CERTAIN

Certification for Ethical and Regulatory Transparency in Artificial Intelligence

D3.1: COMPREHENSIVE LEGAL ANALYSIS AND MAP

A Foundational Overview of EU Regulation on Artificial Intelligence

Co-funded by the European Union

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

Work package	WP3
Task	T3.1
Due date	30/11/2025
Submission date	28/11/2025
Deliverable lead	UT
Version	1.0
Authors	Olena Denysenko (UT), Janika Bachmann (UT), Martin Hayford (UT)
Reviewers	Isabelle Landreau (IPS), Sebastian Neumaier (SPU)
Abstract	This report provides a foundational legal analysis to support the CERTAIN project's mission of enabling ethical, auditable, and regulation-ready AI systems in the European Union. It maps the core structure and obligations of the EU AI Act and situates it within the broader regulatory ecosystem, including data protection, cybersecurity, and digital services legislation. Using a doctrinal-policy synthesis approach, the report examines the legal obligations facing AI providers, deployers, and data holders, while identifying the transitional compliance mechanisms emerging ahead of finalised standards and official guidance. Key challenges, such as regulatory uncertainty, industry response, and enforcement gaps are explored in depth. This mapping exercise serves as a critical first step in aligning legal requirements with practical implementation pathways for responsible AI innovation across Europe.
Keywords	EU AI Act, Artificial Intelligence regulation, High-risk AI systems, Harmonised standards, Data Governance, AI Transparency, AI compliance, EU AI regulatory landscape, AI governance

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	14/10/2025	1st edit	Martin Hayford (UT)
V0.2	03/11/2025	2nd edit	Yasaman Yousefi (DEX)
V1.0	27/11/2025	3rd edit (official review)	Isabelle Landreau (IPS), Sebastian Neumaier (SPU)

Grant Agreement No: 101189650 | **Topic:** HORIZON-CL4-2024-DATA-01-01
Call: HORIZON-CL4-2024-DATA-01. | **Type of action:** HORIZON-IA

REVIEWERS COMMENTS

Sebastian Neumaier	SPU	Date of review: 27.11.2025
The deliverable provides a comprehensive legal analysis of the EU AI Act and its interaction with related regulations (GDPR, DGA, Data Act, DSA, DMA, CRA, NIS2, eIDAS2, sectoral laws). It maps obligations for AI providers, deployers, and other actors, explains risk-based classification, and outlines compliance pathways. The report aims to serve as a foundational resource for the CERTAIN project, bridging legal requirements with practical implementation strategies. My detailed review (included in the document itself) concerns with improving clarity, usability, and technical completeness. In particular, section 2.1 would benefit from clarifying overlapping roles with examples. Further suggestions focus on adding practical elements such as summary tables per stakeholder, extra columns for artefacts in obligation tables, and compliance checklists. Minor comments regarding the clarification of terminology, opt-out mechanisms, and interoperability requirements are included. Further, visual aids are recommended to show relationships between cybersecurity laws and the AI Act, along with diagrams for governance and liability. Overall, a strong point of the document is the structure and depth of analysis, especially the role-based obligations table and the comprehensive coverage of EU legislation. The explanations are clear, and the systematic approach to mapping legal frameworks works well. Adding more practical elements, such as summary tables, diagrams, and concrete examples, would make it even more actionable and useful for technical teams.		
Author's note: While many of the reviewer's comments were addressed certain ones such as the requests for more information per stakeholder, more specific obligation tables, compliance checklists, and liability diagrams remain the domain of an upcoming deliverables in WP3—D3.4 Guidelines for entering AI data markets and D3.5 Multidisciplinary guidelines for AI stakeholders.		

Isabelle Landreau	IPS	Date of review: 26/11/2025
For structural revisions, the document requires two main additions: a list of definitions for core terms like content and data space, and a discussion on the impact of SRB case law. Regarding Page 3, the discussion should be broadened to include the AI AGENT and the general stakeholder classification, positioning this discussion immediately before addressing the everyday user. I found the work to be quite complete and particularly appreciated Part 3 and Part 4.		
Author's note: To address the reviewer's concerns with definitions of several key technical terms, the authors utilized in-line definitions and references to further reading where appropriate rather than introduce a glossary or list of definitions. This serves to better increase the reader's understanding by eliminating the requirement to refer to the beginning of the document for definitions.		

DISCLAIMER

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

The CERTAIN project received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement No 101189650. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. This work has received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI).

COPYRIGHT NOTICE.

Project funded by the European Commission in the Horizon Europe Programme		
Nature of the deliverable:	R (report)	
Dissemination Level		
PU	Public, fully open, e.g. web (Deliverables flagged as public will be automatically published in CORDIS project's page)	☒
SEN	Sensitive, limited under the conditions of the Grant Agreement	☐

*

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This deliverable supports CERTAIN's overarching goal of fostering a trustworthy, legally grounded, and technically robust Artificial Intelligence (AI) ecosystem by providing a foundational legal and regulatory synthesis of the European Union's evolving AI governance landscape. It responds to the growing demand for clarity around legal obligations, compliance pathways, and institutional roles under the AI Act and related legislative instruments, offering both a conceptual map and a practical resource for stakeholders navigating this new regulatory environment.

At the centre of this work is the shift from voluntary ethical frameworks to a binding, risk-based model of AI regulation in the EU. The report outlines the structure and obligations of the AI Act, situates it within the broader digital legal ecosystem, including the GDPR, DSA, DGA, Data Act, and cybersecurity legislation, and identifies critical areas of legal overlap, ambiguity, and operational uncertainty. Special attention is paid to how these instruments impose role-specific duties on providers, deployers, and data holders, and how current compliance mechanisms such as CE marking, technical documentation, and conformity assessment may evolve with the introduction of harmonised standards and delegated guidance.

Methodologically, the report is grounded in a desk-based, integrative analysis of binding legal texts, official guidance, and high-quality policy materials. A thematic synthesis approach structures the landscape into four legal domains (AI, Data, Content, and System) making visible the regulatory intersections and practical implications for actors across the AI value chain.

Key findings emphasise that although the AI Act has entered into force, many of its implementation tools remain under development. This legal-technical gap presents significant challenges for organisations seeking to align with the regulation in its early stages. The report identifies not only areas of regulatory uncertainty, such as definitional ambiguities and institutional fragmentation, but also forward-looking opportunities for alignment through standardisation, certification schemes, and improved institutional coordination.

For the CERTAIN project, this deliverable serves as a critical foundation for technical work on compliance tooling and certification processes. By translating legal complexity into actionable insights, it enables more targeted development of support instruments for data holders, dataspace providers, and AI system developers. Looking ahead, CERTAIN is well positioned to guide stakeholders through the transitional phase of AI Act implementation by developing technical tools, engaging with standardisation processes, and helping operationalise the Act's requirements in a clear, auditable, and scalable manner.

LIST OF TABLES

ABBREVIATIONS

AI	Artificial Intelligence
AML	Anti-Money Laundering
AVMSD	Audiovisual Media Services Directive
CAD	Corporate Sustainability Due Diligence Directive
CAPA	Corrective and Preventive Actions
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CERTAIN	Certification for Ethical and Regulatory Transparency in Artificial Intelligence
CJEU	Court of Justice of the European Union
CPR	Construction Products Regulation
CRA	Cyber Resilience Act
CTO	Chief Technology Officer
Data Act	(EU Legislation on Data Sharing)
DGA	Data Governance Act
DMA	Digital Markets Act
DPO	Data Protection Officer
DPIA	Data Protection Impact Assessment
DSA	Digital Services Act
DSM	Directive on Copyright in the Digital Single Market
EC	European Commission
eIDAS2 (or IDAS)	Regulation (EU) No 910/2014 on electronic identification and trust services (as proposed to be amended)
EEA	European Economic Area
EEC	European Economic Community
EMEAI	Europe, Middle East, Africa, and India
ETSI	European Telecommunications Standards Institute
EU	European Union
EUDI (or ID)	European Digital Identity (Wallet)
EUDPR	European Data Protection Regulation
EUR	Euro (Currency)
FID	Financial Instrument Directive (or similar, context specific)
FRAND	Fair, Reasonable, and Non-Discriminatory (Terms)
FRIA	Fundamental Rights Impact Assessment
GDPR	General Data Protection Regulation
GPAI	General-Purpose AI
GPSR	General Product Safety Regulation
GPT	General Purpose Technology
HRAIS	High-Risk Artificial Intelligence System
IoT	Internet of Things
IP	Internet Protocol / Intellectual Property

MDR	Medical Devices Regulation
MiFID	Markets in Financial Instruments Directive
ML	Machine Learning
NIS	Network and Information Security (Directive)
PLD	Product Liability Directive
QMS	Quality Management System
RED	Radio Equipment Directive
SCC	Standard Contractual Clauses
SME	Small and Medium-sized Enterprise
SOPs (or SOP)	Standard Operating Procedures
SRB	Case C-413/23 P | European Data Protection Supervisor (EDPS) v Single Resolution Board (SRB) (Concept of personal data)
T3.1 (or T)	Task 3.1 (or Task)
TDM	Text and Data Mining
UK	United Kingdom
UCPD	Unfair Commercial Practices Directive
US	United States
VLOP	Very Large Online Platforms
VLOSE	Very Large Online Search Engines
WP3 (or WP)	Work Package 3 (or Work Package)

INTRODUCTION

1.1 INTRODUCTION AND PURPOSE OF THE DELIVERABLE

This report presents a comprehensive legal mapping and analysis for the CERTAIN project. Its purpose is to establish the non-negotiable compliance baseline that governs all subsequent technical development and implementation across the project. Serving as the foundational legal and ethical constraint within the CERTAIN project framework, this report directly operationalizes our commitment to compliance with pivotal European regulations, especially the EU Artificial Intelligence Act (AI Act).

This report serves as the primary legal constraint and foundational input for the entire project. It focuses on defining "what we must and must not do" from a regulatory and fundamental rights perspective, thereby providing the essential parameters required by the technical partners and tasks.

Within Work Package 3 (WP3), this legal mapping will set the stage for the next deliverable, “D3.2 Ethical Considerations of AI Compliance.” D3.2 will take the step of operationalizing many of the ethics-based legal requirements and solutions. Eventually, WP3 will combine these works and other WP3 works into a set of guidelines to be used by varied actors within the AI and associated data fields.

1.1.1 Political Landscape as of 2025

The EU AI Act, the world’s first comprehensive legal framework for artificial intelligence, continues to evolve within a rapidly shifting political and regulatory environment. Its development has been shaped by two major forces: the EU’s long-standing commitment to human-centric digital governance and the disruptive emergence of large-scale General-Purpose AI (GPAI) models during the legislative process. From the outset, the AI Act has been driven by the aim of safeguarding fundamental rights, reflected in early, non-negotiable bans on “unacceptable risk” practices such as social scoring and manipulative behavioural systems.

This rights-protective orientation has coexisted with growing political pressure to support innovation and competitiveness, generating ongoing debate about the regulatory burden on businesses and the balance between safety and flexibility. Throughout 2024 and 2025, competitiveness concerns intensified. Influential reports and industry lobby groups argued that the strict rules could hamper Europe's ability to compete with the US and China. This created a key tension point: the push for strict safety versus the need for innovation support.

Member States have meanwhile focused on designating national competent authorities, including Market Surveillance and Notifying Authorities, in line with the obligations applying from August 2025 [1]. This process has raised concerns about the administrative capacity and resources required for effective enforcement across all jurisdictions.

In parallel, a major development was the finalisation of the voluntary Code of Practice for GPAI models in August 2025. Although voluntary, the Code establishes a legally endorsed roadmap for model governance, with commitments from major non-EU technology firms. Its adoption signals the EU’s expectation that GPAI governance will evolve through a mixture of regulatory and soft-law instruments. At the same time, broader political discussions have become increasingly polarised between those prioritising continuity in the EU digital rulebook and those advocating for deregulatory adjustments to stimulate competitiveness.

The Digital Omnibus Proposal (2025): Emerging Uncertainty

On November 19, 2025, the European Commission introduced the Digital Omnibus Regulation Proposal[1], a legislative package described as a set of technical amendments aimed at reducing administrative burdens and

[1] https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal

improving the coherence of the EU's digital rulebook. According to the Commission, the proposal is intended to "optimise the application of the digital rulebook, lower compliance costs, and stimulate competitiveness."

However, the proposal has generated substantial political and legal controversy. Early analyses from civil society organisations, legal scholars, and several political groups in the European Parliament argue that some elements, particularly proposed changes to the GDPR, may significantly alter long-standing European data protection guarantees[2].

The proposed amendments have limited political consensus. Several Member States previously expressed reluctance to reopen the GDPR, and multiple political groups in the European Parliament have voiced strong opposition. Because the Digital Omnibus must still be negotiated and adopted through the ordinary legislative procedure, and given the level of resistance, it is uncertain whether the proposal will advance in its current form, or within the AI Act's core implementation timeline (2025-2027). At present, all existing digital legislation, including the GDPR, and AI Act deadlines, remains fully in force.

The Digital Omnibus proposal introduces an additional layer of uncertainty into the regulatory landscape that the CERTAIN Project aims to navigate. While none of the proposed amendments currently alter the legal obligations analysed in this deliverable, the scope and potential impact of the proposal, particularly on data governance, AI training practices, and enforcement structures, mean that its evolution may influence compliance pathways in the medium term.

Given the project's objective to support transparent, auditable, and regulation-ready AI ecosystems, CERTAIN will continuously monitor regulatory developments, including negotiations on the Digital Omnibus, positions emerging from the European Parliament and Council, and any amendments that may affect data processing rules, the rights of data subjects, or the legal requirements for AI providers and deployers.

Until any reforms are formally adopted and enter into application, the current legal framework, including the AI Act as enacted in 2024 and the existing GDPR, remains the authoritative basis for compliance and constitutes the legal foundation for the analyses and operational recommendations developed within this deliverable.

1.1.2 Methodological Approach

This deliverable adopts an integrative, doctrinal-policy synthesis methodology designed to anchor the CERTAIN project's technical and governance activities in a rigorous understanding of the EU's evolving regulatory landscape for AI. It establishes the legal and compliance foundation for the project by mapping relevant obligations, identifying practical implementation mechanisms, and highlighting areas of legal–technical ambiguity that require further operational clarification.

The methodology is grounded in a desk-based, non-empirical approach, drawing on authoritative legal texts, official guidance, and high-quality institutional analyses. The aim is to translate the abstract legal framework, particularly the AI Act and its intersection with related instruments, into practical compliance insights for actors across the AI value chain. While doctrinal in orientation, the methodology is also forward-looking, geared toward supporting technical tool development, certification pathways, and stakeholder engagement within CERTAIN.

The analysis was guided by a set of core research questions, including:

- What are the main EU legal instruments governing AI and data use?
- What obligations do they impose on different actors (e.g., providers, deployers, data holders)?
- How do these legal regimes interact or overlap?
- What timelines, enforcement mechanisms, and penalties are foreseen?
- What practical compliance pathways currently exist or are emerging?
- Where are the remaining gaps in legal clarity, regulatory readiness, or stakeholder alignment?

The **scope of analysis** is defined by the jurisdictional boundaries of the European Union legal framework. Three core analytical objectives guided the synthesis. First, to identify and examine the primary EU legal

[2] https://noyb.eu/en/digital-omnibus-first-legal-analysis

instruments relevant to AI and data governance, including the AI Act and foundational digital legislation such as the GDPR, DGA, DSA, and Data Act. Second, to map the broader regulatory landscape, including interpretive guidance produced by EU administrative and advisory bodies. And third, to provide a structured overview of emerging compliance mechanisms, ranging from technical documentation and CE-marking pathways to harmonised standards, that are shaping the operationalisation of legal obligations across the AI lifecycle.

The **source base** was built through targeted, purposive searches across key institutional repositories, including EUR-Lex, the European Commission's register of documents, the European AI Office portal, and outputs from national supervisory bodies. While academic commentary was not a primary focus, a limited number of high-quality policy analyses were included where they provided insight into institutional thinking or stakeholder alignment. Selected perspectives from civil society and industry were referenced to illuminate regulatory debates and compliance challenges.

To move from source collection to analysis, a structured thematic framework was applied. Rather than adopting a formal coding protocol, the synthesis process focused on extracting and interpreting key legal and operational insights. For each relevant provision or instrument, the analysis examined the core legal principles, the interpretive stance taken by EU institutions, and the practical compliance implications for affected actors. Instances of potential regulatory tension, such as those between the AI Act's transparency obligations and GDPR-based data minimisation rules, were flagged and discussed where they may impact implementation feasibility.

This interpretive work was then organised into four overarching thematic domains (AI, Data, Content, and System) reflecting the horizontal and interdependent nature of the regulatory frameworks under review. Finally, legal obligations were mapped to potential compliance tools and strategies, situating the AI Act within the broader ecosystem of EU digital regulation and governance infrastructure. The result is a legal foundation that supports CERTAIN's work in developing tools, certification mechanisms, and practical guidance for a diverse range of AI actors.

1.1.3 Structure of the Deliverable

This deliverable is structured to provide both a conceptual overview and a detailed legal-regulatory mapping of the evolving EU framework for artificial intelligence, data governance, and digital technologies. The structure follows a logical progression from legislative foundations to analysis of the legal landscape, its interlays, and gaps, and to implementation mechanisms, with an emphasis on clarity, traceability, and practical relevance for the CERTAIN project.

Section 2 presents an overview of the EU's core legal instruments relevant to AI and data governance. The analysis is organised around four thematic clusters: Artificial Intelligence, focusing primarily on the AI Act; Data, addressing the GDPR, DGA, Data Act, and related instruments; Content targeting the legislations on copyright, intellectual property, consumer protection; and System, covering adjacent legislation such as the Cybersecurity Act, Cyber Resilience Act, and sector-specific frameworks.

Section 3 offers an in-depth examination of the central tensions and unresolved challenges shaping the implementation of EU AI regulation. It begins by exploring the dynamic between regulation and innovation, followed by a discussion on the misalignment between the rapid pace of AI advancement and the comparatively slower timelines of regulatory design and enforcement. The section then turns to the emerging role of harmonised standards as a key compliance mechanism, emphasising both their potential and their current state of incompletion. It also addresses the complex relationship between data governance and AI, unpacking practical challenges related to data quality, re-use, and legal interoperability. A focused analysis of transparency obligations under the AI Act highlights both the normative intent and the technical ambiguities surrounding implementation. This is complemented by a brief overview of copyright concerns in the context of AI-generated content. The section concludes with a synthesis of industry responses to the evolving regulatory landscape and a reflection on the implementation roles and capacities of EU-level and national authorities.

Section 4 explores how the obligations established by the AI Act can be operationalised in practice. It discusses current and emerging compliance tools, including the anticipated harmonised standards.

Section 5 summarises the report's mapping of the legal landscape and highlights the Act's transitional nature, noting that many practical instruments such as harmonised standards and codes of practice are still in development. For the CERTAIN project, this section defines the next phase: moving from legal analysis to

active implementation through the creation of compliance tools, certification pathways, and engagement with regulators and standardisation bodies to foster trustworthy AI across sectors.

2 OVERVIEW OF EU LEGISLATION ON ARTIFICIAL INTELLIGENCE

In this section, we situate the EU Artificial Intelligence Act (Regulation (EU) 2024/1689) [2] within the wider legal framework that shapes how AI can be built, deployed, and used. While the AI Act is the first legislation designed specifically for AI, it does not stand alone. Its provisions work in parallel with a range of pre-existing EU laws that regulate the inputs AI systems rely on, the outputs they generate, the infrastructures they operate within, and the responsibilities of those who develop and deploy them. To understand AI governance in the EU, therefore, we need to approach it not as a single law but as an interlocking set of regimes.

To make this complexity more accessible, the following overview groups relevant EU laws thematically rather than presenting them as a long catalogue. We begin with **AI-specific legislation**, focusing on the AI Act itself. From there, we turn to **data**, the essential resource for training and deploying AI, where rules on privacy, data reuse, and access directly shape what is possible. We then look at **content**, where questions of copyright and intellectual property determine how outputs can be lawfully created, used, and monetized. Finally, we consider the **systemic context**, including rules on product safety, consumer protection, and cybersecurity that ensure AI systems can function safely within society. Framing the legislation in this way helps reveal how the AI Act operates as part of a larger ecosystem, rather than as an isolated intervention.

By following this structure, the section situates the AI Act within the broader EU legal ecosystem and highlights not only the rules themselves but also the links between them. This framing also prepares the ground for the analytical chapter that follow, which takes up specific cross-cutting issues such as transparency, copyright, and accountability. In doing so, the report underscores that regulating AI is not a matter of a single statute but of navigating a multidimensional framework where technology, law, and governance evolve together.

Co-funded by the European Union

2.1 ARTIFICIAL INTELLIGENCE

The cornerstone of the European Union's regulatory framework for artificial intelligence is **the EU AI Act,** which came into force on 1 August 2024, with obligations gradually coming into effect over the following three years. As the first comprehensive law of its kind worldwide, the AI Act embodies the EU's ambition to place human rights, safety, and trust at the centre of AI development, while simultaneously fostering innovation and global competitiveness. It is both a legal instrument and a political statement: Europe intends to lead by example in shaping the global governance of AI.

The regulation covers all types of AI across a wide range of sectors, excluding AI systems used solely for military, national security, research, or non-professional purposes. As a piece of product regulation, the AI Act does not confer individual rights, but instead sets obligations for providers and professional users of AI systems. In practice, this means the Act is directly relevant for those developing, importing, distributing, or deploying AI in a professional or commercial context, as well as organizations integrating AI into their services or products. By contrast, individual citizens using AI tools privately (for example, experimenting with generative AI applications at home) are not subject to obligations under the Act. For them, the law operates indirectly, ensuring that the AI tools they interact with meet EU standards of safety, transparency, and respect for fundamental rights.

The **scope of the Act** is deliberately expansive. It applies not only to providers, developers, and deployers within the EU but also to actors outside the Union whose systems are placed on or used in the EU market. This extraterritorial reach ensures that AI systems affecting European residents must comply with EU rules, regardless of where they are built. By design, the AI Act thus projects European standards globally, making compliance with EU rules a prerequisite for accessing one of the world's largest markets.

2.1.1 Actors in the AI Value Chain

The AI Act establishes a role-based system of responsibilities, recognising that different actors participate in the AI lifecycle in distinct ways. Obligations are not uniform across all entities but depend on whether an organisation develops, distributes, imports, or uses an AI system. This structure reflects the practical reality that accountability differs between those who design AI, those who commercialise it, and those who simply use it within their operations.

In practice, a single company may play multiple roles: for instance, a developer outside the EU is both a provider (globally) and requires an importer (inside the EU) to place the product on the EU market. Clearly identifying one's role is therefore essential before moving to risk classification and specific obligations. Moreover, in smaller companies or research environments, the same technical teams may participate in activities associated with several roles. For example, developing an AI model (provider responsibilities), integrating it into a product (product manufacturer responsibilities), and deploying it internally (deployer responsibilities). While the legal obligations attach to the organisation as a whole, internal overlap means that teams must be aware of how their tasks intersect with different regulatory requirements. This reinforces the importance of clearly assigning responsibilities and documenting workflows within the organisation. Below, we will introduce the main actors, using the terminology given in the AI Act.

Providers

Providers are entities that develop an AI system and place it on the market under their name or trademark. This includes software companies building AI applications, start-ups developing niche models, or manufacturers embedding AI in physical products. Importantly, entities that substantially modify a system or change its intended purpose so that it becomes or remains high-risk are also considered providers.

Example: A Berlin-based start-up develops an AI-powered hiring tool and sells it to companies across Europe. The start-up is the provider and bears full responsibility for ensuring the tool complies with the AI Act, according to the tool's risk level, before being marketed.

Deployers

Deployers (users in a professional context) are entities (companies, public authorities, organisations) using an AI system in the course of their professional activities.

Example: A university in Spain uses an AI-powered exam proctoring tool purchased from a vendor. The university is the deployer and must carry out a FRIA to assess risks to students' rights, as well as ensure oversight and transparency.

Importers

Importers are EU-based entities that place on the EU market an AI system developed outside the Union.

Example: A French distributor imports a U.S.-developed AI medical diagnostic tool for hospitals in Europe. The distributor is the importer and must ensure the tool complies with EU rules before making it available.

Distributors

Distributors are actors in the supply chain who make AI systems available on the market, without being providers or importers.

Example: An Estonian electronics retailer sells smart home devices with embedded AI. The retailer is a distributor and must check that the devices are CE marked and properly documented.

Product Manufacturers integrating AI

When AI is integrated into a physical product covered by EU product safety legislation (e.g., machinery, toys, cars), the product manufacturer is treated as a **provider** of the AI component**,** meaning that they bear all the responsibilities of a provider under the AI Act of the AI component.

Example: A Swedish car manufacturer develops an AI-based driver-assistance system integrated into its vehicles. The company is both the **product manufacturer** and the **provider** of the AI system.

Authorised Representatives

Authorised representatives are entities based in the EU that act on behalf of providers established outside the Union. Their role ensures that there is always a legally responsible contact point within EU jurisdiction for high-risk AI systems placed on the EU market. Crucially, the authorised representative may be addressed by market surveillance authorities in addition to, or even instead of, the provider itself. Moreover, if the authorised representative believes that the provider is acting contrary to its obligations under the AI Act, it has the authority to terminate its mandate. In such cases, it must immediately inform the relevant market surveillance authority and, if applicable, the notified body.

Example: A U.S.-based company develops AI-driven diagnostic software classified as high-risk. To market it in Europe, the company must appoint an authorised representative located in the EU. The representative retains all required compliance documentation and serves as the company's official contact point for regulators.

Everyday Users

Private users are the individuals using AI systems purely for personal, non-professional purposes, for example, using generative AI chatbots, translation apps, or photo-editing tools at home. Everyday users are not subject to obligations under the AI Act. The law is explicitly designed to regulate professional and commercial use, not private activities. Everyday users are consumers with no legal obligations under the AI Act, but awareness of AI's risks and limitations is encouraged.

Affected Persons

In addition to the actors who develop, place on the market, or deploy AI systems, the AI Act also recognises a distinct group of individuals who do not use the AI system themselves but are subject to its operation or its outputs. These include, for example, travellers undergoing AI-supported border checks, patients evaluated by AI-enabled diagnostic tools, job applicants screened by an automated system, or students monitored by AI-based proctoring solutions. Thus, a person using a generative AI app on their phone is an everyday user, but the same person being assessed by an AI-powered border control system is an affected person.

These individuals are not considered "everyday users" and have no obligations under the AI Act. However, they remain fully protected under EU law, including the fundamental rights safeguards embedded in the AI Act (e.g., transparency for AI systems that interact with people, restrictions on high-risk use cases, requirements for human oversight) as well as broader rights under the GDPR and EU fundamental rights law.

While they are not classified as actors in the AI value chain, their rights and interests are central to the regulation's design. Deployers and providers must therefore ensure appropriate information, transparency, and oversight mechanisms so that affected persons understand how AI is used in contexts that concern them.

Note on "AI Agents"

In recent AI literature and technical communities, the term "AI agent" is increasingly used to describe autonomous or agentic AI systems capable of performing tasks, initiating actions, or interacting with other systems with a degree of independence. However, the AI Act does not recognise AI systems themselves as actors or stakeholders. Legal responsibility is always assigned to natural or legal persons, such as providers, deployers, manufacturers, or other regulated entities. Agentic AI systems therefore fall within the existing framework and are regulated according to their risk classification and the obligations of the human actors responsible for them.

2.1.2 Risk-Based Classification System

At the heart of the legislation lies a risk-based classification system, which organizes AI systems into four categories, each subject to different regulatory requirements.

Minimal or no risk: Most AI applications, such as spam filters or AI-driven video games, fall into this category. They can be developed and deployed freely without specific obligations under the Act. Even though these systems are largely free from regulatory obligations under the AI Act, providers are **encouraged** to adopt voluntary codes of conduct to uphold ethical standards.

Limited risk: AI systems like chatbots or AI that detect emotions or generate deepfakes must adhere to **transparency requirements**. Users must be clearly informed when they are interacting with an AI system rather than a human. This ensures individuals are not misled and can make informed decisions.

High-risk AI: This is the most regulated category, serving as the cornerstone of the regulation and subject to the strictest obligations. This category encompasses AI deployed in sensitive areas such as employment decisions, education, law enforcement, border management, and the operation of critical infrastructure or certain medical devices. Providers of high-risk AI systems must adhere to rigorous requirements, including implementing risk management systems, ensuring high-quality datasets and data governance, maintaining detailed technical documentation, incorporating human oversight mechanisms, and guaranteeing the system's robustness, accuracy, and cybersecurity. Additionally, these high-risk systems must be registered in a publicly accessible EU database to enhance transparency.

Unacceptable risk: AI systems that fall under this category are outright prohibited due to their unacceptable risk. These include applications that manipulate human behaviour through subliminal techniques or exploit vulnerable groups, social scoring by public authorities, and most uses of real-time remote biometric identification in public spaces (with exceptions for law enforcement under strict safeguards).

2.1.3 Obligations under the AI Act

As mentioned before, the obligations of the different actors in the AI value chain are not uniform. They vary significantly depending on the *risk level* of the AI system involved. A provider of a minimal-risk chatbot will not face the same regulatory burden as a provider of a high-risk recruitment algorithm, nor will a deployer of a limited-risk transparency AI have the same duties as a deployer of biometric surveillance.

To bring clarity to this layered structure, the following table summarises how the core obligations of the AI Act apply across different roles and risk categories. It illustrates the key responsibilities for providers, deployers, importers, distributors, and other actors, highlighting when compliance measures such as data governance, conformity assessment, fundamental rights impact assessments, or transparency duties become relevant.

Actor	Minimal Risk	Limited Risk	High-Risk
Provider	–	Transparency requirements (Article 50, EU AI Act).	Establish a risk management system: conduct risk management and quality assurance throughout the system's lifecycle. Conduct data governance: ensure high-quality, relevant, and representative training datasets. Prepare and maintain technical documentation to demonstrate compliance. Establish monitoring and reporting procedures, including incident reporting. Carry out conformity assessments before the system is placed on the market. Affix CE marking and ensure the system continues to meet requirements post-market. Ensure that the high-risk AI system is accurate, robust, and cybersecure. Provide instructions for use for the deployers of the AI system. (Article 16, EU AI Act).
Deployer	–	Transparency requirements (Article 50, EU AI Act)	Operate the system according to the provider's instructions. Conduct a fundamental rights impact assessment (FRIA) when deploying high-risk AI systems in sensitive contexts. Monitor system performance and suspend use if risks or anomalies arise. Ensure human oversight where required (e.g., final decision not left for AI alone). (Article 26, EU AI Act).
Importer	–	–	Verify that the system complies with the AI Act before it enters the EU market. Ensure conformity assessment procedures have been carried out. Keep technical documentation available for supervisory authorities. Cooperate with market surveillance authorities and take corrective action if needed. (Article 23, EU AI Act).
Distributor	–	–	Verify that the AI system bears CE marking and includes all required instructions. Check that the system has not been tampered with. Cooperate with authorities in case of non-compliance. (Article 24, EU AI Act).
Product Manufacturer	–	–	Ensure both the product and the AI component meet applicable safety and AI Act requirements. Integrate AI conformity assessment into the overall product conformity process.
Authorised Representative	–	–	Hold a written mandate from the provider to carry out compliance tasks. Verify that the EU declaration of conformity and conformity assessment have been completed. Keep essential records (technical documentation, certificates, contact details) for at least ten years. Supply regulators with documentation and system information on request. Cooperate with authorities in risk management, registration in the EU database, and access to system logs. Notify authorities if the provider fails to meet obligations and, if necessary, terminate the mandate. (Article 22, EU AI Act).

Table 1. Role- and Risk-Based Obligations Under the AI Act

A sign "–" used in the table above means that no legal obligations under the AI Act are placed upon an actor. However, the ethical considerations are still expected.

Importantly, importers, distributors, deployers, manufacturers or other third parties can **become legally considered as providers** and thus take on the provider's obligations (Article 25, EU AI Act). This happens if they rebrand a system under their own name or trademark, if they substantially modify the system after it has been placed on the market, or if they change its intended purpose in a way that turns it into a high-risk AI system. In such cases, the law treats them as the new provider, regardless of the original provider.

2.1.4 Regulation of General-Purpose AI Models

A defining feature of the AI Act is its treatment of general-purpose AI (GPAI) and foundation models, which are AI systems designed to perform a wide range of tasks rather than a single, narrowly defined function. Examples include large language models like ChatGPT. The regulation recognizes that these models pose unique challenges due to their scale, adaptability, and potential societal impact. Under the AI Act, providers of GPAI models are required to meet transparency obligations, including publishing summaries of the training data used. This allows regulators, researchers, and the public to understand the sources that inform the model's behaviour and ensures accountability in the development process.

Importantly, the Act distinguishes between **open-source and proprietary models**. When a GPAI model's weights and architecture are released under a free and open-source license, the requirements are somewhat reduced: providers need only to produce a training data summary and adopt a copyright compliance policy. This reflects a recognition that open-source models allow for external scrutiny, which reduces the regulatory burden on providers while still ensuring transparency and legal compliance.

For **GPAI models with systemic risks**, the stakes are higher. These are models, proprietary or open-source, with substantial computational power (exceeding 10^{25} floating-point operations) that could influence large parts of society or critical sectors. Providers of such models must undergo a thorough evaluation process, which includes comprehensive risk assessments, the implementation of risk mitigation measures, and reporting of serious incidents. These provisions aim to prevent harmful or unintended consequences of high-capacity AI systems, ranging from errors in decision-making to broader societal disruptions, and highlight the EU's cautious but forward-looking approach to regulating frontier AI.

By framing GPAI in this way, the AI Act establishes a nuanced, proportionate approach: smaller-scale or open-source models face lighter obligations, while high-impact, potentially systemic systems are subject to stricter scrutiny, reflecting their potential to affect safety, rights, and public trust across the EU.

The **regulatory timeline** for general-purpose AI under the AI Act is also clearly defined. From 2 August 2025 onwards, the AI Act's requirements for GPAI models became applicable to **new models** placed on the EU market. Providers of **existing GPAI models** that were already operational before this date are granted a transitional period and must ensure full compliance by 2 August 2027. This phased approach balances regulatory certainty with practical feasibility, allowing providers time to adapt to the new obligations while ensuring that all GPAI models on the EU market meet uniform standards.

2.1.5 Governance Framework

The **governance framework** of the Act combines EU-level coordination with national-level enforcement. At the centre of this architecture is the **European AI Office,** established within the European Commission as the hub of AI expertise and supervision. The AI Office is tasked with supporting innovation by fostering a coherent ecosystem for trustworthy AI; and carrying direct supervision powers over general-purpose AI models, particularly those considered to pose systemic risks. These powers include the ability to request information and documentation from model providers, conduct independent evaluations, demand corrective measures, and, where necessary, impose sanctions. In this way, the AI Office becomes both a guardian of compliance and a driver of innovation, ensuring that AI in the EU develops in line with fundamental rights, safety, and public trust.

Member States play a complementary role by designating competent national authorities tasked with overseeing the application of the Act within their jurisdictions. These authorities monitor providers and deployers, carry out inspections, and cooperate with the European AI Office to ensure a harmonized approach across the Union. To facilitate well-informed decision-making, the governance framework embeds structured collaboration between EU institutions, Member States, and the wider expert community, including researchers, industry representatives, civil society, and the open-source ecosystem. This collaborative model ensures that regulatory implementation is informed by the most up-to-date technical and societal insights, while also maintaining accountability to European citizens.

What happens if an actor is not compliant with the EU AI Act?

Compliance with the AI Act is not optional. Once the regulation enters into force, every actor in the AI value chain must align its practices with the requirements laid down in the law. To guarantee this, the EU has established a comprehensive enforcement system that combines penalties, supervision, and phased implementation deadlines. The result is a framework that makes compliance both mandatory and verifiable.

Penalties for non-compliance.

The sanctions under the AI Act are designed to reflect the severity of different types of breaches.

Most serious violations: The use of prohibited AI practices, such as social scoring or manipulative techniques that exploit user vulnerabilities, may result in fines of up to €35 million or 7% of global annual turnover, whichever is higher.

Violations of obligations for high-risk AI systems: Failures such as neglecting conformity assessments, omitting risk management processes, or failing to maintain proper documentation can result in fines of up to €15 million or 3% of global annual turnover.

Supplying incorrect, incomplete, or misleading information to regulators: Such conduct may be sanctioned with fines of up to €7.5 million or 1% of global annual turnover.

Although the Act allows for proportionate fines for small and medium-sized enterprises or start-ups, the substantive obligations themselves apply equally, regardless of company size. Beyond financial penalties, regulators have the authority to withdraw non-compliant systems from the market or impose restrictions until compliance is demonstrated.

Compliance Timeline

The AI Act is also distinctive in that it does not apply in full immediately but rather follows a phased implementation timeline. The regulation entered into force in 2024, but its provisions will take effect gradually.

- 2 February 2025: the ban on AI systems categorized as **unacceptable risk** became applicable.
- 2 August 2025, the first set of obligations for general-purpose AI models, such as transparency and documentation duties, begun to apply.
- 2 August 2026, most AI Act provisions, including the core obligations for high-risk AI systems, will enter into force.
- Finally, 2 August 2027, thirty-six months after entry into force, all remaining obligations (including certain sector-specific adjustments) will become fully applicable.

This phased approach is intended to strike a balance between urgency and feasibility. It ensures that safeguards against the most harmful AI applications are introduced swiftly, while allowing more time for complex obligations to be implemented. Nonetheless, providers and deployers of high-risk or general-purpose AI systems are advised to begin preparations without delay. Establishing the necessary frameworks for documentation, risk management, and conformity assessment can be time-consuming, and early preparation is the only way to avoid disruption once the rules become fully enforceable.

The enforcement provisions of the AI Act underline a clear message: non-compliance will carry significant financial, legal, and reputational consequences. The extent to which non-compliance becomes publicly visible depends on the type of enforcement action taken. While the AI Act does not mandate systematic publication of every infringement, national competent authorities may publish decisions, sanctions, or corrective measures, consistent with established practices in EU product safety and data protection enforcement. Significant cases, such as orders to withdraw or suspend high-risk AI systems, prohibitions on deployment in sensitive contexts, or litigation before national courts, are likely to become publicly known through official communications or media reporting. In addition, the European AI Office is expected to disseminate aggregated information and notable enforcement outcomes as part of its supervisory and coordination functions. As a result, reputational consequences may arise both from the formal publication of enforcement actions and from the practical visibility of compliance failures in the market. By contrast, those who prepare early and integrate compliance into their organisational processes will not only ensure smoother market access but also enhance user trust and competitiveness in the rapidly evolving EU AI landscape.

In conclusion, the EU AI Act represents a landmark effort to shape the global approach to AI regulation. By adopting a human-centric, proportionate, and risk-based framework, it seeks to safeguard European citizens' rights and values while fostering an environment where AI innovation can thrive responsibly. As the first

legislation of its kind, the Act is poised to influence international norms, potentially setting a de facto global standard for the governance of AI systems.

In this section, we have outlined the Act's scope, risk-based classification of AI systems, obligations it imposes on providers, deployers, and other actors, treatment of general-purpose models, governance structure, and phased implementation.

2.2 DATA

AI is inseparable from data. Every stage of the AI lifecycle, from training to deployment, depends on the availability, quality, provenance, and lawful collect and use of datasets. Data and the purpose of its use determines not only the accuracy and performance of AI systems but also their ethical and legal acceptability. The European Union has long recognised that data carries multiple legal and societal dimensions: it is protected as a matter of fundamental rights, valued as an economic good, and increasingly treated as a common good within shared European data infrastructures. This multifaceted nature explains why AI governance cannot be understood without examining the broader EU data framework. The challenge lies in balancing competing interests: enabling access to data for innovation, safeguarding personal information, respecting intellectual property, and ensuring fairness in data markets.

This section is particularly relevant for actors operating within European data spaces. A *European data space* is a federated, interoperable ecosystem (technical, legal, and organisational) that enables trusted sharing, access, and reuse of data among participants under common European rules.[3]

Unlike a single centralised data repository, a data space connects distributed datasets through shared standards, identity frameworks, governance models, and interoperability protocols, ensuring that data remains under the control of its original holder while still being securely accessible for reuse.

Within this ecosystem, several key roles exist:

- **Dataspace providers (or dataspace operators)**: entities responsible for delivering and maintaining the technical and governance infrastructure of a data space. They ensure interoperability, enforce access rules, support onboarding, distribute metadata standards, and guarantee compliance with overarching EU frameworks such as the Data Governance Act and the Data Act. Importantly, dataspace providers do *not* own or exploit the data; they operate the trusted environment in which sharing occurs.
- **Data holders**: organisations (public-sector bodies, companies, research institutions, hospitals, mobility operators, etc.) that generate or control data and decide under what conditions it may be shared. They must abide by GDPR, trade secrets rules, and sectoral regulation when making data available.
- **Data users / data consumers**: entities accessing and reusing the data within the space, such as AI developers, SMEs, public authorities, or researchers, who must comply with usage conditions, licensing, and legal safeguards.
- **Data intermediaries** (as defined in the DGA): neutral, regulated organisations that facilitate data exchange or pooling without exploiting the data for their own benefit. They provide secure mechanisms for permission management, data access, and data sharing across participants.

Together, these actors form the operational backbone of European data spaces. Because data spaces are designed to enable lawful, trustworthy, and standardised data reuse, the regulatory obligations examined in this section (GDPR constraints, TDM rules, data-sharing rights, protections for sensitive data, and limits on cross-border transfers) are directly relevant to their governance and daily functioning.

This section will explore five main themes:

- Personal data and fundamental rights. GDPR sets strict principles for processing personal data and limits automated decision-making. For AI, this ensures privacy and accountability, especially in high-risk systems.

[3] https://digital-strategy.ec.europa.eu/en/policies/data-spaces

- Data access and sharing. The Data Governance Act (DGA) fosters trusted data sharing via intermediaries and altruism, while the Data Act creates enforceable rights for users to access and share IoT/connected product data under fair conditions.
- Proprietary vs. open data / Copyright and training data. The DSM Directive introduces text and data mining (TDM) exceptions with opt-outs, and the Database Directive protects investment in structured datasets. Both set the rules for when AI may lawfully train on protected works or databases.
- Sensitive data and ethical/legal dilemmas. The GDPR prohibits processing of special category data except under narrow grounds, while the AI Act demands strict dataset quality for high-risk uses. This dual regime balances innovation with protection of fundamental rights.
- Cross-border governance and data flows. GDPR limits international transfers of personal data, and the DGA extends safeguards to sensitive non-personal datasets. These rules reinforce the EU's digital sovereignty by keeping strategic data under trusted conditions.

2.2.1 Personal Data

A central concern for AI is the processing of personal data, which lies at the heart of the EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) [3]. The GDPR remains the backbone of EU data governance, applying to any AI system that processes personal data of individuals in the EU, regardless of where its provider is established. For AI developers and deployers, this means that compliance with the AI Act does not replace GDPR obligations but exists alongside them. At its heart, the GDPR sets out foundational principles that govern all personal data processing activities. These include:

- Lawfulness, fairness, and transparency: data must be processed in a lawful manner, with clear information provided to individuals.
- Purpose limitation: data may only be collected for specified, explicit, and legitimate purposes.
- Data minimisation: only the data necessary for the intended purpose should be collected.
- Accuracy: personal data must be kept accurate and up to date.
- Storage limitation: data should not be kept longer than necessary.
- Integrity and confidentiality: appropriate security measures must protect data against unauthorised processing, loss, or damage.
- Accountability: organisations must be able to demonstrate their compliance with these principles.

These key principles of the GDPR directly shape how AI systems may be trained and operated. For instance, AI models that rely on massive datasets scraped from the internet must ensure that the data was collected and processed on a valid legal basis, such as consent or legitimate interest[4]. For scientific research purposes, Article 89 GDPR also provides specific flexibilities, permitting certain processing under appropriate safeguards, provided that a valid legal basis is still established. Moreover, Article 22 of the GDPR places limits on automated decision-making that produces legal or similarly significant effects, such as access to credit, employment opportunities, healthcare services, education, housing, public benefits, or decisions affecting a person's legal status or civil rights, requiring human oversight in such cases. This provision has clear relevance for high-risk AI systems used in contexts like recruitment, credit scoring, or law enforcement.

The AI Act reinforces these safeguards by requiring that high-risk AI systems be trained on datasets that are relevant, representative, and free of errors and biases "as far as possible[5]." This reflects a proportionate, risk-based obligation: providers must take all reasonable and technically feasible measures to ensure data quality, while recognising that full elimination of bias or error may not always be achievable in practice. In this way, the

[4] **Legitimate interest** (Article 6(1)(f) GDPR) is a legal basis that permits an organisation to process personal data when it has a real, lawful interest to pursue. For example, ensuring network security, detecting fraud, or improving a service. The processing must be necessary for achieving that interest, and it must pass a balancing test that weighs the organisation's interest against the individual's rights and freedoms. If the individual's privacy would be disproportionately affected, legitimate interest cannot be used. Public authorities cannot rely on this basis when performing their official tasks.

[5] The practical interpretation of this requirement will be further detailed through forthcoming harmonised standards, which are intended to operationalise this qualitative obligation into concrete technical guidance and measurable criteria.

GDPR and the AI Act form a complementary regime: the GDPR sets out general rights and obligations for personal data, while the AI Act introduces sector-specific requirements to ensure that datasets powering sensitive AI systems meet strict quality standards. Taken together, they reflect the EU's commitment to a human-centric digital environment in which innovation must respect privacy and dignity.

The GDPR **grants individuals (data subjects) a robust set of rights**, including the right to access their data, rectify inaccuracies, erase data under certain circumstances ("right to be forgotten"), restrict processing, data portability, and object to certain uses of their data, such as direct marketing. Organisations processing personal data are required to uphold these rights through clear policies and processes.

Controllers and processors have substantial obligations, such as maintaining detailed records of processing activities, implementing appropriate technical and organisational security measures, and, in many cases, appointing Data Protection Officers (DPOs). They must also notify supervisory authorities and affected individuals of personal data breaches under strict timelines.

The GDPR remains a cornerstone of the EU's digital regulatory architecture, embodying a human-centric approach to data protection that continues to shape global privacy practices. It complements newer instruments like the AI Act by providing the essential rules for lawful personal data processing, thereby creating a coherent framework that safeguards individual rights while supporting responsible technological innovation across the European digital economy.

2.2.2 Data Access and Sharing

While privacy concerns dominate discussions on personal data, an equally pressing issue in AI governance is access to non-personal and industrial data. AI systems are only as strong as the data they rely on. Access to large, diverse, and high-quality datasets is a prerequisite for building competitive models, yet such access is unevenly distributed. Today, a handful of companies dominate data resources, from consumer behaviour data generated through connected devices to industrial sensor data locked within proprietary ecosystems. This creates risks of market concentration and structural dependency: smaller firms, public institutions, and researchers are left at a disadvantage, while large technology providers reinforce their dominance. From the EU's perspective, this is not merely a technical or economic problem, but also a matter of sovereignty: if AI innovation depends on closed data silos controlled outside Europe, Europe's ability to set its own course in AI governance becomes limited.

The **Data Governance Act (DGA)** (Regulation (EU) 2022/868) [4], applicable since 24 September 2023, tackles this challenge by building a trusted infrastructure for voluntary data sharing. The DGA is a cross-sectoral instrument that aims to regulate the reuse of publicly held, protected data, by boosting data sharing through the regulation of novel **data intermediaries** (neutral, regulated entities that facilitate data sharing without exploiting the data) and by encouraging the sharing of data for altruistic purposes. Both personal and non-personal data are in scope of the DGA, and wherever personal data is concerned, the GDPR applies.

The DGA provides harmonized basic conditions under which **protected public sector data re-use** might be permitted. The re-use must satisfy the principles of proportionality, non-discrimination, and objective justification, and it must comply with intellectual property rights. Public sector bodies will have two months to decide on the re-use request and they may charge fees for the re-use of data, but only to an extent that does not exceed the necessary costs. If a public sector body denies a re-use request, the applicant must be informed of the reasons for the refusal and may challenge the decision under national administrative law. A refusal means that the dataset cannot be accessed or reused for any downstream purpose, including AI training, unless another legal basis or access regime exists (e.g., open data under the PSI/Open Data Directive, contractual licensing, or research exceptions under sectoral legislation). The DGA does not create a right to access protected public-sector data, but rather establishes conditions under which re-use may be permitted; public bodies may therefore legitimately deny access where disclosure would violate confidentiality, privacy, IP rights, or national-security restrictions.

Another important contribution of the DGA is the introduction of data intermediaries – neutral entities that facilitate data exchange between holders and users without exploiting the data themselves. The DGA defines a set of rules for providers of data intermediation services to ensure that they will function as trustworthy organisers of data sharing or pooling within the Common European Data Spaces.

These providers must only use the data to share it with the data users, not for their own purposes or benefit; separate their data intermediation services from the other services they provide by operating the intermediary service through a legally separate entity. For AI, this means creating structured pathways for companies,

hospitals, or research institutions to share valuable datasets with innovators while protecting confidentiality and intellectual property.

Another concept introduced by the DGA is **data altruism.** Data altruism is about individuals and companies giving their consent or permission to make available data that they generate, voluntarily and without reward, to be used for objectives of general interest. Entities that make available relevant data based on data altruism will be able to register as 'data altruism organisations recognised in the Union'. These entities must have a not-for-profit character and meet transparency requirements as well as offer specific safeguards to protect the rights and interests of citizens and companies who share their data.

Importantly, the DGA does not create open data pools that all market actors, including dominant technology companies, can freely exploit. Access to shared data is always purpose-bound, governed by strict conditions, and mediated by neutral intermediaries that are prohibited from monetising or repurposing the data. Certain datasets, such as those shared through data altruism, may be used only for objectives of general interest and not for commercial advantage, ensuring that data-sharing mechanisms do not reinforce existing market power imbalances.

A common European consent form for data altruism will allow the collection of data across Member States in a uniform format, ensuring that those who share their data can easily give and withdraw their consent. It will also give legal certainty to researchers and companies wishing to use data based on altruism. The DGA thus directly addresses one of the biggest bottlenecks in AI development – the reluctance of actors to share data due to lack of trust or fear of misuse. By embedding principles of transparency, neutrality, and accountability into data-sharing mechanisms, the DGA paves the way for wider access to high-value datasets critical for AI innovation.

Building on this foundation, the **Data Act** (Regulation (EU) 2023/2854) [5], applicable from 12 September 2025, introduces substantive rights and obligations to ensure that data circulates fairly in the EU economy. The EU Data Act represents a comprehensive regulatory framework governing data generated by connected devices (products that obtain, generate, or collect data concerning their use or environment and can communicate product data via electronic communications service, physical connection, or on-device access) and Internet of Things (IoT) products across economic sectors. The regulation was published in 2023 and became applicable from 12 September 2025.

This regulation applies to manufacturers of connected products placed on the market in the EU and providers of related services, irrespective of the place of establishment of those manufacturers and providers. Non-EU entities that make connected products available or offer services in the EU must designate a legal representative in one of the Member States to ensure compliance with the regulation.

The legislation addresses the imbalance where manufacturers and service providers traditionally maintain exclusive control over data generated by users through their connected products. One of its most significant provisions is the **user's right to access and share data generated by connected devices**. This includes the right to request that data holders make such data available to third parties of the user's choice, excluding gatekeepers under the Digital Markets Act (for more details on this, see section 2.3.2). Data holders must make data available to users without undue delay, free of charge, in a comprehensive, structured, commonly used and machine-readable format. To ensure this right is technically workable, the Data Act introduces interoperability obligations: data must be provided using standardised, well-documented formats and, where relevant, through secure APIs. The corresponding technical standards are currently being developed by CEN/CENELEC to support consistent implementation across sectors.

For AI, this opens up vast new opportunities: sensor data from cars, smart homes, or industrial machinery, previously siloed by manufacturers, can now be accessed by users and shared with third parties. This creates an ecosystem where smaller AI firms or research consortia can develop new services without being excluded by data lock-ins.

The Data Act also requires that business-to-business (B2B) data sharing happen under fair, reasonable, and non-discriminatory terms (FRAND), preventing dominant players from leveraging their control over data to impose unfair conditions. Similarly, business-to-government (B2G) provisions mandate data access in cases of exceptional public interest, such as natural disasters, pandemics, or energy crises, enabling AI systems to be deployed in real time for crisis management, resource allocation, or early-warning systems.

While the Data Act and the Data Governance Act expand the framework for access to and sharing of certain types of non-personal and industrial data[6], the GDPR remains the central reference point whenever personal data is involved. GDPR does not primarily facilitate sharing but rather sets the conditions under which personal data can be processed, transferred, or repurposed. This has direct implications for AI, where questions often arise around secondary use, whether data collected for one purpose can legitimately be reused for training or improving AI systems. Equally significant are the provisions on anonymization and pseudonymization, which determine when datasets fall outside the scope of GDPR and become more easily shareable. In this sense, GDPR acts as both a safeguard for fundamental rights and a structural constraint within which new data-sharing frameworks like the DGA and Data Act must operate.

For AI governance, the mentioned regulations are critical because they determine which datasets are accessible for training, how they can be shared, and under what conditions, thereby shaping the development and deployment of AI models across Europe. Together, these instruments move beyond a purely protective stance on data to actively foster an environment in which data can circulate responsibly. The shift marks an evolution in EU digital policy: from focusing primarily on privacy and individual rights to building a structured data economy that sustains innovation while embedding safeguards.

2.2.3 Training Data and Copyright

Building on the discussion of data access and sharing, the use of protected content for AI training represents a crucial intersection between innovation and intellectual property law. While the Data Governance Act and the Data Act create structured pathways for accessing non-personal and industrial datasets, AI developers often rely on copyrighted works, including text, images, music, or databases, to train models. These works are legally protected under EU copyright law, creating a dual imperative: on one hand, enabling the creation of powerful AI systems, and on the other, respecting the rights and incentives of content creators. Navigating this balance is essential for fostering an AI ecosystem that is both innovative and legally compliant. Copyright in the European Union has long been governed by a combination of harmonized directives, member state legislation, and case law, aiming to protect authors and rightsholders while allowing limited exceptions for public interest purposes. For AI, the directives most relevant are the **Directive on Copyright in the Digital Single Market (DSM Directive)** (Directive (EU) 2019/790) [6] and the **Database Directive** (Directive 96/9/EC) [7].

The **DSM Directive** was explicitly designed to adapt copyright law to the digital age, addressing challenges posed by digital reproduction, dissemination, and large-scale automated processing of protected works. Its provisions on **text and data mining (TDM) exceptions** are particularly significant for AI. Under the DSM Directive, both researchers and commercial entities may process copyrighted works using automated techniques to extract knowledge, patterns, or insights, without seeking individual authorizations, provided that such processing is done for specific purposes and respects lawful access agreements.

The Directive also incorporates an **opt-out mechanism for rightsholders (**authors, performers, publishers, or other owners of copyright-protected works), meaning that they can indicate if they do not wish for their works to be mined. Rightsholders exercise this opt-out by reserving their rights in a machine-readable form, such as through metadata, robots.txt exclusions, or similar technical measures, so that automated text-and-data-mining tools can detect and respect the restriction. This creates a calibrated system: AI developers can train models on large volumes of data efficiently, but rightsholders retain control over their works' use. The DSM Directive, therefore, embodies the EU's effort to enable innovation while preserving rightsholders' economic and moral rights.

Complementing the DSM Directive, the **Database Directive** provides protection for collections of data where substantial investment has been made in obtaining, verifying, or presenting the contents. For AI, this is particularly relevant in sectors such as finance, healthcare, and industrial IoT, where structured datasets may be proprietary. The Directive establishes rights that prevent unauthorized extraction or reuse of a significant

[6] Not all industrial data falls within the scope of these instruments: highly sensitive machine-level data, safety-critical operational data, and trade secrets remain protected and may only be accessed under strict conditions that preserve confidentiality.

portion of the database, yet it also allows limited exceptions for analytical or research purposes, enabling AI developers to leverage valuable structured datasets without violating intellectual property law.

For AI practitioners, these rules shape the datasets they can access and how models are trained. Text, images, music, and video used in model training often fall within copyright or database rights, meaning developers must carefully navigate permitted uses under the DSM Directive and Database Directive. This includes ensuring lawful access to content, respecting opt-outs and complying with contractual or licensing restrictions. In practice, this can influence decisions about whether to use open-source datasets, licensed commercial datasets, or datasets drawn from public sources.

The distinction between **proprietary and open data** becomes central. Open-access or open-license datasets allow broad reuse for AI training with minimal legal friction, whereas proprietary works require careful legal assessment. For high-capacity models like general-purpose AI, which rely on extremely large and diverse datasets, understanding and applying these copyright rules is critical to avoiding infringement, mitigating risk, and ensuring that outputs can be lawfully distributed.

It is important to note that copyright law will reappear in the **Content** section of this report, but with a different emphasis. There, the focus will shift from inputs used for AI training to the outputs generated by AI models, exploring how the DSM Directive and other copyright instruments apply to AI-produced works, derivative content, and potential liability issues. By addressing copyright from both the input and output perspectives, the report underscores the EU's comprehensive approach: ensuring AI systems can be trained on rich datasets while safeguarding creators' rights and maintaining legal clarity for innovators.

2.2.4 Sensitive Data

Another critical dimension of the debate on AI and data arises when the data itself is inherently sensitive. **Biometric identifiers, health information, financial records, and other "special categories" of personal data** fall under heightened protection in the EU because their misuse poses serious risks to fundamental rights. The GDPR once again establishes the foundation here: Article 9 explicitly prohibits the processing of special category data except under narrowly defined circumstances, such as explicit consent, public health needs, or scientific research subject to safeguards. This creates a challenging landscape for AI developers, many of whom see sensitive datasets as highly valuable for innovation (for example, training diagnostic algorithms on patient records or developing fraud detection systems with financial transaction data).

The **AI Act** adds another layer by tying dataset quality and governance directly to risk classification. High-risk AI systems, such as biometric identification, employment screening, or healthcare diagnostics, are required to use **training, validation, and testing datasets that are relevant, representative, free of errors, and complete** (Article 10). This provision implicitly acknowledges that biases or inaccuracies in sensitive datasets can translate into harmful real-world outcomes, from discriminatory hiring practices to wrongful medical diagnoses. At the same time, the AI Act does not override GDPR restrictions: developers cannot simply justify the use of sensitive data by appealing to model performance. Instead, they must demonstrate both **lawful grounds for processing under GDPR** and **compliance with dataset governance obligations under the AI Act**, creating a dual compliance burden.

The ethical dilemmas are therefore unavoidable. On one hand, access to sensitive datasets could dramatically improve the accuracy and fairness of AI systems, especially in domains like healthcare where underrepresentation is a known problem. On the other, the risks of surveillance, discrimination, or unauthorized secondary use are amplified when data relates to the most intimate aspects of people's lives. The EU's approach is to err on the side of caution, embedding strong legal protections while leaving carefully regulated openings for socially valuable AI innovation.

2.2.5 Cross-Border Governance and Data Flows

AI development is global in scope: models are trained across distributed datasets, deployed in international markets, and refined through global research networks. Yet EU law draws a firm boundary around how data can cross borders, balancing the benefits of openness with the need to protect sovereignty and fundamental rights. The **GDPR** sets the baseline: personal data cannot be freely transferred outside the EU/EEA unless the destination country ensures an "adequate" level of protection or unless appropriate safeguards (such as Standard Contractual Clauses) are in place.

For AI companies, this means that training or outsourcing activities involving personal data must navigate stringent compliance checks. The collapse of the EU–US Privacy Shield and its eventual replacement by the **EU-US Data Privacy Framework (DPF)**[7] illustrates how geopolitics and legal uncertainty shape the contours of AI data flows (Implementing Decision EU 2023/1795) [8]. The EU-US DPF, adopted in 2023, introduced stronger safeguards, than the invalidated EU-US Privacy Shield, including enhanced oversight, limits on US government access to EU personal data, and a new redress mechanism for individuals. Only US organisations that self-certify and commit to the DPF principles are eligible to receive data under this regime. While the DPF provides a legally stable pathway for many AI developers and cloud providers, its long-term durability remains uncertain, as civil society groups have already announced potential legal challenges. For AI companies relying on US infrastructure or partners, the DPF therefore offers an important, but potentially fragile, basis for compliance with GDPR cross-border transfer rules.

While the DPF governs transfers of personal data, the **Data Governance Act (DGA)** extends data-flow principles to certain categories of non-personal and public-sector data. Public authorities that permit re-use must ensure that such data is not transferred to third countries where legal environments could undermine EU protections, unless robust contractual and technical measures are in place. In practice, this prevents scenarios where datasets critical for AI training, such as mobility or energy consumption records, are extracted into jurisdictions with weaker data governance, creating risks of misuse or loss of strategic control.

These restrictions reflect more than privacy concerns: they are part of a broader strategy of **digital sovereignty**. By controlling data flows, the EU seeks to ensure that European values and standards are not diluted in a borderless digital economy. For AI, the impact is double-edged: while restrictions limit the frictionless use of global datasets, they also incentivize the creation of **European Data Spaces**[8] where trusted, interoperable infrastructures facilitate intra-EU data sharing. In this sense, the governance of cross-border flows is not only about protection but also about shaping the geography of AI innovation, ensuring that Europe retains strategic autonomy in an AI race dominated by global players.

It is worth noting that questions remain about the risk of indirect access to EU-generated data through corporate structures, such as non-EU parent companies benefiting from models or synthetic data produced by EU subsidiaries. While these scenarios highlight potential tensions between data sovereignty and global innovation networks, they are precisely the issues the Data Governance Act, Data Act, and the forthcoming European Data Spaces aim to address by imposing governance, contractual, and technical safeguards to prevent unauthorised onward transfers.

In conclusion, data lies at the core of AI. In the EU, the regulatory landscape for data is not only about privacy but also about access, sharing, copyright, and sovereignty. Together, the different instruments determine which datasets are available for AI training, how they may circulate, and under what safeguards.

Legislations covered in this section:

- **General Data Protection Regulation (GDPR):** Governs all personal data processing in AI, ensures rights of individuals, limits automated decision-making, and sets rules for transfers outside the EU.
- **Data Governance Act (DGA):** Builds trust frameworks for voluntary data sharing (public sector reuse, intermediaries, data altruism) while ensuring safeguards.
- **Data Act:** Grants users rights to access/share IoT and connected product data; imposes FRAND conditions for B2B sharing; introduces business-to-government access in emergencies.
- **Directive on Copyright in the Digital Single Market (DSM Directive):** Introduces text and data mining (TDM) exceptions, with opt-outs for rightsholders, directly affecting AI training on copyrighted works.
- **Database Directive:** Protects databases with substantial investment from extraction/reuse, relevant for proprietary structured datasets in sectors like health or finance.
- **AI Act (cross-referenced):** Requires high-quality datasets for high-risk AI systems, complementing GDPR restrictions.

[7] https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

[8] https://digital-strategy.ec.europa.eu/en/policies/data-spaces

Together, these instruments demonstrate how the EU seeks to build not only a human-centric data protection regime, but also a competitive, sovereign, and innovation-friendly data economy in which AI can develop responsibly.

2.3 OUTPUTS

When discussing artificial intelligence, much of the regulatory debate so far has cantered on the *inputs* used to train models: data, access, and sharing. Yet, the other side of the picture is equally important: the *outputs* that AI systems generate and circulate. In this report, "output" is understood broadly. It covers not only digital material created or shaped by AI, such as text, images, music, or video, but also outputs that are embedded into physical products, for example, in connected toys, autonomous vehicles, or smart household devices.

This broader conception matters because different types of AI outputs raise different legal challenges. Digital outputs relate to questions of authorship, copyright, online safety, and platform governance, while physical AI-enabled outputs raise issues of liability, consumer protection, and product safety. EU law addresses both categories, ensuring that what AI systems produce, whether a synthetic news article or a malfunctioning connected device, is safe, lawful, and trustworthy.

2.3.1 Copyright and Intellectual Property in AI Outputs

A central challenge in the governance of AI-generated output is how it interacts with the EU's copyright and intellectual property (IP) framework. Copyright law in Europe is harmonized primarily through directives, which set minimum standards that Member States transpose into national law. For AI, two main questions arise: **(1)** whether AI-generated outputs themselves can enjoy copyright protection, and **(2)** how the rights of existing human creators are respected when their works are reproduced, transformed, or competed with by AI systems.

The cornerstone here is the **Directive on Copyright in the Digital Single Market (DSM Directive)** (Directive (EU) 2019/790) [9]. While best known for introducing the press publishers' right and platform liability rules (Articles 15–17), the Directive also laid important groundwork for the AI era. Notably, it introduced two key exceptions for ***t*ext and data mining (TDM):**

- **Article 3** allows TDM for scientific research purposes, without requiring prior authorization.
- **Article 4** allows TDM for commercial purposes, but rightsholders can "opt out" by reserving their rights in machine-readable form.

This opt-out mechanism has become especially relevant with the rise of generative AI models, which are trained on vast datasets that often include copyrighted works such as books, images, music, or journalistic articles. If a rights holder has not opted out, their works can be lawfully used for training, though questions remain about whether outputs that mimic an artist's style or reproduce substantial parts of a work fall under permissible use.

The DSM builds on the earlier **InfoSoc Directive** (Directive 2001/29/EC), which remains the backbone of EU copyright by harmonizing reproduction, distribution, and communication rights, as well as exceptions and limitations [10]. Together, these directives establish the fundamental principle that even in the AI era, human authorship and rightsholder consent remain the default, with TDM exceptions representing carefully crafted carve-outs.

Beyond copyright itself, the **Database Directive** (Directive 96/9/EC) also plays a role [7]. It grants protection to databases where there has been a substantial investment in obtaining, verifying, or presenting the contents. AI models trained on structured datasets may therefore need to consider database rights in addition to copyright.

Other parts of the IP framework reinforce these protections. The **IP Enforcement Directive** (Directive 2004/48/EC) ensures rightsholders can seek remedies such as injunctions and damages if their works are unlawfully reproduced or distributed through AI systems [11]. Meanwhile, the **Trade Secrets Directive** (Directive (EU) 2016/943) protects confidential know-how and proprietary datasets from misappropriation, an issue of growing importance as AI developers rely on both open and closed training corpora [12].

Together, these frameworks highlight the tension between fostering innovation through broad access to training materials and protecting the legitimate interests of creators, rightsholders, and data owners. While definitive answers about authorship of AI-generated works remain unsettled, the EU has already created a legal environment where AI systems cannot exist entirely outside of the copyright and IP system.

2.3.2 AI Outputs, Platforms and Content Moderation

Beyond copyright and intellectual property, another major dimension of output governance lies in how platforms moderate, curate, and disseminate information. The EU has long recognized that digital intermediaries are not neutral conduits but actors that shape public discourse and access to information. With the rise of AI-powered content generation and recommendation systems, questions of responsibility, liability, and transparency have become even more pressing.

The centrepiece of EU law in this domain is the **Digital Services Act (DSA)** (Regulation (EU) 2022/2065)., which became applicable in February 2024 [13]. The DSA modernises the rules governing digital services in the EU, especially online platforms, and aims to create a safer, fairer, and more transparent online environment. Together with the Digital Markets Act (DMA), it forms the backbone of the **EU's Digital Services Package**[9]. The DSA sets out harmonised rules for all digital services that connect consumers with goods, services, or content, with a strong focus on intermediary services such as:

- Online platforms (e.g. marketplaces, app stores, social media);
- Hosting services (e.g. cloud storage providers);
- Internet service providers and domain name services.

The regulation applies to services offered to users in the EU, regardless of where the provider is established, affirming the EU's commitment to extraterritorial enforcement in the digital domain. It introduces a tiered system of responsibilities, with obligations increasing based on the size, nature, and societal impact of the service:

- All intermediary services must establish contact points, provide terms of service in clear language, and cooperate with authorities.
- Hosting services and online platforms must act on illegal content notices, maintain notice-and-action mechanisms, and explain content moderation decisions to users.
- Online marketplaces are required to trace traders and ensure consumer protection by identifying who is selling on their platforms.
- Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), those with over 45 million users in the EU, face the most stringent obligations. These include conducting risk assessments related to disinformation, illegal content, and impact on fundamental rights; implementing mitigation measures and independent audits; providing greater algorithmic transparency and enabling researcher access to platform data.

These obligations are highly relevant to AI: recommendation algorithms, content ranking, and automated detection tools fall within the scope of the DSA's risk assessments and transparency requirements. In practice, this means that platforms deploying AI moderation systems must evaluate not only their effectiveness but also their potential biases, over-blocking, or chilling effects on freedom of expression. This aligns with the broader EU effort, including the AI Act and GDPR, to ensure that automated decision-making respects user rights and operates under democratic oversight.

Complementing the DSA is the **Digital Markets Act (DMA)** (Regulation (EU) 2022/1925), which entered into force in November 2022, with all the obligations becoming applicable in March 2024 [14]. This legislation targets a small number of dominant digital platforms, known as **gatekeepers**, that act as bottlenecks between businesses and users in the online economy. The DMA applies only to designated gatekeepers (e.g., major app stores, search engines, and social networks), which are companies that:

- Provide one or more core platform services (e.g. search engines, app stores, social networking, operating systems, web browsers, cloud services, online marketplaces, and advertising services);
- Have a significant impact on the internal market;
- Operate as an important gateway for business users to reach end users;
- And enjoy an entrenched and durable position in the market (or will soon reach one).

[9] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

Companies meeting quantitative thresholds (e.g. €7.5+ billion in annual EU turnover and 45+ million monthly active EU users) must self-notify the European Commission, which confirms their gatekeeper status. The list of designated gatekeepers so far includes seven companies: Alphabet Inc. (Google), Amazon Inc., Apple Inc., Booking, ByteDance Ltd. (TikTok), Meta Platforms, Inc., and Microsoft Corporation.

The DMA seeks to ensure that core digital markets remain open, fair, and competitive, by imposing ex-ante obligations on powerful tech companies that control access to digital ecosystems. It addresses structural issues, such as self-preferencing, data lock-ins, and unfair conditions, that cannot be easily tackled through traditional antitrust enforcement, which is often slow and case-specific. Once designated, gatekeepers must comply with a set of do's and don'ts designed to curb unfair practices and open up digital markets.

Obligations:

- Allow users to uninstall pre-installed apps.
- Enable interoperability with third-party services (e.g. messaging platforms).
- Share performance marketing and ad data with business users.
- Ensure fair access to app stores, payment systems, and device functionalities.

Prohibitions:

- Self-preferencing their own services in rankings or app stores.
- Reusing personal data across services without user consent.
- Locking in users or business customers through unfair tying or bundling.

Gatekeepers must demonstrate compliance through internal reporting and may be subject to independent audits. The DMA is particularly relevant to startups and SMEs, as it aims to level the playing field and prevent gatekeepers from abusing their market dominance to block rivals or extract unfair terms. By requiring fair access to platforms, app stores, and key digital infrastructures, the DMA enhances innovation and market access for smaller players across the EU.

While the DMA does not regulate artificial intelligence directly, its impact on AI governance is substantial. Many general-purpose AI tools and recommendation systems are embedded in services offered by gatekeepers, such as search engines, content feeds, or advertising platforms. The DMA's provisions, particularly those related to data access, interoperability, and transparency, affect how these AI-powered systems are deployed and governed. For example, rules that require gatekeepers to share data with business users or prevent self-preferencing can influence how AI algorithms rank, recommend, or filter content. The DMA does not replace content-safety obligations under the DSA, but the two acts together constrain both what platforms may do with data and how they must manage platform effects on information flows.

Complementing the DSA and the DMA, the **Audiovisual Media Services Directive (AVMSD)** (Directive (EU) 2018/1808)**,** regulates video-sharing platforms and traditional broadcasters, requiring them to protect minors, limit incitement to violence or hatred, and ensure the prominence of European works [15]. As platforms increasingly integrate AI tools for age verification, content labelling, or targeted advertising, AVMSD obligations intersect with technical implementation choices.

Together, these instruments reflect the EU's shift from a laissez-faire approach to platform governance toward an accountability regime, where intermediaries are held responsible for systemic effects of the technologies they deploy. In the AI context, this means that platforms cannot hide behind automation: whether moderation is human or algorithmic, they remain accountable for ensuring compliance with fundamental rights and democratic values.

2.3.3 Consumer Protection and Safety Rules

Alongside intellectual property and platform regulation, a core component of "output" governance in the EU concerns consumer protection and product safety. Unlike liability law, which provides remedies once harm has occurred, consumer law establishes ex ante safeguards to prevent unfair practices and ensure that goods and services, including those powered by AI, can be trusted in the first place. This is particularly relevant as AI-generated outputs increasingly appears in commercial contexts, shaping advertising, personalisation, and user interfaces.

The EU **Unfair Commercial Practices Directive (UCPD)** (Directive 2005/29/EC) provides the general framework for preventing deceptive, aggressive, or otherwise unfair practices that distort consumer decision-making [16]. In the AI era, this extends to risks such as manipulative design, hyper-personalised targeting, or

misleading representations of AI-generated outputs. The Directive requires that traders communicate in a transparent manner, prohibits misleading omissions, and sets minimum standards of fairness in digital commerce. Enforcement actions in recent years have already shown how these provisions apply to online platforms, subscription models, and targeted advertising, which are increasingly mediated by AI systems.

Complementing this, the **Sale of Goods Directive** (Directive (EU) 2019/771) modernises consumer rights in the context of digital goods and services [17]. It requires that products conform to contractually agreed characteristics, including functionality, compatibility, and security, standards that apply equally to AI-enabled devices and digital services. If an AI-powered product fails to perform as promised, consumers are entitled to remedies such as repair, replacement, or reimbursement. This provision is particularly important where AI systems continuously evolve through updates or learning, raising questions about the scope of a seller's obligations over time.

A more recent and highly relevant instrument is the **General Product Safety Regulation (GPSR)** (Regulation (EU) 2023/988), which is applicable from December 2024 [18]. The GPSR updates the EU's safety framework for non-harmonised products, explicitly covering risks stemming from new technologies, including artificial intelligence. Its scope is broad: it requires manufacturers to assess and mitigate foreseeable risks to consumers, including those linked to software updates, connectivity, and algorithmic behaviours. Importantly, the GPSR introduces stronger recall and market surveillance mechanisms, ensuring that unsafe AI products can be withdrawn swiftly. For AI systems not covered by sectoral safety laws (such as medical devices or automotive software), the GPSR acts as a catch-all safeguard.

Together, these instruments build a layered system of protection that anticipates the challenges AI brings to consumer markets. Whereas the UCPD focuses on fairness in commercial communication and persuasion, the Sale of Goods Directive secures contractual expectations, and the GPSR establishes baseline product safety obligations. In the AI context, this means that consumers must not only be shielded from manipulative or deceptive uses of AI-generated content but also be confident that AI products and services meet essential safety standards. These preventive rules complement liability frameworks, which address harm retrospectively, ensuring that AI's integration into the consumer marketplace is both trustworthy and accountable.

2.3.4 Liability

Whereas consumer protection and product safety rules aim to prevent unfair practices and ensure that AI products meet essential standards before reaching the market, a further dimension of "output" governance addresses what happens when harm nonetheless occurs. In such cases, questions of liability and compensation become central. Harms can take many forms: misleading or defamatory digital content, faulty decisions embedded in software services, or unsafe actions carried out by AI-enabled physical products such as toys, household devices, or vehicles. To close existing gaps, the EU has moved to update and expand its liability regime, ensuring that individuals harmed by AI outputs are not left without effective remedies.

The **New Product Liability Directive (PLD)** (Directive (EU) 2024/2853)**,** is a new version of the original **1985 Directive (85/374/EEC),** which will modernize the EU's strict liability framework and address the complexities of today's digital, data-driven, and AI-integrated products [19]. It responds to the need for consumer protection and legal clarity in the age of software, cybersecurity risks, and evolving product ecosystems. The Directive ensures consumers can claim compensation without proving negligence while expanding the range of entities and scenarios under liability. **EU Member States have until 9 December 2026 to transpose the new Product Liability Directive into their national laws**. The new directive will apply to products placed on the EU market from that date onward, while products placed on the market before 9 December 2026 will continue to fall under the scope of the 1985 Directive [20].

The revised PLD covers all companies placing products on the EU market, including: manufacturers, importers, authorized representatives, and fulfilment service providers; software developers and companies integrating AI or digital elements into products, online marketplaces, and entities that substantially modify a product.

It explicitly extends liability to standalone and embedded software, digital services, and AI-enabled products, closing gaps where victims of harm caused by intangible outputs might otherwise have struggled to obtain compensation. The directive preserves the principle of **strict liability**: claimants must demonstrate a product defect, the occurrence of damage, and a causal link between them. Importantly, the definition of compensable damage now explicitly includes loss or corruption of data, recognizing the growing value of digital assets.

In situations where the technical or scientific complexity makes it excessively difficult for claimants to prove a defect or causation, courts are empowered to **presume a product was defective** and caused the harm, provided it is probable. This eases the burden of proof in cases involving advanced technologies like AI. To address the asymmetry in access to technical information, courts may order producers or other liable parties to disclose relevant evidence under their control. This disclosure is subject to safeguards for trade secrets, aiming to ensure fair proceedings without compromising confidential business information.

The Directive also recognises the complexity of AI supply chains: liability is no longer limited to traditional manufacturers. Under certain conditions, distributors, software developers, and even online platforms can be held liable, particularly when they play a decisive role in product safety or functionality. It also acknowledges that product defects may arise from software-related issues, such as failed updates, malfunctioning algorithms, or unintended interactions with other digital systems. This has direct implications for AI developers and users, reinforcing the directive's relevance to AI governance and risk management.

For cases involving latent damage, especially relevant in sectors like medical technology, the long-stop limitation period is extended from 10 to 25 years, giving claimants more time to seek redress when harm emerges long after the product was placed on the market.

As previously mentioned, the new liability framework is not confined to physical products. AI-generated content itself (text, images, decisions, or recommendations) can also trigger harm. Examples include financial advice generated by an AI service leading to loss, medical decision-support outputs causing misdiagnosis, or defamatory content generated by large language models damaging reputations. In these scenarios, liability rules ensure that responsibility is not diffused into technical complexity: providers or deployers of AI remain accountable for outputs and their consequences. Thus, the PLD anchors the EU's approach to safety and redress in the age of AI.

In conclusion, the EU approach to regulating AI-generated outputs rests on a dense but complementary set of legal instruments, each addressing a different aspect of outputs produced by AI systems. Taken together, these measures create a framework designed to ensure that AI-generated output, whether digital or physical, is lawful, safe, and trustworthy.

Legislations covered in this section:

- **Directive on Copyright in the Digital Single Market (DSM Directive):** Introduces text and data mining (TDM) exceptions, preserves rightsholder consent, and sets rules for training AI on copyrighted works.
- **InfoSoc Directive:** Establishes baseline copyright harmonisation on reproduction, distribution, and exceptions.
- **Database Directive:** Protects databases built with substantial investment, relevant for AI trained on structured datasets.
- **IP Enforcement Directive & Trade Secrets Directive:** Provide remedies for unlawful use of works and protect confidential training corpora.
- **Digital Services Act (DSA):** Imposes tiered obligations on intermediaries and platforms, with strong risk assessment, transparency, and accountability requirements for AI-driven moderation and recommendation systems.
- **Digital Markets Act (DMA):** Restrains dominant "gatekeeper" platforms, ensuring fair access, interoperability, and data-sharing, indirectly shaping AI deployment within core digital markets.
- **Audiovisual Media Services Directive (AVMSD):** Safeguards minors, limits harmful content, and applies to video-sharing platforms using AI-driven tools.
- **Unfair Commercial Practices Directive (UCPD):** Prevents manipulative or misleading AI-mediated commercial practices, including dark patterns and hyper-personalised targeting.
- **Sale of Goods Directive:** Ensures conformity, functionality, and security in AI-enabled goods and digital services, granting remedies if outputs fail.
- **General Product Safety Regulation (GPSR):** Applies from December 2024, requiring risk assessment and recall mechanisms for unsafe AI-enabled products.
- **New Product Liability Directive (PLD, revised):** Expands strict liability to cover AI-enabled software and services, easing burdens of proof and extending compensation rights to digital harms.

Together, these instruments show the EU attempt to ensure that AI-generated outputs are lawful, safe, and trustworthy.

2.4 SYSTEM

In the previous sections, we looked at how EU law governs the **data** that feeds AI systems and the **content** they produce. In this section, the focus shifts to the **system** dimension — understood here as the technical and sectoral environment in which AI operates. This includes the rules that determine how AI systems are designed, tested, and deployed in practice, how their resilience and safety are ensured, and what conformity and cybersecurity standards they must meet before reaching the market. To do this, the EU builds on its broader product safety, cybersecurity, and conformity assessment frameworks, embedding AI within a long-standing model of technical regulation. The overarching aim is to ensure that AI is not just lawful in principle but also robust, secure, and trustworthy in real-world settings.

2.4.1 Cybersecurity and Digital Resilience

AI systems are only as trustworthy as their weakest technical component. A model that performs well in the lab may still pose systemic risks if it can be hacked, manipulated, or weaponised in deployment. Recognising this, the EU has placed cybersecurity at the heart of its digital rulebook, applying both horizontal and sector-specific measures to products and services that integrate AI.

EU cybersecurity legislation combines horizontal, product-level, and organisational rules that together establish the security baseline for AI systems. The most relevant instruments are the EU Cybersecurity Act, the Cyber Resilience Act (CRA), and the NIS2 Directive. Each addresses a different layer of cybersecurity risk and together they materially shape how AI can be safely developed, deployed, and supervised in the EU.

The **Cyber Resilience Act** (Regulation (EU) 2024/2847), which entered into force on 10 December 2024, with most of the obligations becoming applicable from 11 December 2027, is particularly significant [21]. It introduces cybersecurity requirements for all **products with digital elements**, from connected devices to software applications. Once fully in force, it will oblige manufacturers to:

- design and develop products with appropriate security-by-design and by-default measures;
- patch and update products throughout their lifecycle to address vulnerabilities;
- provide transparent security information to users;
- undergo conformity assessments before products enter the EU market.

For AI, this means that systems integrated into consumer devices, industrial equipment, or software services must not only function as intended but also resist cyberattacks and data breaches. The CRA is also aligned with the EU's product-safety model, meaning non-compliant products can be withdrawn from the market.

The **NIS2 Directive** (Directive (EU) 2022/2555) complements this by imposing network and information security obligations on **essential and important entities**, including operators in energy, transport, healthcare, finance, and digital infrastructure [22]. Many of these sectors already deploy AI extensively, making NIS2's requirements on risk management, incident reporting, and supply-chain security directly relevant. AI providers working with critical infrastructure operators will need to demonstrate compliance with NIS2 standards.

Additionally, the **EU Cybersecurity Act** (Regulation (EU) 2019/881) establishes a **European cybersecurity certification framework**, under which AI products and services can be certified against common standards [23]. Certification may become a key trust signal for AI systems, particularly in sensitive contexts such as healthcare or financial services, where security breaches can have severe consequences. Certification is voluntary at EU level but can be required by other legislation for high-assurance use-cases.

While all three instruments promote risk management, supply-chain security, and resilience, they operate at different levels: the Cybersecurity Act focuses on standards and certification, the CRA on product lifecycle requirements, and NIS2 on organisational governance and incident response. Certification under the Cybersecurity Act can support CRA and NIS2 compliance, while CE marking under the CRA provides product assurance, and NIS2 ensures operational resilience.

The AI Act (Article 15) requires high-risk AI systems to be robust, accurate, and cyber-secure. The CRA's product requirements and the Cybersecurity Act's certification schemes provide concrete methods to demonstrate compliance with these obligations, especially for AI integrated into products. NIS2's incident reporting aligns with the AI Act's monitoring and reporting requirements, creating a coherent framework for rapid detection and response. All three instruments stress supply-chain integrity, a critical factor for preventing

attacks such as data poisoning or tampering with AI models and training data. CE marking and certification also serve as trust signals in the market, supporting the safe and transparent deployment of AI.

Taken together, these instruments show how cybersecurity is not an optional add-on but a core legal requirement for AI systems in the EU. By embedding AI into broader digital resilience frameworks, the EU aims to reduce systemic vulnerabilities and increase user trust in AI-enabled technologies.

2.4.2 Digital Identity

In addition to ensuring AI systems are resilient and secure against cyber threats, the EU also emphasises trust in digital interactions and identity management. This is where the **eIDAS2 Regulation (Electronic Identification, Authentication and Trust Services)** (Regulation (EU) 2024/1183) comes into play [24]. By providing a harmonised framework for electronic identification, authentication, and trust services across the EU, eIDAS2 underpins secure AI deployment, particularly in contexts where systems interact with verified users, process sensitive information, or perform transactions. In other words, while the Cybersecurity Act, CRA, and NIS2 focus on protecting the system itself, eIDAS2 ensures that the humans and organisations interacting with AI can be reliably identified and trusted, strengthening the overall integrity of AI-enabled services.

The eIDAS2 Regulation is the European Union's ambitious update to the 2014 eIDAS Regulation, reflecting the evolving digital landscape and the growing need for secure, interoperable, and user-controlled digital identity solutions across the EU. It came into force on 20 May 2024. This regulation aims to empower individuals and businesses with trusted and privacy-preserving digital identities usable throughout the EU, while ensuring greater sovereignty over personal data and facilitating the growth of the Digital Single Market.

eIDAS2 significantly expands the original scope of the 2014 regulation. While eIDAS1 primarily focused on cross-border recognition of national eIDs and the provision of trust services (such as digital signatures and certificates), eIDAS2 introduces a new concept: **the European Digital Identity Wallet (EUDI Wallet)**[10]. This Wallet will allow all EU citizens, residents, and businesses to store and share identity data and credentials (such as driver's licenses, diplomas, bank account information) in a secure, standardized, and user-controlled format. The regulation applies to public and private service providers, digital identity issuers, qualified trust service providers, and wallet app developers.

One of the core innovations of eIDAS2 is the **mandatory acceptance** of the EUDI Wallet by very large online platforms (VLOPs) and essential public service providers, ensuring its practical usability across key sectors. The regulation also guarantees **interoperability** of the wallet across all EU Member States, allowing users to access services across borders with a consistent digital identity.

Crucially, eIDAS2 emphasizes **user control and data minimization**. Individuals retain the right to choose which credentials to share and with whom, through mechanisms such as selective disclosure. This approach limits unnecessary data collection and fosters greater trust in digital interactions. Additionally, the regulation modernizes the legal framework for **qualified trust services**, extending its scope to include new services like electronic archiving, electronic ledgers, and electronic attestations of attributes.

While eIDAS2 is not an AI-specific regulation, its implications for AI governance are significant, particularly in identity verification, fraud prevention, and personal data access for AI systems. By establishing user-controlled, verifiable identities, eIDAS2 strengthens transparency and traceability in digital interactions involving AI (for example, chatbots handling sensitive services or algorithmic decision-making). Trustworthy digital identity infrastructure also facilitates ethical deployment of AI in high-risk sectors, such as finance or healthcare, by ensuring accurate identity proofing and compliance with data protection and non-discrimination principles.

2.4.3 Sectoral Legislations

While cross-sectoral AI regulations provide the foundational legal framework for the development, deployment, and use of AI technologies across all industries, it is important to recognize that many AI applications operate within

[10] https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487738/EU+Digital+Identity+Wallet+Home

specific sectors subject to their own dedicated regulatory regimes. These sectoral laws impose additional, often more stringent obligations that complement general AI governance rules and address the unique risks, ethical considerations, and operational realities inherent to each sector.

AI systems often operate in highly regulated environments where sector-specific rules define safety, performance, and risk management requirements. The EU has developed multiple sectoral regulatory frameworks that apply to AI-enabled products and services, complementing horizontal legislation on cybersecurity, resilience, and digital identity.

Disclaimer: This overview is not exhaustive. The EU has numerous sectoral regulations, and here we highlight some selected cases for the purpose of illustrating how AI intersects with specific industries.

Health. The **Medical Device Regulation (MDR)** (Regulation (EU) 2017/745) governs AI-applications in healthcare, including diagnostic algorithms, robotic surgery, and patient monitoring systems [25]. It imposes strict requirements for clinical evaluation, risk management, and post-market surveillance. AI-specific challenges include validating continuously learning models, documenting updates, and ensuring explainability for clinicians and patients. Compliance ensures that AI supports healthcare outcomes safely and reliably.

Finance. In financial services, AI is subject to both general consumer protection and sector-specific rules, such as the **Markets in Financial Instruments Directive (MiFID II)** (Regulation 2014/65/EU) and anti-money laundering regulations [26]. These frameworks impose obligations on algorithmic trading, fraud prevention, risk management, and transparency. AI tools used for credit scoring, investment advice, or anti-money laundering must adhere to strict governance and accountability standards to protect consumers and maintain market integrity.

Machinery & Industrial Equipment. The **Machinery Regulation** (Regulation (EU) 2023/1230)**,** replacing Directive 2006/42/EC, sets essential safety requirements for machinery, including those with AI components [27]. Obligations cover design, construction, risk assessment, safeguarding measures, and maintenance. Autonomous or semi-autonomous functions must operate safely, fail gracefully, and not endanger operators or bystanders.

Connected & Radio Devices. The **Radio Equipment Directive (RED)** (Directive 2014/53/EU) applies to AI embedded in IoT devices, drones, smart wearables, and other connected equipment [28]. Compliance ensures electromagnetic compatibility, safe spectrum use, and reliable performance without interfering with other systems.

By acknowledging the importance of sectoral legislation, this report highlights that a comprehensive legal analysis of AI governance cannot rely solely on cross-sectoral frameworks. Instead, it must consider how these general rules interface with the sectoral regulatory landscape, creating a multi-layered governance system. The forthcoming case studies (Section 3) will explore in detail how sector-specific laws intersect with cross-sectoral AI regulations. This examination will reveal both synergies and challenges in ensuring that AI technologies are effectively governed according to the distinct needs and risks of each field.

In conclusion, the “System” dimension of AI governance focuses on the technical, operational, and sectoral environment in which AI systems function. EU law addresses both the resilience and safety of AI systems and the trustworthiness of the humans and organisations interacting with them. Together, these frameworks aim to ensure that AI is robust, secure, and reliable in practice, not just compliant in principle.

Legislations covered in this section:

- **Cyber Resilience Act:** Imposes security-by-design and lifecycle requirements for digital products, including AI-enabled devices and software.
- **NIS2 Directive:** Sets organisational and network security obligations for essential and important entities deploying AI.
- **EU Cybersecurity Act:** Establishes EU-wide certification schemes for products and services, supporting trust and compliance.
- **eIDAS2 Regulation:** Provides a harmonised framework for digital identity and trust services, enabling secure interactions with AI systems.
- **Medical Device Regulation:** Ensures safety, performance, and post-market monitoring for AI applications in healthcare.
- **Machinery Regulation:** Sets safety and operational requirements for AI-enabled machinery and industrial equipment.

- **Radio Equipment Directive:** Ensures electromagnetic compatibility, safe spectrum use, and reliable operation of connected AI devices.
- **Sectoral financial regulations (MiFID II, AML):** Apply to AI in algorithmic trading, credit scoring, and fraud prevention, ensuring market integrity.

These instruments demonstrate that EU AI governance is **multi-layered**: horizontal rules establish baseline security and trust, while sector-specific regulations address context-specific risks. The combination of system-level and sectoral frameworks ensures that AI technologies can be deployed safely, transparently, and reliably across diverse domains.

3 ANALYSIS OF THE AI REGULATORY LANDSCAPE

This section examines the evolving framework of artificial intelligence regulation in the European Union, with a focus on the AI Act and its interaction with other key legislative instruments. The aim is to highlight the current and the most pressing legal and practical challenges rather than to provide an exhaustive or all-encompassing analysis – an impossible task given the rapid pace of technical and market developments in this field.

Our discussion concentrates on areas of regulatory complexity, implementation hurdles, and compliance burdens. Broader questions relating to the ethical, social, or human-rights implications of AI, while equally important, will be addressed in other deliverables of this project, where they will be explored in greater depth. The goal here is to provide clarity on the legal and operational issues shaping the current and near-future AI governance landscape, offering a foundation for informed discussion and further research.

3.1 REGULATION VS. INNOVATION

The European Union has an objective to become a global leader in AI. This goal is explicitly articulated in the 2025 AI Continent Action Plan, which states that “Europe must act with ambition, speed and foresight to shape the future of AI in a way that enhances our competitiveness, safeguards and advances our democratic values and protects our cultural diversity.” [29]. However, to achieve such a leading position, considerate efforts are still to be put in place. And the AI Act is being regarded as an essential element of this strategy, as a unifying framework with a clear set of rules, that are supposed to avoid market fragmentation and at the same time enhance the trust in and the use of AI technologies.

But of course, the EU’s efforts are not existing in a vacuum. There are other strong players in the global race for AI leadership. The EU’s approach can be considered unique compared to competitors. While the United States has largely taken a market-driven path, prioritizing rapid innovation with minimal regulatory barriers, and China has pursued a state-led model emphasizing large-scale deployment with strong state oversight, the EU has sought to occupy a **middle ground**: enabling innovation while embedding ethical safeguards into the technological fabric from the outset.

The AI Act serves as the flagship of this dual ambition. By defining clear risk categories, mandatory requirements for high-risk systems, and transparency rules for certain AI applications, the legislation aims to ensure that trustworthiness becomes a baseline market condition**.** The EU’s hope is that this will not only protect fundamental rights but also serve as a competitive advantage, differentiating “trustworthy European AI” in the global market in the same way that the General Data Protection Regulation (GDPR) became an international reference point for data protection.

Similarly, the EU's data governance framework, encompassing both the Data Act and Data Governance Act, represents a parallel attempt to balance innovation with protection in the data economy that fuels AI development. These acts embody the same European approach of seeking competitive advantage through trustworthy, well-regulated markets rather than unfettered technological development. By establishing clear rules for how data can be shared safely and ethically, the Act seeks to address one of AI's fundamental bottlenecks: access to high-quality training data. European AI developers often cite limited access to large, diverse datasets as a competitive disadvantage compared to their US and Chinese counterparts, who benefit from less restrictive data collection environments and larger domestic markets [30]. In such a case, regulations seem to be the needed and missing element for further innovation.

3.1.1 Chilling Effect of Over-Regulation

Despite its noble objectives, the EU AI and data regulations face criticism from parts of the technology and business community, particularly over the **risk of stifling innovation**, so potentially doing the opposite of what it is intended to do and setting the EU far back in the race for AI leadership.

Some experts argue that regulating AI at this stage is premature and potentially counterproductive [31]. As we have discussed in the previous section, the pace of AI development is way faster than any regulatory timelines, and thus at such an early stage, legislation risks being obsolete almost as soon as it is enacted. Rather than fostering innovation, excessive or inconsistent regulation may create uncertainty, discourage investment, and slow Europe’s progress in becoming a global AI leader.

Moreover, with AI projects proliferating at an unprecedented scale, the strict regional rules might push developers to relocate to less regulated jurisdictions. If that is the case, the EU might face **the risk of AI "brain drain"** further limiting European innovating capabilities. This risk is compounded by the absence of a global consensus. Even if the EU succeeds in establishing a rigorous framework, would it have any binding effect on state-sponsored or independent developers operating in countries like China, Iran, or South Korea?

Darren Thomson, Field CTO EMEAI at Commvault, underscores how divergent approaches between major economies add to this challenge [31]. While the EU AI Act prioritises comprehensive oversight and transparency, the UK has opted for a lighter, innovation-first touch, and the US is pressing forward with its own AI Action Plan that largely downplays regulatory hurdles. So many AI developers will be faced with a strategic choice between adhering to stricter European rules or relocating to jurisdictions where innovation faces fewer regulatory constraints and progresses at a faster pace.

However, the AI Act applies to any AI developer worldwide if their products or services are deployed in the EU market. At such simply relocating to another jurisdiction will not fully eliminate the requirement to comply with the AI Act, as long as the companies aspire to be present in the EU market. But in the worst-case scenario, the EU's stricter legal framework may lead some developers to exclude the European market, opting either not to train models on European data or perhaps delay or altogether not deploy cutting-edge solutions in the European market to avoid legal hurdles or potential fines under the AI Act, thereby limiting both innovation within Europe and users' access to top-tier AI products.

Which is not a hypothetical concern, as we have seen cases like this before. Meta, for example, postponed the launch of its AI assistant by nearly a year after the Irish Data Protection Commission raised privacy concerns [32]. And when finally introduced in 2025, the tool was rolled out in a restricted form, without image processing and without training on European user data. Similarly, Meta's Ray-Ban smart glasses with integrated AI features reached European markets later than other regions due to regulatory uncertainty [33]. Apple as well delayed the introduction of its flagship AI-powered services, such as Apple Intelligence and enhanced SharePlay, from 2024 to 2025 in Europe in order to meet the Digital Markets Act requirements [34]. Critics argue that while some regulation is essential, the EU risks fostering a culture of where European firms prioritize meeting legal obligations over experimenting with bold new technologies, and at the same time non-EU developers could sidestep the EU entirely, depriving European users of access to cutting-edge AI solutions and undermining Europe's ambitions for global AI leadership.

3.1.2 Counterpoint: Regulation as a Driver of Trust, Safety and Market Uptake

While many industry stakeholders resonate with the argument of regulation stifling innovation, there is strong evidence, and historical precedent, that **well-crafted regulation can actually accelerate adoption and innovation**.

Experts note that the first government or region to successfully establish comprehensive AI rules can shape the global regulatory conversation, earning a **"first-mover" advantage** [35]. The EU's track record with the GDPR demonstrates how regional regulation can set global standards, encouraging companies worldwide to adopt similar practices. Similarly, by advancing the AI Act the EU positions itself as a leader in AI policy, potentially influencing AI governance beyond its borders. And the emerging concerns from the tech industry regarding any new legislation is simply an expected part of the process, despite how scary they might sound. The implementation of the GDPR was accompanied by similar pushback and loud counterarguments from various tech lobbyists warning that it will stifle innovation. Yet, nowadays, the GDPR is widely considered as a worldwide standard for data protection. We shall see if the AI Act might have the same influential power.

Moreover, public trust remains a major barrier to uptake of AI technologies. Concerns about bias, transparency, misuse, and safety often delay or block AI integration, particularly in sensitive sectors such as healthcare, finance, and public administration. Experts confirm that these trust issues are not simply a matter of individual users' perceptions but stem from the underdevelopment of a regulatory ecosystem capable of guaranteeing AI's trustworthiness [36]. They argue that visible regulatory enforcement is crucial for building public confidence, as internal organizational safeguards alone are insufficient. Regulation can address this trust gap by providing clear quality benchmarks, independent oversight, and public accountability, thereby establishing a framework that makes AI trustworthy enough to be integrated into society on a bigger scale.

When AI systems are certified to meet high safety and ethics standards, users, whether individuals, businesses, or governments, can adopt them with greater confidence. Moreover, predictable legal frameworks reduce uncertainty for investors. Rather than fearing sudden legal restrictions, companies know the "rules of

the game" and can plan long-term innovation strategies accordingly. In this sense, regulation is not simply a brake but a **foundation for sustainable innovation**. So the key to AI and data innovations is not the absence of regulation, but its design**.** Regulations that are clear, consistent, and proportionate can foster innovation, rewarding companies that invest in safe, ethical, and reliable technologies.

3.1.3 Perspective Summary

The debate over "regulation vs. innovation" is often framed as a zero-sum game. In reality, the EU's challenge is to ensure that regulation and innovation become **mutually reinforcing forces**. For AI, this means creating legal certainty, proportionate obligations, and adaptive mechanisms that evolve alongside technology. If done well, the AI Act could become not just a regulatory milestone, but a unique asset, positioning Europe as the home of safe, ethical, and globally competitive AI. As such, there is a need to continue facilitating compliance with the AI and data governance legislations, providing support, particularly for smaller innovators, and remaining open to discussion and feedback from the tech industry.

3.2 AI'S RAPID PACE VS. REGULATORY TIMELINES

The speed at which AI technologies develop has no parallel in modern legislative history. Innovations that once took decades to move from laboratory prototypes to mass adoption can now do so in a matter of months. Generative AI tools are perhaps the most vivid example: within a single year, large language models progressed from being research projects to deployed products with hundreds of millions of users, sparking global debates about misinformation, deepfakes, and workforce transformation.

By contrast, EU legislative processes are deliberate and multi-layered. From the European Commission's proposal to the European Parliament and Council negotiations, through to transposition into national law (where applicable) and eventual enforcement, regulatory cycles typically span three to five years. Even "fast-tracked" laws rarely conclude in less than 18 months. This creates an unavoidable gap: by the time a regulation enters into force, the technology in question has already evolved, sometimes beyond recognition.

And such a mismatch has practical consequences. Regulations risk becoming outdated before they are even implemented, leaving critical gaps in oversight and protection. But on the other hand, when lawmakers try to anticipate future developments, they may over-regulate hypothetical scenarios, introducing compliance burdens for risks that never materialize. Both outcomes can undermine the EU's dual ambition: to become a leader in AI innovation and a global standard-setter in AI governance.

3.2.1 The Inherent Flaw: Legislation is Reactive, Tech is Proactive

As we can see, the asymmetry is built into the very nature of the two domains. Technological development is proactive. It is driven by experimentation, competition, and rapid iteration. Its objective is to create new possibilities, push boundaries, and capture emerging markets. In AI, this process is intensified by the global race for leadership: companies and research labs are incentivized to release new capabilities as quickly as possible to secure both market share and data advantage.

Legislation, by contrast, is inherently reactive. It responds to problems, risks, and societal pressures that are already visible. Lawmakers require evidence, public consultation, and political consensus. Such steps take their time. This is not a flaw in democratic governance per se; it is a safeguard to ensure legitimacy and broad support. However, when dealing with AI, the lag between "problem emergence" and "policy action" becomes particularly acute.

In practice, this means that many of the most pressing AI policy debates in Brussels today are about current risks that arose from technologies launched two or three years ago, while the next wave of risks might be already forming in the background. This structural delay is not something that can be fixed once and for all; it is an inherent feature of the system. The challenge is to reduce the lag and build mechanisms that allow governance to adjust in near-real time.

3.2.2 Continuous Adaptation as a Necessity

If there is a single lesson from the EU's recent AI legislative journey, it is that AI governance cannot be a "set-and-forget" exercise. Regulatory frameworks must be designed to evolve continuously, responding to technological shifts without restarting the entire legislative process from scratch.

The trajectory of the AI Act itself illustrates this point. When the legislation was first drafted in 2021, the proposal focused primarily on classifying AI systems into risk categories, with detailed requirements for "high-risk" use cases such as biometric identification, credit scoring, or safety-critical infrastructure. At the time, generative AI was barely on the policy radar. Yet, by late 2022 and early 2023, tools like ChatGPT, had transformed public perception of AI almost overnight. The original AI Act text suddenly looked incomplete, failing to address a new class of systems capable of producing text, images, and audio at scale and accessible to millions of users.

In response, EU legislators inserted entirely new provisions into the Act to deal with "general-purpose AI models" and their foundation model architecture. These provisions were negotiated under tight deadlines, underscoring the reactive nature of legislative adaptation. While this flexibility is commendable, it also highlights the need for built-in review clauses, agile rule-making powers for regulatory bodies, and structured stakeholder feedback loops. Without these, every new technological breakthrough will risk triggering a last-minute scramble to retrofit existing laws.

From a regulatory theory perspective, the AI Act sits primarily in the tradition of risk-based command-and-control regulation, in which legal obligations are explicitly defined and tiered according to the severity of risk. This method has the advantage of reducing ambiguity and creating clear compliance thresholds, but it is vulnerable to the speed problem: AI risks evolve far faster than static rules can be revised. As Cajueiro and Celestino note [37], the frequency and unpredictability of AI-related risks, coupled with the diversity of AI applications, make it challenging for prescriptive rules to remain aligned with real-world conditions.

At the same time, the AI Act does contain innovation-driven regulatory elements such as regulatory sandboxes, voluntary codes of conduct, and delegated acts that allow technical updates without reopening the full legislative text [38], [39]. These tools aim to keep pace with technological change by creating space for experimentation and multi-stakeholder oversight. However, in the AI Act, these mechanisms play a supplementary rather than central role.

Looking ahead, the EU faces a choice: it can continue treating AI regulation as a series of discrete legislative projects, or it can embrace a governance model that is modular, adaptive, and anticipatory – blending the certainty of risk-based rules with the flexibility of innovation-driven oversight. This will require not only legal innovation, such as the ability to issue delegated acts or adopt binding technical standards quickly, but also a cultural shift in how the EU approaches technology policy. Policymakers will need to accept that AI governance is not a one-off achievement but a permanent process of iteration, much like the AI systems it seeks to oversee.

3.3 NAVIGATING COMPLIANCE: THE ROLE OF HARMONIZED STANDARDS

The AI Act was conceived as a horizontal regulation designed to establish a single, harmonized framework for artificial intelligence across the EU's internal market. Its objective is to prevent the emergence of fragmented national rules, which could undermine innovation and competitiveness. By providing one set of obligations for AI solutions, the Act promises legal clarity, regulatory certainty, and equal market access, particularly important in an area where developers and users operate across borders by default. All that sounds like a great end-goal, but the road there is still ongoing and quite rocky. From a policy perspective, this harmonization reflects the EU's effort to position itself as a predictable and trustworthy regulator, offering both protection to citizens and a competitive edge to companies that invest early in compliance.

3.3.1 Compliance Burdens for SMEs and AI Providers

Even when a new regulation is designed to be harmonized, putting it into practice can pose a significant challenge. For AI developers and companies, particularly smaller SMEs, the AI Act and data governance legislations, introduce a wide array of obligations that must be interpreted, planned for, and implemented in practice. Understanding the legal text, translating it into concrete operational measures, setting up internal risk management and documentation processes, and ensuring ongoing monitoring can be costly and overwhelming.

Smaller innovators often lack dedicated legal or compliance departments, meaning they may need to hire external consultants or legal advisors, which is a costly and time-consuming requirement. Even for companies with some internal expertise, the process of dissecting the regulation, deciding which internal procedures need to be adjusted, and training teams on new obligations can significantly slow down development and innovation. In some cases, these burdens may discourage entry into the EU market entirely.

The challenge is twofold: first, to understand what the AI Act requires in abstract legal terms, and second, to translate those requirements into practical, operational steps that can be applied to real-world AI systems. Without effective support mechanisms, companies risk expending excessive resources on compliance rather than product development, inadvertently creating a barrier for smaller innovators who lack the same financial or technical capacity as larger firms. In short, the AI Act's promise of harmonization is only as valuable as the ability of its users to navigate and implement it efficiently.

3.3.2 Harmonized Standards as a Tool to Reduce the Burden

Given these burdens, **harmonized standards** are designed to offer practical guidance and reduce uncertainty, translating legal requirements into actionable steps for AI providers. To bridge the gap between high-level legal obligations and practical implementation, the EU relies on harmonized standards – voluntary technical specifications developed by bodies such as CEN, CENELEC, or ETSI. When the European Commission cites these standards in the Official Journal of the EU, compliance with them creates a **"presumption of conformity"** with the law. For AI developers, this means that instead of interpreting abstract legal requirements on their own, they can follow detailed, technical, industry-approved methodologies to demonstrate compliance.

In theory, such standards are a powerful tool to lower compliance costs and increase legal certainty. Rather than reinventing the wheel for each product, companies could rely on pre-defined protocols for risk management, data governance, testing, documentation, and post-market monitoring. Harmonized standards could also help ensure that regulators, conformity-assessment bodies, and developers are all speaking the same technical language when evaluating AI systems.

Moreover, there is growing interest in developing cross-regulatory compliance mappings. Many obligations under the AI Act intersect with parallel frameworks such as the GDPR, NIS 2, DORA, and the Cyber Resilience Act, to name a few. In practice, technical standards that operationalise shared concepts, such as risk management, security controls, documentation, and incident reporting, could, in the future, help organisations reuse compliance efforts across different digital regulations. Although such crosswalks are not yet formalised, they represent an important opportunity to reduce compliance burdens, especially for SMEs, and a potential area for future standardisation work.

If drafted well, these standards will be particularly important for smaller innovators who do not have the resources to build extensive compliance systems from scratch. Clear technical guidance can turn abstract

legal principles into practical checklists, making it possible for SMEs to compete on a level playing field with large technology companies.

3.3.3 Delays, Risks, and Recommendations

The challenge is that **the harmonized standards required for the AI Act do not yet exist**, and their development will take time. Standards bodies must translate broad legal obligations into precise technical norms. The effectiveness of harmonized standards hinges on timely availability, but as things stand, those standards lag behind. Drafting technical norms from the AI Act's legal text takes time, and the first batch of standards is only expected shortly after 2 August 2026, after most of the AI Act's requirements (except for Article 6) come into effect [40]. This delay could make the **early compliance costly and uneven**: large firms could afford to develop internal interpretations and hire consultants, while smaller players might struggle. However, in October 2025, the CEN and CENELEC have **adopted an exceptional package of measures**[11] to ensure that the standards will be available by Q4 2026.

The integration of data governance requirements adds further complexity to standards development timelines. The need to align AI, data governance, and other various standards requires unprecedented coordination between different European and international standards organizations. Moreover, unlike traditional product standards, AI and data governance standards must account for rapidly evolving technologies and changing data flows. Standards for data altruism, for instance, must anticipate future AI capabilities and data use patterns that may not yet be fully understood. This requires standards development processes that are more adaptive and iterative than traditional approaches.

There are already ongoing efforts to release compliance burdens, such as the production of the Code of Practice, that provide additional guidance specifically for providers GPAI. Furthermore, initiatives such as **regulatory sandboxes, phased rollouts, and interim guidance** can help smooth the transition. Sandboxes allow innovators to test AI systems under real-world conditions while under regulatory supervision, phased rollouts gradually introduce obligations to reduce compliance shocks, and interim guidance clarifies how to apply requirements before harmonized standards are fully in place. Together, these measures can help prevent early overburdening, particularly for SMEs and new entrants.

Moreover, the production of simpler and more accessible tools (for example, interactive online platforms) can help companies assess their AI systems, identify risk classification, and determine the applicable requirements. While several such solutions already exist on the market, they are not issued by the European Commission and might therefore be perceived as lacking authoritative weight. Additionally, because these are private solutions, SMEs may need to incur extra costs for licensing, implementation, or external consultancy to ensure full compliance. This highlights the need for the European Commission to develop its own accessible tools to provide authoritative, cost-effective guidance for all AI providers and deployers.

3.3.4 Perspective Summary

The discussed compliance challenges are real, but they are not insurmountable when addressed proactively. Supporters of AI and data governance might argue that these obstacles are transitional. Once harmonized standards, conformity assessment procedures, and EU-wide guidance are in place, compliance should become simpler and more predictable. Initiatives such as regulatory sandboxes, phased implementation, and open guidance aim to cushion the adjustment period and level the playing field.

However, if these measures are mismanaged or delays persist, the regulatory overlaps risk eroding the AI Act's credibility as a truly harmonized framework, and could leave innovators, particularly those with limited resources, lost in the maze of EU obligations.

[11] https://www.cencenelec.eu/news-events/news/2025/brief-news/2025-10-23-ai-standardization/?utm_source=substack&utm_medium=email

3.4 DATA GOVERNANCE AND AI: CHALLENGES AND PRACTICAL IMPLICATIONS

Data is the backbone of AI development and plays a crucial role in machine learning (ML). The development, training, and operation of AI systems fundamentally rely on large volumes of (preferably, high-quality) data. The availability, accessibility, and proper governance of datasets directly affect model performance, reliability, and fairness. For developers, data is not merely an input; it is an operational resource that must be carefully curated, processed, documented, and maintained. At the same time, the EU regulatory landscape imposes a variety of obligations on how data can be collected, stored, shared, and reused. In this section, we examine the most pressing data-related tensions that arise from overlapping legal frameworks and explore how they manifest in day-to-day AI development and deployment.

3.4.1 Overlapping Obligations

The AI Act is intended to **align with the existing EU legislation**, such as the GDPR/EUDPR, the Digital Services Act (DSA), the Digital Markets Act (DMA), Cybersecurity Act, product-safety directives and many other legislations that can become relevant depending on the type of AI solution. In principle, this alignment should avoid duplicate or conflicting requirements. For example, the AI Act's provisions on data governance are supposed to complement, rather than duplicate, GDPR's requirements for lawful data processing.

Despite these ambitions, **practical inconsistencies remain a real risk**. Several provisions of the AI Act overlap with existing frameworks, creating uncertainty about which obligations prevail**.** Experts note that these differing objectives can create tangible legal tensions [41]. Sitting between these frameworks, AI developers are often caught in a **regulatory paradox**: one regulation pushes toward more extensive data collection and retention for accountability, while others insists on reducing data processing to safeguard privacy and, increasingly, to minimise environmental impact (as reflected in sustainability instruments, such as the **Corporate Sustainability Reporting Directive (CSRD)**, which requires large companies to report on environmental impacts, including the energy use and resource intensity of digital systems).

For instance, while the AI Act demands that developers of high-risk systems maintain detailed logs and performance records to ensure traceability, the GDPR/EUDPR requires that personal data be retained only for *as long as necessary*. This raises the question: how can an AI provider reconcile the duty to store information for audits with the obligation to delete it when no longer strictly needed? Similarly, the AI Act's emphasis on algorithmic explainability and continuous monitoring may require additional processing of personal data, potentially conflicting with GDPR's principle of data minimization.

Further complicating the picture, the Data Governance Act and Data Act introduce a pro–data-sharing ethos into the EU regulatory landscape, which could be fundamental in putting the EU in that position of a global leader in AI. These laws aim to facilitate access to data for innovation, research, and public benefit, creating mechanisms for data intermediaries, data altruism, and mandatory sharing of industrial data. While this approach complements the AI Act's ambition to foster trustworthy AI, it can also clash with the restrictive stance of GDPR/EUDPR and the AI Act's own auditing obligations. Developers may find themselves encouraged to open up datasets while simultaneously being constrained by strict privacy requirements and long-term traceability duties – a regulatory paradox that is particularly challenging for smaller players lacking compliance resources.

When considering the interplay between all the regulations concerned with data governance, it becomes evident that AI developers face a dense web of overlapping obligations. These frameworks collectively impose requirements ranging from lawful data collection and anonymization to contractual safeguards and sector-specific restrictions. While these rules aim to protect fundamental rights and ensure fair competition, they also create complexity for innovation, particularly in high-risk sectors such as healthcare, mobility, or financial services, where access to sensitive or protected data is often indispensable for training robust AI models. This regulatory tension explains the growing interest in **synthetic data as a compliance and innovation tool**. Synthetic datasets can replicate the statistical properties of real-world data without including personal identifiers, thereby offering a legally and technically viable way to balance data protection obligations with the practical needs of AI development.

3.4.2 Legal Implications on the Use of Synthetic Data

Synthetic data can be defined as "artificial data that is generated from original data and a model that is trained to reproduce the characteristics and structure of the original data" [42]. It has emerged as a powerful tool for AI development, particularly in areas where real-world data is sensitive, scarce, or costly to obtain. In healthcare, for example, patient records contain highly sensitive personal information that cannot be freely shared. By generating synthetic datasets that preserve statistical properties and patterns of the original data without containing actual personal information, developers can train and test AI systems while avoiding privacy violations. Similarly, IoT devices, wearable health trackers, or industrial sensors produce large volumes of data that may include personal or proprietary information. Synthetic data can replicate these patterns for model training, ensuring operational efficiency and compliance with data protection rules.

A key legal advantage of synthetic data lies in its potential to bypass certain GDPR obligations. Properly generated synthetic data, when it can be shown to be effectively anonymised, may fall outside the scope of the GDPR and related EU data protection rules [43]. For AI developers, this means that where synthetic data does not qualify as personal data for the relevant recipient, obligations such as consent management, data minimisation, and retention limits may no longer apply. Effectively, synthetic data allows developers to train, test, and validate AI systems while reducing the compliance burden associated with handling sensitive personal information.

However, the exemption from GDPR obligations is neither automatic nor absolute. The legal threshold for when synthetic or pseudonymised data ceases to be personal data has been further clarified by the Court of Justice of the European Union in its **2025 Single Resolution Board (SRB) ruling** (C-413/23 P)[12]. The Court held that whether data is considered "personal" depends on the specific recipient's ability to re-identify individuals, applying a recipient-centred "means reasonably likely to be used" test (a key legal standard under the GDPR used to determine whether a natural person is identifiable and, consequently, if data protection laws apply). Under this approach, data derived from personal information may be considered non-personal for a recipient who:

- lacks the re-identification key,
- does not possess additional datasets or contextual information enabling linkage,
- has no legal entitlement or practical capacity to re-identify individuals, and
- cannot realistically apply techniques that would undermine anonymisation.

At the same time, the ruling preserves strict obligations for the original data controller: where synthetic data is derived from personal data, information duties and other controller responsibilities arise at the point of collection, regardless of the recipient's ability to identify individuals.

This judgment marks a significant departure from earlier, more rigid regulatory interpretations that treated all pseudonymised data as personal data, regardless of context. Following SRB, the legal status of synthetic data depends not only on the quality of the data-generation techniques but also on the factual circumstances surrounding its disclosure and use. If re-identification remains reasonably possible, whether by the developer, a collaborating entity, or any party with access to auxiliary information, the dataset will still constitute personal data and remain fully subject to GDPR obligations.

These developments create a more nuanced but also more **innovation-friendly** legal environment. Developers must now be able to demonstrate both the robustness of their synthetic-data techniques, and the absence of "reasonably likely" re-identification means for the intended recipient. This elevates the importance of documenting technical safeguards, architectural separation between synthetic-data pipelines and raw-data environments, and privacy risk assessments. At the same time, SRB creates new opportunities: in many cases, synthetic data can more confidently be treated as non-personal, enabling compliant data sharing, AI training, and cross-sector collaboration with reduced regulatory friction.

The AI Act explicitly recognizes synthetic data as a legitimate alternative to personal or non-anonymous data, particularly for high-risk AI systems (Articles 10 and 59). The legislation treats synthetic data as equivalent to

[12] https://curia.europa.eu/jcms/upload/docs/application/pdf/2025-09/cp250107en.pdf

non-personal data for the purposes of training, validation, and testing, emphasising its role in addressing bias, supporting explainability, and improving traceability. Where bias detection or system validation cannot be fully achieved using synthetic data, the processing of real personal data remains permissible but must be strictly necessary and accompanied by strong technical safeguards, documentation, and fundamental-rights protections. This regulatory framing positions synthetic data not only as a privacy-preserving solution but also as a means to streamline compliance for AI developers.

Beyond privacy, synthetic data facilitates broader access and re-use under the Data Governance Act (DGA) and the Data Act. The DGA explicitly highlights data synthesization as an acceptable method to protect personal and confidential business information while enabling the sharing, analysis, and reuse of data across sectors such as health, environment, energy, and finance. By using synthetic data, AI developers can leverage public datasets without infringing on trade secrets or contractual limitations, promoting innovation while remaining within the regulatory framework. These provisions are particularly relevant for SMEs and startups that may lack extensive legal resources to navigate complex compliance landscapes.

Finally, synthetic data can improve data quality, fairness, and representativeness. It allows oversampling of underrepresented groups, correction of imbalance in training corpora, and safe dissemination of rich datasets for scientific research, simulation, and public-policy modelling. The European Commission's Joint Research Centre highlights its potential for free sharing and re-use, supporting innovation in areas where access to high-quality data has traditionally been limited.[xliv]

Taken together, synthetic data, especially in light of the SRB ruling, has become both a privacy-preserving mechanism and a strategic tool for advancing AI innovation. When properly generated and governed, it allows AI developers to meet regulatory expectations while accelerating responsible deployment across sensitive and high-impact domains.

3.4.3 Cross-Border Data Challenges

Beyond the EU's internal legal tensions, the global nature of AI development introduces additional challenges. AI systems are rarely developed within the confines of a single jurisdiction; training often relies on cloud infrastructure hosted outside the EU, outsourced data labelling, or datasets obtained from third countries. This raises significant compliance questions under the GDPR's rules on international data transfers, which require either an adequacy decision, standard contractual clauses (SCCs), or other legal safeguards.

The AI Act does not directly regulate cross-border data transfers, but its obligations on dataset governance, traceability, and documentation mean that compliance cannot be isolated from transfer rules. For example, an AI developer using U.S.-based cloud providers may face simultaneous obligations: under the AI Act to log, retain, and document training data for auditability, and under GDPR to ensure that any personal data transferred outside the EU is subject to equivalent protection. The complexity of reconciling these frameworks can deter smaller players from engaging in global collaborations.

In this context, synthetic data emerges again as a potential enabler. If generated in a way that eliminates the possibility of re-identification, synthetic datasets are not subject to GDPR restrictions on personal data transfers. This allows developers to collaborate across borders and leverage global cloud infrastructures without triggering the same compliance hurdles, making synthetic data both a privacy-preserving and innovation-supporting tool in international AI development.

3.4.4 Perspective Summary

The regulation of data in the AI context illustrates one of the most intricate intersections of EU law. The AI Act's emphasis on high-quality, traceable, and representative datasets aligns in principle with the GDPR's requirements for lawful, proportionate, and secure processing. Yet this alignment also creates practical friction. Developers must satisfy parallel, and sometimes competing, obligations: ensuring robust documentation and system oversight under the AI Act while observing strict data-minimisation, purpose-limitation, and retention rules under the GDPR.

Synthetic data emerges as a powerful mitigating instrument. Following the CJEU's 2025 SRB ruling, whether synthetic (or pseudonymised) datasets fall within the scope of the GDPR now depends on the recipient's realistic ability to re-identify individuals. When synthetic data is robustly generated and recipients lack the means reasonably likely to permit re-identification, such data may be treated as non-personal, creating new opportunities for model training, testing, and validation with reduced regulatory constraints. Conversely, poorly

generated or insufficiently safeguarded synthetic datasets remain personal data and trigger full GDPR obligations. In this way, synthetic data can serve both the AI Act's objectives, such as bias mitigation, explainability, and improved data quality, and the broader data-sharing mechanisms established under the Data Governance Act and the Data Act.

Cross-border data governance adds another layer of complexity. Although the AI Act does not regulate international transfers directly, its requirements for auditability and dataset documentation interact tightly with the GDPR's stringent rules on data exports. In this setting, synthetic data again offers a pragmatic path: by reducing or eliminating reliance on personal data, it enables international collaboration, research, and system development without engaging transfer restrictions.

Taken together, these dynamics show that the AI Act does not displace existing EU data protection rules; rather, it amplifies their relevance and operational impact. Organisations that strategically deploy privacy-preserving techniques such as synthetic data, and document their technical and organisational safeguards, can turn overlapping regulatory obligations into an enabler of innovation, strengthening both compliance and competitiveness within the EU's evolving digital ecosystem.

Co-funded by the European Union

3.5 AI TRANSPARENCY UNDER THE EU AI ACT: RULES, IMPLEMENTATION, AND EMERGING ISSUES

Transparency is one of the cornerstones of the EU's regulatory approach to artificial intelligence. Its importance lies on several levels. First, transparency provides regulators with visibility to evaluate compliance with safety standards, data governance obligations, and fundamental rights protections. Second, it acts as a trust-building mechanism for users and society at large, demonstrating that AI systems are not impenetrable "black boxes" but can be explained and scrutinized. Third, it serves as a legal bridge between technical complexity and enforceable accountability.

The AI Act recognizes that transparency is not a single, uniform requirement. Instead, it encompasses three interlinked dimensions:

- System-level transparency: explainability, documentation, and traceability for developers and regulators.
- Provider-level transparency: public registration, disclosure of training data, model architecture, limitations.
- User-facing transparency: clear notices when individuals interact with AI or encounter AI-generated content.

These transparency dimensions and their application to different AI systems and models are discussed below.

3.5.1 Transparency for the High-Risk AI Systems

Article 13 of the AI Act states that: "High-risk AI systems shall be designed and developed in such a way as to ensure that their operation is sufficiently transparent to enable deployers to interpret a system's output and use it appropriately."[13] Providers are required to accompany such systems with clear and comprehensive instructions for use, delivered in an appropriate format, that detail the system's identity, characteristics, intended purpose, performance metrics, limitations, foreseeable risks, human oversight measures, input data specifications where relevant, and maintenance requirements. These instructions must be accessible and comprehensible to deployers, ensuring that they can not only understand how the system functions but also use it in a manner that aligns with safety, fundamental rights protections, and compliance obligations. These are the requirements as they are set out in the EU AI Act. However, the practical and technical understanding of transparency are yet to be elaborated.

The EU AI Act demands an appropriate type and degree of transparency for high-risk AI systems. For now, there is no unified understanding of what that means in practice or what would be sufficient to demonstrate compliance. The picture is incomplete because the harmonized European standards, which are expected to operationalize these obligations, have not yet been finalized or published. This legal uncertainty creates a compliance dilemma: providers are legally obliged to implement transparency but lack concrete benchmarks for how much explanation or documentation will be "enough."

The transparency obligations for high-risk AI systems enter into force from 2 August 2026, and most likely the harmonized standard will be available before that date. In the meantime, AI developers can draw on established best practices to reduce compliance risks. These include:

- Documenting design choices, model limitations, and performance evidence in detail.
- Providing non-technical instructions for deployers, including guidance on misuse and foreseeable risks.
- Offering interpretable outputs where possible, or at least confidence scores or rationales to contextualize results.
- Maintaining internal records and logs that show good-faith efforts to meet the spirit of transparency.

Once harmonized standards are published, these interim practices can serve as a foundation for full alignment.

[13] AU AI Act, Article 13, para. 1 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

Beyond technical and documentary requirements, the Act also introduces a systematic transparency mechanism: an EU-wide database for high-risk AI systems, to be set up and maintained by the European Commission. Providers must register their HRAIS in this database, which will host technical and compliance information in a publicly accessible format. The database will become operational on 2 August 2026, adding a new layer of public accountability. How commercially sensitive information will be balanced against public transparency remains an open question, to be clarified in future implementing measures.

3.5.2 Transparency for general-purpose AI (GPAI) models

Unlike high-risk AI systems, **general-purpose AI (GPAI) models** are not tied to a specific sectoral application. Instead, they are models trained on vast and diverse datasets, with significant computational power, and capable of performing a **wide range of distinct tasks**. Because these models can be integrated downstream into countless AI systems, their role in the AI Act is structurally different. Transparency obligations here are aimed at ensuring that both the Commission and downstream deployers have a baseline understanding of the models' properties, training processes, and intended uses.

To operationalize these obligations, the Commission has already issued a **Code of Practice for GPAI models,**[14] adopted in July 2025, together with accompanying **guidance** and a **model template**. While adherence to the GPAI Code is voluntary, the providers are allowed to rely on it as a way of demonstrating compliance. In practice, this means that GPAI providers can follow a pre-structured set of obligations rather than interpreting broad legislative requirements on their own. The GPAI Code requires providers to disclose, at minimum, high-level details on model properties (architecture, modalities, size), distribution and licensing terms, intended and acceptable use cases, and key training aspects (data types, compute, and energy requirements).

Major technology companies, including Google, Microsoft, Amazon, Mistral AI, and OpenAI, have signed the GPAI Code, signalling broad industry alignment.[15] By contrast, Meta refused to sign, and Elon Musk's xAI only signed the safety and security chapter. Importantly, however, non-signatories are not exempt: all GPAI providers remain legally bound by the Act's transparency requirements, which are already enforceable.

3.5.3 General Transparency Obligations

Beyond obligations for high-risk AI systems and GPAI models, the AI Act establishes horizontal transparency duties applicable across a wide range of AI applications (Article 50). These rules ensure that end-users and the public are not misled when interacting with AI or encountering AI-generated content, complementing the more technical, provider-focused requirements. They will be applicable from 2 August 2026. In the meantime, the European Commission launched a consultation[16] to develop guidelines and a Code of Practice on transparent AI systems that will help both deployers and providers to identify and label AI-generated content.

Users must generally be informed when interacting with an AI system, unless it is obvious from the context. For developers, this means incorporating visible disclosure mechanisms, such as notices at the start of an interaction. Exceptions exist for certain law enforcement uses, provided safeguards are in place.

AI-generated or manipulated content, including text, images, video, or audio, must be marked in a machine-readable and detectable way to prevent misinformation and deepfakes. While technical standards are still being developed, providers are expected to implement effective, interoperable, and reliable solutions. Deployers of emotion recognition or biometric categorisation systems must inform individuals of their use and comply with EU data protection law, emphasizing protection of fundamental rights in sensitive applications. Similarly, deepfakes and other AI-manipulated media must be disclosed unless exemptions apply (law

[14] https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai

[15] https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai#ecl-inpage-Signatories-of-the-AI-Pact

[16] https://digital-strategy.ec.europa.eu/en/news/commission-launches-consultation-develop-guidelines-and-code-practice-transparent-ai-systems

enforcement, artistic, satirical, or fictional uses), with disclosure designed not to compromise the user experience.

These general transparency obligations establish a baseline of openness that all AI developers and deployers must adhere to, regardless of whether their system is considered high-risk. For companies, compliance will require a combination of technical solutions (e.g., watermarking, disclosure design) and organizational processes (e.g., editorial review, GDPR alignment), ensuring that users can recognize, understand, and properly contextualize their interactions with AI.

3.5.4 Transparency Gaps and Emerging Risks

While the AI Act establishes detailed transparency obligations, practical gaps remain, particularly when AI systems interact with users in ways that are difficult to quantify or foresee. A notable example is AI-driven chatbots and companion systems capable of fostering emotional attachments [44]. The Act requires disclosure that the system is artificial, but it does not address the potential for subtle psychological manipulation or emotional dependency [45]. Developers could argue that occasional emotional bonds do not constitute "significant harm," leaving ambiguity about whether compliance measures are sufficient.

From a compliance perspective, this creates a tension: even if developers fulfil all formal transparency obligations, such as providing clear disclosures, instructions, and documentation, they may still face scrutiny if their systems unintentionally induce harmful behavioural outcomes. The uncertainty is compounded by the fact that existing EU laws, such as the Unfair Commercial Practices Directive (UCPD) or the Digital Services Act (DSA), target interface design rather than conversational content, leaving a regulatory grey zone.

For AI developers, these gaps imply that technical transparency alone may not be enough to mitigate legal or reputational risks. Firms may need to adopt proactive measures beyond the AI Act, such as designing interaction protocols that minimize the likelihood of emotional manipulation, implementing monitoring and reporting systems, and conducting internal risk assessments focused on behavioural impact. This highlights an important principle: transparency is not only a documentation or disclosure exercise but a tool for meaningful accountability, which must increasingly encompass the social and psychological dimensions of AI systems.

3.5.5 Perspective Summary

Transparency is central to the EU's approach to AI regulation, serving as both a compliance mechanism and a trust-building tool. Across high-risk AI systems, general-purpose AI models, and broader AI applications, transparency obligations aim to ensure that AI systems can be understood, traced, and scrutinized by deployers, regulators, and end-users alike. For developers, the implications are clear:

- Do not wait for harmonized standards – adopt best practices now to demonstrate good faith.
- Prepare for public disclosure through the EU database (2026) by balancing transparency with trade secrets.
- Anticipate broader scrutiny beyond compliance, particularly regarding social and behavioural impacts.

Ultimately, the transparency regime under the AI Act is more than a compliance checklist. It is a framework that pushes AI developers toward accountability: technical, legal, and social. Developers who treat transparency as a core design principle rather than a formal obligation will be better positioned to build trustworthy, legally robust, and socially sustainable AI.

3.6 COPYRIGHT

Copyright has rapidly emerged as one of the most contentious areas in the governance of artificial intelligence. In September 2025, AI company Anthropic agreed to a record $1.5 billion settlement with U.S. book authors who alleged that millions of copyrighted works had been copied and stored without permission during model training [46]. While the company did not admit wrongdoing, the size of the settlement demonstrates the enormous stakes involved when copyrighted material is at issue. Although this case arose under U.S. law, it underscores a global reality: questions about how AI models are trained, and whether authors and creators are fairly compensated, now sit at the very centre of regulatory debates.

In the European Union, copyright is regulated through 13 directives and 2 regulations[17], such as the InfoSoc Directive (2001/29/EC) and the more recent Copyright in the Digital Single Market (DSM) Directive (2019/790). These instruments harmonize key rights of authors and rightsholders across Member States, while also introducing exceptions such as text and data mining (TDM). Importantly, EU law is premised on the principle of human authorship and grants exclusive rights to reproduce, distribute, and communicate works to the public, unless exceptions apply.

While the AI Act itself does not alter copyright law, its interaction with these directives is crucial: AI developers must rely on the DSM Directive's TDM rules when sourcing training data, and questions about authorship or ownership of AI-generated outputs must be resolved within the existing EU copyright framework. This means that copyright issues in AI are not governed by a single, unified regime, but rather by the interplay between longstanding EU copyright law and the new horizontal obligations introduced by the AI Act.

3.6.1 Copyright in Training Data

One of the most controversial aspects of AI development concerns the data used to train general-purpose models. These systems are built on vast datasets often scraped from the internet, which means they inevitably contain copyrighted books, articles, images, and other creative works. High-profile lawsuits, such as the one filed by The New York Times against OpenAI, allege that copyrighted material was accessed and reused without permission. Similar cases have been launched by authors, publishers, and image libraries, pointing to a growing conflict between creators and technology companies over the legality of large-scale data harvesting.

In the EU, the DSM Directive provides a partial framework for lawful use. Article 3 allows text and data mining (TDM) for research purposes, while Article 4 establishes an opt-out mechanism for commercial uses, enabling rightsholders to reserve their rights and prevent their works from being included in training datasets.

However, even when copyright holders are entitled to control the use of their works, enforcement in practice is extremely difficult. Developers rarely disclose exactly what goes into their training datasets, and creators may not even know their works have been copied. Some experts argue [47] that a possible solution could be collective licensing: a system where rights holders pool their works into a common framework, and AI firms pay a license fee to use them. This would avoid millions of individual negotiations. However, such systems are not yet designed for AI training, and questions remain about how to identify which works were used and how royalties should be fairly distributed. Still, the push for remuneration is gaining traction in Brussels, reflecting growing pressure from publishers, authors, and cultural organisations to ensure creators' share in the value extracted from their works.

The EU AI Act tries to close some of these gaps by imposing new obligations on GPAI model providers under Article 53. The Copyright chapter of the GPAI Code of Practice further explains how the industry can comply with the obligations under Article 53.

Companies must adopt a copyright compliance policy that ensures EU copyright law is respected, particularly when rights holders have opted out of text and data mining. For example, machine-readable protocols such as "robots.txt" files must be observed when crawling websites. Providers are also required to publish a summary of the content used for training their models, based on a template to be issued by the European AI

[17] https://digital-strategy.ec.europa.eu/en/policies/copyright-legislation

Office. These summaries should list major datasets or describe other data sources, enabling rights holders to exercise their rights, even if trade secrets and business confidentiality limit the level of detail.

In addition, GPAI providers must implement safeguards to ensure their models do not reproduce copyrighted training material in outputs, for instance by memorising and then regurgitating entire passages or images. They are also expected to avoid sources that are known to host pirated content when scraping the internet. To make this obligation workable, the European Commission has announced that a dynamic list of such infringing sites, maintained by competent EU and EEA bodies, will be made available on an official EU website. While these measures mark an important step, they stop short of guaranteeing that training data is always lawfully acquired, since providers are not required to verify the legality of third-party datasets.

The drafting of the GPAI Code of Practice illustrates how politically sensitive copyright transparency became [48]. Early drafts contained stronger obligations for providers to disclose detailed information about the datasets they used, which could have given rightsholders and the public a clearer picture of how copyrighted works were being processed. But these proposals were gradually watered down during negotiations. Civil society groups like COMMUNIA repeatedly warned [48] that shifting from broad, public-facing transparency to more limited bilateral disclosures weakened accountability and risked leaving authors in the dark. By the time the final version was adopted in July 2025, obligations had been diluted to “sufficiently detailed summaries” that balance transparency with trade secrets. This arc shows how lobbying pressures from industry led to compromises that still leave significant information gaps for creators and rightsholders.

3.6.2 Copyright in AI Outputs

A second dimension concerns the legal status of AI-generated works. Under current EU copyright law, **human authorship is essential** for a work to qualify for protection. This principle is rooted in the premise that copyright protects the expression of the author's own intellectual creation, and human creativity and decision-making are the core criteria. Works produced solely by machines, without meaningful human involvement, are therefore **not eligible for copyright protection** [49].

However, AI-assisted outputs may qualify if they incorporate a sufficient degree of human creativity, such as through prompt engineering, editing, curation, or creative choices that shape the final result. But of course, arises the question of how much human expression is enough to be considered “sufficient” and how to operationalize this.

This ambiguity creates risks for businesses using AI-generated content commercially, from marketing materials to software code. This legal ambiguity places creators and businesses in a grey zone. Without clear guidelines, companies publishing AI-generated content face uncertainty over **who owns the rights**, whether they can claim authorship, or if copyright applies at all. To navigate this, many industry players resort to practical shortcuts: some disclaim any ownership of AI-generated outputs, while others transfer or assign rights to humans in the creative chain to ensure legal clarity. Despite these adaptations, the lack of consistent EU-wide guidance leaves creators and users in a grey zone, complicating rights management and commercial exploitation.

The AI Act and the Codes of Practice attempted to address this ambiguity, but the drafting process revealed how fraught the issue is. Early drafts of the GPAI Code of Practice proposed downstream compliance mechanisms to prevent AI from generating outputs similar to copyrighted works. Critics argued these amounted to output filters that risked over-blocking and restricting lawful expression. After civil society pushback, this measure was replaced with a focus on “memorisation” – the tendency of models to regurgitate training data verbatim. Image-generation models have been shown to reproduce stock-photo watermarks from Getty Images [50], while music AI tools sometimes generate melodies that are near-identical to existing songs. Such cases demonstrate how memorisation can manifest in practice, creating real risks of infringement and litigation. They also highlight why vague commitments to implement “technical safeguards” may not be enough to reassure rightsholders that their works will not resurface in AI outputs. In the final version of the Codes of Practice, all explicit references to memorisation were dropped. Instead, model providers are required to implement “appropriate and proportionate technical safeguards” to prevent outputs that unlawfully reproduce copyrighted training data [48].

This shift illustrates two key points. First, regulators are struggling to define legally sound and technically workable safeguards for copyright at the output stage. Second, compromises made in the drafting of the Code of Practice reveal the tension between rights-holder protection and fundamental rights such as freedom of expression. Notably, open-source GPAI developers were treated more leniently: rather than imposing

contractual prohibitions they could not realistically enforce, the Code only requires them to warn users that infringing uses remain unlawful [48].

Taken together, these provisions show that copyright at the output level remains largely underdeveloped in EU law. While the AI Act introduces new transparency and compliance obligations for training data, it leaves the fundamental question of authorship and ownership of AI-generated outputs essentially unresolved.

3.6.3 Perspective Summary

Looking ahead, copyright will remain one of the thorniest questions in EU AI governance. The AI Act and GPAI Codes of Practice establish important transparency and compliance frameworks, but fundamental questions about authorship, ownership, and remuneration of AI-generated works remain unresolved. Experience with these voluntary and regulatory mechanisms, including technical safeguards, rights-holder opt-outs, and emerging best practices, may provide valuable insights for future legislative reforms. Over time, these lessons could inform the development of more comprehensive rules that balance creators' rights, technological innovation, and practical enforceability, ensuring that EU copyright law evolves in step with AI capabilities.

In addition, the Court of Justice of the European Union (CJEU) is now being asked to address these issues for the first time in Case C-250/25[18], referred by a Hungarian court. The case involves a news publisher claiming that Google's AI chatbot, Gemini, reproduced and communicated press content without authorization. Among the questions before the Court are whether AI-generated outputs can constitute copyright infringement, whether the use of copyrighted content for training models constitutes reproduction, and how exceptions for text and data mining or temporary reproductions apply [51]. The decision could clarify whether even short extracts of press publications require consent and compensation and will likely have a decisive impact on the application of EU copyright law to AI. This landmark case underscores that the evolution of AI-related copyright is not only driven by legislation and best practices but will also be shaped by judicial interpretation, which could in turn inform future EU reforms.

[18] https://curia.europa.eu/juris/liste.jsf?num=C-250/25

3.7 INDUSTRY RESPONSE

The passage of the AI Act marked a landmark moment in European digital regulation. However, the law's adoption and early implementation have been anything but smooth. The process reveals a dynamic interplay between regulatory ambition, industrial competitiveness, and political influence. This sub-section traces how key industry actors have responded to the AI Act, analyses compliance implications for different groups, from large tech companies to SMEs, and reflects on the risk that regulatory burdens may disproportionately affect smaller players and reinforce market concentration. It also considers how the interests of end-users and citizens feature in this debate. Finally, it looks at mitigation options and what the future might hold.

3.7.1 Tech Sector Push-Back and Lobbying in Brussels

From the moment the European Commission published its proposal for the AI Act, industry stakeholders mobilized. Associations representing major global technology firms sought to influence the definition of "high-risk" systems, the obligations on general-purpose AI models, and the implementation timelines. Even as late as September 2025 the EU-wide debate on whether to pause or delay the roll-out of the AI Act is still ongoing [52].

Open letters and public statements, such as "Stop the Clock"[19] from European companies emphasized the need for a regulatory framework that supports research and does not drive innovation outside the EU. They warn that the growing regulatory complexity and uncertainty around compliance pathways risk slowing AI development in the EU and undermining the competitiveness of European industries. Lobbying for a pushback is not limited to industry. Several Member States, including Poland, Sweden and Czech Republic, are voicing similar concerns and calling for a pause in the AI Act implementation [53].

However, the current trajectory of the AI Act reflects a recurring pattern in European regulation of digital technologies. Initially, industry voices argue that regulation is premature, burdensome, and risks stifling innovation. Yet, once the legal framework crystallizes, companies typically pivot towards compliance, using the new rules even as a strategic advantage (via "trustworthy AI" branding, for example). Similar dynamics occurred under the General Data Protection Regulation (GDPR), where early resistance shifted to adaptation and advocacy of compliance as part of corporate value-proposition.

With the AI Act now in force and many obligations set to become applicable in a phased manner, large providers are already announcing governance frameworks, compliance teams, and certification readiness. This suggests that the lobbying phase is giving way to a compliance phase. But this shift does not eliminate concern: adaptation may favour established companies, while smaller actors could struggle to keep pace.

3.7.2 Divergent Stakeholder Perspectives

The AI Act's impact cannot be understood through the lens of industry alone. Its reception varies widely across stakeholders, reflecting deeper divides in resources, priorities, and values. The interests of Big Tech, SMEs, and civil society diverge significantly. Large multinational firms, such as Microsoft, Google, Meta, and OpenAI, possess the resources to absorb compliance costs, hire legal experts, and participate directly in standardization committees. For them, the long-term benefit of harmonized EU rules outweighs short-term adjustment costs, especially as compliance can become a barrier to entry for smaller competitors.

By contrast, small and medium-sized enterprises (SMEs) might struggle the most with the administrative burden associated with conformity assessments, documentation, and ongoing monitoring obligations. Some fear that the AI Act could reinforce market concentration by making compliance prohibitively expensive for smaller developers and startups [54]. The risk is that compliance asymmetry will lead to market consolidation, where large firms expand their dominance by meeting regulatory standards more easily and offering "compliance-as-a-service" to smaller players, thereby increasing dependency.

[19] https://aichampions.eu/#stoptheclock

Amid industry pressure, the original purpose of the AI Act to protect citizens' rights and safety, remains the essential point of reference. Public support for AI regulation in Europe has consistently been high, reflecting concerns about discrimination, privacy violations, and algorithmic manipulation. In response to the lobbying attempts to delay the implementation of the AI Act 31 civil society organizations sent an open letter[20] to the European Commission urging the EU Commission and the Member States to stay on track with the AI Act implementation.

While these groups share a common awareness of the AI Act's far-reaching implications, their motivations diverge sharply. Large technology firms often call for slower implementation or clearer guidance, citing complexity and innovation risks, but in practice, they possess the resources to adapt swiftly once the rules take effect. Smaller companies, by contrast, may also support a delay, yet for different reasons: uncertainty and limited capacity to absorb compliance costs make immediate implementation genuinely challenging. Civil society organizations take the opposite stance, viewing delays as a threat to accountability and to the protection of fundamental rights. These contrasting positions reveal a structural divide: for industry, the AI Act represents a regulatory hurdle to manage; for civil society, it is a long-awaited safeguard to uphold.

Ultimately, it remains an open question which path the EU will follow and whose interests will be prioritized in the process: the commercial logic of market actors, satisfying the delay request, or the normative commitment to citizens' rights and public trust in AI, by sticking with the intended AI Act timeline.

3.7.3 Perspective Summary

The ongoing debates surrounding the AI Act's implementation reflect a deeper tension within Europe's approach to digital governance: how to ensure that artificial intelligence develops in a way that is both globally competitive and fundamentally safe for individuals and society. While large technology companies advocate for more flexibility and SMEs voice concerns over compliance burdens, the common objective should remain the creation of trustworthy and human-centric AI that upholds European values of transparency, fairness, and accountability.

Achieving this balance requires not only regulatory discipline but also practical support for innovation. Policymakers must ensure that AI developers, regardless of their size, have the tools, clarity, and time needed to adapt to the new framework without being disadvantaged. Several instruments that can help level this playing field, such as harmonised standards and regulatory sandboxes, have already been introduced and discussed in Section 3.3 of this analysis. These mechanisms, once fully operational, will be essential to translate the legal intent of the AI Act into fair and workable compliance pathways.

[20] https://edri.org/our-work/open-letter-european-commission-member-states-keep-ai-act-national-implementation-on-track/

3.8 EU-LEVEL VS. NATIONAL IMPLEMENTATION

The EU regulatory framework for AI is designed as a **multi-level governance system**, in which responsibilities are distributed between EU institutions and the Member States. While the European Commission and the newly established **AI Office** set the overall direction, guidance, and coordination mechanisms, national authorities carry the primary responsibility for implementation, supervision, and enforcement. This dual structure reflects the broader logic of European integration: strategic coherence at the Union level combined with administrative flexibility at the national level. However, it also introduces substantial risks of divergence, fragmentation, and uneven readiness across Member States. The effectiveness of the AI Act will depend not only on its legal design but also on how consistently and equitably it is implemented throughout the Union.

3.8.1 Uneven Readiness Across Member States

Although the AI Act introduces a harmonised set of obligations, the starting conditions among Member States vary substantially [55]. Northern and Western European countries have made significant investments in digital governance and AI policy infrastructures. Many already operate national AI strategies, ethics councils, or innovation hubs that can be adapted to meet the new regulatory requirements. For instance, Finland's AuroraAI programme (completed in 2023) has established institutional frameworks that closely align with the AI Act's principles of accountability, transparency, and ethical AI development [56].

By contrast, several Central and Eastern European Member States face challenges arising from limited institutional resources, lower levels of digitalisation, and less experience in supervising complex technological systems [57]. These disparities reflect broader trends in EU digital policy, where well-resourced administrations have been early adopters of digital innovation, while others continue to face significant capacity gaps.

A key illustration of these disparities lies in the uneven development of support mechanisms such as regulatory sandboxes and testing facilities – instruments that are central to the AI Act's aim of combining innovation with safety. As of late 2025, only a handful of Member States[21] have operational or pilot AI sandboxes. Others are still in early planning stages or lack sufficient funding and technical expertise to launch them.

This uneven rollout is shaped not only by administrative maturity but also by political prioritisation. In countries where AI innovation is treated as a strategic economic priority, regulators have acted quickly to establish experimentation environments. Elsewhere, particularly in states with smaller digital industries or more limited policy coordination, sandboxes have received less attention. Consequently, AI developers in certain Member States enjoy early access to supportive compliance and testing frameworks, while their counterparts elsewhere face uncertainty and limited opportunities for regulatory experimentation.

3.8.2 Political Misalignment

These disparities in readiness also translate into divergent political priorities and implementation strategies. While the European Commission and the European AI Office define the high-level architecture of the regulation, national governments and industries are shaping the practical rollout. This dynamic has given rise to tensions, as Member States seek to adapt the AI Act to their domestic administrative realities and industrial interests.

For example, German Federal Ministry for Digital Transformation and Government Modernisation has circulated a draft position paper advocating for a one-year extension on high-risk AI deadlines, simplified documentation requirements, and broader research-testing exemptions – a proposal that reflects industrial concerns and a desire to preserve innovation space [58]. Such divergence is not unique to Germany. Analysis of national implementation plans across the Union reveals that many Member States are still in early stages of designating competent authorities, establishing regulatory sandboxes, and aligning domestic law with EU-level requirements [59]. Where national regulatory capacity is limited, political actors may favour a more

[21] https://artificialintelligenceact.eu/ai-regulatory-sandbox-approaches-eu-member-state-overview/

incremental approach, arguing that strict deadlines and heavy compliance burdens could hamper domestic innovation ecosystems or impose disproportionate costs on SMEs.

The political consequences of this misalignment are significant. If national authorities diverge in how they interpret definitions, set enforcement priorities, or apply sanctions, the risk of a fragmented internal market increases. Divergent approaches could create competitive imbalances between Member States, regulatory arbitrage opportunities for providers, and ultimately undermine the EU's strategic objective of a coherent, high-trust AI ecosystem.

3.8.3 Talent Centralization and Brain Drain

Beyond political differences in implementation priorities, a subtler but equally significant challenge lies in the distribution of expertise across the EU's multi-level governance structure. The institutional asymmetries are compounded by **skills and expertise shortages** [60]. Implementing the AI Act requires a highly specialised workforce (legal experts, AI auditors, conformity assessors, and risk analysts) all of whom are in short supply. As the AI Office in Brussels scales up its operations, it has become a magnet for such talent, attracting professionals from national administrations, academia, and industry.

While this centralisation may benefit EU-level coordination, it risks deepening the capacity gap at the Member State level, where regulatory authorities are already under strain. The resulting **"brain drain"** could further delay national implementation, weaken supervisory quality, and make Member States more dependent on external consultants or EU-issued guidance. This structural imbalance may inadvertently shift the centre of interpretative authority toward Brussels, reducing Member States' ability to tailor or contest implementation practices, and introducing new tensions into the subsidiarity principle underpinning EU governance.

Active talent migration also leads to the uneven distribution of AI expertise across the EU. Recent data on AI talent flows reveals [61] that countries like Germany, France, and Italy are already experiencing outbound migration of AI professionals, particularly to Switzerland, the UK, and the United States. France, uniquely among large EU economies, is undergoing a net brain drain, while Germany faces a notable outflow to the US – a pattern driven by global competition for technical talent and the prestige of non-EU research ecosystems. This trend risks exacerbating intra-EU capacity asymmetries. Some Member States, especially those with smaller digital sectors or weaker academic–industry pipelines, may struggle to develop or retain sufficient AI governance expertise.

The potential outcome is a multi-speed Europe in AI governance, where both innovation and compliance progress at uneven rates. Developers may even relocate or collaborate across borders to access more favourable regulatory environments, leading to concentration of AI research and development in already-advanced Member States. This pattern risks reinforcing the existing **digital divide** [62] within Europe, where countries with robust infrastructures continue to advance, while those with weaker administrative and financial capacities lag further behind. Such asymmetry could weaken the consistency of enforcement, distort competition across the single market, and challenge the EU's ambition to build a coherent and inclusive AI governance framework.

3.8.4 Perspective Summary

For the CERTAIN project, recognising these structural and political tensions is critical. It underscores the need for compliance tools and frameworks that are not only legally robust but also flexible enough to account for national disparities in timelines, capacity, and institutional structures. It also highlights the importance of engaging with national regulators, digital ministries, and innovation agencies – each of which may interpret and operationalise the AI Act differently. Bridging these gaps will be essential to ensure that the project's outputs can be effectively applied across the European Union.

4 METHODS OF COMPLIANCE

While the previous sections of this report analysed the legal and institutional framework of the EU AI Act, this section turns to a practical question: **how can organisations achieve compliance in the absence of harmonised standards?** The AI Act establishes comprehensive obligations for actors across the AI value chain but deliberately refrains from prescribing a single, uniform method for fulfilling them. Much of the operational detail, the "how" of compliance, remains under development through harmonised European standards, certification schemes, and codes of practice.

To situate this discussion, it is useful to recall the key milestones in the AI Act's legislative and implementation timeline, which shape the timeframe within which organisations must act.

AI Act Timeline	Milestone / Applicability
12 Jul 2024	Published in the Official Journal of the EU
1 Aug 2024	Act enters into force (legal existence starts; no obligations yet)
2 Nov 2024	Member States must designate supervisory & fundamental rights authorities
2 Feb 2025	Enforcement begins: Ban on unacceptable-risk AI, AI literacy requirements take effect
2 May 2025	Commission to publish voluntary codes of practice
2 Aug 2025	Obligations kick in for: GPAI providers, notified bodies, transparency, governance, penalties; national authorities & penalty regimes must be set up
2 Aug 2026	Full application of the Act (except Article 6.1 regarding specific high-risk systems)
2 Feb 2026	Commission issues post-market monitoring guidance (Article 6 related)
2 Aug 2027	Complete application including all high-risk provisions

Table 2. Timeline of the EU AI Act and related implementation milestones

Understanding these milestones is crucial, as they determine when specific obligations take effect and how rapidly organisations must adapt. In the meantime, companies and public organisations cannot simply wait. They must rely on existing compliance infrastructures, such as data protection frameworks, cybersecurity standards, and risk management systems, to meet AI Act requirements as far as possible and to prepare for the forthcoming harmonised standards. In this sense, "methods of compliance" refers not only to future technical standards but also to the practical and procedural tools that organisations can already use to ensure that AI is lawful, safe, and trustworthy.

The goal of this section is therefore two-fold:

1. To provide a step-by-step pathway to operationalise AI Act compliance in the current transition phase;
2. To outline the emerging instruments that will define the EU's operational compliance framework in the coming years.

Together, these two groups represent the continuum of AI governance in Europe: from established compliance systems that already support lawful and ethical AI to forthcoming mechanisms that will translate the AI Act's principles into operational reality.

4.1 OPERATIONALISING COMPLIANCE UNDER THE AI ACT

In the absence of harmonised standards, compliance must be operationalised through **direct interpretation of the AI Act**[22], particularly the articles which set out the essential requirements and documentation duties. The process can be conceptualised as a sequence of interdependent steps designed to identify obligations, manage risks, and maintain traceable records throughout the AI system's lifecycle.

This section outlines a series of practical pathways to operationalise compliance in a structured and legally coherent manner, focusing primarily on **providers of high-risk AI systems**, who face the most extensive obligations under the Act.

4.1.1 Determining Roles, Risks and Establishing an AI Inventory

The first step in achieving compliance is to develop a comprehensive AI register – an internal inventory listing all AI systems that an organisation develops, integrates, or uses. Each entry should include the system's intended purpose, the business process it supports, and its technical characteristics. This inventory provides a clear compliance perimeter and enables organisations to map legal obligations to specific systems. It also serves as the foundation for the risk classification and conformity assessment processes that follow.

It is equally important to record the organisation's **role** in relation to each system (provider, deployer, importer, distributor, or product manufacturer integrating AI). The AI Act assigns distinct obligations depending on the actor's role within the AI value chain (see Section 2.1.1). Determining the appropriate role is a critical early compliance task, as it defines the applicable obligations and the corresponding level of responsibility.

The next step involves classifying each AI system based on the **four-tier risk taxonomy** set out in the Regulation (see Section 2.1.2). It is crucial to identify potential risk indicators, such as whether the system falls under an Annex III high-risk use case (e.g., employment, education, essential services, or law enforcement). High-risk systems demand the most extensive compliance actions, and the remainder of this section focuses primarily on their operationalisation.

4.1.2 Obligations for Providers of High-Risk AI Systems

High-risk AI systems are subject to interlocking obligations addressing quality, transparency, safety, and accountability. These obligations can be translated into operational structures and documentation processes as follows.

[22] For related efforts to translate AI Act's obligations into operational guidance, see Machado, A., Jiménez Mérida, M., Deo, A., & Pathak, A. (2025). *AI Act Governance: Best Practices for Implementing the EU AI Act.* Initiative for Applied Arificial Intelligence. https://www.appliedai.de/en/insights/ai-act-governance-best-practices-for-implementing-the-eu-ai-act/

Risk Management System – Article 9. Providers must establish a continuous, documented risk management process that identifies, analyses, and mitigates foreseeable risks throughout the AI lifecycle. A dynamic risk register should document all potential hazards, including those related to safety, security, and fundamental rights.

Key Compliance Method	Specific Procedures / Practices
Risk Identification & Assessment	Conduct a Fundamental Rights Impact Assessment (FRIA) or equivalent internal assessment to identify potential harms such as bias, exclusion, or privacy violation.
Foresight & Misuse Analysis	Develop Reasonably Foreseeable Misuse Scenarios identifying how the system could be repurposed or fail unpredictably; document and regularly review them.
Risk Mitigation & Validation	Implement and document Risk Control Measures (e.g., bias mitigation, human review thresholds, model retraining). Validate effectiveness through testing and user feedback loops.
Residual Risk Evaluation	Quantify remaining risks after mitigation and justify their acceptability in light of intended purpose and safeguards.

Table 3. Key compliance methods under the AI Act, Article 9

Maintaining an up-to-date risk register linking identified hazards to implemented mitigations is essential. Such system not only fulfils legal obligations but also supports transparent and auditable decision-making.

Data Governance and Data Quality – Article 10. Providers must ensure that the data used for training, validation, and testing are relevant, representative, and free from errors. This requires clear documentation of data sources, collection methods, labelling, and preprocessing steps, as well as bias testing and performance evaluation.

Key Compliance Method	Specific Procedures / Practices
Data Provenance & Documentation	Maintain a Dataset Register listing all data sources, licensing status, and collection methods. Include version histories and data lineage records.
Bias Detection & Representativeness Testing	Use quantitative metrics (e.g., demographic parity, equal opportunity) and expert review to detect sampling bias; document test results and applied corrections.
Data Cleaning & Validation	Apply automated and manual quality checks to identify errors, duplicates, and inconsistencies. Document correction and validation procedures.
Ongoing Data Quality Monitoring	Schedule regular re-evaluations after each retraining cycle to monitor dataset drift and maintain fairness and integrity.

Table 4. Key compliance methods under the AI Act, Article 10

Where personal data are involved, the requirements of the General Data Protection Regulation (GDPR) remain applicable. Maintaining detailed records of dataset provenance and bias mitigation measures will be central to demonstrating compliance.

Technical Documentation – Article 11 and Annex IV. Providers must prepare detailed technical documentation demonstrating compliance. This documentation serves as the primary evidence for conformity assessment and must be maintained throughout the system's lifecycle.

Key Compliance Method	Specific Procedures / Practices
Comprehensive Technical Documentation File	Create a technical documentation file (see all details in Annex IV of the AI Act), which must include: general description of the system and its intended purpose; system architecture, algorithms, and components; data governance documentation; results of testing and validation; human oversight mechanisms; cybersecurity measures put in place; and the post-market monitoring plan.

Table 5. Key compliance methods under the AI Act, Article 11 and Annex IV

The documentation must be kept up to date, reflecting any modifications or retraining of the system, and the documentation must be accessible to regulators and conformity assessment bodies upon request.

Logging and Traceability – Article 12. High-risk AI systems must be designed with automatic logging capabilities to enable traceability of decisions and outputs. Logs should capture relevant events, system versions, inputs and outputs, and user interactions, while maintaining data security and integrity. Such traceability is vital for post-market monitoring and accountability, especially in cases of malfunction or harm.

Key Compliance Method	Specific Procedures / Practices
Event Logging	Configure the system to record timestamps, user interactions, and decision outputs in tamper-resistant logs.
Audit Trail Management	Use secure storage solutions that prevent modification of log files; establish retention policies consistent with risk level.
Log Review Procedures	Conduct periodic reviews of logs to identify anomalies, system errors, or misuse patterns.

Table 6. Key compliance methods under the AI Act, Article 12

Transparency and Provision of Information – Article 13. Providers must ensure that deployers receive clear, accurate, and accessible information on system capabilities, limitations, and operational conditions.

Key Compliance Method	Specific Procedures / Practices
User Instructions	Develop an Instruction Manual specifying intended use, data inputs, performance metrics, and known limitations.
Residual Risk Disclosure	Communicate possible risks (e.g., false positives, bias) transparently in user documentation.
Interface Transparency	Ensure user-facing systems provide visible indications of AI involvement where relevant.

Table 7. Key compliance methods under the AI Act, Article 13

Human Oversight – Article 14. Human oversight must be built into system design to ensure that humans can understand, intervene in, and override automated decisions when necessary. Oversight procedures should specify the scope of operator control, intervention thresholds, escalation protocols, and training requirements. Providers are expected to demonstrate that these procedures effectively prevent or mitigate potential harms.

Key Compliance Method	Specific Procedures / Practices
Oversight Design	Define explicit human intervention points where an operator can override or stop the system.
Training and Role Assignment	Develop and deliver operator training programmes ensuring users understand system capabilities and escalation protocols.
Monitoring Tools	Implement dashboards or alerts that allow real-time supervision of system behaviour and outputs.

Table 8. Key compliance methods under the AI Act, Article 14

Accuracy, Robustness, and Cybersecurity – Article 15. Providers are responsible for ensuring their AI systems achieve a high level of technical reliability. Measures include robustness testing, bias evaluation, model drift analysis, and protection against adversarial attacks or data poisoning.

Key Compliance Method	Specific Procedures / Practices
Performance Evaluation	Establish accuracy benchmarks aligned with the system's intended purpose; perform cross-validation and stress testing.
Robustness Testing	Conduct adversarial testing to identify vulnerabilities to model poisoning or input manipulation.
Cybersecurity Controls	Implement encryption, access control, and vulnerability management procedures for AI models and associated data pipelines.
Model Drift Monitoring	Continuously monitor performance metrics to detect model drift and retrain as needed.

Table 9. Key compliance methods under the AI Act, Article 15

Conformity Assessment and CE Marking – Article 16. Before placing a high-risk AI system on the market, providers must undergo a conformity assessment. Depending on the type of system, this may involve self-assessment or third-party evaluation by a notified body.

Key Compliance Method	Specific Procedures / Practices
Preparation for Assessment	Compile and verify completeness of Annex IV documentation and risk management evidence.
Assessment Pathway Selection	Identify the applicable conformity module (self-assessment or third-party review).
EU Declaration of Conformity	Draft and sign the declaration confirming compliance with the AI Act requirements.
CE Marking and Registration	Affix the CE marking and register the system in the EU database prior to placing it on the market.

Table 10. Key compliance methods under the AI Act, Article 16

Quality Management System (QMS) – Article 17. Providers are expected to establish and maintain a Quality Management System (QMS) ensuring consistent control over design, development, verification, and maintenance activities.

Key Compliance Method	Specific Procedures / Practices
Process Control	Establish standard operating procedures (SOPs) for data collection, model training, validation, and deployment. Ensure every development stage is documented and reviewed.
Version Management	Maintain a traceable version-control system documenting dataset changes, algorithmic updates, and model iterations.
Quality Audits	Conduct internal audits to verify adherence to QMS policies and assess effectiveness of implemented controls.
Corrective and Preventive Actions (CAPA)	Define procedures for identifying, reporting, and correcting non-conformities, ensuring feedback loops for continuous improvement.

Table 11. Key compliance methods under the AI Act, Article 17

The QMS acts as the organisational backbone of compliance, integrating AI-specific procedures into existing corporate governance structures.

Post-Market Monitoring – Chapter IX. Compliance under the AI Act is not limited to the moment an AI system is placed on the market. Providers and deployers of high-risk AI systems are required to implement continuous monitoring and oversight throughout the lifecycle of the system. Post-market monitoring, as specified in Chapter IX of the AI Act, involves systematically tracking the system's real-world performance to identify any deviations, unexpected behaviour, or emerging risks.

Key Compliance Method	Specific Procedures / Practices
Monitoring Plan	Collect real-world performance data and user feedback.
Incident Detection & Reporting	Define "serious incident" criteria and reporting pathways to national authorities.
Lifecycle Documentation Updates	Update technical files to reflect modifications or corrective measures.
Preventive Review	Verify effectiveness of corrective actions through regular audits.

Table 12.Key compliance methods under the AI Act, Chapter IX

Adopting an ongoing compliance framework will ensure that AI systems remain safe, reliable, and trustworthy even as they evolve in use. By embedding continuous oversight into AI operations, the AI Act creates a proactive approach to risk management, aligning technological innovation with the protection of users and broader societal interests.

4.1.3 Obligations Beyond Providers

Although providers bear the primary burden of compliance, other actors also have defined duties:

- Deployers must operate AI systems according to the provider's instructions and, for certain high-risk contexts (e.g., employment), conduct a Fundamental Rights Impact Assessment (FRIA) before deployment (Article 27, AI Act).
- Importers and distributors must ensure that documentation and CE marking are in place.
- Manufacturers integrating AI must ensure that both the product and the AI component meet applicable conformity requirements.

These interdependent obligations reflect the AI Act's multi-actor accountability model, ensuring that all stages of the AI value chain uphold safety and transparency.

4.1.4 Integrating with Existing Compliance Frameworks and Practices

The compliance methods outlined above do not operate in isolation. In most cases, they can and should be integrated into existing organisational compliance frameworks, allowing companies to build on structures already in place rather than creating parallel systems. This approach reflects one of the AI Act's central objectives: to harmonise AI-specific obligations with the EU's broader regulatory landscape, thereby avoiding unnecessary administrative burden and ensuring coherence across compliance domains.

For example,

- **Data protection and privacy governance** under the GDPR can be directly aligned with the AI Act's data governance requirements (Article 10). Organisations that already perform Data Protection Impact Assessments (DPIAs) can extend them into Fundamental Rights Impact Assessments (FRIAs), reducing duplication and ensuring coherence between privacy and broader ethical safeguards.
- **Cybersecurity and system integrity** obligations under the NIS2 Directive and sectoral safety laws naturally complement the AI Act's provisions on robustness and accuracy (Article 15). Existing security risk management and incident response procedures can be expanded to cover AI-specific risks such as model poisoning, adversarial attacks, or data manipulation.
- **Product-safety and conformity frameworks** already used in sectors such as machinery, medical devices, and vehicles provide ready-made pathways for integrating AI conformity assessments (Article 16).

By embedding AI Act compliance into these familiar systems, organisations achieve synergies across regulatory regimes. This not only streamlines administrative work but also strengthens overall governance and trustworthiness. In practice, the AI Act thus acts as an umbrella framework, aligning AI-related obligations with the EU's long-standing legal architecture on safety, data protection, and cybersecurity.

4.1.5 Organizational Implementation of Compliance

While the above-mentioned frameworks provide the external scaffolding for compliance, actual implementation happens inside organisations. Firms must translate these general principles into internal governance processes, operational routines, and accountability mechanisms. In other words, where the previous subsection focused on the regulatory environment, the next one turns to the organisational systems that make compliance feasible in practice.

Most companies already operate internal compliance systems developed in response to other regulatory requirements. These systems can be expanded to accommodate the AI Act without being rebuilt from scratch. Common organisational methods include:

- **Internal AI governance policies.** Many European technology firms have established internal AI ethics charters defining principles such as fairness, transparency, and accountability. These voluntary policies provide a strong foundation for the formal compliance structures required under the AI Act.
- **Cross-functional compliance teams.** Integrating expertise from legal, technical, data protection, and ethics domains ensures that compliance processes address all relevant risk dimensions.
- **Documentation and audit trails.** Maintaining up-to-date technical documentation, logs, and version histories supports both AI Act compliance and broader quality assurance.
- **Third-party assurance and certification.** In the absence of finalised conformity standards, organisations may seek external verification through independent audits or industry certification schemes.
- **AI compliance checklists.** Such checklists serve as internal control tools that translate legal requirements into concrete operational steps, such as confirming that risk management procedures are in place, that technical documentation is up to date, or that transparency obligations have been fulfilled. They are particularly useful for ensuring consistency across teams and for documenting compliance readiness during internal or external audits.

These internal mechanisms are not mandated by law but demonstrate organisational maturity and readiness. Establishing them early can substantially reduce exposure to regulatory or reputational risks once enforcement begins.

4.2 EMERGING INSTRUMENTS FOR AI ACT COMPLIANCE

Several new mechanisms, mainly the harmonized standards and codes of practice, introduced by or linked to the AI Act will define how compliance is demonstrated in the coming years.

4.2.1 Harmonised Standards

To make compliance measurable and predictable, the EU encourages reliance on harmonised European standards developed by standardisation bodies like CEN, CENELEC, and ETSI. The harmonized standards are designed to offer practical guidance and reduce uncertainty, translating legal requirements into actionable steps for AI providers. When the European Commission cites these standards in the Official Journal of the EU, compliance with them creates a **"presumption of conformity"** with the law. For AI developers, this means that instead of interpreting abstract legal requirements on their own, they can follow detailed, technical, industry-approved methodologies to demonstrate compliance. This reduces uncertainty for businesses and helps ensure consistent implementation across the EU.

As of 2025, these standards are still under development. The majority of the technical standards are expected to be published already after the corresponding AI Act obligations become applicable, shortly after 2 August 2026. Moreover, some standards are expected to be finalised throughout 2027. The detailed work program of the CEN and CENELEC Joint Technical Committee 21 can be tracked on the official website[23].

Expected Scope of Harmonised Standards under the AI Act

The forthcoming harmonised European standards, currently being developed under the Commission's standardisation request to CEN and CENELEC, will operationalise the legal requirements of Articles 8–17 of the AI Act by specifying verifiable processes, metrics, and evidence requirements [63]. They are expected to specify measurable processes, metrics, and documentation across the AI lifecycle, providing a concrete basis for conformity assessment.

These standards will set out how organisations must identify and mitigate risks, ensure data quality and representativeness, maintain comprehensive logs, and document transparency and human-oversight measures. They will also define quality-management and conformity-assessment procedures that integrate compliance throughout development and post-market monitoring. Together, these harmonised standards will form the operational backbone of the AI Act's implementation, creating a unified European compliance framework that transforms high-level legal principles into concrete, testable obligations for AI providers. Their adoption will mark a decisive step from interpretive compliance toward a standardised, measurable, and auditable model of AI governance.

4.2.2 Codes of Practice for General-Purpose AI (GPAI)

The GPAI Code of Practice is a voluntary, non-binding instrument introduced on July 10, 2025, developed through a multi-stakeholder process involving independent experts. It serves as a compliance-support tool under the AI Act, helping providers of general-purpose AI models meet key legal obligations concerning transparency, safety, security, and copyright. It is not legislation itself, but a practical implementation guide that complements and facilitates the enforcement of the AI Act, especially Articles 53 and 55.

The Code introduces a structured approach to help GPAI providers comply with the AI Act's requirements in a practical and harmonized manner. It consists of three chapters, each mapped to specific AI Act obligations.

- Transparency: Providers are expected to maintain up-to-date, standardized documentation for each model, including technical specifications, intended uses, limitations, and performance evaluations. A standardized **Model Documentation Form**[24] is provided to enhance comparability and accountability.

[23] https://standards.cencenelec.eu/dyn/www/f?p=205:22:0::::FSP_ORG_ID,FSP_LANG_ID:2916257,25&cs=1827B89DA69577BF3631EE2B6070F207D

[24] https://ec.europa.eu/newsroom/dae/redirection/document/118118

- Copyright: Signatories commit to respecting the EU Copyright Directive, including the use of state-of-the-art tools to identify and filter out copyrighted material where rights holders have opted out. This is especially crucial for training datasets used to develop large-scale models to ensure that content used respects intellectual property rights, minimizes legal risks, and upholds the principles of fairness and transparency in the development process.
- Safety and Security: For providers of GPAI models with systemic risk, the Code lays out expectations for conducting risk assessments, implementing risk mitigation measures, establishing safety and security protocols, and reporting serious incidents. Providers must also define internal roles and responsibilities related to AI risk governance, ensuring accountability across organizational levels.

Providers adhering to the Code will submit documentation and reporting to the AI Office, which may be used to assess compliance with binding legal requirements of the AI Act. While the Code itself does not impose penalties, failure to comply with its principles, particularly by large-scale or systemic providers, may invite scrutiny and could complicate future regulatory interactions under the AI Act.

4.2.3 Regulatory Sandboxes

The AI Act also mandates the creation of regulatory sandboxes. These are supposed to be the supervised environments managed by national authorities where AI systems can be tested under real-world conditions. Sandboxes allow providers, especially startups and SMEs, to experiment with AI under regulatory guidance, reducing compliance uncertainty before full-scale deployment. Every Member State must establish at least one AI regulatory sandbox by 2 August 2026.

4.3 SUMMARY AND OUTLOOK

The AI Act's obligations are being phased in gradually, with full applicability by 2027. However, regulators expect companies, especially those handling high-risk systems, to start preparing now. During this transitional period, compliance should be seen as progressive alignment rather than immediate perfection. The key message is that early preparation equals smoother compliance. Legal requirements are known; the methods are still maturing. Companies that embed transparency, accountability, and documentation now will be best positioned once harmonised standards are finalised.

While forthcoming harmonized European standards will provide concrete technical benchmarks, the foundation of compliance already exists. Organisations can therefore rely on existing standards and procedures (such as GDPR practices, conformity assessment models, and structured checklists) to meet AI Act obligations even before new harmonised standards take effect. The integration of these practices into everyday operations will not only ensure legal conformity but also enhance public trust and competitiveness in Europe's AI ecosystem.

In the longer term, as the European AI Office issues further guidance and standardisation efforts mature, these methods will converge into a stable and predictable compliance framework. Until then, the most effective strategy for any organisation is to combine proactive governance with adaptive learning, building on existing tools today while preparing for the harmonised compliance ecosystem of tomorrow.

5 CONCLUSIONS

The adoption of the EU AI Act represents a pivotal moment in the governance of AI technologies, shifting the European regulatory model from soft-law principles to a binding, risk-based framework. This report has outlined the AI Act's architecture, situated it within the existing EU law, analysed the AI regulatory landscape, and introduced the key implementation mechanisms that will shape future compliance practices.

For the CERTAIN project, this mapping exercise serves as a critical foundational step. Understanding the legal and institutional landscape is essential for developing effective tools, guidelines, and certification pathways that align with the EU's evolving regulatory vision.

While the Act has formally entered into force, many of its practical elements remain under development. Harmonised European standards, codes of practice, and sector-specific guidance will play a central role in translating legal obligations into actionable requirements. Until these are finalised, organisations must rely on existing frameworks to guide their AI-related risk management. CERTAIN can bridge this gap by helping stakeholders interpret current obligations and prepare for forthcoming requirements through tailored support and technical tooling.

From a policy and institutional perspective, the next phase will require close coordination among European and national authorities. The European AI Office, will play a central role in supervising implementation, issuing interpretative guidance, and monitoring systemic risks related to general-purpose AI models. National supervisory bodies will need to develop technical expertise, align enforcement practices, and ensure proportionality in applying the new rules, particularly to small and medium-sized enterprises (SMEs). Equally important will be maintaining a consistent interpretation of the AI Act across Member States to prevent regulatory fragmentation within the Single Market.

Several forward-looking challenges warrant continuous attention. The most immediate is the timely finalisation of the harmonised standards and the avoidance of implementation delays. As these standards define the practical tests and metrics for compliance, any postponement would prolong uncertainty for providers and deployers alike. Additionally, the dynamic nature of AI innovation may require periodic revision of these standards to reflect technological and ethical developments, ensuring that the regulatory framework remains future-proof. The next few years will test how effectively organisations can integrate legal, ethical, and technical requirements into the design and deployment of AI systems.

Moreover, the ongoing legislative debate surrounding the 2025 Digital Omnibus Regulation Proposal adds an additional layer of uncertainty to the wider digital rulebook. While its impact remains speculative until formally adopted, CERTAIN will continue to monitor these developments to ensure that future project outputs remain aligned with any adjustments to the EU's digital governance framework.

Looking ahead, CERTAIN's focus will move from mapping to active intervention: providing compliance tools for dataspace providers, AI developers, and deployers; streamlining certification procedures; and testing the proposed solutions across multiple sectors. Equally important will be raising awareness among companies, especially SMEs, and contributing to a broader ecosystem of trustworthy AI through engagement with standardisation bodies and regulators. This report lays the groundwork. The next phase will be about building on it, through collaboration, experimentation, and continuous learning.

6 REFERENCES

[1] Digital Watch Observatory. (2025, August). *EU AI Act oversight and fines begin this August*. Retrieved from https://dig.watch/updates/eu-ai-act-oversight-and-fines-begin-this-august

[2] Regulation (EU) 2024/1689. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance).* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

[3] Regulation (EU) 2016/679. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).* https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[4] Regulation (EU) 2022/868. *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) (Text with EEA relevance).* https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng

[5] Regulation (EU) 2023/2854. *Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance).* https://eur-lex.europa.eu/eli/reg/2023/2854

[6] Directive (EU) 2019/790. *Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance.).* https://eur-lex.europa.eu/eli/dir/2019/790/oj/eng

[7] Directive 96/9/EC. *Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31996L0009

[8] Implementing Decision EU 2023/1795. *Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (notified under document C(2023)4745) (Text with EEA relevance).* https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj

[9] Directive (EU) 2019/790. *Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance.)* https://eur-lex.europa.eu/eli/dir/2019/790/oj/eng

[10] Directive 2001/29/EC. *Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.* https://eur-lex.europa.eu/eli/dir/2001/29/oj/eng

[11] Directive 2004/48/EC. *Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (Text with EEA relevance).* https://eur-lex.europa.eu/eli/dir/2004/48/oj/eng

[12] Directive (EU) 2016/943. *Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their*

unlawful acquisition, use and disclosure (Text with EEA relevance). https://eur-lex.europa.eu/eli/dir/2016/943/oj/eng

[13] Regulation (EU) 2022/2065. *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) (Text with EEA relevance)*. https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng

[14] Regulation (EU) 2022/1925. *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) (Text with EEA relevance)*. https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng

[15] Directive (EU) 2018/1808. *Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.* https://eur-lex.europa.eu/eli/dir/2018/1808/oj/eng

[16] Directive 2005/29/EC. *Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (Text with EEA relevance)*. https://eur-lex.europa.eu/eli/dir/2005/29/oj/eng

[17] Directive (EU) 2019/771. *Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC (Text with EEA relevance)*. https://eur-lex.europa.eu/eli/dir/2019/771/oj/eng

[18] Regulation (EU) 2023/988. *Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC (Text with EEA relevance)*. https://eur-lex.europa.eu/eli/reg/2023/988/oj/eng

[19] Directive (EU) 2024/2853. *Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC (Text with EEA relevance)*. https://eur-lex.europa.eu/eli/dir/2024/2853/oj/eng

[20] Council Directive 85/374/EEC. *Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.* https://eur-lex.europa.eu/eli/dir/1985/374/oj/eng

[21] Regulation (EU) 2024/2847. *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) (Text with EEA relevance)*. https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

[22] Directive (EU) 2022/2555. *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) (Text with EEA relevance)*. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

[23] Regulation (EU) 2019/881. *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) (Text with EEA relevance). https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

[24] Regulation (EU) 2024/1183. *Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.* https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng

[25] Regulation (EU) 2017/745. *Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance).* https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng

[26] Directive 2014/65/EU. *Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast) Text with EEA relevance*. https://eur-lex.europa.eu/eli/dir/2014/65/oj/eng

[27] Regulation (EU) 2023/1230. *Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC (Text with EEA relevance).* https://eur-lex.europa.eu/eli/reg/2023/1230/oj/eng

[28] Directive 2014/53/EU. *Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance.* https://eur-lex.europa.eu/eli/dir/2014/53/oj/eng

[29] European Commission. (2025, April 9). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: AI Continent Action Plan.* (Report COM(2025) 165 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0165

[30] Lee, K. F. (2018). *AI superpowers: China, Silicon Valley, and the new world order.* Harper Business.

[31] Davies, M., Cohen, I., Thomson, D., & Scantlebury, H. (2025, September 30). *The EU AI Act: A step in the right direction, or an uneven playing field?* Innovation News Network. https://www.innovationnewsnetwork.com/the-eu-ai-act-a-step-in-the-right-direction-or-an-uneven-playing-field/60382/

[32] Fratta, S. (2024, June 10). *Building AI technology for Europeans in a transparent and responsible way.* Meta Newsroom. https://about.fb.com/news/2024/06/building-ai-technology-for-europeans-in-a-transparent-and-responsible-way/

[33] Browne, R. (2025, February 21). *Google, Meta execs blast Europe over strict AI regulation as Big Tech ups the ante.* CNBC. https://www.cnbc.com/2025/02/21/google-meta-execs-blast-europe-over-strict-ai-regulation.html

[34] Montgomery, B. (2024, June 21). *Apple delays launch of AI-powered features in Europe, blaming EU rules.* The Guardian. https://www.theguardian.com/technology/article/2024/jun/21/apple-ai-europe-regulation

[35] Wheeler, T. (2023, June 15). *The three challenges of AI regulation.* Brookings. https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation/

[36] Knowles, B., & Richards, J. T. (2021, March). *The sanction of authority: Promoting public trust in AI.* In Proceedings of the 2021 ACM conference on fairness, accountability, and transparency (pp. 262-271). https://doi.org/10.1145/3442188.3445890

[37] Cajueiro, D. O., & Celestino, V. R. R. (2025). *A Comprehensive Review of Artificial Intelligence Regulation: Weighing ethical principles and innovation.* Journal of Economy and Technology. https://doi.org/10.1016/j.ject.2025.07.001

[38] Marchant, G. E., & Allenby, B. (2017). *Soft law: New tools for governing emerging technologies.* Bulletin of the Atomic Scientists, 73(2), 108–114. https://doi.org/10.1080/00963402.2017.1288447

[39] Burd, J. T. (2021). Regulatory sandboxes for safety assurance of autonomous vehicles. J. Law Public Affairs, University of Pennsylvania, 7 (1). https://heinonline.org/HOL/LandingPage?handle=hein.journals/penjuaf7&div=8&id=&page=

[40] Bertuzzi, L. (2025a, May 16). *EU's AI Act standards to be ready on the heels of legal application deadline.* Specialist news and analysis on legal risk and regulation. MLex. https://www.mlex.com/mlex/articles/2341169/eu-s-ai-act-standards-to-be-ready-on-the-heels-of-legal-application-deadline

[41] Mateiciuc, E. (2025). *The adoption and harmonisation of regulation (EU) 2024/1689 (AI Act) and regulation (EU) 2018/1725 (EUDPR): challenges and best practices.* Challenges of the Knowledge Society, 208-220.

[42] Riemann, R. (n.d.). *Synthetic Data.* TechSonar blog of the European Data Protection Board (EDPB) https://edps.europa.eu/press-publications/publications/techsonar/synthetic-data_en.

[43] Finocchiaro, G., Landi, A., Polifrone, G., Ruffo, D., & Torlontano, F. (2024). *The Regulatory Future Of Synthetic Data Data. Synthesis as a resource for scientific research, innovation, and public policy in the European legal landscape*. https://doi.org/10.5281/zenodo.13342141

[44] Haeck, P. (2025a, August 21). *My AI friend has EU regulators worried.* Politico. https://www.politico.eu/article/ai-friends-experts-worried-artificial-intelligence-chatbot-digital-technology/?utm_source=substack&utm_medium=email

[45] Henning, M. (2025, August 27). *Is your AI trying to make you fall in love with it?* Euractiv. https://www.euractiv.com/news/is-your-ai-trying-to-make-you-fall-in-love-with-it/

[46] Oremus, W. (2025, September 5). *AI firm Anthropic reaches landmark $1.5B copyright deal with book authors.* The Washington Post. https://www.washingtonpost.com/technology/2025/09/05/anthropic-book-authors-copyright-settlement/?utm_source=alert&utm_medium=email&utm_campaign=wp_news_alert_revere&location=alert

[47] Quintais, J. P. (2025). *Generative AI, copyright and the AI Act.* Computer Law & Security Review, 56, 106107. https://doi.org/10.1016/j.clsr.2025.106107

[48] Nobre, T. (2025, July 21). *Our thoughts on the final version of the GPAI Code of Practice.* COMMUNIA Association. https://communia-association.org/2025/07/21/our-thoughts-on-the-final-version-of-the-gpai-code-of-practice/

[49] Fritz, J. (2024). *The notion of 'authorship' under EU law—who can be an author and what makes one an author? An analysis of the legislative framework and case law.* Journal of Intellectual Property Law & Practice, 19(7), 552–556. https://doi.org/10.1093/jiplp/jpae022

[50] Booth, R. (2025, June 9). *London AI firm says Getty copyright case poses 'overt threat' to industry.* The Guardian. https://www.theguardian.com/technology/2025/jun/09/stability-ai-getty-lawsuit-copyright

[51] The Court of Justice to rule for the first time on the interaction between generative AI. (2025, June 19). NautaDutilh. https://www.nautadutilh.com/en/insights/the-court-of-justice-to-rule-for-the-first-time-on-the-interaction-between-generative-ai-and-copyright-five-things-you-need-to-know/

[52] Haeck, P. (2025b, October 2). *EU readies for timeout on enforcing AI rules.* POLITICO. https://www.politico.eu/article/eu-prepares-ground-pause-artificial-intelligence-rules/

[53] Haeck, P. (2025c, June 23). *Swedish PM calls for a pause of the EU's AI rules.* POLITICO. https://www.politico.eu/article/swedish-pm-calls-to-pause-eu-ai-rules/

[54] Kutscher, S. (2025). *The EU AI Act: law of unintended consequences?* Technology and Regulation, 2025, 316–334. https://doi.org/10.71265/krne7205

[55] Galindo, L., K. Perset and F. Sheeka (2021). *An overview of national AI strategies and policies.* OECD Going Digital Toolkit Notes, No. 14, OECD Publishing, Paris, https://doi.org/10.1787/c05140d9-en

[56] Räisänen, S. (2023, December 11). *What we learned from AuroraAI: the pitfalls of doing ethics around unsettled technologies*. Finnish Center for Artificial Intelligence. https://fcai.fi/eab-blog/2023/12/11/what-we-learned-from-auroraai-the-pitfalls-of-doing-ethics-around-unsettled-technologies

[57] European Commission (2025, June 16). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future.* COM(2025) 290 final. https://digital-strategy.ec.europa.eu/en/library/state-digital-decade-2025-report

[58] Bertuzzi, L. (2025b, October 29). German digital ministry asks for significant softening, delays of EU AI Act. MLEX. https://www.mlex.com/mlex/articles/2405099/german-digital-ministry-asks-for-significant-softening-delays-of-eu-ai-act?utm_source=substack&utm_medium=email

[59] *Overview of all AI Act National Implementation Plans.* (2025). Future of Life Institute. https://artificialintelligenceact.eu/national-implementation-plans/?utm

[60] Van Haeften, W., Zhang, R., Mariani, S.-B., Lub, X., Ravesteijn, P., & Aertsen, P. (2024). *Bridging the AI Skills Gap in Europe: A Detailed Analysis of AI Skills and Roles.* 37th Bled eConference Resilience Through Digital Innovation: Enabling the Twin Transition (2024): 385-402. https://ris.utwente.nl/ws/portalfiles/portal/468248830/9789612868710.pdf#page=401

[61] Pal, S. (2024, July 31). Where is Europe's AI workforce coming from? Interface. https://www.interface-eu.org/publications/where-is-europes-ai-workforce-coming-from

[62] Varisco, L., & Pattinson, M. (2025). *Bridging the digital divide.* A Policy Brief from the Policy Learning Platform for a smarter Europe. Interreg Europe.

[63] Soler, G. J., De, N. S., Bassani, E., Sanchez, I., Evas, T., André, A., & Boulangé, T. (2024). *Harmonised Standards for the European AI Act.* JRC Publications Repository. https://publications.jrc.ec.europa.eu/repository/handle/JRC139430