and the 5Rights Foundation) expressed[42] their concerns to the European Commission about growing pressure to suspend or delay the implementation and enforcement of the AI Act. They noted that it firmly opposed "*any attempt to delay or re-open the AI Act, particularly in light of the growing trend of deregulation of fundamental rights and environmental protection, which risks undermining key accountability mechanisms and hard-won rights enshrined in EU law across a wide range of protections, including for people, the planet, justice and democracy. The EU "simplification" agenda should not be used to drive deregulation, especially in the absence of credible evidence that this would be necessary or effective*"; and that, *"instead of unravelling the EU rulebook, which includes hard-won legal protections for people, the Commission should focus on the full implementation and proper enforcement of its rules, like the AI Act"*.

Source: Authors' own elaboration.

The challenges outlined above demonstrate that the AI Act, while comprehensive in scope, is marked by structural tensions that will strongly influence its practical application. These tensions are not accidental; they are inherent to the Act's ambition of safeguarding fundamental rights while fostering AI development. Their resolution will depend less on textual interpretation alone than on consistent enforcement, the development of guidance by EU and national authorities, and the interaction of the AI Act with parallel regulatory frameworks. This sets the stage for the next chapter, which addresses the interplay between the AI Act and other instruments of EU digital regulation.

[42] EDRi, 2025, *Open letter: European Commission must champion the AI Act amidst simplification pressure.*

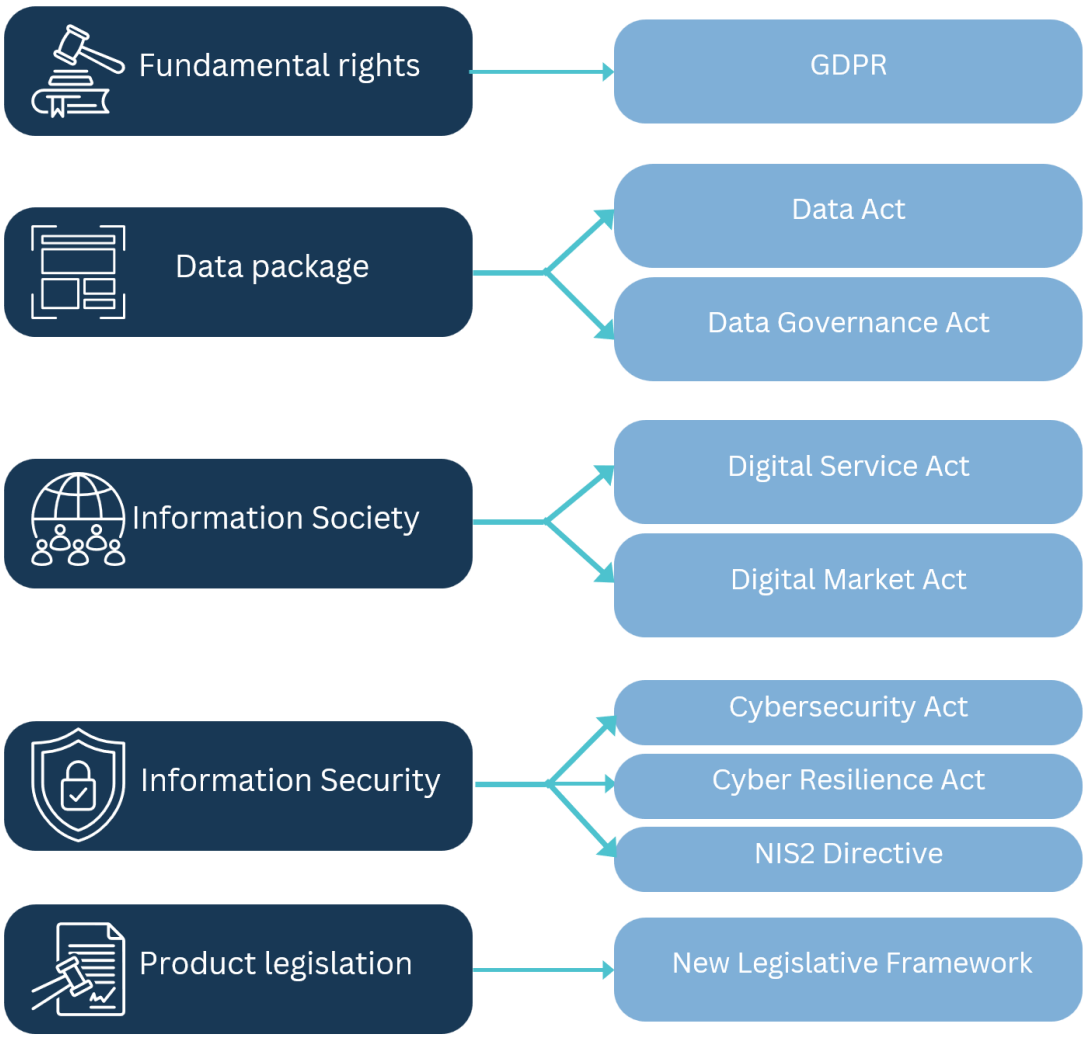
3. THE AI ACT'S INTERPLAY WITH OTHER DIGITAL LEGISLATION

3.1. Introduction – a bird's eye overview of the principal relevant EU digital legislation in the scope of this study

As has been noted above, the impact of the AI Act on the AI industry (and the broader digital economy) is only one part of the puzzle. The digital economy is strongly regulated by a large canon of EU legislative initiatives, each of which tries to address one component of the digital market. All of these must be analysed and understood in sufficient detail in the study in order to evaluate how they impact AI and where the interplays with the AI lie. Even when the AI Act states that it does not affect other laws or is without prejudice to them, many overlaps might arise in practice.

In the sections below, we will examine **a range of EU legislative initiatives** that can be broadly grouped as follows:

Figure 2: EU legislative initiatives in the digital economy and AI Act overlaps



Source: Authors' own elaboration.

In the sections below, for each of these legal frameworks, this study will describe:

- Its **objectives,** i.e. a short statement of what the legislation aims to achieve;
- Its **regulatory philosophy** (i.e. how did the legislation aim to affect the market at the EU and global level, and to what extent did it leave a margin for Member State policy and appreciation?
- Its interplay with the AI Act, notably:
  - Are there direct or indirect **overlaps** (i.e. identical or similar obligations that exist both in the digital legislation being examined and in the AI Act)?
  - Are there direct or indirect **gaps** (i.e. topics that would logically need to have been covered in either the digital legislation being examined or in the AI Act, but which are in practice covered by neither)?
  - Where the relationship between the digital legislation and the AI Act is likely to create problems or barriers in the AI market, notably in terms of **coherence, consistency or effectiveness –** i.e. whether the legislation contains obligations that are directly or indirectly contradictory or where the overhead created by the cumulative application of both legal frameworks is excessive taking into account the regulatory objectives and the actual risks.

3.2. Analysis of EU digital legislation and the interplay with the AI Act

3.2.1. The General Data Protection Regulation (GDPR)

a. Objectives of the GDPR

The GDPR[43] is the **central legislative instrument** of the European Union's data protection framework. Adopted in 2016 and applicable since 2018, it replaced Directive 95/46/EC[44] (1995 Directive) with a directly applicable regulation intended to overcome fragmentation in Member State laws and to provide a **harmonised legal framework** for personal data protection across the Union. As explicitly stated in Article 1, the GDPR "*lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data*," "*protects* ***fundamental rights and freedoms*** *of natural persons and in particular* ***their right to the protection of personal data***," and provides that "*the* ***free movement of personal data within the Union*** *shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data*"[45].

[43] European Commission, 2016, *Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016, General Data Protection Regulation (GDPR)*, OJ L 119, 4 May 2016, pp. 1–88.

[44] European Commission, 1995, *Directive 95/46/EC of the European Parliament and of the Council, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, OJ L 281, 23 November 1995, pp. 31–50.

[45] Article 1, GDPR.

This **dual objective** reflects the regulation's attempt to balance the fundamental right to data protection with the legitimate interests of organisations processing personal data and the broader goal of facilitating the free flow of personal data within the internal market while maintaining high standards of protection.

The GDPR also sought to modernise data protection law for the digital age. The 1995 Directive was conceived in a largely pre-digital era and was increasingly insufficient to cope with the challenges of globalisation, internet platforms, large-scale data sharing, and automated processing[46]. The regulation's preamble acknowledges this modernisation imperative in Recital 6, noting that "*rapid technological developments and globalisation have brought new challenges for the protection of personal data*[47]*.*

At the same time, Recital 4 clarifies that the right to the protection of personal data is not absolute but must be interpreted in relation to its function in society and balanced against other fundamental rights in accordance with the principle of proportionality[48]. Read together, these considerations show that the GDPR's modernisation agenda was twofold: to adapt the Union's data protection framework to technological realities and to ensure its continued relevance in an era of cross-border data flows, while embedding data protection within a broader fundamental rights balance that includes freedom of expression, the right to conduct business, and safeguarding public interests.

b. Regulatory philosophy of the GDPR

The GDPR embodies a **horizontal and principle-based regulatory philosophy**[49]. Its scope is comprehensive: it applies to all personal-data processing operations, across both public and private sectors, regardless of industry, technology, or context[50]. Unlike product- or sector-specific legislation, it does not regulate particular goods, services, or markets. Instead, it regulates a specific activity – the processing of personal data – and in doing so establishes a baseline of protection that applies consistently across the Union.

Central to this philosophy is the GDPR's technology-neutral and principle-driven approach. Rather than prescribing detailed technical rules that risk becoming obsolete, the regulation articulates broad principles intended to be applicable across all technological and organisational contexts. Article 5 sets out the key principles: lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability[51].

---

46 Hustinx, P., 2014, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, p. 26.

47 Recital 6, GDPR.

48 Recital 4, GDPR.

49 Recitals 10 and 13, GDPR; Article 2(1) and Article 5, GDPR.

50 Recitals 10 and 14, GDPR; Article 2, GDPR.

51 Article 5, GDPR.

Controllers and processors are required not only to comply with these principles but also to be able to demonstrate such compliance, making accountability an overarching organisational duty[52].

The Regulation is also **risk-based**, to a certain extent. Its obligations are calibrated to the risks posed to the rights and freedoms of individuals, recognising that not all processing operations present the same level of impact on individual rights[53]. Provisions such as data-protection impact assessments[54], security obligations[55], and the tiered approach to fines exemplify this proportionality[56]. The risk-based model allows the GDPR to be comprehensive yet flexible, with more demanding obligations applying where processing is likely to result in high risks, while less onerous obligations apply where the risks are low.

This combination of horizontal scope, technology neutrality, principle-based norms, role-based accountability, and a risk-calibrated application embodies the GDPR's regulatory philosophy. It ensures that the framework remains resilient in the face of technological change, while maintaining the core objective of protecting fundamental rights consistently across sectors, markets, and processing contexts.

c. Interplay with the AI Act

The relationship between the GDPR and the AI Act is expressly recognised in the latter. Article 2(7) AI Act provides that the act is without prejudice to Union law on the protection of personal data, and Recital 10 confirms the **primacy of the GDPR** whenever personal data are processed in the context of AI systems[57]. This ensures that the GDPR continues to govern all personal-data processing, while the AI Act overlays a product-safety style regime focused on the design, development and deployment of AI systems. Hence, although built on different regulatory philosophies, the interaction between the GDPR and the AI Act produces three distinct dynamics: (i) areas of overlap, where the two regimes impose parallel or similar obligations (for example, ex-ante assessments, transparency duties and security requirements); (ii) areas of inconsistency, where obligations diverge or recalibrate one another; and (iii) gaps, where neither regime provides sufficient clarity on how obligations should be reconciled in practice.

Legal basis under the GDPR in general, and the specific issue of legitimate interests

Under the GDPR, any processing of personal data (including its collection, analysis, or reproduction) requires a specific legal basis, which must fall within the confines of Article 6 GDPR[58].

[52] Articles 5(2), 28(1) and (3)(h) GDPR.

[53] Recitals 74-77 and 84, GDPR; Articles 24, 32 and 35, GDPR.

[54] Article 35, GDPR.

[55] Article 32, GDPR.

[56] Article 83(1) and (2), GDPR.

[57] Article 2(7) and Recital 10, AI Act.

[58] Article 6 GDPR.

In AI contexts, **Article 6(1)(f) GDPR – the "legitimate interests"** legal basis – is widely regarded as the **most relevant and frequently invoked basis**, particularly since consent (Article 6(1)(a)) is often impracticable and contractual or legal obligation bases (Articles 6(1)(b)–(c)) rarely map neatly onto AI training or deployment scenarios.

The interpretation of legitimate interest is, however, significantly affected by the AI Act, which **indirectly shapes the balancing test** that lies at the heart of Article 6(1)(f)[59].

Article 6(1)(f) of the GDPR provides that processing of personal data is lawful where it is "*necessary for the purposes of the legitimate interests pursued by the controller or by a third party*" except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject[60]. This ground is applied through a balancing test that weighs organisational interests against individual rights.

As Hacker has argued, the AI Act alters this balancing test, since compliance with AI Act obligations – such as risk assessments, traceability and fundamental rights safeguards – effectively recalibrates proportionality under Article 6(1)(f), raising the threshold for justification by embedding AI-specific requirements (e.g., explainability, robustness, monitoring) into the analysis[61]. Moreover, while the GDPR allows broad reliance on legitimate interests subject to safeguards, the AI Act designates certain practices as inherently risky, requiring conformity assessments or imposing outright prohibitions, and removing or at least reshaping the assessment by the AI system provider[62]. Thus, even if the balancing would favour the data controller under GDPR, the AI Act may still restrict the processing[63]. Divergence across Member States compounds the problem, as supervisory authorities already apply Article 6(1)(f) with varying strictness[64]. The overlay of AI-specific duties risks further undermining harmonisation.

Conceptually and as a matter of doctrine, the regimes of the AI Act and the GDPR remain distinct. Yet, in practice, compliance with the AI Act affects a controller's claim that its interests are "legitimate" - a controller cannot plausibly claim that its interests outweigh the data subject's rights where the AI system itself is unlawful under EU law. In this sense, the AI Act shapes the balancing test indirectly.

Impact assessments and the problem of divergent 'high risk' thresholds

Both the GDPR and the AI Act impose *ex ante* assessment obligations where risks to individuals' rights are heightened but do so according to divergent conceptions of 'high risk'.

Article 35 GDPR obliges controllers to conduct a Data Protection Impact Assessment (DPIA) whenever processing is "likely to result in a high risk to the rights and freedoms of natural persons,"[65] setting out the planned processing, its necessity and proportionality, and measures to address identified risks.

---

59 Hacker, P., 2024, *The AI Act between Digital and Sectoral Regulations*, Bertelsmann Stiftung, p. 21.

60 Article 6(1)(f) GDPR.

61 Hacker, P., 2024, p. 21.

62 Hacker, P., 2024, p. 21.

63 Hacker, P., 2024, p. 21.

64 Hacker, P., 2024, p. 21.

65 Article 35, GDPR.

Similarly, Article 27 AI Act requires deployers of high-risk systems to perform a Fundamental Rights Impact Assessment (FRIA)[66].

The duplication of assessments already creates compliance overheads, as organisations may need to carry out parallel DPIAs and FRIAs, covering clearly related and partially overlapping issues, but subject to different authorities and procedural requirements. However, the difficulty runs deeper: the two instruments **do not define 'high risk' in the same way**. Under the GDPR, risk is evaluated contextually, by assessing the likelihood and severity of impact on data subjects. Under the AI Act, 'high risk' is a regulatory classification, irrespective of the granular risk profile in a given deployment.

This divergence has practical consequences. While GDPR 'high risk' determinations under Article 35 are contextual and dynamic – sensitive to the actual severity and likelihood of harm in a particular processing operation – the AI Act imposes a formal, ex ante designation tied to product categories and use cases. This ambiguity had already been flagged at the proposal stage by the Centre for European Policy Studies (CEPS, 2022), which underlined the uncertainty over whether categorisation as 'high risk' under the AI Act should automatically trigger a DPIA under Article 35 GDPR[67]. This point remains unaddressed in the adopted AI Act, and as Hacker notes, the incongruence means that the same system may simultaneously be 'high risk' under one regime but not under the other, or vice versa[68].

This creates two layers of friction. First, organisations face a **duplication of compliance burdens**: a single deployment may require both a DPIA and an FRIA, covering overlapping subject matter but subject to different procedural standards and authorities. Second, **accountability structures differ**. The GDPR allocates responsibility through the controller/processor model, whereas the AI Act relies on lifecycle roles such as provider, importer, distributor and deployer. This can result in different actors being held liable for different aspects of the same AI deployment. For example, if an update by a provider alters system performance, the provider may be responsible under the AI Act, while the deployer may still be required to revisit its DPIA under the GDPR. This fragmented allocation raises compliance costs and risks of inconsistent enforcement.

While the lack of alignment generates burdens in practice, it is not strictly a legal inconsistency but the product of two different regulatory logics. Harmonisation could reduce compliance overhead, but would also risk flattening the distinct protective rationales of each framework.

Transparency and human oversight

GDPR Articles 13 and 14 require controllers to inform data subjects about the collection and use of their personal data, including purposes, legal basis, retention periods, recipients of personal data and rights of data subjects[69], while Article 22 provides safeguards in the case of decisions based solely on

[66] Article 27, AI Act.

[67] Bogucki, A. et al., 2022, *The AI Act and Emerging EU Digital Acquis: Overlaps, Gaps and Inconsistencies*, CEPS In-depth Analysis No. 2022-02, September 2022, p. 9.

[68] Hacker, P., 2024, p. 21-22.

[69] Article 13 and 14, GDPR.

automated processing by requiring that individuals be informed and able to obtain meaningful human review[70].

Additionally, Article 15(1)(h) entitles data subjects to "meaningful information" about automated decision-making[71].

In parallel, the AI Act frames comparable obligations partly as organisational design duties and partly as individual rights. Article 26(11) requires deployers of high-risk systems to notify affected persons when such systems are used[72]; Article 86 grants affected individuals a right to request and receive an explanation of the role of a high-risk AI system in decisions producing legal or similarly significant effects[73]; and Article 14 requires that high-risk systems be designed with mechanisms enabling effective human monitoring and intervention[74]. Thus, **while the GDPR articulates transparency and oversight as individual rights, the AI Act frames them as organisational responsibilities embedded in product design**, supplemented by a specific right of explanation in defined high-impact scenarios.

Security and traceability

GDPR Article 32 requires controllers and processors to implement appropriate technical and organisational measures to ensure security, including integrity, confidentiality and resilience[75], and Article 30 requires them to maintain records of processing activities[76]. The AI Act mirrors these obligations through a product-safety lens: Article 12 requires providers of high-risk systems to ensure automatic logging[77], Article 11, in conjunction with Annex IV, mandates comprehensive technical documentation to demonstrate conformity[78], and Article 26(6) requires deployers to retain records of use[79]. These provisions converge in their aim of ensuring accountability and auditability, but they also risk duplication, as organisations must maintain parallel documentation and record-keeping structures to satisfy both regimes.

Moreover, the overlap raises interpretative challenges: for example, AI Act Article 15(5) obliges providers to ensure robustness, accuracy and cybersecurity throughout the lifecycle of high-risk systems, which interacts with GDPR Article 32's requirement of "appropriate" security. Both impose open-textured duties, but the AI Act standard is technologically specific and lifecycle-focused, while the GDPR standard remains risk-based and contextual. This difference can create uncertainty as to which benchmarks must be met to avoid liability under both frameworks.

---

70 Article 22, GDPR.

71 Article 15(1)(h), GDPR.

72 Article 26(11), AI Act.

73 Article 86, AI Act.

74 Article 14, AI Act.

75 Article 32, GDPR.

76 Article 30, GDPR.

77 Article 12, AI Act.

78 Article 11 read with Annex IV, AI Act.

79 Article 26(6), AI Act.

Sensitive data and executability of rights

Article 9 of the GDPR prohibits the processing of special-category data (such as health or biometric data) unless an exception under Article 9(2) applies[80]. By contrast, Article 10(5) AI Act allows the processing of special categories of personal data for bias monitoring, detection and correction in high-risk AI systems, subject to appropriate safeguards; but it does not create an independent legal basis under the GDPR[81]. This creates an uneasy tension: the AI Act incentivises processing that, under the GDPR, would only be permissible where a valid derogation exists under Article 9(2) of the GDPR[82]. The result is that deployers may find themselves simultaneously **expected under the AI Act to use sensitive data** for bias correction, while **struggling to identify a valid GDPR legal basis** to do so[83]. Recital 70 of the AI Act gestures towards the "*substantial public interest*" derogation in Article 9(2)(g) GDPR[84], but this reference does not itself confer a sufficient legal basis: it remains for Union or Member State law to define the conditions under which controllers may actually rely on this ground. Moreover, as noted by Hacker, this provision on bias monitoring does not apply to generative AI, where it would also be relevant to address risks of discrimination and representational bias[85].

Moreover, the **executability of data subject rights** is uncertain once personal data has been absorbed into AI systems. Access, rectification, erasure and objection remain guaranteed under Articles 15-22 of the GDPR, yet neither framework provides workable methods to action these rights when data has been dispersed into model weights, embeddings or captured in logs retained for AI Act traceability. User prompts may themselves contain personal data, but once stored for monitoring, they cannot be selectively erased without compromising system integrity. **Controllers remain bound to honour requests they cannot technically fulfil**, while providers are required to preserve evidence for conformity. The result is not a legislative void, but an implementation problem. Rights exist on paper, but their operational delivery is practically infeasible[86].

Regulatory sandboxing

As mentioned above, Articles 57-59 AI Act provide for controlled environments for testing AI systems, but they do not relax GDPR obligations[87]. Participants must still identify a legal basis for data processing under the GDPR, even when processing is purely experimental. This is particularly difficult where testing requires special categories of personal data.

---

80 Article 9, GDPR.

81 Article 10(5), AI Act.

82 Article 9(2), GDPR.

83 See also Van Bekkum, M. et al., 2023, *AI Data Governance – Overlaps Between the AI Act and the GDPR*; and Baloup, M., 2022, *Using Sensitive Data to De-Bias AI Systems: Article 10(5) AI Act*; both of which discuss the tensions arising from Article 10(5) AI Act and its reliance on GDPR exceptions.

84 Recital 70, AI Act Baloup, M., 2022

85 Hacker, P., 2024, p. 23.

86 Bogucki, A. et al., 2022, p. 10.

87 Article 57-59, AI Act.

Recital 140 AI Act provides that regulatory sandboxes may rely on the "substantial public interest" ground under Article 9(2)(g) GDPR to permit the use of personal data originally collected for other purposes, subject to strict conditions and safeguards[88]. Yet all other GDPR obligations remain applicable, and **Member States may diverge in their interpretations**. Some authorities may accept reliance on Article 9(2)(g) for sandboxing of, for example, health-related data, while others may insist on explicit consent from each data subject. The absence of a harmonised approach means that the same AI pilot could be legally viable in one Member State's sandbox, but impossible in another[89]. For providers seeking to test cross-border services, this uncertainty erodes the value of sandboxes and may ultimately discourage their use.

Accountability

Under the GDPR, accountability in relation to compliance with the principles (ensuring a lawful basis, transparency, security, etc.) attaches primarily to the **controller**, who determines the purposes and means of personal data processing. Under the AI Act, by contrast, accountability attaches to **lifecycle roles**: the provider bears design and conformity obligations (technical documentation, risk management, post-market monitoring, corrective actions), while the deployer must use the system as instructed, ensure human oversight, keep logs and records, and (where applicable) perform an FRIA. On paper, therefore, the allocation of responsibility and liability is functionally distinct: the GDPR governs the **legality of processing**, while the AI Act governs the **safety and conformity of the AI system**. Yet in practice, the same actor (for example, an employer using an AI system) may simultaneously be both controller under the GDPR and deployer under the AI Act, leading to overlapping duties that must be coordinated.

The complexity of these overlaps is magnified in multi-actor supply chains. For instance, consider a high-risk AI recruitment system supplied by a provider to an employer, where the employer is a public authority or a private entity providing public services, thus warranting an FRIA under Article 27 AI Act. The employer, as deployer (and typically the data controller under the GDPR), must perform a DPIA under Article 35 GDPR and an FRIA under Article 27 AI Act before putting the system into use. If the provider later issues an update that materially changes the system, it must revisit its conformity assessment under the AI Act. It is less clear if, and at which point, the employer must also refresh its DPIA and FRIA for the altered system, even though the change is entirely outside its control and may not be entirely understandable or visible to the deployer. If both parties are required to reassess, this results in costly duplication (and in fragmentation, since different deployers may come to different conclusions); if only the provider acts, the employer's risk analysis soon becomes outdated. Neither framework clarifies how responsibility is divided in such scenarios, leaving organisations exposed to regulatory second-guessing and inconsistent contractual arrangements.

[88] Recital 140, AI Act.

[89] See also Van Bekkum et al., 2023, which discusses the continued applicability of GDPR obligations in sandboxes and the reliance on Article 9(2)(g) GDPR, even though it does not directly address Member State divergences.

A further **asymmetry** lies in the scope of impact assessments. The GDPR requires controllers to carry out **DPIAs in a wide range of risky processing situations** (e.g. large-scale use of special-category data, extensive profiling, or automated decisions with legal or similarly significant effects). By contrast, the AI Act requires an **FRIA only in limited circumstances**[90]. This narrower approach was already flagged as problematic at the proposal stage in the CEPS in-depth analysis[91], since it **leaves a gap** between the broader ex ante safeguards under the GDPR and the more limited triggers under the AI Act. The adopted AI Act has not addressed this mismatch.

Enforcement

Beyond these substantive obligations, regulatory coordination remains **fragmented**. The GDPR concentrates cross-border enforcement through the one-stop-shop mechanism and the European Data Protection Board, whereas the AI Act entrusts oversight to national market-surveillance authorities and the new AI Office, with data-protection authorities involved only in certain circumstances. This **institutional split** risks **parallel investigations**, **duplicative requests** for information and **inconsistent remedies** where the same conduct may amount both to unlawful processing and to an AI-system non-conformity.

Taken together, these challenges confirm that the main challenge in the interplay between the AI Act and the GDPR is not an absence of law, but the cumulative weight and misalignment of overlapping frameworks. Without **stronger coordination** between supervisory authorities, **clearer guidance** on the executability of rights, and **harmonisation of sandbox practices**, the interaction of the GDPR and the AI Act risks slowing adoption, raising compliance costs and fragmenting enforcement across the Union.

3.2.2. The Data Act (DA)

a. Objectives of the DA

The Data Act (DA)[92], adopted on 13 December 2023, is a central pillar of the European Strategy for Data[93] and complements the Data Governance Act as part of the Union's wider digital acquis. Its overarching objective is to establish a **harmonised framework governing access to and use of data**, thereby fostering a **fair, competitive and innovative data economy** across the internal market.

At its core, the DA pursues four interlinked aims. First, it secures for users of connected products and related services the right to access and use the data they generate, and to share that data with third parties under fair, reasonable and non-discriminatory (FRAND) conditions[94].

---

[90] Article 27, AI Act.

[91] Bogucki, A. et al., 2022, p. 10.

[92] European Commission, 2023, *Regulation (EU) 2023/2854 of the European Parliament and of the Council, 2023, on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)*, OJ L, 13 December 2023.

[93] European Commission, 2020, *Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A European strategy for data*, COM(2020) 66 final, Brussels, 19 February 2020.

[94] Chapter II Data, Act.

This is intended to rebalance the asymmetry between manufacturers or service providers and end-users, ensuring that the economic value of data can be more widely realised.

Second, it addresses imbalances in contractual relationships by preventing the imposition of unfair terms in data-sharing agreements, particularly where one party enjoys a stronger position[95]. These provisions are designed to enhance fairness and legal certainty in business-to-business arrangements, thereby lowering barriers to data use for small and medium-sized enterprises.

Third, the DA provides for mechanisms by which public authorities and Union institutions may request access to privately held data in situations of exceptional need (such as public emergencies), or where the data is required for the performance of statutory tasks[96]. These provisions are accompanied by safeguards to protect trade secrets, intellectual property and fundamental rights.

Fourth, the DA promotes a competitive and resilient European cloud and edge services market by ensuring switching and interoperability between providers, tackling vendor lock-in and reducing dependency on non-EU providers[97]. In parallel, it strengthens protections against unlawful third-country access to non-personal data, thereby reinforcing the Union's digital sovereignty.

Beyond these four core aims, the DA also introduces dedicated rules on interoperability of data spaces and data processing services[98] and a framework for international transfers of non-personal data and protection against unlawful third-country access[99]. These elements situate the DA as a transversal framework, ensuring that rights of access, contractual fairness, public-sector requests, and cloud portability are embedded in a wider governance structure that addresses sovereignty, interoperability and enforcement.

b. Regulatory philosophy of the DA

The DA is not a rights-based instrument in the manner of the GDPR, nor a product-safety instrument like the AI Act. Instead, it **embodies a market-making philosophy**, seeking to establish the conditions under which data can circulate more widely, fairly and efficiently across the internal market. Its central regulatory logic is economic: the legislator assumes that greater access to data, if organised under fair, reasonable and non-discriminatory (FRAND) conditions, will reduce structural asymmetries, lower barriers to entry, and unlock new opportunities for innovation and competition.

This philosophy is reflected in the Act's **horizontal scope**. It is largely[100] and deliberately not confined to particular sectors, products or services, but sets baseline rules that apply across the Union, cutting across vertical industries and technological domains.

---

95 Chapter IV, Data Act.

96 Chapter V, Data Act.

97 Chapter VI. Data Act.

98 Chapter VIII, Data Act.

99 Chapter VII, Data Act.

100 Arguably with the exception of the chapter II on connected products.

The aim is to reduce fragmentation by providing a common set of principles for access to data from connected products and related services, for fairness in contractual relationships, for public-sector requests in situations of exceptional need, and for switching and interoperability in cloud and edge markets. In doing so, the Act positions itself as a transversal layer in the EU's digital landscape, complementing sectoral frameworks without displacing them.

A second defining feature of its philosophy is **rebalancing asymmetries of power in the data economy**.

The Act recognises that the benefits of data-driven innovation have been disproportionately concentrated in the hands of manufacturers, large service providers and non-EU cloud actors, leaving users, smaller firms and public authorities with limited access. By prohibiting unfair contractual terms, mandating FRAND conditions for sharing, and creating enforceable switching rights, the Act seeks to address structural imbalances and enable a broader distribution of the economic value of data[101].

At the same time, the Act reflects a **European model of trust and sovereignty**, promoting innovation and competition while maintaining high standards of protection for individuals, trade secrets, intellectual property, and guarding against unlawful third-country access.

In this way, the DA seeks not only to unlock the economic potential of data but also to ensure that its circulation strengthens the Union's strategic autonomy and its capacity to set global standards.

c. Interplay with the AI Act

The DA was finalised before the adoption of the AI Act, and does not contain explicit cross-references to the AI Act or to artificial intelligence in general. The AI Act, in turn, mentions the DA only once in its recitals, in the narrow context of cross-border transfers of non-personal data during real-world testing[102]. The AI Act underscores that such transfers must be accompanied by appropriate safeguards in accordance with Union law, citing the DA and the Data Governance Act as relevant instruments. Despite this limited acknowledgement, in practice, the two acts meet in several places.

AI systems are **inherently data-driven**, and when embedded in connected products or related services, they **trigger both frameworks simultaneously**.

On the one hand, the DA secures for users access and portability rights over "readily available"[103] product and related-service data[104]. On the other hand, the AI Act imposes obligations on the AI functionality of those same products, including requirements relating to risk management[105], data

[101] On the economic value of data, see Krämer, J. et al., 2020, *The Role of Data for Digital Markets Contestability: Case Studies and Data Access Remedies*, CERRE Report.

[102] Recital 141, Data Act.

[103] Article 2(17,) Data Act.

[104] Article 2(15), 2(16) and 4(1), Data Act.

[105] Article 9, AI Act.

governance and dataset quality[106], technical documentation[107], logging/traceability[108], transparency/instructions[109], accuracy/robustness/cybersecurity[110], and, where applicable, conformity assessment[111].

For example, an AI-enabled agricultural machine generates sensor data during use, to which the farmer has access and portability rights under the DA, while the manufacturer must comply with AI Act duties to ensure the robustness, accuracy and traceability of the predictive algorithms processing that data.

The overlap is equally visible in cloud and edge environments: where datasets are hosted or processed on cloud or edge services, the DA's switching and interoperability rules require cloud service providers to enable dataset export and service switching[112]. Those rules do not oblige disclosure or transfer of model architectures, learned parameters or other protected digital assets. In those cases, the DA focuses on portability, not on preserving the integrity of compliance logs required under the AI Act. This means that, even when portability rights may be satisfied in accordance with the DA, continuity in audit trails and documentation required for AI Act traceability could be disrupted, leaving some lock-in risks intact. At the same time, a structural gap remains: while the DA ensures that users and third parties can obtain certain data in structured, machine-readable formats under FRAND conditions, it does not guarantee that the datasets are representative, accurate or error-free[113], nor that they enable replication of functionality in another (competing) AI system. Compliance with the AI Act's stricter dataset-quality standards under Article 10, therefore, remains the exclusive responsibility of AI providers. The two instruments thus diverge: one facilitates access, the other demands quality.

The scope is similarly limited for user inputs: prompts entered on a connected product or its related service fall within scope only insofar as they are actually retained in a retrievable form as "readily available" product or related-service data, in which case they must be made available to the user (and on request to a third party under FRAND terms). By contrast, parameters or weights derived from those prompts in the course of model training or fine-tuning constitute derived information and are excluded[114].

However, the picture is more complex in cloud contexts. If such parameters or prompts are treated as "co-generated data" (Art. 23(c) DA), and are not protected as trade secrets or intellectual property, they could be considered exportable/portable when switching providers, though this will depend heavily on the circumstances. In that sense, the boundary on access to AI-system-related data, including training, validation and testing datasets, is clear.

---

106 Article 10, AI Act.

107 Article 11, AI Act.

108 Article 12, AI Act.

109 Article 13, AI Act.

110 Article 15, AI Act.

111 Article 16(f), AI Act.

112 Article 23-31 and 33-36, Data Act.

113 Bogucki, A. et al., 2022, p. 7.

114 Recital 15, Data Act.

The Data Act guarantees access to data at the product/related-service layer and, in cloud/edge contexts, switching of datasets. Access to AI-stack components (such as weights and parameters) is generally excluded, but could exceptionally be required where these qualify as "co-generated data," are not protected as trade secrets, and the AI application or model can contractually be used by the customer outside the originating cloud environment.

A further point of interaction arises in relation to **public-sector access**. Under the DA's "exceptional need" regime, public bodies (and certain Union institutions) may request access to privately held data, subject to strict necessity and safeguards, with reinforced protection for trade secrets and limits on use[115]. Separately, under the AI Act, market-surveillance authorities can require providers to hand over documentation and, where appropriate, the training/validation/testing datasets (and, in narrowly defined conditions, even source code) for conformity assessment and enforcement[116].

Where the same operator is both a DA "data holder" and an AI Act "AI system provider", concurrent requests may need to be reconciled and sequenced to respect both sets of safeguards and confidentiality duties. The difficulty is that these regimes can apply simultaneously but for different purposes: DA requests serve urgent public policy needs, while AI Act requests ensure regulatory compliance. Without coordination, operators may face duplicative or even conflicting duties – for example, being required to share the same dataset under the DA with strict limits on reuse, while also providing it in full to a Member State authority under the AI Act for conformity checks – without guidance on sequencing or precedence.

Finally, the interplay also extends to **experimental contexts**. The AI Act permits real-world testing and regulatory sandboxes under the supervision of competent authorities[117].

These regimes are expressly without prejudice to other Union law[118] and require appropriate safeguards, including for transfers of non-personal data to third countries with DA/DGA protections. In practice, data used in testing remains subject to DA access/portability and to the DA's trade-secret protections. Because DA compliance is enforced by Member State competent authorities, and the AI Act does not provide a mechanism to integrate them into sandbox supervision, **participants may face divergent supervisory expectations**.

Even though DA rules are harmonised, authorities could interpret safeguards differently in practice (for example, one authority may insist that portability rights be fully maintained during testing, while another may deprioritise them), thereby **undermining the legal certainty that sandboxes are meant to provide**.

More generally, effective **cooperation between the authorities responsible for the DA and those enforcing the AI Act will be essential**; without such coordination, there is a risk of parallel

[115] Articles 14-15 and 17, Data Act.

[116] Article 74(12)-(14), AI Act.

[117] Article 57-59, AI Act.

[118] Recital 140, AI Act.

investigations, duplicative oversight or inconsistent remedies for the same AI-enabled product or service.

3.2.3. The Data Governance Act (DGA)

a. Objectives of the DGA

The Data Governance Act[119] was adopted on 30 May 2022 and was the first major legislative instrument adopted under the European Commission's European Strategy for Data[120] (thereafter to be followed by the Data Act, which was discussed in the preceding section).

The DGA responds to a long-standing challenge in EU digital policy: how to unlock the economic and societal potential of data while maintaining trust, sovereignty, and fundamental rights protections. It sits within a broader regulatory ecosystem that includes the Data Act, the GDPR, the Digital Markets Act and the AI Act, and is intended to complement rather than override existing sector-specific or horizontal data rules.

The DGA's core objective is to foster **trustworthy data sharing by establishing new institutional and procedural frameworks** to enable the reuse of protected public-sector data (Chapter II), the intermediation of data between parties (Chapter III), and the voluntary sharing of data for altruistic purposes (Chapter IV). Moreover, it provides the legal basis for the establishment of the European Data Innovation Board (EDIB – Chapter VI). It also lays the groundwork for sector-specific European data spaces as a further mechanism to drive innovation and economic growth.

Generally, the DGA aims to enhance the availability of high-quality data in order to encourage innovation, including in AI development, while preserving individual rights, trade secrecy, and the strategic autonomy of the Union. It reflects a distinctly European approach to the data economy, based on the principles of trust, fairness, and control, backed by a bespoke regulatory framework and governance mechanism.

b. Regulatory philosophy of the DGA

Rather than mandating data access or imposing data portability obligations, the DGA focuses on facilitation, creating a regulated environment in which both public and private actors can voluntarily share data under clear legal safeguards. To this end, the DGA introduces:

- A regime for the **reuse of public-sector data** that is subject to commercial confidentiality, statistical confidentiality, intellectual property rights or personal data laws (Chapter II), including harmonised conditions and technical requirements for secure access;

[119] European Commission, 2022, *Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)*, OJ L 152, 3.6.2022, pp. 1-44.

[120] European Commission, 2020, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions,* A European strategy for data, *COM(2020) 66 final*, Brussels, 19 February 2020.

- A new category of **data intermediation services** (Chapter III), including data marketplaces and sharing platforms, provided by entities that facilitate data sharing between data holders and users, especially those that enable data subjects to exercise control over their personal data. These entities must be independent, neutral, and registered with national authorities;
- A framework for **data altruism** (Chapter IV), provided by legal persons that collect data voluntarily made available by individuals or organisations for general interest purposes (e.g. scientific research) that wish to be recognised as "data altruism organisations", allowing individuals and companies to "donate" data for the public good;
- A specific **governance system**, relying on prior notification and registration of the regulated intermediaries at the EU and national level, under the supervision of national authorities; and
- The creation of a **European Data Innovation Board** (Chapter VI) to advise on best practices and ensure consistent implementation across Member States.

The DGA generally has the objective of making more data available in the EU, as well as increasing trust in voluntary data sharing and reducing barriers to the reuse of data.

In terms of regulatory philosophy, it does so by creating a specific and regulatory strict legal framework, under which data sharing intermediaries are regulated on demanding but equal terms across the European Union. In order to be able to refer to themselves as data sharing intermediaries, they must register at the national level, as a result of which they will be included in an EU-level register maintained by the European Commission[121]. Thereafter, their activities are subject to supervision by a designated competent authority in the Member State where they are established. At the time of finalisation of this study (September 2025), the register contains twenty-four data sharing intermediaries across six Member States.

When considering the interplay with the AI Act, the provisions in relation to data intermediation services are particularly salient, as is the role of the European Data Innovation Board.

c. Interplay with the AI Act

The DGA was adopted in May 2022, fairly shortly after the publication of the Commission's proposal for an AI Act, and it is thus not particularly surprising that it contains no provisions addressing artificial intelligence in particular, other than through two fairly oblique references in the recitals (noting respectively that the vision of a common European data space "*could be pivotal for the rapid development of artificial intelligence technologies*" (recital 2); and that the terms of use offered by data intermediation services "*should not be dependent on whether a potential data holder or data user is using other services, including storage, analytics, artificial intelligence or other data-based applications, provided by the same data intermediation services provider or by a related entity*"

[121] European Commission, accessed on 1 October 2025, *The EU register of data intermediation services*.

(recital 33)). Since the DGA was intended to be technologically neutral and sector agnostic, it is unsurprising that **no article addresses AI explicitly**.

While abstract and high-level, these references in the recitals nonetheless hint at a potential role of the DGA in relation to the AI Act.

The AI Act imposes **relatively demanding data governance obligations** on AI providers (notably for training data in relation to high-risk AI systems[122]), and creates potential trustworthiness concerns in relation to an AI system user's control over the data that they entrust to an AI system (as training data, input material, or as a prompt). The AI Act requires the implementation of appropriate data governance and management practices in relation to training data, and notes that such data sets should "*be relevant, sufficiently representative, and, to the best extent possible, free of errors and complete in view of the intended purpose of the system. In order to facilitate compliance with Union data protection law, such as Regulation (EU) 2016/679 (the GDPR)*[123]. Specialised data intermediation services might be suitable as a way of providing assurances on this point, since imposing this duty uniquely on the AI system provider creates an additional compliance burden on them, and the providers of AI systems arguably have a conflict of interest in relation to some of this data (in the sense that they have no direct incentive to make sure that any data is accessible or available to any other party).

A second potential area of interplay is the **European Data Innovation Board** (EDIB), established under Article 29 of the DGA, as an expert group consisting of "*representatives of the competent authorities for data intermediation services and the competent authorities for the registration of data altruism organisations of all Member States, the European Data Protection Board, the European Data Protection Supervisor, ENISA, the Commission, the EU SME Envoy or a representative appointed by the network of SME envoys, and other representatives of relevant bodies in specific sectors as well as bodies with specific expertise*" (a phrasing that is clearly sufficiently broad to encompass interactions with the AI Office or AI Board where relevant).

The Board has a broad range of tasks, including a mandate to assist the Commission "in addressing fragmentation of the internal market and the data economy in the internal market by enhancing cross-border, cross-sector interoperability of data as well as data sharing services between different sectors and domains, building on existing European, international or national standards, *inter alia* with the aim of encouraging the creation of common European data spaces". The mandate is arguably broad enough to use the EDIB as a vehicle to support the role of data-sharing intermediaries in the AI market, thus reducing the burdens and dependence on AI system providers with respect to training data. At a high level, the interplay with the AI Act thus rests on access to data required by the AI systems, and/or on data that would be of interested to users of AI systems.

[122] Article 10, DMA.

[123] Article 10(3), DMA.

3.2.4. The Digital Services Act (DSA)

a. Objectives of the DSA

The Digital Services Act[124] (DSA) is a cornerstone of the European Union's strategy to **modernise the regulation of online intermediaries and platforms**, ensuring a safer, more transparent, and accountable digital environment. Adopted to address the challenges posed by the exponential growth of digital services and the emergence of dominant online platforms, the DSA has the objective of modernising online content regulation laws and preventing illegal content from spreading online.

At its core, the DSA seeks to enhance user safety by imposing due diligence obligations on online platforms, particularly with respect to illegal content, goods and services. It mandates platforms to act swiftly on illegal content once notified, while safeguarding users' rights to freedom of expression and access to information. The Act also introduces requirements for algorithmic transparency, as well as obligations for Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) to assess and mitigate systemic risks—such as disinformation, discriminatory outcomes, and threats to public health and safety—posed by the operation of their services.

A key objective of the DSA is to establish accountability through transparency. It obliges digital services to disclose how content is moderated, how advertising is personalised, and how recommender systems function. This includes publishing transparency reports, providing explanations for content removals, and granting users the right to contest platform decisions.

Finally, the DSA aims to preserve the integrity of the internal market by creating uniform rules that reduce legal fragmentation and regulatory divergence across Member States. It introduces a framework of cooperation between national Digital Services Coordinators and the European Commission, thereby ensuring consistent enforcement and supervision.

b. Regulatory philosophy of the DSA

In terms of approach, the DSA imposes a **tiered set of legal obligations** on online intermediary services, proportionate to their role, size, and societal impact. These obligations apply to a **wide spectrum of service providers, including mere conduits, caching services, hosting services, and online platforms, with additional duties for VLOPs and VLOSE**s.

At the most basic level, all intermediary services benefit from limited liability for third-party content under certain conditions, provided they act as passive conduits or hosts and respond appropriately to notifications of illegal content. They are also required to implement notice and action mechanisms, enabling users to report illegal content effectively, and must provide clear terms and conditions, especially concerning content moderation and algorithmic decision-making.

[124] European Commission, 2022, *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)*. OJ L 277, 27.10.2022, pp. 1–102 (DSA).

Hosting services and online platforms face more stringent obligations, including the requirement to act expeditiously to remove illegal content upon receiving notice and to inform users about takedown decisions. They must also maintain an internal complaint-handling system, cooperate with national authorities, and report criminal offences to law enforcement where appropriate.

For online platforms, especially those with a large reach, the DSA mandates transparency reporting, advertising disclosures, and user redress mechanisms. They must also ensure traceability of traders using their services, particularly in marketplaces, through a "Know Your Business Customer" (KYBC) obligation.

The most stringent obligations are reserved for VLOPs and VLOSEs, including conducting annual systemic risk assessments, implementing mitigation measures, submitting to external audits, and granting data access to regulators and researchers. These entities are under enhanced scrutiny due to their potential impact on public discourse, democratic processes, and fundamental rights.

In essence, the DSA establishes a robust compliance framework for online intermediaries, balancing innovation with public accountability and user protection.

c. Interplay with the AI Act

At an initial, conceptual level, the interplay with the AI Act occurs in two ways. Firstly, AI systems can be used for content generation or manipulation; such content can then be shared through intermediary services. Secondly, AI systems and models might be a part of intermediaries' core offering or be used by online intermediaries for content moderation.

The starting point for exploring the interplay between AI Act and DSA at a legal level is to consider the roles they establish and the extent to which they may overlap. In the following paragraphs, we discuss substantive areas where, in many instances, their respective roles could be seen as overlapping.

Transparency on the use of AI

Whether used as part of a core offering or a mechanism for content moderation, AI systems deployed by intermediary services faced **extended transparency obligations**. Firstly, potential providers and deployers under the AI Act have to, e.g., inform natural persons when they are interacting directly with an AI system[125]. Secondly, the DSA requires intermediary services to create annual, publicly available reports on their content moderation practices[126], including information on the use of automated tools. These could clearly include AI systems used e.g., for content filtering. In principle, there is no direct overlap between the respective transparency obligations; however, overlaps can occur when AI systems that are used by intermediary services for content moderation are designated as high-risk AI systems or build on general-purpose AI models with systemic risk. In any case, guidance on AI Act's transparency obligations should include its current and potential interplay with DSA's measures of the same kind.

[125] Article 50, AI Act.

[126] Article 15, DSA.

Risk management frameworks

Both instruments place **risk management obligations** on the entities they regulate. Article 34 of the DSA requires VLOPs and VLOSEs to assess potential systemic risks stemming from the design, functioning and use of their services, tied to angles such as: design of algorithmic systems, content moderation systems or data-related practices; Article 35 requires corresponding mitigation measures. On the other side, Article 17(1)(g) of the AI Act requires providers of high-risk AI systems to have a risk-management system in place, as part of a quality management system. Moreover, providers of general-purpose AI models with systemic risk have to assess and mitigate systemic risks tied to their development, placing on the market or use, in line with Article 55(1)(b).

As a result, there is a risk of a practical overlap of risk management obligations, creating certain complexities. A first point to note is that for the AI Act, such obligations exist only for the providers of AI systems. If VLOPs/VLOSEs only act as the deployers of an AI system (e.g., using one provided by another entity), the obligations are distinct – while they may be burdensome and connected, there is no overlap in regulatory obligations. In contrast, if a VLOP/VLOSE acts as a provider of the AI system or model it uses on its platform/search engine – by developing it, placing on the market or putting into service under its own name - then a factual overlap can exist, in particular when the system is considered to be high-risk. In practice, this risk seems limited. Hacker supports this assessment, stating that VLOPs' and VLOSEs' "AI applications (...) are outside of the high-risk area of the AI Act, as this generally excludes e-commerce and search engines"[127].

A second problem can occur when VLOPS and VLOSEs act as providers of general-purpose AI models with systemic risk. In doing so, we should exclude a situation where one major entity is separately running, e.g., a VLOP in the form of a social media platform, and providing access to a general-purpose AI model in an unconnected manner, as obligations placed by each Act would simply run concurrently. The scenario where both lines of service are provided within a single digital service seems possible, but is currently less common. When someone is, e.g. using Google Search and this search engine adds a response box based on Google Gemini (a large language model), it does not automatically mean that Google is providing a general-purpose AI model; rather, it uses it itself.

Should an overlap of risk management obligations emerge, the AI Act takes this into account. Article 9(10) allows for AI Act requirements to be combined with existing frameworks established to comply with the DSA. Recital 118 of the AI Act seeks to provide a line of guidance here, adding that in this context, the AI Act's obligations should be presumed to be covered by DSA-based risk management frameworks, unless significant systemic risks not covered by AI Act emerge and are identified in related AI models.

Overall, the overlap of risk management obligations between the DSA and the AI Act appears to be very narrow, although the impacts when an overlap occurs could be significant. As a result, guidance dedicated to this scenario would still be valuable.

[127] Hacker, 2024, p. 17.

AI-generated or manipulated content

Obligations tied to the **detection and disclosure of AI-generated or manipulated content** are another interaction expressly noted in the AI Act[128]. The DSA requires VLOPs and VLOSEs to mitigate systemic risks related to such content where it "*resembles existing persons, objects, places or other entities or events and falsely appears to a person to be authentic or truthful*"[129], e.g., by placing prominent markings on it. The AI Act's Article 50, on the other hand, obliges providers of generative AI systems to ensure that AI-generated or manipulated content is marked as such. If a single entity is responsible e.g. both the VLOP and the AI system used for generating content, then the obligations would overlap. If the AI systems are instead deployed by another party than the VLOP, e.g., by embedding it, then the two entities must work in tandem (including at the technical level), to ensure availability and cohesion of content markings.

Illegal content generated through AI

The AI Act contains no explicit obligation to moderate AI outputs[130]. However, Article 55 of the AI Act does oblige providers of GPAI models with a systemic risk to assess and mitigate those risks, with recital 110 indicating that "***the dissemination of illegal, false, or discriminatory content***" should be seen as such a risk. It is worth noting that this risk has been increasingly identified and mitigated by many GPAI providers in recent years[131]. The DSA, on the other hand, focuses on moderation of content after it is hosted (not at the time of generation). The two pieces of legislation are compatible in this regard, since they focus on different stages in the content lifecycle. This can create problems of dispersed enforcement, where the content generating party might make different assessments than the host. Guidance on content moderation covering the interaction between the AI Act and DSA, exploring synergies and practical conflicts, would thus be quite useful. For VLOPs and VLOSEs in particular, it could be conveyed through a code of practice, developed under Article 56(2)(d) of the AI Act.

Intermediary liability

For intermediary liability, the AI Act explicitly states that it does "not affect" the provisions on the liability of providers of intermediary services as set out in Chapter II of the DSA[132]. Instead, **the AI Act complements the obligations of providers who embed AI systems or models into their DSA-covered services**[133]. An example would be YouTube's use of AI to edit users' videos[134].

---

128 Recital 120, AI Act.

129 Article 35(1)(k), DSA.

130 Hacker, P., 2024, p. 20.

131 Gao, L. et al., 2025, *"I cannot write this because it violates our content policy": understanding content moderation policies and user experiences in generative AI products*, in Proceedings of the 34th USENIX Conference on Security Symposium (SEC '25). USENIX Association, USA, Article 192, 3727-3746.

132 Article 2(5) and recital 11, AI Act.

133 Recital 118, AI Act.

134 Germain, T., 2025, *YouTube secretly used AI to edit people's videos. The results could bend reality*.

A noteworthy interaction in this context exists between the DSA's liability exemption for hosting providers, which depends on the providers not having actual knowledge of the illegal character of transmitted content[135], and the AI Act obligations that may lead to closer analysis and monitoring of the transmitted content, which potentially increases the chance of a provider obtaining knowledge of illegal content. Interestingly enough, Article 7 of the DSA might be solving this interplay by stating that the hosting exemption remains in place where providers "*take the necessary measures to comply with the requirements of Union law*", which would include the AI Act. A confirmation of this reading of the law would be useful, either by the AI Office or a judicial decision.

Researcher access to data

An interesting interplay between the DSA and the AI Act emerges with respect to **researchers' access to data and information about AI systems and models**. Article 40(4) of the DSA enables access by "vetted researchers" to data held by VLOPs and VLOSEs, for the purpose of studying systemic risks and related mitigation measures. There is no direct counterpart to this provision in the AI Act[136]. What may happen, however, is that researchers could use Article 40 of the DSA in order to obtain data for "*independent, decentralized and comprehensive risk analyses*"[137], potentially related to AI Act compliance.

In this context, it is also worth noting that the AI Act mandates the creation of a scientific panel of independent experts (Article 68), established by the Commission, which has, i.a., a role in alerting the AI Office to systemic risks related to general-purpose AI models. Article 91(3) enables duly substantiated requests for information to be conveyed by the panel to providers of general-purpose AI models. Therefore, in this context, the AI Act does enable researcher access to data on AI models for the purpose of studying systemic risks, though only to a narrow group of researchers. What remains to be seen is whether members of the AI Act's scientific panel will use the DSA to obtain data, and what information they will be able to share with the wider scientific community.

Concluding remarks

The overlap between obligations placed by the AI Act and DSA was, to a large extent, predicted by the EU legislators, including specific lines of overlap (transparency on the use of AI; risk management practices; AI-generated/manipulated content; intermediary liability; researchers' access to data). However, there is significant space for interpretation and implementation here, in areas such as:

- providing guidance on current and potential interplay of transparency obligations for intermediaries services providing or deploying AI systems;
- sufficiency of risk management practices under DSA and AI Act for VLOPs and VLOSEs acting as providers of general-purpose AI models with systemic risk;

[135] Article 6(1), DSA.

[136] Hacker, P., 2024, p. 19.

[137] Hacker, P., 2024, p. 21.

- harmonisation of marking schemes for AI-generated or manipulated content, under both DSA and AI Act;
- establishing a code of practice for intermediaries tackling illegal, AI-generated content, that covers both generation (AI Act) and moderation (DSA);
- legal clarity over the application of Article 7 DSA to the hosting liability exemption, in the light of the AI Act's extended monitoring duties; and
- strategic use and development of DSA and AI Act provisions regulating researchers' access to data on AI systems and models.

In pursuing these activities, it would be beneficial to establish close lines of collaboration between competent authorities, the Digital Services Coordinators and the European Board for Digital Services (established/designated by the DSA), and their counterparts from the AI Act framework (e.g. the AI Office and the national competent authorities).

3.2.5. The Digital Markets Act (DMA)

a. Objectives of the DMA

The Digital Markets Act (DMA)[138] is a central component of the EU's digital strategy. It aims to ensure fair and contestable digital markets, notably by imposing **ex-ante obligations on the largest and most powerful digital platforms, referred to in the DMA as "gatekeepers**." The DMA can be considered a targeted component of the EU's general competition policy, which is built around Articles 101 and 102 of the Treaty on the Functioning of the EU (TFEU). Those general rules are sometimes slow and difficult to apply in digital markets, due to the difficult of defining specific markets, determining dominance in those markets, and assessing potential market abuse. The DMA corrects this problem by more unambiguously identifying which players clearly have a dominant position through a gatekeeper designation and by pre-emptively imposing certain obligations on those gatekeepers, irrespective of any initiative from any other players in that market.

b. Regulatory philosophy of the DMA

At its core, the **DMA is a competition-focused regulatory tool** that complements existing competition law in Europe, but addresses structural and systemic risks to competition before harm occurs. Its primary goal is to curb unfair practices and reduce barriers that hinder smaller businesses, startups, and innovative firms from entering or expanding in digital markets dominated by a few powerful players.

[138] European Commission, 2022, *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)*, OJ L 265, 12.10.2022, pp. 1-66.

Much of the DMA only applies to so-called gatekeepers, which are defined as an undertaking that provides one or more core platform services (CPS). A company generally qualifies as a gatekeeper if it meets three cumulative criteria:

- It has a significant impact on the internal market;
- It operates a core platform service that serves as an important gateway for business users to reach end users;
- It enjoys, or is expected to enjoy, an entrenched and durable position in its operations.

To operationalise these general criteria, the DMA sets quantitative thresholds based on annual turnover in the Union, market capitalisation, and user numbers. For example, a company with at least €7.5 billion annual EEA turnover, a market capitalisation of at least €75 billion, and more than 45 million monthly active end users and 10,000 yearly active business users in the EU may be presumed to be a gatekeeper.

The Commission formally designates a gatekeeper through an administrative process, after giving the company the opportunity to respond[139]. Once designated, the gatekeeper has six months to comply with the core obligations set out in the DMA. The list of designated DMA gatekeepers is published online[140], including the CPS for which they are considered to be gatekeepers. At this time, no AI services are considered as a designated CPS, so there are no designated gatekeepers for AI systems in the EU (although major AI providers, such as Alphabet, Microsoft and Amazon, are listed as gatekeepers for non-AI CPS).

For designated gatekeepers, the DMA contains a mix of self-executing obligations (which are general and immediately applicable) and obligations that require further specification by the Commission[141].

The **core obligations** are listed in Articles 5, 6, and 7 DMA. The self-executing obligations of Article 5 include notably requirements such as:

- Prohibiting the combination or cross-use of personal data from different services without user consent[142];
- Prohibiting practices that prevent business users from offering the same products or services to end users through third-party online intermediation services or through their own direct online sales channel at prices or conditions that are different from those offered through the online intermediation services of the gatekeeper (i.e. measures that restrict business users from offering better conditions on other platforms)[143];
- Allowing end users to access and use, through its CPS, content, subscriptions, features or other items, by using the software application of a business user, including where those end users

[139] Article 3, DMA.

[140] European Commission, *Designated Gatekeepers under the Digital Markets Act (DMA)*.

[141] Subject to the procedures set out in Article 8, DMA.

[142] Article 5(2), DMA.

[143] Article 5(3), DMA.

acquired such items from the relevant business user without using the CPS of the gatekeeper (i.e. allowing interactions between the CPS and the software of a business user)[144];

- Prohibiting practices that require business users or end users to subscribe to, or register with, any further CPS listed in the gatekeeper's designation decision or which meet the thresholds of the DMA, as a condition for being able to use, access, sign up for or registering with any of that gatekeeper's CPS (i.e. no "mandatory cross-selling of CPS").

These provisions could potentially mitigate or some lock-in challenges in the AI industry, but are, of course, dependent on prior designation as a gatekeeper.

The provisions of Article 6 (which are susceptible to specification via implementing legislation) allow the Commission to more granularly specify enforcement measures. Key obligations include:

- A prohibition on a gatekeeper's use, in competition with business users, of any data that is not publicly available that is generated or provided by those business users in the context of their use of the relevant CPS or of the services provided together with, or in support of, the relevant CPS, including data generated or provided by the customers of those business users)[145].
- A ban on self-preferencing[146]: Gatekeepers cannot rank their own services more favourably in search results or rankings.
- A duty to enable interoperability with third-party services in certain cases[147]. Gatekeepers are not allowed to restrict the ability of end users to switch between and subscribe to different software applications and services that are accessed using the CPS of the gatekeeper.
- A duty to provide effective data portability and access to data generated by business users and end users[148].
- An obligation to allow business users fair and non-discriminatory access to app stores, search engines, or social networking services[149].

c. Interplay with the AI Act

While the DMA does not target AI systems per se, **it can be applied to designated CPS that may involve AI technologies**, particularly where the permissible CPS categories include operating systems, cloud services, and virtual assistants. Moreover, AI systems may be supporting components of designated CPS, such as AI-enabled browsers or search engines: an AI-driven search engine, virtual assistant, or content recommender system (such as components of Microsoft Copilot, Google

144 Article 5(5), DMA.
145 Article 6(2), DMA.
146 Article 6(5), DMA.
147 Articles 6(6) and 6(7), DMA.
148 Articles 6(9) and 6(10), DMA.
149 Article 6(12), DMA.

Assistant, or Amazon Alexa) could fall under the DMA if provided by a designated gatekeeper and identified as a CPS.

The same applies to AI APIs offered through cloud platforms (such as OpenAI APIs distributed through Microsoft Azure, or Google's Vertex AI APIs), which could trigger DMA obligations if the cloud platform provider is a gatekeeper for that CPS.

As of yet, **no AI system has been designated as a core platform service**. Thus, at present, the DMA's obligations cannot be readily applied to any AI system provider. Conceptually, though, a designation seems feasible for at least end-user AI systems, since Article 2.2 of the DMA indicates that a CPS can be:

> *(a) online intermediation services;*
>
> *(b) online search engines;*
>
> *(c) online social networking services;*
>
> *(d) video-sharing platform services;*
>
> *(e) number-independent interpersonal communications services;*
>
> *(f) operating systems;*
>
> *(g) web browsers;*
>
> *(h) virtual assistants;*
>
> *(i) cloud computing services;*
>
> *(j) online advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by an undertaking that provides any of the core platform services listed in points (a) to (i);*

Since a virtual assistant is defined as "*a software that can process demands, tasks or questions, including those based on audio, visual, written input, gestures or motions, and that, based on those demands, tasks or questions, provides access to other services or controls connected physical devices*"[150], at least some input-response focused AI systems could qualify. Moreover, cloud computing services could undoubtedly also encompass a part of the AI stack. In contrast, hardware components of the AI stack are not targetable as CPS under the DMA. Thus, designation as a gatekeeper under the DMA is viable for many parts of the AI stack, but not all.

The consequences of a gatekeeper designation could be far-reaching for AI system providers. As noted above, under Article 5 of the DMA, gatekeepers may not combine or cross-use personal data from different services, nor may they require cross-selling between their CPS (i.e. where an AI system is designated as a CPS, the service provider may not require business users to purchase another CPS as a condition for using a CPS).

[150] Article 2(12), DMA.

Depending on how Article 6 is implemented, AI system providers could also be prohibited from using customer AI inputs as training data or be banned from self-preferencing their AI services[151].

Furthermore, as AI becomes increasingly integrated into general-purpose digital interfaces (such as search engines, voice assistants, or enterprise productivity suites), the risk that gatekeepers may leverage control over AI-powered functionalities to distort competition is growing. This risk has been duly recognised, including by the creation of an Artificial Intelligence sub-group to the High-Level Group for the Digital Markets Act[152], specifically established with the purpose of ensuring coherence and effective complementarity in the implementation of the obligations set out in the DMA and of other sectoral regulations applicable to designated gatekeepers with regard to AI.

As a result, for AI systems that comprise, or are a component of, a designated CPS, within or through gatekeeper-controlled services, the DMA's obligations on data access, interoperability, anti-self-preferencing, and fair commercial terms could have far-reaching implications. This raises challenges, since the scope of the DMA (focusing on gatekeepers and CPS) is not aligned with the scope of the AI Act (focusing on AI system providers of high-risk systems and GPAI systems with systemic risks). Thus, there is a risk of both overlaps (with AI system providers being targeted by both sets of legislation) and gaps (being covered by one, but not the other).

However, as noted already, AI systems are thus far not designated directly as a CPS, although they are undoubtedly a component of some CPSs (such as Google Search, which now integrates Gemini AI by default).

This also implies that targeted intervention would be possible, notably through further specification of the Article 6 obligations that have been set out above, which could be aligned with those of the AI Act. This could be a useful instrument to curb lock-in or other competition law risks, while minimising the divergence between the application of the laws.

3.2.6. The Cybersecurity Act (CSA)

a. Objectives of the CSA

The Cybersecurity Act (CSA)[153] was adopted on 17 April 2019 and entered into force on 27 June 2019. It was introduced against the backdrop of rising concern about the cybersecurity resilience of digital products and services within the internal market, as well as growing geopolitical tensions around technological infrastructures. The CSA has the objective of **placing the EU in a more central position in ensuring a harmonised and effective approach to cybersecurity**.

[151] Bogucki, A. et al., 2022, p. 10.

[152] European Commission, 2025, *Fourth meeting of the Digital Markets Act High-Level Group – DMA first anniversary*, 7 March 2025.

[153] European Commission, 2019, *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*. OJ L 151, 7.6.2019, pp. 15–69.

The Regulation serves two principal policy purposes. First, it **strengthens the mandate of the European Union Agency for Cybersecurity (ENISA)**, transforming it from a coordination body into a permanent agency with enhanced operational and advisory powers.

ENISA is tasked with supporting Member States and EU institutions in preventing and responding to cybersecurity incidents, fostering cooperation, and developing sectoral guidance (Title II).

Secondly, and more significantly in the context of this study, the Cybersecurity Act establishes a **legal framework for EU-wide cybersecurity certification for ICT products, services, and processes (Title III)**. This framework allows for the creation of harmonised cybersecurity certification schemes across the Union, with a baseline of common characteristics defined in the CSA. Such schemes are intended to reduce market fragmentation, build trust in digital solutions, and increase the uptake of secure-by-design technologies. Certification under these schemes remains voluntary unless otherwise mandated by sectoral legislation, though it may become a de facto requirement in procurement or liability contexts.

The Act is widely seen as laying the institutional foundation for a more cohesive EU cybersecurity policy, while leaving open the path for future mandatory schemes in critical areas such as cloud computing and AI systems. It also complements horizontal instruments such as the NIS2 Directive and the more recent Cyber Resilience Act, thereby contributing to a layered and evolving cybersecurity framework across the EU.

b. Regulatory philosophy of the CSA

The Cybersecurity Act is **first and foremost an institutional framework**: it does not create significant legal obligations for any category of service providers as such; rather it ensures that ENISA has a permanent operational mandate in relation to cybersecurity (as opposed to its prior mandate, which was always temporary and principally focused on coordination and identification of best practices), and on allowing European cybersecurity schemes to be created and given legal authority. Under the CSA, a procedure for the creation of EU cybersecurity certification schemes is defined, along with a potential scope (covering ICT products, services and processes). Each scheme will specify one or more levels of assurance (basic, substantial or high), based on the level of risk associated with the envisioned use of the product, service or process. Depending on the scheme, conformity assessment can be done either on the basis of self-assessment or third-party certification via conformity assessment bodies (CABs), comparable to traditional product legislation.

Once adopted, Article 57 of the CSA provides that, as a general rule, national schemes that become covered by a European cybersecurity certification scheme shall cease to produce effects as of the approval of the European scheme. This is a remarkably strong effect, since it ensures that the schemes can effectively establish clear harmonisation at the EU level, and automatically overrule divergent national schemes.

The establishment of an EU-level certification scheme is complex, however, since it requires significant consensus-building.

As of yet, only one scheme (the EU Common Criteria (EUCC) scheme[154]) has been formally adopted[155], which was able to build on significant prior efforts and strong pre-existing EU-level consensus[156], with further work ongoing on separate schemes for 5G technologies[157] and cloud computing (EUCS)[158].

c. Interplay with the AI Act

No work has been initiated thus far for an AI system cybersecurity certification under the CSA. **Such an effort to create a European AI cybersecurity scheme under the CSA nonetheless is contemplated in the AI Act itself**, which explicitly notes that high-risk AI systems that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to the CSA shall be presumed to comply with the cybersecurity requirements set out in Article 15 of the AI Act (Article 42.2). Thus, an AI cybersecurity scheme under the CSA is explicitly viable from a legal perspective, and could be used to demonstrate compliance with the AI Act too (without being mandatory – CSA-based certification would be just one option for the provider of a high-risk AI system to demonstrate that they've satisfied the security requirements of the AI Act).

It is worth recognising, though, that this option may not be highly attractive in the market. The AI Act already applies a product safety approach based on risk levels, which includes but is not limited to cybersecurity concerns. For high-risk AI systems, where conformity assessment is mandatory, a **product conformity assessment would already comprise the relevant cybersecurity requirements of the AI Act**. Obtaining a separate cybersecurity certification that's recognised under the CSA would require a separate effort and investment, and would only demonstrate compliance with one single aspect of the AI Act, without removing the need (and obligation) of undergoing a broader conformity assessment. At best, an **AI Act cybersecurity scheme could be positioned as a standardised method for tacking the cybersecurity elements of the conformity assessment**, which would be sufficient for the conformity assessment bodies to accept the security level of the AI system as adequate. It is, however, not certain that this would reduce costs or efforts for AI system providers that are required to undergo a conformity assessment.

Moreover, the AI Act also contains a separate approach for GPAIs with systemic risks, for which a specific Safety and Security Chapter[159] has been created in its specific GPAI Code of Practice.

Claiming compliance with this Chapter is, in practice, adequate for GPAI providers to access the EU market, making **formal certification against a European cybersecurity scheme an investment without a guaranteed return**.

---

154 ENISA, 2021, *EUCC Cyber Certification Scheme V1.1.1*.

155 European Commission, 2024, *Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)*, C/2024/560, OJ L, 2024/482, 7.2.2024.

156 The scheme is based on the renowned international standard Common Criteria, which has been in use for issuing cybersecurity certificates in Europe and internationally for around 30 years.

157 ENISA, 2024, *Certification Scheme EU5G*.

158 ENISA, 2020, *European Cybersecurity Certification Scheme for Cloud Services*.

159 ENISA, 2020, *Candidate EUCS Scheme v1.0*.

Thus, **a European AI cybersecurity scheme under the CSA might have advantages in terms of fostering greater trust, but would be insufficient to obtain easy access to the European AI market**.

3.2.7. The Cyber Resilience Act (CRA)

a. Objectives of the CRA

The Cyber Resilience Act (CRA)[160] is part of the European Union's response to the growing risks associated with the interconnectivity and digitalisation of products and services, particularly the proliferation of Internet-connected devices and software-integrated technologies. The Act was adopted by the European Commission on 15 September 2022 and formally adopted by the co-legislators in 2024, becoming the first EU-wide legislation to impose horizontal (non-sector specific, unlike the AI Act) cybersecurity requirements on **products with digital elements** ('PDEs'). The provisions of the CRA will apply as of December 2027[161]. with certain reporting obligations and the rules on conformity assessment bodies applying earlier, starting 11 June 2026.

The CRA has the objective of **enhancing cybersecurity across the EU by establishing common requirements for products with digital elements** (both hardware and software) available on the market and used to connect to a device or network. The CRA emerges from a policy landscape increasingly shaped by the securitisation of digital infrastructure, where economic competitiveness, public safety, and geopolitical autonomy intersect.

The principal objectives of the CRA are:

1. To ensure a **high common level of cybersecurity for PDEs**, such as smart devices, operating systems, and embedded software, by imposing mandatory cybersecurity requirements throughout the product lifecycle[162];

2. To **close regulatory gaps** by extending obligations not only to manufacturers but also to importers and distributors within the EU market[163], following a model similar to product safety law under the New Legislative Framework (NLF);

---

[160] European Commission, 2024, *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)*. OJ L, 2024/2847, 20.11.2024.

[161] However, as a transitional provision, the CRA provides that products with digital elements that have been placed on the market before 11 December 2027 shall be subject to the requirements of the CRA only if, from that date, those products are subject to substantial modifications. This means that those products with digital elements can continue to be commercialized as long as no substantial modification is brought to them. Moreover, PDEs that already conform to other European Union harmonisation legislation, such as machines under the Radio Equipment Directive and Machinery Regulation, have a little more time before they must comply with the CRA. For those products and services, the CRA will apply on 11 June 2028, or subject to the expiry provisions referred in the relevant harmonisation legislation. It is important to note that this specific transitional provision for products covered by other European harmonisation legislation does not provide a free-for-all for these products and services. If a substantial modification is brought to such product and services, a new certification will always have to be obtained. In that case the requirements of the CRA will have to complied with in addition to the other European harmonisation legislation requirements. In short, those products and services will be deemed not to fall under the scope of the CRA between 11 December 2027 and 11 June 2028, as long as no substantial modification is brought to the product or service after the entry into application of the CRA.

[162] Articles 5–10, CRA.

[163] Articles 12–14, CRA.

3. To impose **obligations for vulnerability handling and incident reporting**, ensuring that manufacturers remain responsible for security even after products are placed on the market[164]. Manufacturers must conduct conformity assessments, implement cybersecurity-by-design principles, and report actively exploited vulnerabilities and severe incidents within 24 hours;

4. To **reduce market fragmentation** by harmonising national cybersecurity rules and removing barriers to cross-border trade caused by divergent technical requirements. At the same time, the CRA aims to make cybersecurity a unique selling proposition of EU PDEs;

5. To **protect end-users**, including consumers and businesses, by increasing transparency and enabling more informed purchasing decisions through mandatory declarations of conformity and post-market surveillance mechanisms.

b. Regulatory philosophy of the CRA

In terms of approach, the CRA intervenes in the market by **mandating that PDEs are designed, developed, and maintained with appropriate cybersecurity measures throughout their lifecycle**. This is achieved by imposing requirements both on economic operators and PDEs. In general, PDEs may only be placed on the market if they meet certain cybersecurity requirements. This, therefore, requires the conduct of a cybersecurity risk assessment, taking into account the following elements:

- The PDE's use case;
- Essential functionalities;
- Supporting functionalities;
- Functions assets;
- Data assets;
- Interfaces;
- Communication types;
- Operational environment;
- Attack surfaces; and
- Threats

In addition, the manufacturer will have to implement vulnerability handling by identifying vulnerabilities, addressing them, performing security testing, making available security updates for at least 10 years, disclosing vulnerabilities, and sharing information.

The cybersecurity risk assessment must be documented and included in the technical documentation. The product must undergo a conformity assessment, with an EU declaration of conformity and CE-marking (comparable to what is required under the AI Act).

Certain products with digital elements are designated as important or critical and are subject to additional requirements. These are products with a greater inherent cybersecurity risk or PDEs used in the security sphere.

[164] Articles 10 and 11, CRA.

Thus, where the Cybersecurity Act introduced a voluntary cybersecurity certification framework and NIS 2 requirements on important and essential entities, the CRA introduces mandatory requirements applicable to nearly all digital products placed on the EU market, irrespective of whether they are certified. These obligations are directly enforceable and backed by regulatory oversight, market surveillance, and significant penalties for non-compliance (Article 53). Where the Cybersecurity Act is institutional and procedural, the CRA is substantive and prescriptive, embedding cybersecurity requirements into product design and lifecycle management.

c. Interplay with the AI Act

At a high level, the interplay between the CRA and the AI Act lies in the fact that **AI systems are often a product with a digital element**. The base rule is that, where multiple types of product legislation apply to the same product with digital elements, the requirements set out in all those laws apply cumulatively. This means that under each of those laws (including the AI Act for high-risk AI systems), a conformity assessment would have to be performed, and an EU declaration of conformity drafted up. Considering the administrative burden, the CRA provides that manufacturers may draft a single declaration of conformity, containing the identification of all Union legal acts concerned (Article 13). This means that a single document can be established to covers the declaration of conformity for all relevant product legislations.

Since the CRA is a more recent instrument than the AI Act, the interplay is actually specifically addressed in Article 12 of the CRA. As a general principle, paragraph 1 of that Article notes that PDEs that also qualify as high-risk AI systems are deemed to comply with the cybersecurity requirements set out in Article 15 of the AI Act if they fill the essential cybersecurity requirements set out in Part I of Annex I of the CRA; the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in Part II of Annex I of the CRA; and the achievement of the level of cybersecurity protection required under Article 15 of the AI Act is demonstrated in the EU declaration of conformity issued under this Regulation. Essentially, for PDEs that qualify as high-risk AI systems, the Annexes of the CRA become a critical evaluation criterion under the AI Act.

Conformity assessments for such PDEs must, however, still be done in accordance with the requirements of the AI Act (not of the CRA), with the exception of important and critical PDEs; for those, the more stringent procedures of the CRA apply.

Thus, interactions between the AI Act and the CRA have been considered explicitly in the existing body of legislation. More complex situations can occur in relation to hybrid systems that combine AI and non-AI digital components. Where the entire system is a PDE, and the AI components are also produced by the same manufacturer of the PDE, then no particular problem should arise – the PDE must undergo the usual conformity assessment, which comprises the AI component and takes the characteristics of the AI component into account.

If, on the other hand, the AI system is a component of the PDE insourced from a third party manufacturer, the AI system will in principle have undergone a conformity assessment under the AI Act and/or under the CRA, and the PDE manufacturer may take this assessment of the AI component into account as a part of its due diligence obligations under the CRA. Finally, if the manufacturer of the PDE chooses to also bring the AI system to the market as an independent product, then it will have to assess that product under the AI Act – which may, indeed, require a new assessment of a system that was already assessed when it was purely a component of the original PDE.

It is also worth noting that the conformity assessment of the AI Act is largely a one-off obligation that applies before bringing a product onto the market, and where post-market monitoring focuses only on high-risk AI systems as such. The CRA includes post-market monitoring of the PDE as a whole.

More generally, the question has been raised whether the reliance on conformity assessment methodologies is not more conducive to risk acceptance, whereas effective trust requires continuous risk management[165]. This is especially true for hybrid systems, where risks may arise at one point in the product cycle (e.g. training of AI) or in one specific component, with harms that follow elsewhere and significantly later (e.g. at application time, or even further downstream), in a manner that could not necessarily be foreseen during the conformity assessment of an AI system itself.

3.2.8. The NIS2 Directive (NIS2)

a. Objectives of the NIS2 Directive

The NIS2 Directive[166] has the objective of contributing to a **high common level of cybersecurity across the EU, in the context of network and information systems**. It seeks to improve upon its predecessor, the NIS1 Directive.

b. Regulatory philosophy of the NIS2 Directive

In terms of approach, it does so by requiring specific attention to be paid to **essential and important entities through national cybersecurity strategies, well-developed institutional and enforcement frameworks, and specific cybersecurity requirements** tailored to such entities.

Essential and important entities are defined by the role played by the services they operate, with essential entities being subject to more stringent requirements.

[165] Laux, J. et al., 2023, *Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk*, Regulation & Governance, vol. 18(1), p. 27.

[166] European Commission, 2022, *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. OJ L 333, 27.12.2022, pp. 80–152.

To this end, the Directive points to 18 sectors, splitting them into:

- 11 sectors of high criticality[167]: energy; transport; banking; financial market infrastructures; health; drinking water; waste water; digital infrastructure; B2B ICT service management; public administration; and space;
- 7 other critical sectors[168]: postal and courier services; waste management; manufacture, production and distribution of chemicals; production, processing and distribution of food; manufacturing; digital providers; and research.

Such entities may be public or private, and they are mostly going to be larger organisations (although there is a pathway to including crucial SMEs and micro-SMEs in the scope of the Directive).

Core pillars of the NIS2 Directive are:

- **National cybersecurity strategies** – Member States have to adopt such strategies, and ensure they include: objectives and priorities; governance frameworks; risk assessment and response mechanisms; a list of key related authorities and stakeholders; and a plan for cybersecurity awareness among citizens[169];
- **Authorities** – Member States have to designate or establish a set of authorities reinforcing the Directive's goals, namely: competent authorities for cybersecurity and supervision of the Directive's implementation, single points of contact, cyber crisis management authorities and computer security incident response teams (CSIRTs);
- **Collaboration** – On both national and Union levels, the Directive contains multiple provisions aimed at improving collaboration involving the indicated authorities and other stakeholders. This covers both short-term initiatives (such as incident response) and long-term ones (such as knowledge and best practice sharing). Specific initiatives set up by the Directive include a CSIRTs network[170] and a European cyber crisis liaison organisation network (EU-CyCLONEe)[171];
- **Cybersecurity requirements for essential and important entities** - These include an increased role of management bodies in cybersecurity; risk assessment and management duties; and use of suitable technical, operational and organisational measures. The minimal package of said measures is to include elements such as policies (for risk analysis and information system security), incident handling measures, supply chain security measures and more[172];
- **Enforcement and supervision** – Member States have to ensure that competent authorities under the Directive are in a position to enforce and supervise its implementation, including through direct interactions with entities. Powers at the authorities' disposal include on-site inspections, security audits and scans, as well as requests for information, data and evidence[173].

[167] Annex 1, NIS2 Directive.
[168] Annex 2, NIS2 Directive.
[169] Article 7, NIS2 Directive.
[170] Article 15, NIS2 Directive.
[171] Article 16, NIS2 Directive.
[172] Article 21, NIS2 Directive.
[173] Articles 32 and 33, NIS2 Directive.

c. Interplay with the AI Act

At a high level, the interplay with the AI Act lies in the **use or (less frequently) provision of AI systems or models by essential and important entities** and the need to ensure cybersecurity in this context.

The **AI Act does not expressly refer to the NIS2 Directive**. At the same time, the potential for overlap between the two instruments is tangible, mainly where one considers overlapping duties of entities acting as both actors regulated under NIS2 and AI Act. Examples could include a health body using AI for managing patient data (becoming a deployer of AI) or a bank offering an AI chatbot for investment advice (provider and deployer). Moreover, many uses of AI by essential and important entities are likely to brush against the high-risk criterion of the AI Act, precisely due to the sensitive nature of the services they provide.

Moving onto specific lines of overlap: essential and important entities (NIS2 entities) have to establish and apply cybersecurity **risk management measures**[174]. The AI Act requires the presence of a risk management system for high-risk AI systems. Similarly to DSA, as described in s. 3.2.4 of this study, Article 9(10) allows for merging or combining risk management measures.

Beyond general risk management measures, each legislative instrument requires taking (to a varying extent) specific **cybersecurity measures**. The AI Act's Article 15 lays out a relatively direct list of measures for development and design of high-risk AI systems, enhancing their robustness and resilience; these include AI-tailored steps such as protection against data or model poisoning attacks. While these steps are mostly relevant to providers of AI systems (some of whom can be covered by NIS2, as earlier mentioned), the AI Act also pulls deployers into cybersecurity efforts, albeit in a less direct manner; by requiring them to use the system in line with instructions, assign human oversight to sufficiently expert users, and ensure the appropriateness of input[175].

Article 21 of NIS2 sets out a list of angles that should be included in cyber-risk management, including, e.g., incident handling, supply chain security, the use of cryptography and/or encryption, as well as the use of multi-factor authentication. These are all considered from the perspective of users (of network and information systems). The Directive is not focused on the development side of cybersecurity, like the AI Act is.

Incident reporting is a further overlapping area. In the AI Act's Article 73, there is an obligation to report serious incidents with high-risk AI systems to market surveillance authorities. While the core obligation is placed on the provider of AI systems, the provision also indicates a role for deployers in notifying the provider (or even the authority directly).

In NIS2, essential and important entities have to report significant incidents to CSIRTs and/or competent authorities – irrespective of whether they are providers or deployers. The timelines and processes for reporting are different between the AI Act and NIS2, with NIS2 generally having shorting reporting periods.

[174] Article 21, NIS2 Directive.

[175] Article 26, AI Act.

Overall, **the AI Act could have addressed the overlap(s) with the NIS2 Directive more directly** – it is tangible and likely enough to warrant this. Incident reporting shows well how essential and important entities using AI systems might have a dual reporting burden in case of incidents, with different reporting timelines and (potentially, depending on national implementation choices) different authorities to report to. The burden could be seen as tripled if we add GDPR data breach obligations. Some NIS2 overlaps are covered by broad alignment provisions – for example, in the case of risk management measures. However, just as with the DSA, combining such regimes in practice may be a challenging task for entities falling within both legislative acts.

3.2.9. The New Legislative Framework (NLF)

a. Objectives of the NLF

The New Legislative Framework (NLF) is **not a specific legislation, but rather refers to a set of EU legal instruments that was first adopted in 2008 and further developed thereafter**, to improve the internal market for goods by strengthening product safety, ensuring uniform application of technical legislation, and enhancing the conformity assessment and market surveillance systems.

Core legal acts within the NLF are notably:

- Regulation (EC) No 765/2008[176], relating to accreditation and market surveillance;
- Decision No 768/2008/EC[177], relating to the marketing of products, including CE marking;
- Regulation (EU) 2019/1020[178], on market surveillance and compliance of products

The NLF contains no specific requirements for specific product categories.

These are adopted by separate legislation (Directives or Regulations), including, at this time[179]:

1. Toy Safety – Directive 2009/48/EU;
2. Transportable pressure equipment – Directive 2010/35/EU;
3. Restriction of Hazardous Substances in Electrical and Electronic Equipment – Directive 2011/65/EU;
4. Construction products – Regulation (EU) No 305/2011;
5. Pyrotechnic Articles – Directive 2013/29/EU;

[176] European Commission, 2008, *Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93*. OJ L 218, 13.8.2008, pp. 30–47.

[177] European Union, 2008, *Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC*. OJ L 218, pp. 82–128.

[178] European Commission, 2019, *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*. OJ L 169, 25.6.2019, pp. 1–44.

[179] European Commission, 2008, *New legislative framework*.

6. Recreational craft and personal watercraft – Directive 2013/53/EU;
7. Civil Explosives – Directive 2014/28/EU;
8. Simple Pressure Vessels – Directive 2014/29/EU;
9. Electromagnetic Compatibility – Directive 2014/30/EU;
10. Non-automatic Weighing Instruments – Directive 2014/31/EU;
11. Measuring Instruments – Directive 2014/32/EU;
12. Lifts – Directive 2014/33/EU;
13. ATEX – Directive 2014/34/EU;
14. Radio equipment – Directive 2014/53/EU;
15. Low Voltage – Directive 2014/35/EU;
16. Pressure equipment – Directive 2014/68/EU;
17. Marine Equipment – Directive 2014/90/EU;
18. Cableway installations – Regulation (EU) 2016/424;
19. Personal protective equipment – Regulation (EU) 2016/425;
20. Gas appliances – Regulation (EU) 2016/426;
21. Medical devices – Regulation (EU) 2017/745;
22. In vitro diagnostic medical devices – Regulation (EU) 2017/746;
23. EU fertilising products – Regulation (EU) 2019/1009;
24. Drones – Commission Delegated Regulation (EU) 2019/945 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems;
25. Batteries – Regulation (EU) 2023/1542;
26. Machinery – Regulation (EU) 2023/1230 (replacing Directive 2006/42/EC that entered into force before the NLF, still applicable until 20/1/2027);
27. Ecodesign requirements for sustainable products – Regulation (EU) 2024/1781;
28. Artificial Intelligence Act – Regulation (EU) 2024/1689;
29. Cyber Resilience Act – Regulation (EU) 2024/2847;
30. Packaging and Packaging Waste – Regulation (EU) 2025/40.

These frameworks further specify the general rules of the NLF. As the list above indicates, **the AI Act and CRA are considered to be a part of the NLF framework** (numbers 28 and 29 in the list above).

b. Regulatory philosophy of the NLF

The general regulatory logic of the NLF is that the three foundational legal acts are common to all types of products, whereas product-specific requirements are set out in the individual product-specific legislations listed above.

The three foundational acts can be very briefly summarised as follows:

Regulation (EC) No 765/2008 – Accreditation and Market Surveillance

The regulation creates the basis for the operation of national accreditation bodies (NABs), the role of conformity assessment bodies (CABs), and the processes for verifying compliance in the market. It also creates the basic framework for CE marking. It establishes the NLF's standard rules for:

- The appointment and role of the NABs;
- The accreditation of CABs by NABs, in principle within each Member State, and tied to specific normative frameworks for specific product categories;
- The presumption of conformity for NABs – once peer reviewed under the Regulation, each NAB is deemed to be competent for all of its relevant harmonised standards;
- Community market surveillance for relevant (NLF-covered) products sold in the EU. Member States must appoint market surveillance authorities and define their areas of competence. These authorities will then ensure compliance with NLF standards in their Member State;
- Controls procedures on products entering the EU market, including by checking the existence of appropriate documentation and (where applicable) CE markings;
- Finally, the rules in relation to CE marking, including the principle that the manufacturer applying the CE mark thereby becomes responsible and liable for ensuring compliance with NLF rules.

Regulation (EC) No 765/2008 is arguably the cornerstone of the NLF, as it creates most of the key concepts that all NLF frameworks rely upon.

Decision 768/2008/EC – Marketing Framework

The second component of the NLF is Decision 768/2008/EC on a common framework for the marketing of products. **This Decision quite literally provides a "template" for EU product legislation** in its Annexes. The main body of the Decision is quite short, and principally defines how conformity assessment procedures under the NLF are supposed to work, what the role is for key stakeholders (e.g. manufacturer, importer), and how the EC declaration of conformity must be used.

The bulk of the Decision consists of its three Annexes: the first providing a template with reference provisions for community harmonisation legislation for products; the second describing permitted conformity assessment procedures; and the last providing a template for declarations of conformity.

Regulation (EU) 2019/1020 – Market Surveillance and Compliance

Finally, the third NLF pillar is 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. This Regulation focuses on market surveillance and compliance of products within the EU internal market.

The purpose of this Regulation is to **strengthen market surveillance for products subject to EU harmonisation legislation**, ensuring that only compliant and safe products reach the EU market.

It defines obligations for economic operators (manufacturers, importers, distributors, fulfilment service providers), who:

- Must ensure the existence and availability of proper compliance documentation;
- Must act quickly on non-compliance;
- Need to have a responsible operator established in the EU.

It also empowers market surveillance authorities to conduct inspections, request documentation, take corrective measures, and block unsafe or non-compliant products. Finally, it establishes a network for coordinated enforcement (the Union Product Compliance Network).

Thus, the NLF provides a fairly flexible, mature and stable framework for product assessment.

c. Interplay with the AI Act

As the list above indicates, **the AI Act is a part of the NLF, at least with respect to high-risk AI systems**. The reality is a bit more nuanced, in the sense that some high-risk AI systems were already subject to the NLF, simply because the AI systems were a component of a product that fell within the scope of one of the legislations listed above. Where the AI system was indeed a part of a product that is already subject to a third-party conformity assessment (meaning that it is subject to an NLF law that already requires third-party assessment), that third-party assessment remains in place. However, where the AI system is not related to a regulated product, the AI Act allows ("*at least in an initial phase of application of this Regulation*", as recital 125 notes) conformity assessment by the provider under its own responsibility. I.e. **for those AI systems, self-assessment and CE marking are permitted** (with the only exception of AI systems intended to be used for biometrics, which still require third-party conformity assessment).

More precisely, the self-assessment procedure can be used only if:

- The high-risk AI system is not listed in the Annex III use cases (which enumerate high-risk AI systems by domain, such as biometric identification or education);
- The provider has applied a quality management system and performed a conformity assessment as per Annex VI; and
- The system is not subject to cybersecurity certification under a European cybersecurity certification scheme.

This procedure is outlined in Article 43 of the Regulation.

Additionally, even if a system is listed in Annex III, the self-assessment path may still be used if the harmonised standards or common specifications cover all relevant essential requirements.

In all cases, as was already discussed above, providers must prepare and maintain technical documentation, issue the EU declaration of conformity, and affix the CE marking to indicate compliance.

Thus, there is a **clear integration between the AI Act and the NLF, but the logical coherence between those two instruments is harmed through the complex scope of the AI Act**. The AI Act is only coherent with the NLF for high-risk AIs, but this requires a difficult ad-hoc assessment of the risk profile of AI systems, and GPAIs were carved out of the NLF logic entirely. The interplay is clear; coherence much less so.

4. EU LEVEL GOVERNANCE – THE ROLE OF THE AI OFFICE

4.1. Introduction – the AI Office in the AI Act

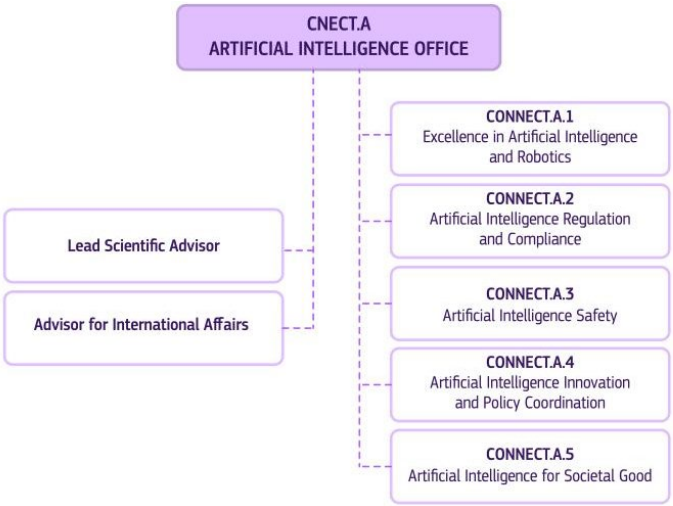
Under the AI Act, the AI Office (AIO) was created within the European Commission (EC) as the centre of AI expertise, forming the **foundation for a single European AI governance system**. It was established in January 2024 by a Commission Decision[180], in advance of the AI Act's entry into force on 1 August 2024; presumably, to give it time to prepare for its crucial role. As Novelli et al note, "in implementing the AI Act, much will depend on *getting the AI Office right*"[181]. For the purposes of this study, this includes exerting positive influence over the relationship between AI Act and other EU legislation.

The AIO is generally tasked with:

- Supporting the AI Act and enforcing rules on general-purpose AI models and systems;
- Strengthening the development and use of trustworthy AI;
- Fostering international cooperation;
- Supporting its cooperation with institutions, experts and stakeholders, including the AI Board

Member States are to support the AIO in these tasks[182]. Structurally, the AIO has been set up within the European Commission's Directorate-General for Communications Networks, Content and Technology (DG CONNECT), in a team comprising five units and two advisors, reflecting its mandate:

Figure 3: AIO's structure



Source: European Commission, 2025.

[180] European Commission, 2023, *Decision No 1/2023 of the Joint Committee of the Regional Convention on pan-Euro-Mediterranean Preferential Rules of Origin of 7 December 2023 on the amendment of the Regional Convention on pan-Euro-Mediterranean preferential rules of origin*. OJ L, 2024/390, 19.2.2024. http://data.europa.eu/eli/dec/2024/390/oj.

[181] Novelli, C. et al., 2025, *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, European Journal of Risk Regulation 16(2), pp. 566-590, p. 575.

[182] Article 64(2), AI Act.

4.2. Principal role and responsibilities

4.2.1. General role

The starting point in the AI Act for defining the AIO's role is Article 3(47), which describes it as "*contributing to the implementation, monitoring and supervision of AI systems and general-purpose AI models, and AI governance, provided for in Commission Decision of 24 January 2024*;". As Cancel-Outeda notes, this wording highlights that the **AIO is not a separate EU agency**[183], and as Novelli et al note, it **does not grant the AIO a separate legal personality**[184].

Article 3(47) also adds that references to the AIO are to be construed as references to the EC. **What is less clear, however, is the extent to which the reverse is intended – for references to the EC to be construed as references to the AIO.** This is not a purely theoretical question – as an illustrative numerical example, the "AI Office" appears 96 times in the Act; "the Commission" – 279. Being at least partially responsible for duties allocated to the EC would place a considerable burden on the AIO – a risk covered in section 4.3.1 of this study. On one hand, this one-way equivalency could be understood as intended, preventing this extension of responsibilities on the EC as a whole. On the other hand, it is hard to imagine key EC-oriented obligations of the AI Act being conducted without any input from the AIO.

4.2.2. Direct compliance

The **AIO's direct compliance obligations are targeted towards general-purpose AI models**. Article 88(1) grants the EC the exclusive powers to supervise and enforce the corresponding Chapter V of the AI Act, and it is expressly stated that the EC "shall entrust the implementation of these tasks to the AI Office". Interestingly enough, this is to happen "without prejudice to the powers of organisation of the Commission", **further convoluting the actual allocation of responsibilities between EC and AIO**. For AI systems based on a general-purpose AI model from the same provider, the AIO has all the powers of a market surveillance authority to monitor and supervise compliance with AI Act[185].

4.2.3. Providing guidance

The AIO has a **diverse range of duties that could be described as providing guidance**. Article 62(3)(b) of the AI Act states that the AIO shall "develop and maintain a single information platform providing easy-to-use information in relation to this Regulation for all operators across the Union". There are two points of note here; firstly, the guidance is supposed to be for operators (an umbrella term in AI Act for a "provider, product manufacturer, deployer, authorised representative, importer or distributor"[186]). Secondly, this broad obligation appears in an article that is focused on SMEs and start-ups; however, operators within the Act are a far larger group than just those smaller-scale entities.

---

[183] Cancel-Outeda, C., 2024, *The EU's AI Act: A framework for collaborative governance*, Internet of Things, vol. 27, p. 7.

[184] Novelli, C. et al., 2025, p. 577.

[185] Article 75(1), AI Act.

[186] Article 3(8), AI Act.

Another line of guidance that the AIO is to provide is more operational, in the form of templates. From the same article comes the duty to "provide standardised templates for areas covered by this Regulation, as specified by the Board in its request". Moreover, Article 25(4) of the AI Act states that the AIO may develop and recommend model contractual terms for agreements between providers of high-risk AI systems and their third-party suppliers. This is reminiscent of model contractual clauses for GDPR-compliant data transfers to third parties. For more direct guidance, the AIO may be asked by national competent authorities to provide support and guidance in the establishment of regulatory sandboxes[187]. Finally, for public procurement procedures related to AI systems, the AIO is to "evaluate and promote the convergence of best practices"[188].

At the time of writing, two noteworthy AI Act guidance documents have been published. Firstly, the 'Guidelines on the scope of obligations for providers of general-purpose AI models under the AI Act', published on 18 July 2025[189]. Secondly, the 'Template for the Public Summary of Training Content for General-Purpose AI models', published on 24 July 2025[190]. The Guidelines are published as a Communication from the EC, as the document's legal author. Interestingly enough, the Guidelines mention that the Template "is currently being prepared by the AI Office"[191].

4.2.4. Receiving and gathering information

This broadly defined role revolves around **receiving information from other actors for further action and/or analysis.** In the AI Act, it is narrowed down to three subsets: general-purpose AI models, regulatory sandboxes and the scientific panel.

For general-purpose AI models with systemic risk, their providers have to report any serious incidentsto the AIO (and national competent authorities), together with potential corrective measures[192]. It is not fully clarified what the follow-up from the AIO is supposed to be. The AIO also has the power to request a variety of information from the authorised representatives of providers of general-purpose AI models[193].

For regulatory sandboxes, the AIO is to receive information from national competent authorities on the sandboxes' establishment[194], performance[195], and suspension/termination[196]. The AIO is also to index them in a public registry[197].

---

187 Article 57(15), AI Act.

188 Article 62(3)(d), AI Act.

189 European Commission, 2025, *Guidelines for providers of general-purpose AI models*.

190 European Commission, 2025, *Explanatory Notice and Template for the Public Summary of Training Content for general-purpose AI models*.

191 European Commission, 2025, *Guidelines on the Scope of Obligations for Providers of General-Purpose AI Models under the AI Act (18 July 2025)*, p. 10.

192 Article 55(1)(c), AI Act.

193 Article 54, AI Act.

194 Article 57(15), AI Act.

195 Article 57(16), AI Act.

196 Article 57(17), AI Act.

197 Article 57(15), AI Act.

For the scientific panel (advisory body established by Article 68 of the AI Act), the AIO is to receive notifications of systemic risks related to general-purpose AI models[198].

4.2.5. Codes of practice and conduct

The AIO has **an express role in the creation and implementation of codes of practice and conduct in the AI Act.** Within this piece of legislation, codes of practice can be distinguished from the codes of conduct in that the former are akin to compliance (semi-regulatory) instruments, aimed at ensuring that the Act's legal obligations are implemented in practice. Codes of conduct are defined more as voluntary adherence instruments, aimed at raising the standards in the AI ecosystem.

The AIO's role with respect to codes of practice is expressed within the chapter on general-purpose AI models. Participants in the codes are to regularly report to the AIO[199], and the AIO has to monitor and evaluate the achievement of the objectives of the codes by participants and their contribution to the proper application of the EU AI Act[200]. A potentially broad duty lies in Article 56(8), wherein the AIO will "encourage and facilitate the review and adaptation of the codes of practice, in particular in light of emerging standards. The AI Office shall assist in the assessment of available standards".

For codes of conduct, the AIO is to encourage and facilitate their creation, where they are intended to foster the voluntary application to AI systems, other than high-risk AI systems[201], and where they would create specific requirements for all AI systems (including those aimed at deployers)[202].

At the time of writing, the General-Purpose AI Code of Practice was released on 10 July 2025. Rather than being the work of the EC alone, it is "a voluntary tool developed by 13 independent experts, with input from over 1,000 stakeholders"[203]. The EC has endorsed it, and the AIO's email address is indicated as the contact point for signatories.

4.2.6. European Artificial Intelligence Board (EAIB)

The EAIB, established under Article 65 of the AI Act, is a body composed of Member States' representatives, tasked with advising and assisting the EC and Member States in the consistent and effective application of the AI Act. **The AIO attends its meetings, but without voting power**[204].

198 Article 90, AI Act.

199 Article 56(5), AI Act.

200 Article 56(6), AI Act.

201 Article 95(1), AI Act.

202 Article 95(2), AI Act.

203 European Commission, 2025, *General-Purpose AI Code of Practice now available*.

204 Article 65(2), AI Act.

4.2.7. Scientific panel

For the scientific panel, the AI Act is tasked with establishing systems and procedures to prevent and manage conflicts of interest affecting the panel members[205]. **The panel may also ask the AIO for assistance in the performance of its tasks**[206].

4.2.8. Awareness-raising

In the previously mentioned, broadly-phrased article of the AI Act focused on SMEs and startups, lies an obligation for the AIO to "**organise appropriate communication campaigns** to raise awareness about the obligations arising from this Regulation"[207].

4.2.9. Requesting updates of EC guidelines

The AIO may **request the update of EC guidelines** on the implementation of the AI Act[208].

[205] Article 68(4), AI Act.

[206] Article 68(5), AI Act.

[207] Article 62(3)(c), AI Act.

[208] Article 96(2), AI Act.

4.3. Risks and opportunities for the AI Office

4.3.1. Risks

There are several risks and challenges tied to the AIO's operation.

Ambiguity over the general scope of the AIO's duties

There are several facets to this risk. Firstly, as indicated in the previous subsection, the **lack of clarity regarding the extent of the AIO's involvement in AI Act duties allocated to the EC** complicates a clear understanding of the AIO's duties. Secondly, the AIO's role is **built both by the AI Act as well as the EC Decision establishing the AIO**. The Decision arguably widens the AIO's role beyond the AI Act, with broad tasks related to international cooperation, collaboration with the European Centre for Algorithmic Transparency (ECAT) or "fostering actions and policies that reap the societal and industrial benefit of AI technologies"[209].

Next, there is the **optional nature of the AIO's normative remit in the AI Act**. The AIO may develop model contractual clauses related to third-party suppliers; may be asked to support regulatory sandboxes; may invite different stakeholders to work on codes of practice; may ask for updates to EC guidelines. While giving an entity powers to act without requiring it to use them can provide appropriate flexibility, it also leaves uncertainty as to the conditions under which the AIO might choose to intervene.

Overall, as Novelli et al write, for the AIO, there is (still) "*ambiguity in the current normative framework regarding the breadth of its mission scope*", which sets it apart from bodies such as the European Food Safety Authority (EFSA) or the European Medicines Agency (EMA)[210].

Managing the legal and institutional interplay between the AI Act and other legislation

Recital 7 of the EC decision establishing the AIO states that it should not affect the powers and competences of national competent authorities, and bodies, offices and agencies of the Union in the supervision of AI systems. Moreover, the AIO should not duplicate activities (especially guidance) conducted by bodies, offices and agencies acting under sector-specific legislation.

However, **sufficiently clear steps and collaboration schemes required to achieve this overarching goal are, at the time of writing, missing** – as Novelli et al rightly note[211]. The cited authors give an example of data quality and management obligations of providers of high-risk AI systems as an area where EDPB and AIO guidance may overlap. The problem is not that the drafters of the AI Act weren't aware of such possible overlaps, but that the **process for managing them in practice is not elucidated in the Act**.

---

[209] European Commission, 2024, *Commission Decision (EU) C/2024/1459 of 24 January 2024 establishing the European Artificial Intelligence Office*, Article 5.

[210] Novelli, C. et al., 2025, p. 578.

[211] Novelli, C. et al., 2025, p. 577.

Autonomy

As part of the EC and DG CONNECT, the AIO is inherently subject to their strategic, management and resourcing governance, as highlighted by Novelli et al[212]. On one hand, this might be beneficial, as it ensures cohesion; on the other**, if the AIO was not intended to have a degree of autonomy, what was the benefit of identifying the AIO as a separate entity from the EC?** It should be clear when an activity is taken up by the AIO, and when it is undertaken by the EC[213].

Resourcing

As section 4.1.2 of this study shows, the **AIO is tasked with multiple duties, both narrow and broad, both defined and open-ended.** This might result in a **resourcing problem**, affecting the AIO's capacity to perform as intended. To recall an example, receiving and processing reports from participants to the codes of practice might be quite resource-intensive. National competent authorities have budgeting guarantees in AI Act; the AIO does not[214]. Moreover, it competes for experts and expertise with well-resourced companies in the AI sector[215].

Quasi-legislative powers

Finally, concerns could also be raised over **the degree of soft-law power vested in the AIO** (and by extension, the EC) when it comes to codes of practice, mainly those for general-purpose AI models. An argument could be made that, instead of codes of practice under AIO supervision, similar AI Act implementation and interpretation efforts could be made via instruments opened to a degree of scrutiny by bodies such as the European Parliament. Additionally, codes of practice developed together with the industry run the risk of being overly influenced by it. On the other hand, the current approach might be valuable due to its flexibility and proximity to practice, due to the co-creation aspect.

4.3.2. Opportunities and potential recommendations

By 2 August 2028, the EC has to evaluate the functioning of the AI Office[216]. The period of time before this date is perfectly suited for consideration of steps responding to risks identified in the previous subsection. Such steps could include:

- **Clearly distinguishing the activities of the AIO from those of EC as a whole.** This could include a statement clarifying the role and influence of the AIO over codes of practice and conduct;
- in the long term, **considering the increase of AI Office's autonomy and moving it towards a decentralised agency model** (a notion suggested by Novelli et al)[217];
- producing a **map of the AIO's activities that clarifies as many "mays" as possible** in this regard;

[212] Novelli, C. et al., 2025, p. 577.
[213] Novelli, C. et al., 2025, p. 579.
[214] Novelli, C. et al., 2025, p. 577.
[215] Novelli, C. et al., 2025, p. 577.
[216] Article 112(5), AI Act.
[217] Novelli, C. et al., 2025, p. 590.

- considering the role of **Memoranda of Understanding with key bodies responsible for EU legislation interplaying with the AI Act** (EDPB/EDPS, ENISA, EMA, etc.);
- **assessing the funding needs** in the period preceding 2028 – changing the funding structure if needed;
- establishing **mechanisms to fund substantive collaboration with experts** in the field (especially technical ones;
- **adopting a transparent rulebook for the AIO-facilitated codes of practice and conduct**, including open calls, representation quotas (SMEs/civil society/academia), conflict-of-interest rules, minimum reporting metrics, public progress dashboards, and periodic reviews.

5. REFLECTIONS ON FUTURE AI LEGISLATION IN THE EU

5.1. Prior considerations on the role and the impact of the AI Act – what is the place of the AI Act in the EU digital legislative landscape?

Before looking at targeted recommendations on the shorter, medium and longer term, it is worth taking a step back and asking first why EU legislative intervention might be necessary in relation to AI. Why, specifically, would AI systems justify specific legislation at the EU level, beyond existing technology-neutral digital legislation (such as the GDPR, competition law, product safety legislation and so forth), and which has been commented extensively in the sections above? The answer to that question identifies the gap that an AI Act would need to fill.

Two central, unique characteristics of AI systems could warrant specific legislation. Firstly, there is the **broad and unpredictable impact of AI systems on personal agency** – i.e. the fact that AI systems can act autonomously in ways that cannot necessarily be fully anticipated or predicted, and that could create serious harms to individuals or to society as a whole. Secondly, there is the inherent complexity of AI-based ecosystems, where the risks depend on choices made by developers, manufacturers and deployers, in a manner that allows **emergent risks to mutually reinforce and augment each other** (i.e. the combination of AI systems can create greater problems than each AI component individually might be able to cause). This triggers liability problems that are difficult to resolve under existing digital legislation.

These distinctive features – impacts on agency and risk-reinforcing ecosystems – arguably generate risks that strain the assumptions behind existing laws (e.g. full traceability, foreseeable misuse, singular responsibility). Without AI-specific clarifications, regulatory gaps, ambiguity, and enforcement challenges emerge, which can warrant specific legislation, complementing and further refining other digital legislation. The AI Act, in fact, does respond to those unique characteristics via the risk-based model and its regulatory approach that enhances traditional product safety law with more targeted obligations at the design and deployment stages.

5.2. A high-level reflection on the AI Act in the current digital legislative landscape: what are the central recurring problems?

Despite the fact that the AI Act thus corresponds to a specific problem, there are **some indications of negative side effects**. Mapping the AI Act against the broader digital legislative landscape, as this study has done, exposes **three interrelated problems**:

- the **digital legislative landscape has become highly burdensome**. The identification of relevant legal obligations that apply to AI systems, and their impacts in practice, requires access to highly specialised expertise that is not reasonably available to all relevant stakeholders;
- the **digital legislative landscape has become highly fragmented**. An AI system will rarely be subject to a single legal framework (such as the AI Act), nor will it commonly be governed only by the interpretations of a single supervisor/regulator;

An AI service provider seeking to offer its services across the EU market will need to familiarise itself with multiple legal frameworks at the EU and national level, and opinions and interpretations of authorities that can differ from Member State to Member State, and from one economic sector to the next. Since these authorities have different policy priorities, there is a clear risk of contradiction and tension between positions;

- the **digital legislative landscape lacks a consistent logic** across the regulated domains. Each piece of digital legislation (including the AI Act, but also all other legal frameworks examined in this study) was established on the basis of a clear policy problem, a clear policy objective, and a clear regulatory pathway for achieving that objective. However, since they all were developed in relative isolation, they lack a common socket of EU policy principles for the digital market.

5.3. A thinking exercise on a future digital legislative landscape – how should ideal EU digital legislation be composed?

If one accepts the analysis above, it is useful to reflect on **what a more coherent and simpler model could look like** – not with the goal of rejecting alternative models or criticizing current laws, but rather to reflect on how current problems could be gradually mitigated, how new challenges could be addressed in a forward looking manner, and how burdens, fragmentation and incoherences could be resolved or at least prevented from worsening over time.

Essentially, a coherent model could be based on three pillars:

Figure 4: Ideal digital legislative model

Source: Authors' own elaboration.

To reduce the scale of this problem over time, the EU should first aim to establish **the first pillar**: a clear statement of **common EU digital regulatory principles.** These should provide a clear but high level statement of the EU's objectives, principles and values in relation to the European digital society, including on such key issues as digital sovereignty, the role of the market (i.e. of the private sector vs the public sector), competition (in the single market and internationally), the protection of fundamental rights, innovation, public training and awareness, sustainability, and SME-friendliness.

This model was already developed to some extent in the European Declaration on Digital Rights and Principles, albeit without tackling all of the issues mentioned above.

Similarly, the 2020 White Paper on Artificial Intelligence[218] set out a broad agenda for AI systems, covering both regulation (via a risk-based legal framework, the "ecosystem of trust") and promotion of AI innovation and adoption (an "ecosystem of excellence"). The AI Act fairly faithfully implements the "ecosystem of trust" elements (comprising risk-based rules, transparency, prohibitions, and oversight), but falls short in strengthening the "ecosystem of excellence". In short, the White Paper's vision was broader than what the AI Act delivers. Such issues could be tackled more coherently via a common statement of EU digital regulatory principles.

Such a statement, which could take the form of, e.g. a unifying digital act, or perhaps more realistically, a common declaration (building on the European Declaration on Digital Rights and Principles, which reflects regulatory lessons learned through decades of digital policies), could then be applied as a yardstick for the creation of future legislation and for the evaluation of existing legislation.

Such future laws should then ideally comprise a set of **horizontal EU digital legislation,** which expresses and gives force to the principles, and which target broad and non-sector specific policy areas, such as fundamental rights (including but not limited to data protection), competition law (including but not limited to data or digital markets and data governance), digital sovereignty and the role of the market (not presently addressed systematically in EU law, other than via broad rules on state aid and increasingly eroding rules of international trade law), regulatory compliance by market participants (including but not limited to product safety), and governance (including appropriately homogeneous mechanisms of supervision and enforcement that are not dependent on unique bodies for each new legislative initiative). In other words, such idealised legislation would not include a separate AI Act, nor a Data Act (just as there are currently no Cloud Computing, Autonomous Robotics, or Quantum Computing Acts). It would seek to define common rules for all digital products and services.

This horizontal digital legislation would then be interpreted and applied via a **common supervisory/regulatory landscape**, which can build on the current mechanisms of national and EU level supervisory bodies. Crucially, however, the landscape should be simplified, avoiding situations where a multitude of authorities at the national and EU level could claim cumulative competence with potential overlaps and fragmentation. This could be built up gradually by streamlining cooperation between existing regulators for the digital sector – comparable e.g. to the Dutch model of the Cooperation Platform of Digital Supervisors (*Samenwerkingsplatform Digitale Toezichthouders*), or the UK model of a Digital Regulation Cooperation Forum – although it is preferable to opt for single regulators at the national level, each composed of multiple chambers of competences, that should ensure that the horizontal EU digital legislation is interpreted and applied consistently, and in accordance with the common EU digital regulatory principles.

[218] European Commission, 2020, *White paper on artificial intelligence – A European approach to excellence and trust*, COM(2020) 65 final, Brussels.

Moreover, national regulators should be encouraged to escalate strategic compliance questions to the EU level, so that a single opinion can be adopted across the EU, which would harmonise (and override) diverging national opinions. Finally, compliance should be strengthened by ensuring that digital service providers can access EU-level accreditation or certification, providing them with a limited shield against noncompliance claims, and through "comply or explain" regulation – thus facilitating access to a more unified EU digital market, across all sectors.

5.4. Relevance of these reflections to the recommendations in this study

The analysis above in relation to an ideal EU digital regulatory landscape is, of course, naïve, certainly in the short or even medium term. However, if one accepts that, in theory, such a model could be attractive if it could be achieved, then it provides a useful yardstick to define recommendations. Essentially, the question then becomes "What can be done in the short, medium and long term to gradually approach this ideal model, for the AI Act in particular, but also for EU digital legislation in general?".

Relevant recommendations will be provided in the sections below.

5.5. Specific recommendations on the basis of this study

Based on the analysis above, we will present a set of recommendations for future reflection on AI policy and AI legislation in the EU. These are grouped into short-, medium- and longer-term recommendations:

- **Short-term recommendations** can be implemented without change to the AI Act or to other legislation. They focus on optimising the application of the AI Act in relation to other EU digital legislation within the existing legal framework;
- **Medium-term recommendations** focus on optimising the AI Act by considering whether smaller legislative changes would be viable without requiring fundamental changes in the philosophy or general approach of the legislation; and
- **Longer-term recommendations** finally call for fundamental reflections on future digital legislation in the EU – not from the perspective of how existing laws can be amended, but from the perspective of what the legislation should ideally look like on a longer timescale of e.g. 20 years, without considering the 'legacy' of existing laws.

The recommendations should not be considered as suggestions for immediate action, since the AI Act is a recent instrument that has not even entered fully into application – thus, no definitive evidence on impacts or excessively far-reaching conclusions can be presented at this stage. The recommendations should rather be approached as reflections that should be taken into consideration for future regulatory or policy action.

5.5.1. Short term – optimising the application of the AI Act in relation to other EU digital legislation

With respect to short-term recommendations (i.e. those that would not require changes to any legislation), the principal emphasis should be placed on **strengthening interaction and coordination among regulators outside the product compliance supervision ecosystem** (i.e. those whose responsibilities go beyond notifying authorities and market surveillance authorities).

As the overview above has shown, the ecosystem of potentially competent supervisors that can issue guidance and take enforcement action is extremely extensive and very complex, comprising data protection authorities, a large ecosystem of authorities protecting other fundamental rights, the multitude of competent bodies designated under the Data and Data Governance Acts and other information society legislation (e.g., the Digital Services Act) and all of their EU level counterparts and coordinating bodies and networks.

This enhanced interaction and coordination would need to ensure that guidance is coordinated wherever possible at the EU level to mitigate the risk of inappropriate (including inefficient or inequitable) fragmentation and divergences; and that actual challenges and problems in the application of specific laws can be addressed in a consistent and homogeneous manner, or at least that solutions that are deemed appropriate in one Member State are likely to be accepted as compliant in all others.

A second point of attention might be to **better leverage the possibilities for interaction between the various legal frameworks,** since they each offer toolkits (including evidence) that can mutually reinforce each other. By way of example:

- With respect to the **GDPR**, joint operational guidance could be issued by the EDPB and the AI Office on overlaps (DPIA/FRIA), including standardised templates to reduce duplication; or on contentious issues such as the complexity (and occasional impossibility in some instances) in responding to data subject rights requests (e.g. request for personal data to be deleted or corrected in a LLM);
- It could be explored to what extent data sharing intermediaries under the **DGA** could facilitate management of training and/or input data for AI systems, or more generally, to what extent such service providers could be used to facilitate data governance in AI systems ('compliance as a service');
- Clarification could be issued on the extent to which users of AI systems have any rights to training data, input data, parameters and weights under the **Data Act**, since this can be important to mitigate lock-in effects. Note that we do not necessarily see a reason for the expansion of any such rights at this stage, but rather that clarity is needed on this topic;
- Regarding the **DSA**, guidelines improving the clarity and extent of its interaction with the AI Act could be developed with respect to: current and potential interplay of transparency obligations for intermediaries services providing or deploying AI systems; sufficiency of risk management practices under DSA and AI Act for VLOPs and VLOSEs acting as providers of general-purpose AI models with systemic risk. Marking schemes for AI-generated or manipulated content could be harmonised. A code of practice could be established, focused on illegal, AI-generated content, covering both generation (AI Act) and moderation (DSA). The AI Office could spearhead an effort to clarify the impact of AI Act obligations on the hosting exemption from liability. Finally, DSA and AI Act provisions governing researchers' access to data related to AI systems and models could be strategically aligned;
- With respect to the **DMA,** Article 6 allows further specification of legal obligations that are imposed on CPS provided by gatekeepers. For AI systems, these could be aligned with the obligations imposed by the AI on high-risk AI systems and on GPAIs with systemic risks. This would ensure better alignment between these frameworks;
- The possibility of issuing harmonised cybersecurity certification schemes for AI systems (or for GPAIs) under the **CSA** could be explored, since this could potentially facilitate the establishment of appropriate security documentation;
- Similarly, transparency and documentation obligations under the DSA and the **CRA** could be aligned with those of the AI Act by issuing joint guidance on how both legal requirements could be satisfied in a single template.

More generally, of course, it is worth noting that the AI Act still needs to be completed in some respects, including, e.g. issuing requests for harmonised standards and standardisation deliverables under Article 40; this is, however, a matter of continued proper implementation of the AI Act and is thus not considered a recommendation in its own right.

5.5.2. Medium term – optimising the AI Act or other legislation

With respect to medium-term recommendations (i.e. those that would require changes to legislation, by amending the AI Act or by amending other legal texts in relation to their application to AI systems), recommendations are harder to present, given the limited period of applicability of the AI Act thus far.

A few elements can, nonetheless, already be pointed out:

- The legal framework for the **assessment of what constitutes a high-risk AI system** is highly complex, depending on two separate assessment criteria, each linked to its own Annexes under the AI Act, that require appreciation from providers and deployers and where supervisors might take different stances from Member State to Member State. This **should be simplified and generalised** in order to facilitate the application and increase consistency;
- It might be considered to link the notion of GPAIs presenting systemic risks to the concept of a gatekeeper under the DMA, or to replace these with a mutual (shared) concept. In both instances, they effectively are a particular category of service provider that face elevated compliance burdens on the basis of the fact that they clear a certain market threshold (expressed in FLOPs under the AI Act and turnover under the DMA) that allows them to create systemic problems in the market. More generally, an evaluation might be useful as to whether these quantitative thresholds are the optimal solution for detecting systemically high-risk players, especially in view of newer providers such as DeepSeek that claim significantly lower training costs, and in relation to interacting entities (e.g. systems with excessive centrality in the ecosystem, analogous to the classification of banks and other financial market entities). A macro-prudential supervision function might be a more effective way to dynamically detect systemic problems in digital markets;
- Optimisations should also consider whether a **body could be created that could assess behaviour that does not directly follow available guidelines**, either to show that the related AI system is substantially in compliance or that provide evidence of better (cheaper, more effective, or fairer) alternatives to available guidelines. These possibilities build a degree of flexibility into the various Acts and encourage both business and regulatory innovation;
- **Clarifying downstream obligations**. AI ecosystems can become complex and modular, being comprised of multiple AI systems that interact with each other. It is not always clear in these instances who is a provider, a deployer, or both. The hierarchical perspective that is implicit in a word like "downstream" may need to be reconsidered, and with it the structure of obligations, reporting requirements, etc;

- **Simplifying the obligations of deployers**. A fundamental benefit of product legislation is the fact that providers (or manufacturers) shoulder the burden of compliance assessment, thereby relieving their downstream customers of the burden. The same is not true for the AI Act, where deployers face occasionally heavy compliance burdens, which each deployer has to execute independently, even when they use an AI system for the same purposes and in the same manner as other deployers of that same system. Simplification should be sought on this point, e.g. by leveraging the 'block exemption' model of competition law (allowing certain standardised deployments to be exempt from some regulatory obligations provided that they implement the precautions required under the block exemption);
- It should be considered whether **targeted carve-outs or close integrations with other legislation** would be necessary or appropriate, e.g. with respect to the GDPR (where it is not always clear, even today, whether the mere existence and use of LLMs trained on personal data can comply with the principles of the GDPR), or in relation to certain sectors (e.g. much like DORA constitutes a carve-out to a certain degree of the obligations of the NIS2 Directive, one might consider whether AI deployers in highly regulated industries might not warrant a similar carve-out).

5.5.3. Longer term – optimising EU digital legislation, including in relation to the AI Act

All of the recommendations above assume that legislation can be tweaked and optimised, but that the fundamental logic must remain the same. More fundamental reflections are also possible on how an ideal regulatory landscape should look in the longer term, as has been extensively commented on in section 5.3 of this study, which proposed a model for a more ideal EU digital regulatory framework.

Achieving such a framework is undoubtedly a very long-term effort, but one that could be broken up into smaller and more manageable steps. Some of these steps could include:

- A **recast of competition rules**. The basic principles are currently set out in the TFEU, complemented by the DMA. However, the DMA is based largely on core platform services, such as online search engines, app stores, and messenger services – it is not clear whether its rules can be applied to AI systems and in what way. Similarly, the Data Act and the Data Governance Act each aim to tackle competitiveness and innovation in relation to data, not to systems or digital services as such. This divergent approach allows focus, but also creates inconsistencies and potential gaps (e.g. the fact that the AI Act requires a much stronger consideration of fundamental rights than the DMA; or that the Data Act focuses on portability of data without considering the underlying AI stack). A more fundamental reflection is required on whether a more holistic perspective is possible;
- **Simplifying the landscape of targeted stakeholders**. Each legislative framework starts from a different perspective on stakeholders and roles: providers versus deployers; controllers versus processors; service providers versus gatekeepers; data holders versus data users; essential versus important entities; and so forth.

Each of these categories can overlap to some extent, but they never entirely align. This makes for a hugely complex ecosystem that requires significant expertise to navigate. A simplification is in order;

- **Digital sovereignty**. At present, the EU lacks a clear legal framework for digital sovereignty – or what benefits the EU requires and expects from this sovereignty – and discussions frequently get mired in the consideration of whether sovereignty concerns are compatible with international trade obligations. Only oblique references are made to data transfer issues (e.g. in the GDPR and in the Data Act), again without considering other dependencies. Europe needs a more convincing position on this topic, also with respect to AI services;
- **Technological neutrality**. Some of the concerns in this study relate to the fact that legislation is necessarily somewhat siloed: the AI Act obviously focuses on AI systems, the Data Act on connected devices and data sharing, the DMA on online platforms, with frequent emphasis on cloud systems. Regulatory focus on specific technologies might not be optimally conducive for the establishment of a coherent digital market, since these technologies are strongly interrelated;
- Finally, **EU coherence and national supervision** remain a challenge. National level enforcement as such does not appear to raise many questions, but the ever-expanding pantheon of national level supervisory authorities, which are competent to issue diverging interpretations on EU level rules, is a continued area of concern. It might be considered to introduce, in future legislation, mechanisms that are comparable to the stance that the CSA takes on EU level certification schemes: once an EU level position has been agreed (an EU cybersecurity scheme under the CSA, but the same logic could be applied to guidance from an EU level supervisory body in relation to AI), then that automatically invalidates and replaces contrary national level guidance. In this manner, the supervisory ecosystem could be significantly simplified. Alternatively or in addition to this proposal, the introduction of digital competent authorities who provide compliance advice on sets of connected regulations might be considered.

REFERENCES

- AI Champions, 2025, *An ambitious agenda for European AI,* February 2025, p. 42 and following. Available at: https://aichampions.eu/#report.
- Associated Press (AP), 2023, *California governor vetoes proposed AI safety measures.* Available at: https://apnews.com/article/california-ai-safety-measures-veto-newsom-92a715a5765d1738851bb26b247bf493.
- Bertolini, A., 2025, *Artificial Intelligence and Civil Liability – A European Perspective*, requested by the European Parliament's Committee on Legal Affairs, July 2025. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2025/776426/IUST_STU(2025)776426_EN.pdf.
- Baloup, M., 2022, *Using sensitive data to de-bias AI systems: Article 10(5) AI Act*, 2022. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4992036.
- Bogucki, A. et al., 2022, *The AI Act and Emerging EU Digital Acquis: Overlaps, Gaps and Inconsistencies*, CEPS In-depth Analysis No. 2022-02, September 2022. Available at: https://www.ceps.eu/wp-content/uploads/2022/09/CEPS-In-depth-analysis-2022-02_The-AI-Act-and-emerging-EU-digital-acquis.pdf.
- Cancel-Outeda, C., 2024, *The EU's AI Act: A framework for collaborative governance*, Internet of Things, vol. 27. Available at: https://www.sciencedirect.com/science/article/pii/S2542660524002324.
- Chun et al., 2024, *Comparative Global AI Regulation: Policy Perspectives from the EU, China, and the US.* 2024. Available at: https://arxiv.org/abs/2410.21279.
- Ebers, M. et al., 2022, *The European Artificial Intelligence Act: A Critical Assessment*, Law, Innovation and Technology, 2022, 14(1), pp. 1–44. Available at: https://www.mdpi.com/2571-8800/4/4/43.
- EDRi, 2025, *Open letter: European Commission must champion the AI Act amidst simplification pressure.* Available at: https://edri.org/our-work/open-letter-european-commission-must-champion-the-ai-act-amidst-simplification-pressure/.
- ENISA, 2020, *Candidate EUCS Scheme v1.0.* Available at: https://ec.europa.eu/newsroom/dae/redirection/document/118119.
- ENISA, 2020, *European Cybersecurity Certification Scheme for Cloud Services*. Available at: https://certification.enisa.europa.eu/publications/candidate-eucs-scheme-v10_en.
- ENISA, 2021, *EUCC Cyber Certification Scheme V1.1.1*. Available at: https://certification.enisa.europa.eu/publications/candidate-eucc-cyber-certification-scheme-v111_en.
- ENISA, 2024, *Certification Scheme EU5G*. Available at: https://certification.enisa.europa.eu/publications/technical-specifications-consultation-report-specifications-related-certification-embedded-universal_en.

- The EU Artificial Intelligence Act - Up-to-date developments and analyses of the EU AI Act. Future of Life Institute (FLI). Dynamically updated, and available at: https://artificialintelligenceact.eu/.
- European Commission, 1995, *Directive 95/46/EC of the European Parliament and of the Council, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, OJ L 281, 23 November 1995, pp. 31–50. Available at: http://data.europa.eu/eli/dir/1995/46/oj.
- European Commission, 2008, *New legislative framework*. Dynamically updated, and available at: https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en.
- European Commission, 2008, *Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93*. OJ L 218, 13.8.2008, pp. 30–47. Available at: http://data.europa.eu/eli/reg/2008/765/oj.
- European Commission, 2016, *Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016, General Data Protection Regulation (GDPR)*, OJ L 119, 4 May 2016, pp. 1–88. Available at: http://data.europa.eu/eli/reg/2016/679/oj.
- European Commission, 2019, *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*. OJ L 151, 7.6.2019, pp. 15–69. Available at: http://data.europa.eu/eli/reg/2019/881/oj.
- European Commission, 2019, *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*. OJ L 169, 25.6.2019, pp. 1–44. Available at: http://data.europa.eu/eli/reg/2019/1020/oj.
- European Commission, 2020, *Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A European strategy for data*, COM(2020) 66 final, Brussels, 19 February 2020. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0066.
- European Commission, 2020, *White paper on artificial intelligence – A European approach to excellence and trust*, COM(2020) 65 final, Brussels. Available at: https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf.
- European Commission, 2021, *Impact Assessment accompanying the Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, SWD (2021) 84 final (Parts 1/2 and 2/2). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021SC0084.
- European Commission, 2021, *Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, COM(2021) 206 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206.

- European Commission, 2022, *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. OJ L 333, 27.12.2022, pp. 80–152. Available at: http://data.europa.eu/eli/dir/2022/2555/oj
- European Commission, 2022, *Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)*, OJ L 152, 3.6.2022, pp. 1-44. Available at: https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng.
- European Commission, 2022, *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)*, OJ L 265, 12.10.2022, pp. 1-66. Available at: https://eur-lex.europa.eu/eli/reg/2022/1925/2022-10-12.
- European Commission, 2022, *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)*. OJ L 277, 27.10.2022, pp. 1–102 (DSA). Available at: http://data.europa.eu/eli/reg/2022/2065/oj.
- European Commission, 2023, *Decision No 1/2023 of the Joint Committee of the Regional Convention on pan-Euro-Mediterranean Preferential Rules of Origin of 7 December 2023 on the amendment of the Regional Convention on pan-Euro-Mediterranean preferential rules of origin*. OJ L, 2024/390, 19.2.2024. http://data.europa.eu/eli/dec/2024/390/oj.
- European Commission, 2023, *Regulation (EU) 2023/2854 of the European Parliament and of the Council, 2023, on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)*, OJ L, 13 December 2023. Available at: http://data.europa.eu/eli/reg/2023/2854/oj.
- European Commission, 2024, *Commission Decision (EU) C/2024/1459 of 24 January 2024 establishing the European Artificial Intelligence Office*, Article 5. Available at: https://eur-lex.europa.eu/eli/C/2024/1459/oj/eng.
- European Commission, 2024, *Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)*, C/2024/560, OJ L, 2024/482, 7.2.2024. Available at: http://data.europa.eu/eli/reg_impl/2024/482/oj. https://digital-strategy.ec.europa.eu/en/library/implementing-regulation-adoption-european-common-criteria-based-cybersecurity-certification-scheme.
- European Commission, 2024, *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)*. OJ L, 2024/2847, 20.11.2024. Available at: http://data.europa.eu/eli/reg/2024/2847/oj .

- European Commission, 2025, *Explanatory Notice and Template for the Public Summary of Training Content for general-purpose AI models*. Available at: https://digital-strategy.ec.europa.eu/en/library/explanatory-notice-and-template-public-summary-training-content-general-purpose-ai-models.
- European Commission, 2025, *Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act)*, C(2025) 5053 final, Brussels. Available at: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application.
- European Commission, 2025, *Fourth meeting of the Digital Markets Act High-Level Group – DMA first anniversary*, 7 March 2025. Available at: https://digital-markets-act.ec.europa.eu/fourth-meeting-digital-markets-act-high-level-group-dma-first-anniversary-2025-03-07_en.
- European Commission, 2025, *General-Purpose AI Code of Practice*. Available at: https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai.
- European Commission, 2025, *Guidelines for providers of general-purpose AI models*. Available at: https://digital-strategy.ec.europa.eu/en/policies/guidelines-gpai-providers.
- European Commission, 2025, *Guidelines on the Scope of Obligations for Providers of General-Purpose AI Models under the AI Act (18 July 2025)*. Available at: https://digital-strategy.ec.europa.eu/en/library/guidelines-scope-obligations-providers-general-purpose-ai-models-under-ai-act
- European Commission, 2025, *List of Fundamental Rights Protection Authorities under the AI Act*. Dynamically updated, and available at: https://digital-strategy.ec.europa.eu/en/policies/fundamental-rights-protection-authorities-ai-act.
- European Commission, 2025, *Omnibus IV Simplification Package.* Available at https://single-market-economy.ec.europa.eu/publications/omnibus-iv_en
- European Commission, accessed on 1 October 2025, *The EU register of data intermediation services*. Available at: https://digital-strategy.ec.europa.eu/en/policies/data-intermediary-services.
- European Commission, accessed on 1 October 2025, *Designated Gatekeepers under the Digital Markets Act (DMA)*. Dynamically updated, and available at: https://digital-markets-act.ec.europa.eu/gatekeepers_en.
- European Union, 2008, *Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC*. OJ L 218, pp. 82–128. Available at: http://data.europa.eu/eli/dec/2008/768(1)/oj.
- European Parliament, Committee on Industry, Research and Energy, 2025, *Report on European Technological Sovereignty and Digital Infrastructure – Motion for a European Parliament Resolution on European Technological Sovereignty and Digital Infrastructure*, 11 June 2025 (2025/2007(INI)). Available at: https://www.europarl.europa.eu/doceo/document/A-10-2025-0107_EN.html.

- EU AI Champions Initiative, *Stop the Clock – Open Letter.* Available at: https://aichampions.eu/#stoptheclock.
- Forbes, 2025, *AI 50 List*, dynamically updated online source. Available at: https://www.forbes.com/lists/ai50/.
- Gao L. et al., 2025, *"I cannot write this because it violates our content policy": understanding content moderation policies and user experiences in generative AI products.* In Proceedings of the 34th USENIX Conference on Security Symposium (SEC '25). USENIX Association, USA, Article 192, 3727–3746.
- Germain, T., 2025, *YouTube secretly used AI to edit people's videos. The results could bend reality*. Available at: https://www.bbc.com/future/article/20250822-youtube-is-using-ai-to-edit-videos-without-permission.
- Hacker, P., 2024, *The AI Act between Digital and Sectoral Regulations*, Bertelsmann Stiftung.
- House Energy and Commerce Committee, Proposal on Energy and Commerce, 11 May 2025, notably Part 2—Artificial Intelligence And Information Technology Modernization, p.6. Available at: https://docs.house.gov/meetings/IF/IF00/20250513/118261/BILLS-119CommitteePrintSubtitleCpp.pdf
- Hustinx, P., 2014, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, 2014. Available at: https://www.statewatch.org/media/documents/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf.
- KPMG, 2025, *Trust, attitudes and use of artificial intelligence: A global study 2025, Empowering human-AI collaboration for a trusted future*.. Available at: https://kpmg.com/xx/en/our-insights/ai-and-technology/trust-attitudes-and-use-of-ai.html.
- Krämer, J. et al., 2020, *The role of data for digital markets contestability: case studies and data access remedies*, CERRE Report. Available at: https://cerre.eu/wp-content/uploads/2020/08/cerrethe_role_of_data_for_digital_markets_contestability_case_studies_and_data_access_remedies-september2020.p.
- Laux, J. et al., 2023, *Trustworthy artificial intelligence and the European Union AI Act: On the conflation of trustworthiness and acceptability of risk*, Regulation & Governance vol. 18(1). Available at: https://doi.org/10.1111/rego.12512.
- Novelli, C. et al., 2025, *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities,* European Journal of Risk Regulation 16(2), pp. 566-590.
- OECD, 2023, *Regulatory sandboxes in artificial intelligence*, OECD Digital Economy Papers, No. 356, OECD Publishing, Paris. Available at: https://doi.org/10.1787/8f80a0e6-en.
- Pehlivan, C. et al., *The EU Artificial Intelligence (AI) Act: A Commentary*. Wolters Kluwer, 202.
- Sartor, G. et al., 2022, *Thirty years of Artificial Intelligence and Law: the second decade.* 2022, Artificial Intelligence and Law, Volume 30. pp. 521-557.
- Smuha, N.A. et al., 2022, *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*, European Law Journal, 28(1),

pp. 1–14. Available at: https://strathprints.strath.ac.uk/85567/1/Smuha_etal_SSRN_2021_How_the_EU_can_achieve_legally_trustworthy_AI.pdf.

- Smuha, N., ed., 2025, *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*. Cambridge University Press.
- Stanford University Human-Centered Artificial Intelligence, 2025, *Artificial Intelligence Index Report 2025*. Available at: https://hai.stanford.edu/ai-index/2025-ai-index-report.
- Van Bekkum, M. et al., 2023, *AI Data Governance – Overlaps Between the AI Act and the GDPR*. Available at: https://www.sciencedirect.com/science/article/pii/S026736492500010X.
- Van Bekkum M., 2024, *Using sensitive data to de-bias AI systems: Article 10(5) of the EU AI Act.* Available at:https://arxiv.org/abs/2410.14501.
- Veale, M. et al., 2021, *Demystifying the Draft EU Artificial Intelligence Act*, Computer Law Review International, 22(4), pp. 97–112. Available at: https://www.researchgate.net/publication/361298189_Demystifying_the_Draft_EU_Artificial_Intelligence_Act.

ANNEX – OVERVIEW OF THE AI ACT INTERPLAY WITH EU DIGITAL LEGISLATIONS

This Annex provides a structured overview of the main points of interplay identified between the AI Act and other EU digital laws in the course of this study. The table below lists, for each relevant set of provisions: (i) the articles in question; (ii) the type of interplay; (iii) a short description of the issue as it arises in practice, and (iv) recommendations where applicable. The aim is to increase the readability of the analysis and to support policy advisors in identifying areas where legislative or interpretative clarification may be required.

Table 3: GDPR

AI Act Art.	GDPR Art.	Type of interplay	Short description	Recommendations
NA	Art. 6(1)(f)	Inconsistency	Legitimate interests balancing test is indirectly recalibrated by AI Act safeguards; non-compliance with AI Act undermines reliance on Art. 6(1)(f).	Issue joint EDPB/AI Office guidance clarifying how AI Act compliance informs GDPR proportionality analysis.
Art. 27	Art. 35	Overlap	Both FRIA and DPIA require ex-ante assessments but apply different 'high-risk' thresholds and are overseen by different authorities.	Develop joint templates or interoperability guidance to streamline DPIA and FRIA.
Art. 14, Art. 26(11)	Art. 13-14, 22	Overlap	Transparency and human oversight framed as rights (GDPR) vs. system design obligations (AI Act).	Issue joint EDPB/AI Office guidance to align complementarities (rights-based and design-based obligations).
Art. 11, 12, 26(6), 15(5)	Art. 32, 30	Overlap	Security and traceability obligations partly duplicative; GDPR risk-based vs. AI Act lifecycle/product-safety focused.	EDPB and AI Office guidance, supported by harmonised standards (CEN/CENELEC), to clarify benchmarks and avoid duplicative compliance.

AI Act Art.	GDPR Art.	Type of interplay	Short description	Recommendations
Art. 10(5)	Art. 9(1)-(2)	Inconsistency	AI Act requires use of sensitive data for bias monitoring; GDPR allows only under narrow derogations.	Issue joint EDPB/AI Office guidance clarifying how Art. 9(2)(g) GDPR ("substantial public interest"), as referenced in Recital 70 AI Act, can be operationalised for bias monitoring, and extend guidance to cover generative AI, where similar risks of discrimination and representational bias arise.
Arts. 12, 26(6)	Arts. 15-22	Gap	GDPR rights (access, rectification, erasure) difficult to execute once data is embedded in model weights or retained for AI Act traceability.	EDPB and AI Office joint guidance, with technical standards where feasible, on practicable implementation of data subject rights in AI contexts.
Arts. 57–59	NA	Gap	AI sandboxes permit testing but do not relax GDPR obligations, especially with sensitive data.	Harmonise sandbox practice across Member States; clarify GDPR lawful bases in sandbox contexts.
Chapter VII	Chapter VI & VII	Inconsistency	GDPR centralises oversight (one-stop-shop, EDPB), AI Act decentralises it (Member State authorities, AI Office), creating a risk of parallel investigations and inconsistent remedies.	Establish cooperation mechanisms and joint case-handling protocols between DPAs, Member State authorities and the AI Office.

Source: Authors' own elaboration.

Table 4: Data Act

AI Act Art.	DA Art.	Type of interplay	Short description	Recommendations
Art. 10	Ch. II	Gap	DA ensures access/portability rights but does not guarantee representativeness, accuracy, or error-free datasets. Full compliance burden with AI Act dataset-quality rules remains on AI providers.	Develop joint guidance clarifying responsibilities of data holders vs AI providers. Consider technical standards/templates (CEN/CENELEC) to support interoperability and traceability.
Arts. 11, 12, 15(5), 26(6)	Ch. VI	Overlap/gap	DA mandates portability and switching; AI Act requires traceability and documentation. Portability may disrupt continuity in AI Act audit trails.	Develop interoperability and traceability standards, ensuring portability preserves AI Act compliance.
Arts. 74(12)-(14), 75	Ch. V	Overlap	DA permits exceptional-need data requests by public authorities; AI Act empowers Member State authorities and the AI Office to demand datasets for conformity checks. Concurrent requests may create duplicative or conflicting obligations.	Establish cooperation and sequencing protocols between DA competent authorities and AI Office/Member State authorities to avoid conflicts and reconcile requests.
Arts. 57-59	NA	Gap	DA obligations remain fully applicable in AI sandboxes; divergent enforcement by national DA authorities may undermine the legal certainty that sandboxes are intended to provide.	Harmonise sandbox practice across Member States; establish coordination protocols between DA competent authorities and AI Act supervisors.

Source: Authors' own elaboration.

Table 5: DGA

AI Act Art.	DGA Art.	Type of interplay	Short description	Recommendations
Arts. 10, 11, 12, 15(5), 26(6)	Art. 10-12	Overlap	DGA creates a framework for data sharing intermediaries; these provide a built-in trusted governance framework that could be leveraged to enable the AI Act's obligations in relation to data governance.	Explore the opportunities for leveraging regulated data sharing intermediaries as stewards for AI training/input data.
Art. 70	Art. 13	Overlap	Both the AI Act and the DGA require the designation of national competent authorities. Their competences can overlap if data-sharing intermediaries include AI data in their remit (which presently seems to be a hypothetical scenario).	Establish cooperation and sequencing protocols between DGA competent authorities and AI Member State authorities to avoid conflicts and reconcile requests.
Art. 65	Art. 29	Overlap	Parallel governance bodies are created at the EU level: the European Artificial Intelligence Board and the AI Office under the AI Act, and the European Data Innovation Board. Their remits are currently not aligned, leading to potential overlaps.	Establish cooperation and sequencing protocols between the authorities to avoid conflicts and create synergies.

Source: Authors' own elaboration.

Table 6: DSA

AI Act Art.	DSA Art.	Type of interplay	Short description	Recommendations
Art. 50	Art. 15	Overlap	Transparency in providing or deploying AI systems	Guidelines for intermediary services
Arts. 9, 17, 55	Arts. 34-35	Overlap	Risk management frameworks	Guidelines for VLOPs and VLOSEs providing general-purpose AI models
Art. 50	Art. 35	Overlap	AI-generated or manipulated content - marking	Harmonisation of marking schemes under DSA and AI Act
Arts. 34, 35, 55, 56	Arts. 7, 9, 16, 22,	Overlap	Illegal content generated through AI – prevention & moderation obligations	Guidance for intermediary services on content moderation obligations tied to illegal, AI-generated content
Art. 2	Arts. 6, 7	Gap	Intermediary liability	Providing clarity on whether knowledge obtained through compliance with AI Act impacts liability limitations in DSA
Arts. 90-91	Art. 40	Gap	Researchers' access to data on AI systems and models	Developing a strategic approach to enabling researchers' access that aligns DSA and AI Act, both in terms of substance of the requests and vetting procedures

Source: Authors' own elaboration.

Table 7: DMA

AI Act Art.	DMA Art.	Type of interplay	Short description	Recommendations
Art. 6-7; and Art. 50-51	Art. 3	Overlap /Gap	Scoping of the laws, focusing on high-risk/GPAI with systemic risks under the AI Act, and CPS designation for the DMA.	Better alignment between (notably) GPAIs with systemic risks and gatekeeper designation. The notions should not necessarily be fully aligned, but the use of entirely different criteria and procedures leads to gaps and incoherences.
Arts. 8-15, and 53	Arts. 5-6	Overlap	Obligations that are imposed when these respective frameworks apply (focusing on operational matters for the AI Act, and business practices for the DMA)	Better alignment between the obligations; notably, this is possible for Article 6 under the DMA, which could be used to establish specific criteria for AI systems designated as CPS.

Source: Authors' own elaboration.

Table 8: CSA

AI Act Art.	CSA Art.	Type of interplay	Short description	Recommendations
Art. 15 and 42	Title III	Overlap	The CSA allows the adoption at EU level of cybersecurity schemes, and the AI Act adds that certification under such a scheme creates a presumption of compliance with the cybersecurity requirements set out in Article 15 of the AI Act. However, no such scheme currently exists. Even if it did, this would not affect the need for conformity assessment for non-cybersecurity requirements under the AI Act. This erodes the value of CSA certification.	Substantive alignment between AI Act cybersecurity requirements and the requirements for an EU-level cybersecurity scheme should be sought (and also aligned further with the Code of Practice cybersecurity requirements), to build up a common perspective on EU-level cybersecurity expectations.

Source: Authors' own elaboration.

Table 9: CRA

AI Act Art.	CRA Art.	Type of interplay	Short description	Recommendations
Art. 43	Article 12–13	Overlap	Both the CRA and the AI Act require conformity assessments (the former for PDEs in general, the latter for high-risk AI systems; the interplay is addressed by Article 13, which generally indicates that the AI Act's process applies for high-risk AI systems with certain exceptions). This could raise complexities for AI systems that are PDEs which are not high risk (which would need to undergo conformity assessment under the CRA despite not requiring this under the AI Act); and for hybrid PDEs with AI and non-AI components (for which the AI components might be assessed under the AI Act, whereas the non-AI components are covered by the CRA only); and for non-high risk AIs that are qualified as important products with digital elements (which do not require assessment under the AI Act, but which do require assessment under the CRA).	Guidance should be issued on how to address conformity assessment of hybrid PDEs, and clarifying the process and requirements for AI systems that are PDEs which are not high risk.

Source: Authors' own elaboration.

Table 10: NIS2

AI Act Art.	NIS2 Art.	Type of interplay	Short description	Recommendations
Art. 9	Art. 21	Overlap	Both the NIS2 Directive and the AI Act require the implementation of risk management systems, which would apply cumulatively when essential and important entities (under NIS2) provide or deploy high-risk AI systems (under the AI Act).	Guidance should be issued on how the AI Act requirements should be complied with by essential and important entities.
Art. 73	Art. 23	Overlap	Incident reporting obligations to potentially distinct authorities (depending on national implementations) have been defined under NIS2 and the AI Act. This leads to potentially cumulative reporting duties, with the NIS2 Directive being significantly more stringent. The side effect could be that the CSIRTs under NIS2 receive information more quickly, and that the market surveillance authorities under the AI Act receive more detailed information (since they could receive reports later, more information might be available).	Cooperation between the authorities should be ensured to mitigate reporting burdens and to ensure that the same information is available to the authorities.

Source: Authors' own elaboration.

Table 11: NLF

AI Act Art.	NLF Art.	Type of interplay	Short description	Recommendations
Art. 43	N.A. (not a specific act)	Overlap	The AI Act is a part of the NLF in principle, but for AI systems that did not yet fall under another NLF category, the AI Act imposes separate conformity assessment for high-risk AI systems (initially allowing self-assessment for some high-risk systems).	Coherence should be monitored, especially to assess whether the permissibility of self-assessment remains acceptable, and to evaluate whether the parallel process for GPAIs (which are not subject to conformity assessment) remains appropriate.

Source: Authors' own elaboration.

This study explores how the AI Act relates to various other crucial pieces of EU digital legislation, such as the GDPR, the Data Act and the Cyber Resilience Act. It assesses overlaps and gaps between these acts, and shows that, while each of them is individually well targeted, their interplay creates significant regulatory complexity. Finally, it also provides reflections and suggestions for possible evolutions of the AI Act, and of EU digital legislation as a whole, keeping in mind the objective of ensuring that Europe can establish a competitive AI industry.

This document was provided by the Policy Department for Transformation, Innovation and Health at the request of the European Parliament's Committee on Industry, Research and Energy (ITRE).

PE 778.575
IP/A/ITRE/2025-10

Print ISBN 978-92-848-3053-4 | doi:10.2861/9915451 | QA-01-25-212-EN-C
PDF ISBN 978-92-848-3052-7 | doi:10.2861/4863883 | QA-01-25-212-EN-N