EU ACT on Artificial Intelligence: A white paper by ARENA2036

Acknowledgement: TEF AI Matters

What AI providers and deployers need to know

Stand 07. February 2025

Ansprechpartner:

Muhammad Saeed
ARENA2036 e.V.
Pfaffenwaldring 19
70569 Stuttgart
Tel. 0155 60070608
E-Mail: muhammad.saeed@arena2036.de

White Paper
Business and Research Model

ARENA2036

Artificial Intelligence Act in ARENA2036

Authors:

Muhammad Saeed
Research Coordinator
ARENA206 e.V.

Contents

Summary and Acknowledgement

Artificial Intelligence (AI) is growing quickly and changing many industries and society. AI helps improve medical diagnoses, support factory maintenance, and power self-driving vehicles, leading to greater efficiency and innovation. However, to make the most of AI, it must be developed with high standards to ensure reliability, fairness, and security while addressing new risks.

AI also has its challenges. For example, biases in AI systems for credit decisions or hiring can lead to unfair treatment. Minor changes in data, like noise in images, can impact the ability of self-driving cars to spot pedestrians and may lead to dangerous situations. These risks show that we need strong AI governance frameworks that focus on trustworthiness, ethical use, and adherence to changing regulations.

AI differs from traditional software because it learns from large datasets rather than following fixed rules, raising concerns about its trustworthiness. Policymakers, businesses, and researchers collaborate on regulations, like the European Commission's AI proposal, to establish standardized evaluation methods for AI systems, ensuring they are safe, fair, and aligned with our values.

In order to address these challenges, a structured AI catalogue has been introduced. This framework provides ways for both developers and assessors to evaluate AI. For developers, it offers a transparent process for creating AI applications that meet safety, security, and ethical standards. For auditors and regulatory bodies, it provides a systematic method for reviewing AI systems, ensuring compliance and good governance. The assessment looks at AI applications from various angles, including secure software development, data quality, privacy, and ethics.

One important part of this framework is a classification system that divides AI applications into four criticality levels. These levels help identify the potential impact of machine learning applications on individuals, organizations, and the environment, allowing for a risk-based approach to AI governance. Currently, the framework is best for low-risk AI applications that use supervised learning, which is common in business settings.

Integrating AI into small and medium-sized enterprises (SMEs) requires careful planning. Collaboration across engineering, data science, and ethics fields is vital for developing effective solutions. AI projects should target specific industry challenges to ensure they provide real value. Clear communication about AI's capabilities is essential for informed decision-making. Finally, adopting a structured plan will help companies remain compliant and scale their efforts sustainably.

As AI continues to develop, using it responsibly and ethically will be crucial to maximizing its benefits and reducing risks. ARENA2036 aims to encourage AI innovation that meets industry needs and follows regulations, ensuring AI solutions are trustworthy and beneficial to society. By adopting precise assessment methods, promoting collaboration across fields, and supporting regulatory compliance, ARENA2036 seeks to responsibly shape the future of AI.

ARENA2036 thanks Prof. Boris Eisenbart (Swinburne University of Technology), Prof. Matthias Kreimeyer (IKTD, University of Stuttgart), Dr. David Reichert (ARENA2036), and Dr. Jannik Lind (ARENA2036) for their valuable insights and contributions to this topic.

1 Artificial Intelligence Act AI Act https://ai-act-law.eu/

2 Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 (last accessed: 10/16/2024)

3 Artificial Intelligence Standardization Roadmap https://www.dke.de/en/areas-of-work/core-safety/standardization-roadmap-ai (last accessed: 08/23/2024)

4 Solution: Trusted AI by TÜV Austria https://www.tuv.at/trusted-ai-by-tuev-austria/ (last accessed: 08/18/2024)

5 Regulating Artificial Intelligence: The AI Act of the European Union at a glance https://www.plattform-lernende-systeme.de/home-en.html (last accessed: 10/16/2024)

1. Establishing a Regulatory Framework for Responsible AI

We have not awakened to a reality where artificial intelligence (AI) has just existed. The origins of AI as a concept can be traced back to ancient times, reflected in various myths[1]. However, the label "AI" is more recently associated with John McCarthy from the Massachusetts Institute of Technology (MIT), who first introduced the idea at a conference in 1956 held at Dartmouth College.

Technological advancements allowed AI to become more available, both in terms of computing power and the tools and digital data needed to support the development of AI systems.

Since 1956, AI has made remarkable strides in executing "narrow" tasks, often outperforming the average person and sometimes surpassing experts. A notable demonstration of AI's advancement was its crucial victory when the Deep Blue system competed against world champion Garry Kasparov in chess during the 1990s[2].

There is a growing global concern about the need to regulate and/or control AI. The reason for this is that we risk being outpaced by a creation of our own making. Society cannot afford to let AI remain unregulated, as this could result in the technology being misused. AI requires extensive amounts of data to become more intelligent, raising the possibility of infringing on fundamental rights. For instance, an algorithm that analyzes profiles to assess candidates for a job may exhibit bias against individuals of a particular ethnicity, thereby limiting the visibility of their profiles for potential opportunities. These biases in algorithms have significant real-world consequences. In light of this, to mitigate any risk of manipulation or biased outcomes, various regions are moving toward regulating AI.

Let us remember the global issues related to AI regulation. The AI industry is growing quickly and is increasingly important for governments worldwide. Countries compete to lead in AI, and those that succeed in AI innovation will have an advantage in international relations.

Regulating technology is not new. We have seen regulations in the pharmaceutical and medical fields and in technologies that deal with our digital information. The main reasons for regulation include encouraging market growth, standardizing practices, and protecting consumers from potential harm[3]. In the context of AI, risks can arise from its applications. These reasons help justify the need for limits on AI[4].

The reasons for regulating AI can differ from one region to another. For example, the European Union (EU) focuses on protecting human rights, which it calls fundamental rights. These rights are stated in the EU Charter of Fundamental Rights and in laws like the General Data Protection Regulation (GDPR). As technology becomes a more significant part of everyday life, the EU understands that trust is critical for people to accept AI. As consumers, we often use products and services from sources we do not know, and we want to be sure these products are safe, reliable, and ethical. Regulations help ensure this.

Basic rules help consumers trust that new products or services follow these standards. Legislation usually covers more than just the first time a product is sold. It also requires ongoing monitoring of the product while it is in use. Additionally, there must be a system for collecting feedback and taking action if problems arise. This process is called Post Market Surveillance (PMS).

AI brings complex challenges that are both philosophical and practical. As concerns grow about the negative effects AI may have on people, EU lawmakers must ensure AI is used positively. But what is “good AI”? This question is fairly new, but defining "good" has been a long-standing issue with different answers based on various moral beliefs[5]. Because human rights are universally accepted, the EU chose to focus on a human-centered approach to AI rules. In April 2019, the European Commission shared its idea of “good AI” through the Ethics Guidelines[6] for Trustworthy AI[7]. Some criticized that these guidelines were not mandatory. However, in 2021, the EU Commission proposed the Artificial Intelligence Act (AI Act), which includes the ethical standards from the High-Level Expert Group on AI[8]. Since then, the final version has received political agreement and was approved by the EU Parliament in March 2024.

The AI Act applies to all industries using AI, not just one specific sector. It sets product requirements and obligations for everyone involved, called economic operators. This law is meant to complement existing sector-specific laws by focusing on the AI aspects of products.

The AI Act does not require specific rules for different types of AI technology, except for General-Purpose AI systems (GPAI), meaning it does not favour any particular AI technique.

To determine if this law applies to a product, one must first establish whether the product uses AI. Defining AI has been challenging, as there is no universally accepted definition of "intelligence." The push for an AI standard has led governments and international organizations to try to create a shared understanding of AI.

In the AI Act, the EU has proposed a definition that aligns with the Organization for Economic Co-operation and Development (OECD) 's definition[9]. This definition aims to separate AI from simpler software systems, stating it does not include systems that follow only rules set by humans to perform tasks automatically[10].

The AI Act defines an AI system in Article 3 as a machine-based system that can operate at different levels of independence, learn after deployment, and generate outputs like predictions or recommendations based on the input it receives. These outputs can influence both physical and virtual environments.

1 Stanford researcher examines earliest concepts of artificial intelligence, robots in ancient myths
2 20 Years after Deep Blue: How AI Has Advanced Since Conquering Chess
3 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)', OJ L 119 (2016).
4 Chesterman, Simon, From Ethics to Law: Why, When, and How to Regulate AI (April 29, 2023). Forthcoming in The Handbook of the Ethics of AI edited by David J. Gunkel (Edward Elgar Publishing Ltd.), NUS Law Working Paper No. 2023/014
5 Smuha, Nathalie A., Beyond a Human Rights-based approach to AI Governance: Promise, Pitfalls, Plea (February 1, 2020). Published in Philosophy & Technology, 2020
6 Idem from footnote 4, p.5
7 High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI', 8 April 2019
8 European Parliament, 'EU AI Act: first regulation on artificial intelligence'
9 The OECD defines AI systems as follows: "An AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy." Check out OECD, 'Recommendation of the Council on Artificial Intelligence'
10 Check Recital 12 of AI Act

2. Global Reach and Regulatory Scope of the AI Act

The AI Act involves two main parties: the providers[11] and deployers[12] of AI systems. There are also specific responsibilities for importers, distributors, product manufacturers, and authorized representatives of providers. The Act[13] applies to AI system providers and deployers in the EU and those outside the EU if their AI system's output is used within the EU. Although the Act does not define "output," it does describe outputs from AI systems, including content like text, video, or images[14], as well as predictions, recommendations, or decisions that impact physical or virtual spaces[15]. A key question is whether the effects of the AI system occur in the EU, regardless of where the provider or deployer is located.

Similar to the GDPR, the AI Act's major aspect is its reach beyond the EU. It will place significant responsibilities on non-EU companies, even if they do not have a legal presence in the EU. This approach reflects the EU's growing concern over the use of AI by authoritarian governments and its potential impact on individual rights and freedoms. The AI Act aims to create fair regulations and ensure its application is non-discriminatory.
Some people think the new AI Act Regulation will hinder AI innovation in Europe because it is

> The AI Act may become another example of the “Brussels Effect,” a term introduced by Anu Bradford[16], a professor at Columbia University. The “Brussels Effect” means that the EU can set global market rules.

stricter than the rules in some places that allow more self-regulation. However, businesses often prefer having the same standard worldwide instead of dealing with different, often less strict regulations. A consistent standard provides legal certainty, which is important for global companies with many production sites. It is not practical or cost-effective for these businesses to follow different rules[17]. This is why many large non-EU companies globally follow the GDPR and other EU environmental laws.

It is also important to note that the EU was the first to regulate AI. Even though the EU's slow legislative process has delayed discussions on the AI Act, other regions have already set up comprehensive regulations for specific areas of AI[18]. For example, China was among the first to create AI rules, including new rules about recommendation algorithms[19]. Still, the AI Act was the first draft released, which may have encouraged other regions to speed up their legislative efforts.

> The EU plans to promote its approach to artificial intelligence (AI) around the world, using the success of the General Data Protection Regulation (GDPR) as an example[20]. The AI Act focuses on putting people first, ensuring ethics transparency, and protecting fundamental rights. This approach may inspire other countries with similar values, especially since more than 100 countries now have data privacy rules like the GDPR[21].

The AI Act will affect AI providers and users outside the EU if their AI systems or results are used in the EU.

The current global reach of the AI regulation has the potential to set a new standard for how AI is managed. European values have shown a wide appeal, so it is reasonable to think that the AI Act will be adopted around the world.

Global companies often prefer to follow one set of rules, even if those rules are stricter. However, the AI Act's broad reach could make it hard for AI providers in other countries to comply if they do not know that their AI system will be used in the EU.

All relevant operators must know their role in the AI value chain. They should clearly define what their AI systems do to determine if the AI Act covers them.

11 Article 3(3) of P9_TA(2024)0138 AI Act defines providers as *"a natural or legal person, public authority, agency or other body that develops an AI system or a general purpose AI model or that has an AI system or a general purpose AI model developed and places them on the market or puts the system into service under its own name or trademark, whether for payment or free of charge"*
12 Article 3(4) of AI Act defines deployers as "any natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity"
13 Check out Article 2 of AI Act
14 Throughout the text we see that the AIA includes image, audio or video as example of AI-generated content.
15 Check Article 3 and Recital 12 of AI Act
16 Bradford, Anu. (2020). The Brussels Effect: How the European Union Rules the World.
17 Bradford, Anu, The Brussels Effect (2012). Northwestern University Law Review, Vol. 107, No. 1, 2012, Columbia Law and Economics Working Paper No. 533
18 Siegmann, Charlotte, Anderljung, Markus, The Brussels effect and Artificial Intelligence: How EU regulation will impact the global AI market (2022). Centre for the Governance of AI. P.39
19 Check out translation of the text here Translation: Internet Information Service Algorithmic Recommendation Management Provisions – Effective March 1, 2022 (stanford.edu)
20 Siegmann, Charlotte, Anderljung, Markus, The Brussels effect and Artificial Intelligence: How EU regulation will impact the global AI market (2022). Centre for the Governance of AI. P.3
21 Check out interview to Bradford What is the Brussels Effect, and what does it mean for global regulation? (microsoft.com)

3. AI Systems and Applications Governed by the AI Act

This whitepaper discusses the AI Act, which defines AI similarly to the OECD. This similarity is helpful because it keeps the EU aligned with international partners. The EU believes this definition separates AI systems from regular software, making it easier to apply the proper rules. However, some critics say the definition is still too broad.

It is important to note that not all AI technologies classified as AI under the AI Act will have the exact implementation requirements. We must consider how much risk they pose to people's health, safety, and rights.

The EU emphasizes the need for a risk-based approach to ensure reasonable regulations[22]. The AI Act classifies AI systems into four categories: (i) unacceptable risk, (ii) high risk, (iii) limited risk, and (iv) low or minimal risk.

The Commission decides the level of risk by considering how likely it is that an AI system might harm individual health and safety or violate their rights. Depending on the risk level, the rules for these systems range from bans to voluntary guidelines.

The AI Act forbids AI applications that present "unacceptable risks" to people's safety, health, and rights[23].

The AI Act prohibits harmful and abusive practices because they go against Union values[24]. The following systems cannot be sold, used, or operated in the EU:

1. AI systems that use harmful and manipulative "subliminal techniques." [25]
   Example: "An inaudible sound is played in truck drivers' cabins to make them drive longer than is healthy or safe. AI finds the frequency that has the strongest effect on drivers." [26]

2. AI systems that exploit vulnerable groups (due to age or physical or mental disabilities). [27]
   Example: "A doll with a voice assistant encourages a minor to take on increasingly dangerous activities or challenges that appear fun or cool." [28]

3. AI systems for social scoring in the public and private sectors, especially for judging people based on their behavior or personality. [29]
   Example: "An AI system identifies at-risk children needing support based on minor social issues of their parents, like missing a doctor's appointment or getting divorced." [30]

4. Biometric categorization of individuals using their biometric data to guess their race, political beliefs, union membership, religious beliefs, sexual orientation, or personal life. [31]
   Example: "AI systems inferring possible criminal behaviour based on people's facial features or biological traits, including skin colour."

22 European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final, 2020. P. 17
23 Check out Article 5 of AI Act

5. Real-time remote biometric identification in public spaces by law enforcement. [32]
Example: "Every face captured live in public by video cameras is matched in real-time against a database to find a criminal in the crowd."

6. Individual predictive policing, except law enforcement, is based on clear, verifiable facts. [33]
Example: "AI predicts behaviour based only on profiling, like nationality, birthplace, residence, number of children, debt, or type of car, without any reasonable suspicion of criminal involvement based on verified facts and lacking human judgment." [34]

7. Emotion recognition in workplaces and schools, unless for medical or safety reasons (like detecting pilot or driver fatigue to avoid accidents).[35]
Example: "AI recruitment tools assess a candidate's emotions or honesty by analyzing facial expressions, voice tones, or body language during interviews."

8. AI systems that gather biometric data from the internet or Closed Circuit Television (CCTV) footage to create facial recognition databases without consent. [36]
Example: "An AI system that randomly collects facial images from social media, building a large database of faces."

It is important to note that real-time remote biometric identification mentioned in point 5 has specific exceptions related to public safety. Law enforcement may use these systems in public under three strict conditions:

- A "targeted search for specific victims of abduction, human trafficking, or sexual exploitation, as well as searching for missing persons." [37]

- The "prevention of a specific, serious and immediate threat to someone's life or safety or a terrorist attack." [38]

- The "localization or identification" of someone suspected of committing a crime[39] that can lead to a sentence of at least 4 years, allowing for a European Arrest Warrant[40].

If these conditions are met, real-time biometric identification by law enforcement can continue with protections for fundamental rights, including the need for judicial authority involvement and prior impact assessments (unless there is an urgent situation). [41]

These protections also apply to using AI for remote biometric identification of individuals under investigation, such as reviewing protest footage to identify someone who committed a crime.

Finally, this prohibition does not stop private companies from using remote biometric identification for non-law enforcement purposes. They can use such systems (in markets, public transport, and schools) if third-party assessments confirm compliance.

24 Check out recital 28 of AI Act
25 Check out Article 5(1)(a) of AI Act
26 For the sake of clarity, the Commission has presented some examples of the above prohibitions. Some argue that these are borderline fantastical, however, being AI such an innovative technology, who knows where it will take us. Check out https://cor.europa.eu/en/events/Documents/SEDEC/FINAL%20PDF%20AI%20Presentatiofor%20COR%20Sedec%20Committee%20 meeting%2023%2006%2021.pdf
27 Check out Article 5(1)(b) of AI Act
28 Check out https://cor.europa.eu/en/events/Documents/SEDEC/FINAL%20PDF%20AI%20Presentatiofor%20COR%20Sedec%20Committee%20meeting%2023%2006%2021.pdf
29 Check out Article 5(1)(c) of AI Act
30 Check out https://cor.europa.eu/en/events/Documents/SEDEC/FINAL%20PDF%20AI%20 Presentatiofor%20COR%20Sedec%20Committee%20meeting%2023%2006%2021.pdf
31 Check out Article 5(1)(g) of AI Act
32 Check out Article 5(1)(h) of AI Act
33 Check out Article 5(1)(d) of AI Act
34 Check out Recital 42 of AI Act
35 Check out Article 5(1)(f) of AI Act
36 Check out Article 5(1)(e) of AI Act
37 Check out Article 5(1)(h)(i) of AI Act
38 Check out Article 5(1)(h)(ii) of AI Act
39 The list of the 16 crimes in Annex II of AI Act: Terrorism; Trafficking in human beings; Sexual exploitation of children and child sexual abuse material; Illicit trafficking in narcotic drugs and psychotropic substances; Illicit trafficking in weapons, munitions and explosives; Murder; Grievous bodily injury; Illicit trade in human organs and tissue; Illicit trafficking in nuclear or radioactive materials; Kidnapping, illegal restraint and hostage-taking; Crimes within the jurisdiction of the International Criminal Court; Unlawful seizure of aircraft/ships; Rape; Environmental crime; Organised or armed robbery; Sabotage, participation in a criminal organisation involved in one or more crimes listed above.
40 Check out Article 5(1)(h)(iii) of AI Act
41 Check out Article 26 (10) of AI Act

Transitioning to the subsequent category outlined in the AI Act, "high-risk AI systems" refer to those systems that can negatively impact individuals' health and safety or compromise their fundamental rights in several specified applications, products, and sectors. This regulation primarily focuses on this issue.

Before we get into more details, it is important to understand that AI systems can work independently or as part of a product. This can happen whether the system is built into the product (embedded) or provides its functionality without being part of it (non-embedded). [42]

Transitioning to the subsequent category outlined in the AI Act, **"high-risk AI systems"** refer to those systems that can negatively impact individuals' health and safety or compromise their fundamental rights in several specified applications, products, and sectors. This regulation primarily focuses on this issue[43].

The AI system's intended function determines the high-risk framework, consistent with the New Legislative Framework (NLF), which serves as the EU's unified approach to regulating certain products, including machinery, lifts, medical devices, personal protective equipment, and toys.

The AI Act identifies two classifications of high-risk AI systems:

1. AI systems that constitute products or safety components of products governed by specific EU health and safety harmonization legislation (like toys, machinery, lifts, or medical devices) and are mandated to undergo external conformity assessment[44].
2. Independent AI systems utilized in eight designated areas[45]:
    a. Biometric identification, categorization, and emotion recognition (excluding prohibited categories);
    Example: AI systems employed for facial recognition.
    b. Management and operation of critical infrastructure;
    Example: AI systems are used in road traffic, as well as in water, gas, heating, and electricity supply.
    c. Educational and vocational training;
    Example: AI systems for assessing students on tests required for university admission.
    d. Employment, worker management, and access to self-employment;
    Example: AI systems employed to deliver targeted job advertisements, analyze and filter job applications, and evaluate candidates.
    e. Access to and enjoyment of essential services and benefits;
    Example: AI systems are used to evaluate individuals' creditworthiness.
    f. Law enforcement;
    Example: AI systems designed to assist in detecting, investigating, or prosecuting criminal activities.
    g. Migration, asylum, and border management;
    Example: AI systems are tasked with identifying individuals who refuse to be identified or cannot prove their identity during an identity check[46].
    h. Administration of justice and democracy;
    Example: AI systems aimed at aiding in analyzing and interpreting facts concerning judicial authority.

The aforementioned list of high-risk AI systems may undergo updates since the EU Commission is authorized to modify or introduce new use cases if they present comparable risks to those currently listed. However, the Commission can also eliminate categories that no longer involve significant risk to health, safety, and fundamental rights[47].

A stand-alone AI system can be deemed high-risk if it aligns with any of the eight specified areas. Nonetheless, as is often the case, the AI Act has exceptions. It may be exempt if the system does not pose a significant danger to individuals' health, safety, or fundamental rights and does not materially influence decision-making outcomes[48]. This includes the following types of systems:

- Systems designed to carry out a narrow procedural job[49].
- Systems intended to enhance the results of a task previously completed by a human[50].
- Systems aimed at identifying decision-making trends or deviations from established patterns[51].
- Systems designated to perform a task that merely serves as preparation for an assessment pertinent to the high-risk use cases outlined in Annex III[52].

Notably, any AI system that performs profiling of individuals will always be classified at least as high-risk[53].

The following classification of AI system risk is **"limited risk."** These systems have specific disclosure obligations due to their unique interaction with humans, as they could pose manipulation risks. This category includes AI systems that generate or alter image, audio, or video content (e.g., deepfakes[54]), AI systems meant to engage with individuals (such as chatbots), and AI-driven emotion recognition and biometric categorization systems.

By including this provision, the AI Act ensures that EU consumers can make informed choices as they recognize interacting with a machine[55].

Lastly, the final classification is **"minimal risk."** These AI systems do not belong to other categories and present only low or minimal risk, allowing for their development and use within the EU without further legal requirements. Nevertheless, the AI Act envisions the establishment of codes of conduct to urge the providers of non-high-risk AI systems to implement the mandatory requirements applicable to high-risk AI systems voluntarily. These codes of conduct should be founded on specific objectives and key performance indicators to assess the fulfilment of those objectives[56]. This could encompass inclusiveness, fairness, transparency, confidentiality, and environmental sustainability. The Commission and Member States will promote the development and voluntary adherence to these codes[57].

It is crucial to emphasize that existing EU legislation, including the GDPR, remains applicable whenever the use of AI systems falls within the jurisdiction of that law, regardless of whether they are classified as no risk under the AI Act.

42 Check out Recital 12 of AI Act
43 Check out New legislative framework - European Commission (europa.eu)
44 Check out Annex I of AI Act with the list of NLF legislation. Annex I (B) is older-style product safety legislation where Title XII introduces new AI Act–related considerations for future delegated acts in those areas.
45 Check out the list in AI Act
46 Check out recital 33 of AI Act
47 Check out Articles 7 and AI Act
48 Check out Article 6 (3) of AI Act
49 Check out Article 6 (3) of AI Act
50 Check out Article 6 (3) of AI Act
51 Check out Article 6 (3) of AI Act
52 Check out Article 6 (3) of AI Act
53 Check out Article 6 (3) of AI Act
54 Check out Article 3(6) of of AI Act
55 Check out Article 50 of AI Act
56 Check out Recital 165 of AI Act
57 Check out Article 95 of AI Act

4. AI Systems Regulated Under Broader EU Act

The AI Act applies to all AI systems in every sector, requiring them to meet the same risk assessment and legal standards. It works alongside other EU laws, such as data protection, privacy, civil liability, and specific regulations like the Machinery and Medical Devices Regulation (MDR). This broad approach stops companies from picking and choosing which regulations to follow, ensuring everyone meets the exact legal requirements. While this method seems fair and consistent across industries, it can create problems if incorrectly handled, leading to conflicting rules for AI providers.

The AI Act is based on the New Legal Framework (NLF) [58], which aims to improve the EU market and ensure that certain products, like medical devices, machinery, and toys, meet safety and performance standards. According to experts Veale and Zuiderveen Borgesius[59], manufacturers must check their products for safety and performance before they go to market. They do this by meeting specific legal requirements. Once their products meet these standards, they can place a “CE” mark on them, which allows those products to move freely within the EU.

The AI Act states that different EU laws can affect one AI system[60]. For example, a medical device using AI might have risks not covered by the Medical Devices Regulation (MDR) [61]. This means we need to apply several EU laws simultaneously and in a way that works together[62].

The NLF legal rules state that if two rules apply to a situation, the more specific rule should be used first. This ensures that products with AI do not face conflicting regulations[63]. The Commission aimed for this balance when it proposed the AI Act:

“This proposal aims to provide a balanced and practical set of rules for AI that includes only what is necessary to manage risks related to AI. It avoids overly limiting technological progress and does not raise costs unnecessarily for bringing AI solutions to market. [64]”

For example, regarding AI-enabled medical devices, the AI Act seeks to ensure consistency, eliminate overlap, and lessen extra burdens from using both the AI Act and the Medical Device Regulation (MDR) [65]. It allows AI providers to combine the necessary measures to follow the AI Act with the existing procedures already required under the MDR. This means an AI-enabled medical device manufacturer can integrate the testing and reporting steps and the information needed under the AI Act into the current documentation and processes required by the MDR. The MDR is considered the more specific rule, so it takes priority.

However, some conflicts and inconsistencies remain, making it challenging to apply the AI Act alongside other European regulations.

58 New legislative framework, European Commission
59 Veale, Michael and Zuiderveen Borgesius, Frederik, Demystifying the Draft EU Artificial Intelligence Act (July 31, 2021). Computer Law Review International (2021) 22(4) 97-112, P.6
60 Union harmonization legislation refers to Union legislation that harmonizes the conditions for the marketing of product. This list can be found here and also in Annex II of AI Act
61 Check out Recital 64 of P9_TA(2024)0138 Artificial Intelligence Act
62 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 (MDR).

For instance, the AI Act defines high-risk AI systems as those that include products or safety components already covered by European regulations. This means the AI Act and the MDR apply to the same AI-enabled medical devices. The issue is that the MDR does not define a "safety component," leaving uncertainty about what that term means for medical devices[66].

Also, the AI Act interacts with European regulations and other laws, such as the GDPR[67].

The AI Act mentions the GDPR several times and confirms that it works alongside the GDPR. Therefore, both sets of rules apply together. In practice, this means all AI systems must follow the GDPR if they handle the personal data of EU citizens or are used in the EU. However, issues still arise when an AI system processes personal data.

The AI Act does not provide reasons for processing personal data and refers to the GDPR for valid grounds[68]. However, following the GDPR rules for collecting and processing personal data is unclear.

This makes it hard to find legal grounds for processing personal data by Large Language Models (LLMs) because there is no clear controller/data subject relationship (like a contract). Data subjects cannot expect their data to be used for training an app, nor can they object to this processing (since there is no explicit consent). In some cases, AI can process personal data based on the "legitimate interest" [69] justification. However, it must be balanced to protect the rights of data subjects.

The Commission is expected to issue guidelines on how to train AI models without breaking personal data protection rules, including the Data Act, Data Governance Act, and Copyright Directive. Regarding the GDPR, the legal grounds for processing personal data may need to be significantly re-evaluated for AI systems.

The AI Act also connects with the EU Cybersecurity Act[70]. Article 42(2) of the AI Act assumes that high-risk AI systems certified under a cybersecurity scheme will meet the cybersecurity requirements in Article 15 of this Regulation[71]. Article 15 and Recital 49 state that high-risk AI systems should work consistently throughout their lifecycle and achieve proper accuracy, robustness, and cybersecurity in line with accepted standards.

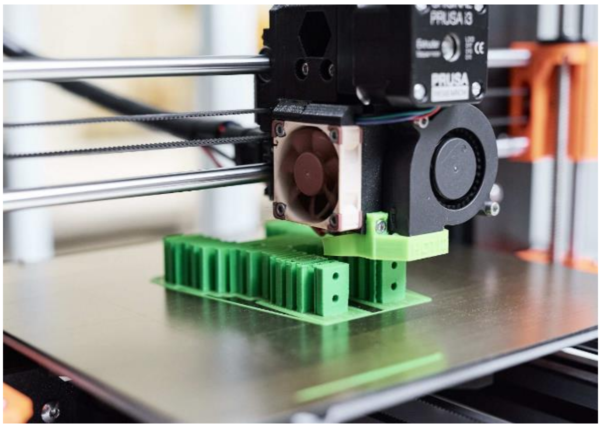
It is important to note that Article 15 is quite general and does not cover all possible cyber threats to AI systems, as highlighted by ENISA[72] in its report on "Artificial Intelligence and Cybersecurity Challenges. [73]" Therefore, if AI developers want the best cybersecurity for their AI systems, they must rely on existing cybersecurity schemes or likely use standards[74] and specifications defined by the Commission[75], which are currently unavailable.

---

63 Commission notice The 'Blue Guide' on the implementation of EU product rules 2022 (Text with EEA relevance) 2022/C 247/01 C/2022/3637, p. 11
64 Explanatory Memorandum AI Act, p. 3
65 Check out Recital 64 of AI Act
66 Article 3(14) of AI Act defines safety component, however, we do not see a similar definition under the MDR.
67 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) (GDPR)
68 Check out Recital 63 of AI Act
69 Check out Article 6(1)(f) 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) (GDPR)
70 Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
71 Check out Art 42(2) of AI Act
72 Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity, ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes.
73 ENISA: AI Cybersecurity Challenges - Threat Landscape for Artificial Intelligence. Artificial Intelligence Cybersecurity Challenges — ENISA (europa.eu)
74 Check out Article 40 of AI Act
75 Check out Article 41 of AI Act
76 Regulation 2022/0272 (CRA).
77 Check out Article 8 of Regulation 2022/0272 (CRA).
78 Essential cybersecurity requirements are in Article 10 and Annex I of Regulation 2022/0272 (CRA).

The EU's cybersecurity measures will include the AI Act and the upcoming Cyber Resilience Act (CRA)[76], which starts in 2024. The CRA[77] requires that products with digital features labelled as high-risk AI systems under the AI Act must also meet key cybersecurity standards set by the CRA[78].

If high-risk AI systems meet the essential cybersecurity requirements set by the CRA, they should be considered compliant with the cybersecurity rules in Article 15 of the AI Act, as long as they are included in the EU declaration of conformity from the CRA[79].



The CRA states that the AI Act is the primary law, and its conformity assessment procedures should be followed. The CRA also clarifies that AI Notified Bodies under the AI Act can check if high-risk AI systems meet the CRA's essential requirements[80]. One exception: if a high-risk AI system is classified as a 'critical product with digital elements' and is subject to the AI Act's internal control, then the conformity assessment should follow the CRA's guidelines for essential cybersecurity requirements. Other aspects of the product can still follow the internal procedures of the AI Act. Because 'critical products with digital elements' have higher cybersecurity risks, a third-party conformity assessment body must be involved.

It is also important to note that providers of high-risk AI must comply with accessibility requirements, including EU directives 2016/2102 and 2019/882. The AI Act ensures that people with disabilities have equal access to technology. Therefore, AI providers must ensure these requirements are part of their design process.In summary, before launching or using a high-risk AI system in the EU market, AI providers must account for various horizontal and sector-specific laws to ensure full compliance with EU regulations. Despite the confusion and overlaps between the AI Act and other laws, the Commission is expected to perform a detailed analysis to clarify how these laws relate.

79 Check out Recital 77 of AI Act
80 Check out Article 8(2) of Regulation 2022/0272 (CRA).

5. Requirements and Obligations

High-risk AI systems have strict requirements. The law does not explain how to meet these technical requirements so that the AI Act will be supported by technical specifications created by European Standardization Organizations (ESOs) [81] at the Commission's request. These standards will turn the AI Act's requirements into clear steps to follow. While these standards are not mandatory, AI providers who follow the harmonized standards from CEN/CENELEC will be presumed to comply with the AI Act. There are still many AI-specific standards being developed. The AI Act outlines requirements for high-risk AI systems in Chapter III, Section 2 (articles 9 to 15). To comply, you should consider the AI system's intended use and what is generally accepted as the current best practice. Table 1 gives a summary of the requirements in Chapter III.

SotA is not clearly defined in the AI Act or other key laws. However, the term appears several times in the AI Act, including references to harmonized standards, common specifications, technical standards, and codes of practice[82].

Table 1: Requirements of High-Risk AI – Systems [83]

Requirement	**Summary**
Risk Management System (RMS)	The RMS system will include steps to manage risks throughout its entire lifecycle: • Identify and assess known and expected health, safety, or fundamental rights risks. • Evaluate risks by analyzing data collected from the post-market monitoring system. • Implement appropriate and targeted risk management measures. The best risk management measures will reduce risks as much as possible while ensuring that the remaining risks are acceptable. This will consider the context and the deployer's technical skills, experience, education, and training. We will pay special attention to vulnerable people and those under 18 years old.
Data and data governance	Data governance practices focus on: • Design choices. • How data is collected and why it was collected. • Preparing data through processes like labeling, cleaning, updating, enriching, and combining. • Key assumptions about what the data is meant to represent. • Checking the availability, amount, and suitability of the datasets needed. • Recognizing biases that could affect health, safety, or lead to discrimination. To avoid errors, training, validation, and testing datasets must: • Be as accurate and complete as possible, with the right statistical qualities for each dataset, especially for the people or groups the system will serve. • Consider the intended use and specific features related to the geographical, behavioral, or functional settings where the system will operate.

81 ESO are the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI).
82 Check out Articles 50(2), 96 & Recitals 116, 121 of AI Act
83 Check out chapter III, Section 2 of AI Act

Requirement	Summary
Technical Documentation	Technical documentation must be created before an AI system is sold or used and should be updated regularly. It should give national authorities and notified bodies clear and comprehensive information to assess whether the AI system meets the required standards. At a minimum, it must include the items listed in Annex IV, which can be adjusted by the Commission's delegated acts. For small and medium-sized enterprises (SMEs), including start-ups, any equivalent documentation should aim to achieve the same goals, unless the competent authority decides otherwise. When a high-risk AI system is made available or put into service, a single technical document must contain all the information required by the legal acts listed in Annex I. Annex IV specifies what the technical documentation must include.
Record Keeping	AI systems must automatically record events during their use. This logging should include: • Documenting events that help identify risks to health, safety, or people's rights. • Monitoring the product after it is available on the market. • Keeping track of how the system operates. • Recording the length of each use of the system. • Maintaining a database for checking the input data. • Noting the input data that results in a match. • Identifying the people involved in checking the results.
Transparency and Information provisions	AI systems must be designed to be clear and easy to understand. This will help users follow the rules and use the system effectively. Each AI system should come with clear instructions for use (IFU) in a suitable digital format or other forms. These instructions must include precise, complete, and easy-to-read information that is relevant and accessible to users.
Human Oversight	AI systems should be designed so that people can effectively supervise them. The aim is to reduce or avoid risks to health, safety, or fundamental rights. To ensure human oversight, providers must include measures that are built-in before the system is used and also identify actions for users to take after the system is running. Users should understand what the system can and cannot do, be aware of any bias in automation, and be able to interpret the output. They should also have the ability to override the output or stop the system if needed. For remote biometric identification systems, two people must independently verify and confirm the results.
Accuracy and Robustness with Cybersecurity	AI systems should be designed to be accurate, strong, and secure, and they must perform well throughout their entire lifecycle. Instructions for use must clearly state the levels of accuracy and the metrics used. High-risk AI systems must be able to handle errors and inconsistencies when they interact with people or other systems. We can achieve strength in these systems by using backup plans or fail-safes. Learning AI systems should be built to reduce the risk of biased outputs affecting future decisions due to 'feedback loops.' Cybersecurity measures must specifically target AI vulnerabilities, including preventing attacks that can change the training data ('data poisoning'), inputs meant to trick the model ('adversarial examples'), and issues within the model itself.

The AI Act outlines responsibilities for those involved with AI systems. It applies not only to economic operators, like providers, importers, and distributors, but also to those who deploy or provide certain AI systems (Chapter IV). Additionally, it includes responsibilities for providers of GPAI models (Chapter V, Section 2) and for GPAI models that carry systemic risk (Chapter V, Section 3). You can find more details about these responsibilities in Table 2.

Table 2: Obligations of AI Act

Obligations	Summary
Providers of High Risk AI systems[84]	Providers must comply with the AI Act. They need to provide transparent information in the AI system and have a Quality Management System (QMS) as required by Article 17. Documentation per Article 18 must be kept for 10 years, and automatically generated logs should be stored for at least six months. Providers must also follow conformity assessment procedures, meet registration requirements in Article 49, affix the CE mark, and create an EU declaration of conformity. Additionally, they must ensure accessibility standards are met and investigate any issues, informing relevant stakeholders of corrective actions.
Importers[85,86]	Importers need to make sure they follow the AI Act. They should check that all the papers and labels needed for their products are ready and correct. They also need to name someone to help them. The packaging should have the importer's name on it. Importers must work with the right authorities and keep important papers for 10 years.
Distributors[87]	Distributors must check that products have the correct CE marking, an EU declaration of conformity, and clear instructions for use. They must also ensure that the provider and importer have fulfilled their responsibilities. If they find any risk to health or safety, they should inform the providers or importers and take necessary actions to fix any issues. Distributors must also notify national authorities about any non-compliance or corrective actions taken. Additionally, they should cooperate with national authorities and provide requested information and documents.
Deployers of High Risk AI Systems[88]	Users must operate the system according to the provided instructions. They should assign qualified people to oversee its use and ensure that the input data is relevant and representative. Users must notify the provider or distributor of any risks or serious incidents and stop using the system if needed. They must follow internal governance rules as outlined by financial service laws if they are financial institutions and keep usage logs for at least six months. Users are also required to meet registration obligations, conduct a data protection impact assessment (GDPR), and cooperate with national authorities.
Transparency for providers and deployers of AI systems[89,90]	AI systems interacting with people should indicate they are AI unless it's obvious. These rules do not apply to systems authorized by law to address crime. AI that creates synthetic content must label it as AI-generated or manipulated. Users of emotion recognition or biometric systems must inform individuals about their use, except when legally permitted to address crime.
Providers for General Purpose AI models[91]	Providers of paid GPAI models must create and maintain technical documents as per Annex XI. They also need to prepare information for other AI system providers looking to integrate the GPAI model.

Companies that offer paid GPAI models must create and keep up-to-date technical documents according to Annex XI. They also need to provide information for other AI system providers who want to use the GPAI model[92].

84 Check out Article 16 of AI Act
85 Check out Article 22 of AI Act
86 Check out Article 23 of AI Act
87 Check out Article 24 of AI Act
88 Check out Article 26 of AI Act
89 Check out Article 50 of AI Act
90 Check out Article 53 of AI Act
91 Check out Article 55 of AI Act
92 Check out Article 25 of AI Act

6. The AI Act Landscape

The AI Act creates a clear set of rules for how to assess, certify, and oversee AI systems. This aims to ensure that AI systems are used safely and ethically. To explain this regulatory system, we will define the roles of the key players involved.

National Level	The AI Act creates a clear set of rules for how to assess, certify, and oversee AI systems. This aims to ensure that AI systems are used safely and ethically. To explain this regulatory system, we will define the roles of the key players involved. [93]
	A Notified Body (NB) [94] is a special type of Conformity Assessment Body (CAB) that is officially recognized under the EU AI Act and relevant EU laws. NBs are responsible for checking if high-risk AI systems meet the required standards. They must follow specific rules about organization, quality management, resources, processes, and cybersecurity. NBs must operate independently from the AI system providers they evaluate, ensuring they are fair and keep information confidential. Articles 31 to 34 of the EU AI Act outline the specific responsibilities and operational guidelines for NBs.
	Notifying Authority (NA) [95]: Each Member State has a Notifying Authority that oversees the process for assessing, designating, and notifying Conformity Assessment Bodies (CABs). They also supervise CABs continuously. NAs are responsible for preventing conflicts of interest and making sure that decisions are fair and unbiased. They separate decision-making from assessment work and do not offer any commercial or competitive services. NAs ensure their staff are well-qualified in areas like information technology, artificial intelligence, and law.
	The Market Surveillance Authority (MSA) [96] is the national body that monitors market activities to ensure they follow legal rules, especially for high-risk AI systems. The MSA checks for compliance, identifies problems, and oversees the corrective actions that AI providers take. Their goal is to protect public interests, health, safety, and fundamental rights.
	National Competent Authority (NCA) [97]: The NCA includes both the National Authority (NA) and the Market Surveillance Authority (MSA). These are the official organizations chosen by EU member states to regulate and ensure compliance of AI systems in their areas. Their main goal is to make sure that AI technologies are safe, secure, and respect people's rights.
EU Level	The Artificial Intelligence Office (AIO) [98] is part of the European Commission. Its main job is to monitor and supervise AI systems, including general-purpose AI models. The AIO helps create clear rules for AI across the EU. It ensures that these rules are followed, supports enforcement, and manages AI governance. The aim is to protect the public interest and maintain high standards.
	The European Artificial Intelligence Board (AIB) [99] is a group that helps ensure the AI Act is carried out consistently and effectively across the EU. It promotes cooperation among the national authorities that enforce these rules, helps share technical and regulatory knowledge, and encourages the use of best practices among Member States.

93 Check out Article 3 (21) of AI Act
94 Check out Article 3 (22) of AI Act
95 Check out Article 3 (19) of AI Act
96 Check out Article 3 (26) of AI Act
97 Check out Article 3 (48) of AI Act
98 Check out Article 3 (47) of AI Act
99 Check out Article 65 of AI Act

The AI Act explains what Notified Bodies (NBs) [100] must do.

1. Conformity Assessment[101]
   - Notified Bodies (NBs) or Conformity Assessment Bodies (CABs) evaluate the AI management system used by providers of high-risk AI systems[102]. They also review the technical documents submitted by these providers. The goal is to ensure that the system follows the rules set by the AI Act and meets necessary standards[102]. Each evaluation ends with an audit report that summarizes the findings, notes compliant areas, and identifies any problems (called "non-conformities") related to the AI Act[103,104].

   - NBs have the access they need to the data used for training, validating, and testing AI systems. This access might happen through application programming interfaces (APIs) or other secure methods. NBs also look at the trained models of the AI system, including important details like weights and architecture, especially if other methods to check compliance are not good enough. If NBs find the tests from the high-risk AI ystem provider lacking, they will perform their own direct testing[105].

2. Issuance of Certificates:
   - After a successful assessment, NBs give certificates to AI system providers, confirming that they comply with the AI Act and its related rules[106].

3. Continuous Monitoring and Surveillance[107]:
   - Once a provider receives a certificate, NBs continue to monitor compliance. They regularly audit the quality management system to make sure the provider still meets the requirements of the AI Act, including any relevant standards.
   - Providers of high-risk AI systems must inform NBs about any changes to their AI management system or the AI system itself[108] that might affect compliance. NBs will review the related documents to approve changes as long as compliance is maintained.

4. Cooperation among Notified Bodies:
   - Notified Bodies (NBs) talk to each other about any refusals, suspensions, or withdrawals of quality management system approvals or EU technical documentation approvals. If requested, an NB must share information about the quality system approvals it has granted[109].

5. Documentation and Reporting:
   - NBs keep records and evidence of all assessments, decisions, and certifications. These records are available to National Competent Authorities (NCAs) for oversight[110].

100 Check out Articles 31, 34 of AI Act
101 Check out Recitals 50,78,86, 123, 125 and Articles 45, 46,57 Section 7 of AI Act
102 Check out Recital 173, Article 43 and Annex VII, Section 5 of AI Act
103 Check out Recitals 66,173, Articles 11, 43 Annex VII, Section 4.3 of AI Act
104 Check out Annex VII, Section 5.3 of AI Act
105 Check out Annex VII, Sections 4.3-4.5 of AI Act
106 Check out Article 44 and Annex VII of AI Act
107 Check out Annex VII, Section 5 of AI Act
108 Check out Annex VII, Sections 3.4 and 4.7 of AI Act

The key responsibilities of National Competent Authorities (NCAs) [111] within the AI Act focus on important roles that ensure good management and supervision of the Act at the national level.

1. Regulatory Oversight:
    - National Competent Authorities (NCAs) can ask providers of non-high-risk AI systems and general-purpose AI models (GPAI) for documents[112]. This helps ensure these providers follow the rules of the AI Act. NCAs also ask for technical documents from high-risk AI system providers when Notified Bodies (NBs) aren't involved[113].

    - NCAs can help provide high-quality data for training AI systems. This supports innovation and helps ensure the data is transparent and reliable[114].
    - NCAs are the main points of contact for communication, regulatory issues, and technical compliance[115].
    - NCAs support the European Commission and share information with each other[116].

2. Support for Innovations:
- NCAs set up national AI regulatory sandboxes. These allow for testing of AI systems and help inform the AI Office (AIO) about progress. Collaboration between NCAs, AIO, and other relevant authorities aids in exchanging knowledge and sharing best practices[117].
- NCAs can guide small and medium-sized enterprises (SMEs) and startups on the AI Act and ensure they understand the Board and Commission's positions. Relevant authorities must be consulted for AI systems under other EU laws[118].

3. Enforcement Actions[119]:
- NCAs, specifically Market Surveillance Authorities (MSAs), oversee corrective actions taken by AI model providers after incidents. They can issue warnings, impose fines, and require compliance with regulations to maintain integrity. NCAs serve as the single point of contact for these matters.

4. Designation, Monitoring, and Coordination of Notified Bodies (NBs) [120]:

- NCAs designate NBs and ensure they meet the qualifications needed under the AI Act for conformity assessments. They monitor and audit NBs to ensure they comply with the AI Act, which includes maintaining competence, impartiality, and other legal and technical requirements[121].

---

109 Check out Article 45, of AI Act
110 Check out Articles 45 AI Act
111 Check out Article 28 of AI Act
112 Check out Article 6, Section 6 and Article 53, Section 1 AI Act
113 Check out Article 11, Section 1 AI Act
114 Check out Recital 68 of AI Act
115 Check out Article 70 of AI Act
116 Check out Article 30 of AI Act
117 Check out Article 57 of AI Act
118 Check out Article 70 of AI Act

The main responsibilities of the AIO[122], based on the rules set by the AI Act and its official website, are as follows:

1. Central Coordination, Governance, and Oversight of GPAI:
    - The AIO is the main coordinating body among EU member states. It provides guidance and support to help implement the AI Act consistently. It encourages the sharing of best practices and ensures alignment across the EU. The AIO also works with EU-level advisory bodies, like the Artificial Intelligence Board, to promote collaboration and ensure that the AI Act is applied coherently in all member states[123].
    - The AIO supervises GPAI, which includes requirements for providers, authorized representatives, and deployers. It ensures compliance with the AI Act and related standards. The AIO creates tools, methods, and benchmarks to evaluate the capabilities and risks of GPAI models. It monitors the actions taken by GPAI providers if they do not comply and can request documentation and information from GPAI providers and their authorized representatives. It can evaluate GPAI models and request measures, such as limiting market availability or recalling the model. The AIO also monitors providers' adherence to their obligations[124].
    - The AIO supports joint investigations for market surveillance of high-risk AI systems. It supervises GPAI compliance and ensures effective implementation of the AI Act by monitoring GPAI providers[125].

2. Policy Development:
    - The AIO provides standardized templates required by the AI Act, such as summaries of training content for GPAI and questionnaires for deployers[126].
    - The AIO shares best practices, helps access AI testing environments, and promotes innovative ecosystems to make the EU more competitive[127].
    - The AIO engages with various stakeholders, like AI developers, small and medium-sized enterprises (SMEs), and experts, to keep the regulatory framework up-to-date with technology and societal needs. It encourages ongoing dialogue to inform policy development and create codes of practice that align with the AI Act[128].

3. Cooperation with Stakeholders:
    - The AIO works with a variety of stakeholders, including national supervisory authorities, GPAI providers, scientific panels (including independent experts), institutions, the European Artificial Intelligence Board, and the European Centre for Algorithmic Transparency (ECAT). This collaboration helps gather and share technical and regulatory expertise, including knowledge from AI sandboxes[129].

119 Check out Recital 153, Article 89 of AI Act
120 Check out Article 38 of AI Act
121 Check out Article 28 of AI Act
122 Check out https://digital-strategy.ec.europa.eu/en/policies/ai-office
123 Check out Recital 148 of AI Act
124 Check out Articles 88, 91, 92 of the EU AI Act

The European Artificial Intelligence Board[130] plays a key role in overseeing and applying the AI Act by the Commission and Member States. It does this through several important activities:

1. It helps coordinate the National Competent Authorities (NCAs) that enforce the AI Act and supports joint market checks[131].

2. It shares technical knowledge and best practices among EU Member States to ensure a clear understanding of the AI Act.

3. It provides strategic advice on how to enforce the regulation, focusing on General Purpose AI models and aiming to create standard approaches and interpretations.

4. It stresses the need for consistent assessments, effective regulatory sandboxes, and the importance of testing AI systems in real-life situations.

5. It advises on how to implement the regulation and offers recommendations on topics like codes of conduct, the development of AI standards, and the use of new technologies.

6. Furthermore, it engages in educational efforts to increase AI knowledge and help the public understand the benefits and risks of AI. It also promotes cooperation across different sectors and countries to enhance the global impact and effectiveness of the regulation.

125 Check out Recitals 112,114, 160, 161, 162, 164 and Article 75 of AI Act
126 Check out Recitals 107,108 and Articles 25, 27, 50, 56, 95 of AI Act
127 Check out Recitals 116, 117, 179 of AI Act
128 Check out Recitals 113, 151 and Article 90 of AI Act
129 Check out Recital 111, 116, 163 and Articles 57, 68 of AI Act
130 Check out Articles 65 and 66 of AI Act
131 Check out Article 74, Section 11 of AI Act

7. AI Act Timelines

The AI Act has had a complicated development process over the past months. There were many discussions, uncertainties, and speculations about the outcome. However, the process concluded successfully with a final political agreement, and the Act was adopted on March 13, 2024. The legislation will take about two months to be formally published in the Official Journal of the EU. The AI Act will officially go into effect twenty days after publication.

To meet our deadlines, we looked at important milestones and actions that need to be completed. You can find the results of this analysis in Table 3.

Table 3: Key Timeline for the Implementation of AI Act

Timeline	**Relevant Action**
13 March 2024	Adoption on the EU Artificial Intelligence Act in the European Parliament's plenary. To meet our deadlines, we identified important milestones and actions that need to be completed. You can find the results of this analysis in Table 3.
22–25 April 2024	Approval of the corrections to the AI Act during the parliamentary plenary session.
Entry into force[132] 1 August 2024	20 days after it is published in the Official Journal of the EU.
Entry into force + Three months 2 November 2024[133]	Member States must create and regularly update a list of public authorities and bodies. They should also publish this list.
Entry into force + Six months[134] 2 February 2025	The date when the rules for banned AI systems will take effect (Chapter II) The date when the general rules will start (Chapter I)
Entry into force + Nine months 2 May 2025[135]	The AIO is ready to publish the codes of practice.

132 Check out Article 113 of AI Act
133 Check out Article 77 of AI Act
134 Check out Article 113 of AI Act
135 Check out Recital 179 and Article 56, Section 9 of AI Act
136 Check out Recital 179 and Article 113 of AI Act
137 Check out Article 56, Section 9 of AI Act
138 Check out Recital 179 of AI Act
139 Check out Recital 179 of AI Act
140 Check out Article 56 of AI Act
141 Check out Article 70, 59 of AI Act
142 Check out Article 73 of AI Act
143 Check out Article 70 of AI Act
144 Check out Article 112 of AI Act
145 Check out Article 6 of AI Act
146 Check out Articles 111 and 113 of AI Act
147 Check out Article 57 of AI Act
148 Check out Article 113 of AI Act
149 Check out Article 111 of AI Act
150 Check out Article 112 of AI Act
151 Check out Recital 174 of AI Act
152 Check out Recital 174 of AI Act
153 Check out Article 111 of AI Act

Timeline	Relevant Action
Entry into force + 12 months 2 August 2025	Chapter III (High-Risk AI Systems) and related sections outline that if the AI Office finds the code of practice inadequate within 12 months, the Commission may establish standard rules for Articles 53 and 55 through implementing acts[136]. Member States must create rules on penalties, prepare governance structures, and ensure compliance checks[137]. They must also inform the Commission about national authorities and provide contact information for competent authorities[138]. The Commission will guide high-risk AI providers on reporting serious incidents and review national authorities' resources every two years[139]. Additionally, the Commission will evaluate the necessity of annual updates to Annex III and Article 5's banned practices, reporting to the European Parliament and the Council[140-144].
Entry into force + 18 months 2 February 2026	The Commission and the consulting AI Board will provide guidelines for the AI Act. These guidelines will include examples of high-risk and non-high-risk AI use cases, as needed by Article 96[145].
Entry into force + 24 months 2 August 2026	The AI Act requires high-risk AI systems listed in Annex III to meet specific obligations, including those in biometrics, critical infrastructure, education, and law enforcement. These obligations apply when significant design changes occur, in line with Article 5 under Article 113(3)(a) [146]. Member States must create at least one national AI regulatory sandbox and can collaborate on this. The EU Commission supports sandbox development, and States can join existing sandboxes if they provide equivalent coverage[147].
Entry into force + 36 months 2 August 2027	Applicability of Article 6(1) (classification rules for Annex I Union harmonization legislation) [148]and obligations of the AI Act: GPAI model providers with products on the EU market 12 months before the AI Act's entry into force must implement essential measures to comply with GPAI obligations[149].
Entry into force + 48 months 2 August 2028[150]	Every four years after the AI Act starts, the Commission will analyze and update the European Parliament and Council on possible changes to AI system transparency and improvements in supervision and governance. The Commission will focus on how enforcement works and if there's a need for an EU agency to close any gaps, suggesting amendments as needed. All reports will be public. The Commission will evaluate the AI Office's effectiveness, checking if it has enough powers and resources to do its job. If necessary, they may enhance its role. The evaluation report will go to the European Parliament and Council. Every four years, the Commission will report on progress in developing energy-efficient standards for general-purpose AI models. This includes exploring the need for additional binding measures. The final report will also be public. The Commission will assess voluntary codes of conduct every three years to improve compliance for low-risk AI system providers and consider adding requirements for environmental sustainability[151].
Entry into force + 60 months 2 August 2029[152]	The Commission will review the AI Act every four years and report to the European Parliament and the Council. An annual assessment will evaluate potential revisions to the lists of high-risk AI systems and prohibited practices.

31 December 2030	AI systems within large-scale IT frameworks, as outlined in Annex X and operational 36 months before the AI Act's enforcement, must comply with the AI Act. Evaluations of these systems will include the AI Act's requirements, especially during updates to the legal acts in Annex X[154].
Entry into force + 84 months 2 August 2031	The Commission must assess its enforcement of the AI Act and report to the European Parliament, the Council, and the European Economic and Social Committee on its initial years of application. If necessary, the final report will include proposals for amendments to the enforcement structure and changes required by the EU agency to address any identified issues[155].

154 Check out Article 111 of AI Act
155 Check out Article 112, Section 13 of AI Act

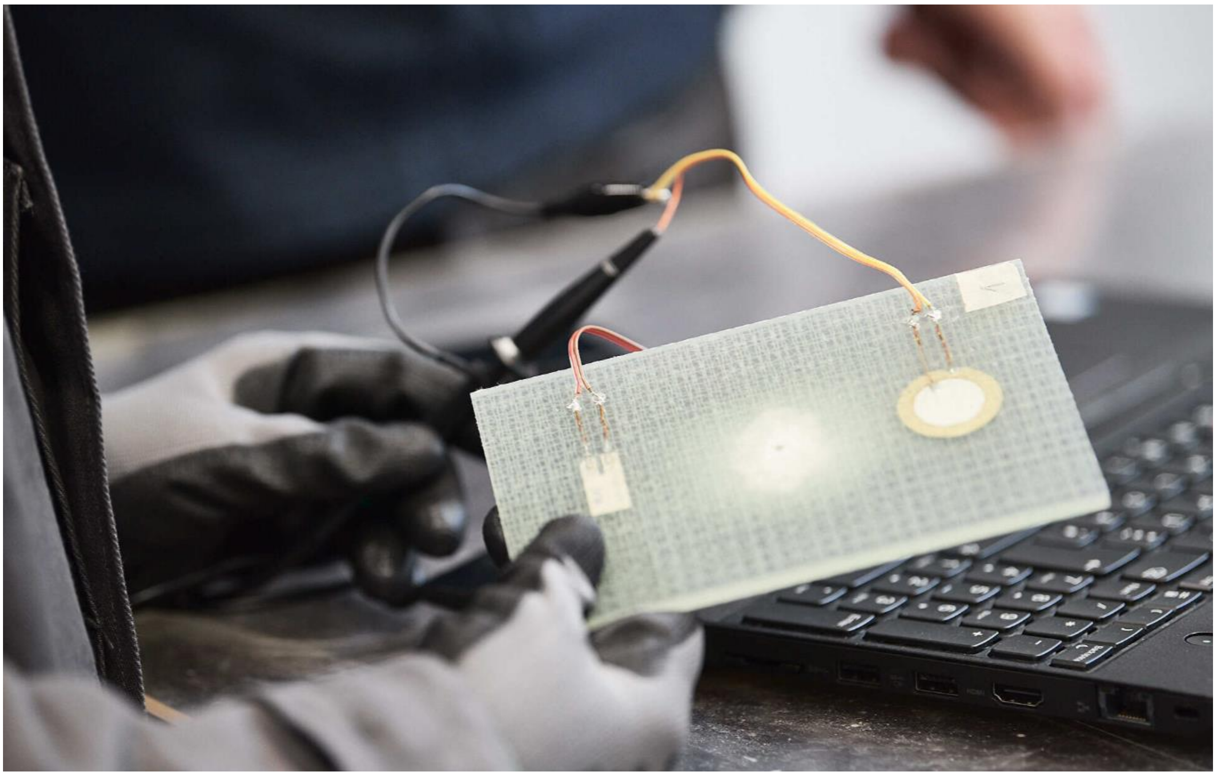
8. Existing AI Products in the Market

The AI Act sets out the term “substantial modification.” This means any unplanned change to an AI system that is already on the market, which could affect how compliant it is or change its intended use[156]. The Act also uses the term “predetermined changes.” This refers to set changes that have already been approved as part of the initial assessment of AI systems, even if these systems continue to learn or evolve after being released[157].

For high-risk AI systems that were already on the market before the AI Act came into effect, the Act only applies if there are significant changes in their design or purpose after the Act starts to apply. The terms “significant change” and “substantial modification” are treated the same in this context[158].

The AI Act exempts AI systems that are part of large-scale IT systems and those that high-risk AI systems used by public authorities. These systems must comply with the Act by the end of 2030 or within six years of the Act's start date.

It is not clear when a high-risk AI system is governed by other EU laws, like those in Annex I section A, and which law takes priority regarding major changes. You can find the answer in the recitals of the AI Act[159]. If a change is not significant under a more specific EU law (such as Regulation 2017/745 MDR), then it should not count as a major change under the relevant parts of the AI Act.



156 Check out Article 3(23) of AI Act
157 Check out Recital 128 and Article 43(4) of AI Act
158 Check out Recital 177 of AI Act
159 Check out Recital 84 of AI Act

9. Understanding AI Act Conformity

The AI Act increases oversight in sectors that were not regulated before. It has different rules for AI providers and deployers based on the level of risk, ensuring that AI systems comply with its requirements. The main ways to comply with the AI Act are:

Use a quality management system (QMS) [160]: The new standard ISO/IEC 42001:2023 for managing Artificial Intelligence (AIMS) is not harmonized with the AI Act yet, but it is expected to become the primary reference for conformity. AIMS should outline how to comply, including strategies, processes for design, development, data governance, testing, validation, risk management, post-market monitoring, and reporting incidents. Providers and deployers of high-risk AI systems must use AIMS. AI providers that follow the conformity routes in Annex VI (internal control) and Annex VII (assessment of QMS and Technical Documentation) must also use it. If AI systems must meet QMS requirements from other EU regulations, AIMS parts can be included.

Create and maintain technical documentation[161]**:** High-risk AI systems that could follow Annex VI (internal control) and Annex VII (assessment of QMS and technical documentation) must have technical documentation (TD) to show compliance with Section 2 in Chapter III of the AI Act. Annex XI (TD for general-purpose AI models, Article 53(1)) and Annex IV (TD referred to in Article 11(1)) explain what the TD must include. This documentation must be prepared before the AI system enters the market. If the AI system must meet TD obligations from other EU regulations, AI Act elements can be included in that documentation.

Follow requirements for high-risk AI systems[162]**:** Chapter III, Section 2 lists the requirements for high-risk AI systems. Although the ISO/IEC JTC 1/SC 42 committee has released several standards, none have yet been harmonized with the AI Act. The legislation states (Article 40) that meeting the harmonized standards of the AI Act assumes compliance with its requirements.

Meet transparency obligations[163]**:** AI system providers, including those offering general-purpose AI systems, and deployers of specific AI systems must follow the transparency rules in Chapter IV, Article 50.

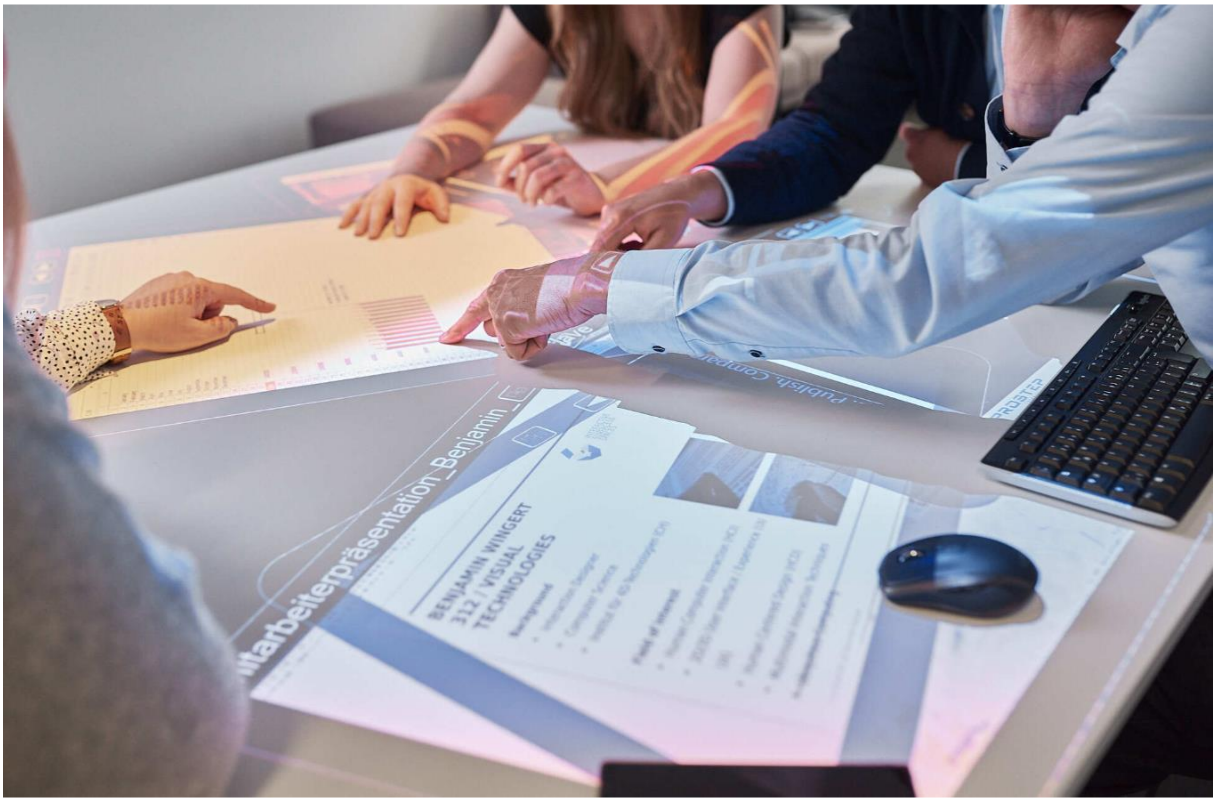
Use sandboxes[164]**:** Member states and competent authorities set up sandboxes. These are controlled environments designed to support innovative AI systems' development, training, testing, and validation. AI systems may use sandboxes before they launch in the market or are put into service. The results (exit reports) from sandboxes can help demonstrate compliance with the AI Act and be part of the required conformity assessment documentation or given to market surveillance authorities.

160 Check out Article 17 of AI Act
161 Check out Articles 11 and 53 of AI Act
162 Check out Articles 8 to 14 of AI Act

Conformity paths: [165]

- If a high-risk AI system must comply with other EU regulations (Annex I, section A), the provider must follow the required assessment procedures. The AI Act's requirements also apply, and Notified Bodies may ask for datasets and the AI model for further testing (Annex VII).
- Internal control (Annex VI) is an option for assessing compliance for high-risk AI systems in Annex III. However, AI systems listed under Annex III point 1 (biometric identification) may have to follow Annex VII assessments, which require the Notified Body to be involved in assessing AIMS and TD.

General-purpose AI (GPAI) models: The AI Office is the leading authority overseeing GPAI models. Article 53 outlines the obligations of GPAI providers, and Annex XI describes the requirements for their technical documentation. These obligations do not apply to providers offering free and open licenses. Additionally, GPAI models with systemic risks face extra requirements, including evaluating model performance, measures to manage systemic risks, and protecting[166] against cybersecurity threats[167]. Compliance with existing codes of practice will be enough for GPAI models regarding systemic risks until new standards are established.



163 Check out Article 50 of AI Act
164 Check out Article 57 of AI Act
165 Check out Article 43 of AI Act
166 Check out Article 51 and 56 of AI Act
167 Check out Article 56 of AI Act

10. Conclusion

The AI Act is being prepared for publication in the Official Journal of the European Union, and people around the world are paying attention. What started as a prediction has become a significant and evolving industry, with some risks involved. The text of the law shows that no one person or group can manage this new area alone. Everyone—providers, deployers, the Commission, the AI Office, the AI Board, member states, National Competent Authorities, the public, and others—must work together to manage and use these systems safely.

As the AI Act moves forward, many are curious about how to get ready for its effects. This white paper aims to help organizations take steps to find out if and how AI systems or models affect them, clarify their responsibilities, understand how to categorize AI systems, and learn the requirements they need to meet and how to meet them. Organizations should know how to follow conformity pathways for their products. This knowledge will help them seek accredited or designated organizations that can help with assessments as needed.

The AI Act encourages providers of high-risk AI systems to start working on compliance voluntarily during the transition period[168]. ARENA2036 agrees with this idea; everyone will have a lot to learn. ARENA2036 values the AI Act and the way the community created this regulation. They understand that publishing the AI Act and achieving compliance are not final goals. Instead, they represent an ongoing process of improving the regulatory framework as technology advances.

168 Check out Recital 178 of AI Act