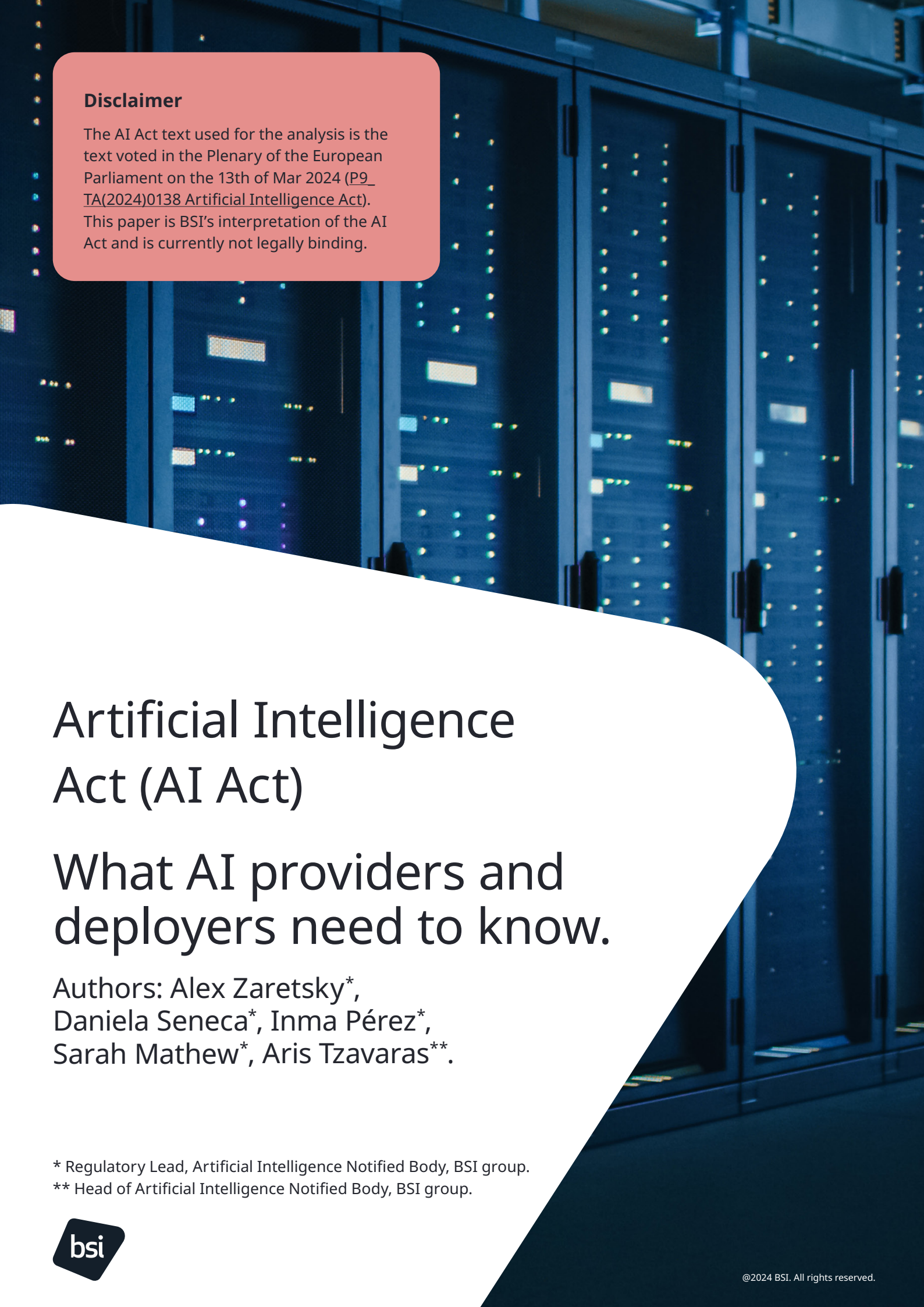
Artificial Intelligence Act

What AI providers and deployers need to know.



Disclaimer

The AI Act text used for the analysis is the text voted in the Plenary of the European Parliament on the 13th of Mar 2024 (P9_TA(2024)0138 Artificial Intelligence Act). This paper is BSI's interpretation of the AI Act and is currently not legally binding.

Artificial Intelligence Act (AI Act)

What AI providers and deployers need to know.

Authors: Alex Zaretsky*, Daniela Seneca*, Inma Pérez*, Sarah Mathew*, Aris Tzavaras**.

* Regulatory Lead, Artificial Intelligence Notified Body, BSI group.
** Head of Artificial Intelligence Notified Body, BSI group.

The need for Artificial Intelligence legislation

We did not wake up to a world where Artificial Intelligence (AI) was just born. The genesis of AI as an idea is evident from ancient times in the form of myths.[1] However, the term "AI" more recently has been attributed to John McCarthy of the Massachusetts Institute of Technology (MIT) who first suggested the concept at a 1956 conference at Dartmouth College.

The **technological evolution permitted AI to become accessible**, both in terms of computation power as well as in terms of the tooling and availability of digital data for facilitating development of AI systems.

Since 1956, AI has shown significant progress in performing "narrow" tasks, in most cases, better than the average human and, in some, better than experts. A landmark victory of AI's progress became clear when the Deep Blue expert system played chess against the world champion Garry Kasparov in the 90s.[2]

Now, why is there an increasing global concern to regulate and/or control AI? The short answer to this question is that we may lose to an opponent we created. **Society cannot afford to leave AI unregulated as this could lead to the misuse of this technology.** AI also needs vast amounts of data to become increasingly intelligent, and there is the risk that fundamental rights would be violated. For example, an algorithm that processes profiles to evaluate candidates for a job position, may be biased against people of a certain ethnicity, limiting exposure of their profiles for opportunities. **These algorithmic biases have serious real-world implications.** In this context, to prevent any form of manipulation or biased outcome, several regions are leaning towards AI regulation.

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

Let's not forget about the geopolitics linked to regulating AI. The AI industry is growing at an extremely rapid pace and AI has become of strategic importance for governments across the world. Countries are competing to win the "AI race" and those able to successfully lead on AI innovation will be well positioned in global affairs.

Regulating a technology sector is not something new. Typical examples are regulations bestowed on the pharmaceutical and medical industries, as well as on more abstract technologies like those processing our digital data.[3] **Justifications behind market regulation includes market acceleration and harmonization as well as protecting consumers from the negative effects of such technologies.** In the context of AI systems, harms may arise from the deployment of AI and its after effects. Therefore, such justifications can be used to limit AI.[4]

Reasons to regulate AI may differ across regions. **The European Union's (EU) approach, for instance, has been characterized by its focus on the protection of human rights – or as it is called in Europe, fundamental rights.** Those rights are enshrined in the Charter of Fundamental Rights of the EU and in other binding legislation such as the General Data Protection Regulation (GDPR). As technology is becoming an ever more central part of citizens' life, the EU understands that **trust, is a prerequisite for AI uptake in Europe**. We use, as consumers, products and services coming from "unfamiliar sources" and we need to have the assurance that those products are safe, trustworthy, and ethical for us to consume. Regulations set the basic "rules of the game", ensuring consumers that unfamiliar sources deliver a product or service that obeys those rules. In most cases, legislation goes beyond the first entry of a product to the market, they additionally **dictate the need for monitoring the product while in use and to deliver feedback to relevant authorities and action** when something goes wrong; this is known as **Post Market Surveillance (PMS).**

The use of AI comes with more sophisticated and nuanced challenges: some philosophical, some practical. Due to the increasing concerns about the adverse impact that AI systems may have on individuals, EU lawmakers have the **challenge of ensuring that AI is used for good.** But what is "good AI"? This quest is relatively new, however, defining what is "good" has been a long-standing question with different answers depending on the moral theory that you consider.[5] For this reason, since human rights are universally recognized, the EU decided to take a human-centric based approach to AI governance[6] and, in April 2019, the European Commission published its conceptualization of "good AI": the Ethics Guidelines for Trustworthy AI.[7] The non-binding nature of these guidelines were criticized, however, in 2021, the EU Commission published the proposal for an **Artificial Intelligence Act (AI Act) that largely codifies the ethics requirements proposed by the High-Level Expert Group on AI in its Guidelines.[8]** Since then, the final text has gained political agreement and has been voted by the EU Parliament in March 2024.

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'

The AI Act is a "horizontal" legislation as it does not target a specific industry sector but rather any industry that uses AI. The AI Act sets requirements that products must comply with, as well as obligations for all parties involved (economic operators). The horizontal nature of this legislation is envisioned to "build on" sectorial legislations, regulating only the AI aspects of those products. Furthermore, because the AI Act is technology agnostic, it does not prescribe specific rules for specific types of AI techniques, with the exemption of General-Purpose AI systems (GPAI).

To determine if the upcoming legislation is applicable to one's product, one must first define whether their product is or uses AI. Unfortunately, the definition of AI has been the "holy grail" of the last decades, as there is no globally acceptable definition of "intelligence." The above-mentioned "AI race" has forced governments as well as supranational and intergovernmental organizations to attempt to find a common definition of AI.

For instance in the AI Act, the EU ultimately suggested a definition aligned to the Organization for Economic Co-operation and Development (OECD)'s AI definition,[9] ensuring the text *"distinguish[es] it from simpler traditional software systems or programming approaches and should not cover systems that are based on the rules defined solely by natural persons to automatically execute operations."*[10]

The AI Act defines an AI system in Article 3 as: "*a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.*"

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." See OECD, 'Recommendation of the Council on Artificial Intelligence'

10 See Recital 12 of AI Act

AI Act scope and territorial implications

There are two key actors caught under the scope of the AI Act which are providers[11] and deployers[12] of AI systems. Moreover, certain obligations have been introduced for importers, distributors, product manufacturers and authorized representatives of providers. The AI Act states[13] that the regulation applies to providers and deployers of AI systems established in the EU, as well as externally, to any provider and deployer of AI systems outside the EU, if the output of the AI system is used within the EU. What "output" means is not defined under the AI Act, however, the definition of AI system refers to outputs in the form of content (generative AI systems) including text, video, or image[14] and *predictions, recommendations, or decisions that can influence physical or virtual environments.*[15] **The key thing to ask here is whether the impact of the AI system occurs within the EU, regardless of where the provider and deployer is established.**

Similar to the GDPR, one of the most important consequences of the AI Act extraterritorial scope is that it will impose significant obligations on non-EU businesses, even if they do not have a legal presence in the EU. The *rationale* behind this approach is linked to the EU's growing concern on how authoritarian governments use AI and its potential impact on the rights and freedoms of individuals. Consequently, the AI Act aims to level the playing field and make the AI Act applicable in a non-discriminatory manner.

Furthermore, it is important to mention that the AI Act will potentially become another example of the phenomenon called the "Brussels Effect," a concept originally coined by Anu Bradford,[16] a professor at Columbia University. The "Brussels effect" refers to *"the EU's unilateral power to regulate global markets."*

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 See Article 2 of AI Act

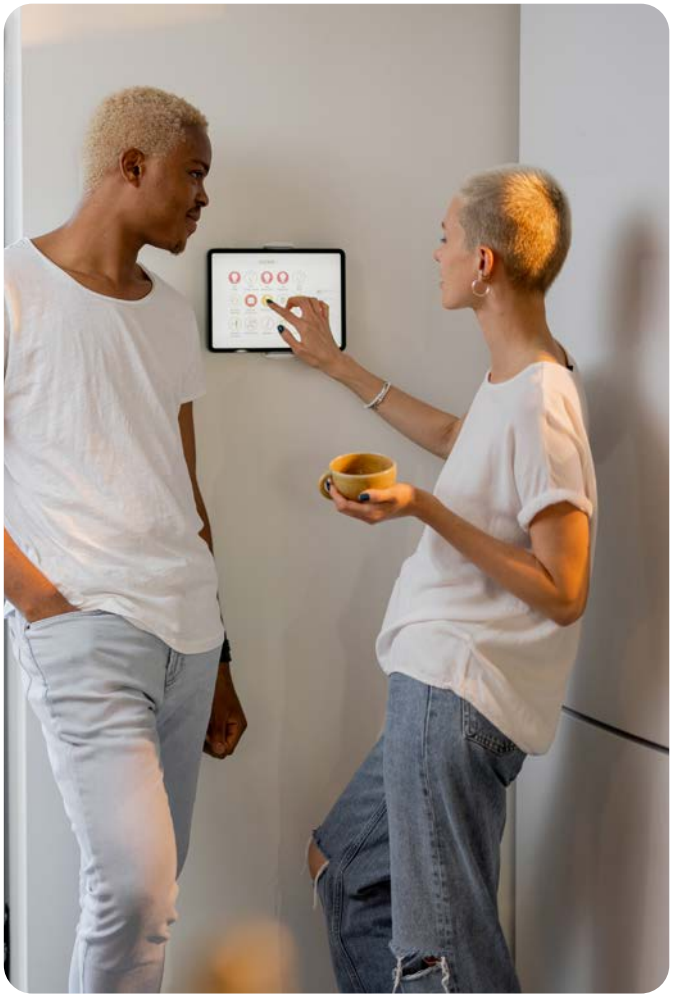
14 Throughout the text we see that the AIA includes image, audio or video as example of AI-generated content.

15 See Article 3 and Recital 12 of AI Act

16 Bradford, Anu. (2020). The Brussels Effect: How the European Union Rules the World.

Some may argue that the upcoming AI Act Regulation will hamper AI innovation in Europe as it is more stringent in comparison to other more flexible countries that encourage self-regulation and voluntary commitments. However, for economic operators, it is more beneficial to adopt a uniform global standard rather than adhering to multiple, including laxer, regulatory standards, as this brings legal certainty. This would be the case for those organizations operating globally, who have multiple production locations where it is not legally, technically, or even economically viable, for the company to comply with multiple regulatory regimes.[17] This business approach would explain why so many large non-EU companies follow the GDPR and many other EU environmental regulations across their global operations.

Let's not also forget that the EU was the first mover when it comes to regulating AI. It is true that due to the slow pace of the EU legislative process, there have been delays in the AI Act negotiations and other jurisdictions have adopted comprehensive regulation for parts of the AI ecosystem before the EU.[18] **For example, China has been one of the first countries to implement AI regulations, including new rules on the use of recommendation algorithms.[19]** Despite this, the AI Act has been the first draft to be published and this may be the reason why other jurisdictions have sped up their legislative processes.



Taking the success of the GDPR adoption as an example, the EU plans to promote its blueprint on AI globally.[20] **It is fair to assume that the AI Act's human-centered approach, strong focus on ethics, transparency and fundamental rights, will serve as an inspiration to like-minded countries.** Especially after seeing over 100 countries today with GDPR-like data privacy rules.[21]

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 See 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 See interview to Bradford What is the Brussels Effect, and what does it mean for global regulation? (microsoft.com)

To sum up, the AI Act will have an extra-territorial impact on AI providers and deployers in non-EU jurisdictions, if their AI systems and/or outputs are used within the EU.

Moreover, its existing extraterritorial scope has the potential to become the gold standard when it comes to AI governance. Experience has proved that European values have a broad appeal, and it is fair to assume that the AI Act will be globally widespread.

Companies operating globally may be glad to follow only one set of rules, even if they are more stringent. However, the extraterritorial scope of the AI Act might raise compliance challenges, especially to those AI providers established in third countries if they are not aware that the output of their AI system will be used in the EU.

Therefore, all relevant operators need to understand which role they play along the AI value chain and **properly determine the scope of their AI systems to see if they fall within the scope of the AI Act.**

AI products falling under the AI Act

As we have seen in this whitepaper, the AI Act's definition of AI is close to the one proposed by the OECD and this seems to be an advantage as it maintains a semantic alignment with international partners. The EU believes that this definition gives a clear criterion for differentiating AI systems from traditional software, thus ensuring a proportionate regulatory approach. **However, this definition has drawn much criticism for still remaining too broad**. In any case, it is important to understand that not all AI technologies defined as an AI system under the AI Act will be subject to obligations, however one must consider the degree of risk they pose to the health, safety, and fundamental rights of individuals.

The EU believes that a risk-based approach is important to help ensure that the regulatory intervention is proportionate.[22] To that end, the AI Act distinguishes between AI systems posing (i) unacceptable risk, (ii) high risk, (iii) limited risk, and (iv) low or minimal risk.

The Commission judges the level of risk by the likelihood that the system may harm the health and safety of specific individuals, and/or potentially violate their fundamental rights. The obligations imposed on such systems range from prohibitions to the voluntary codes of conduct.

The AI Act proposes prohibitions on AI applications that pose *"unacceptable risks"* to people's safety, health and rights.[23]

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

The AI Act considers these practices to be harmful and abusive and should be prohibited because they contradict Union values.[24] Accordingly, these systems would be prohibited to be placed on the market, put into service, or used in the EU:

1 **AI systems that deploy harmful manipulative "subliminal techniques."[25]**

- Example: *"An inaudible sound is played in truck drivers' cabins to push them to drive longer than healthy and safe. AI is used to find the frequency maximising this effect on drivers."*[26]

2 **AI systems that exploit specific vulnerable groups (due to their age, physical or mental disabilities).[27]**

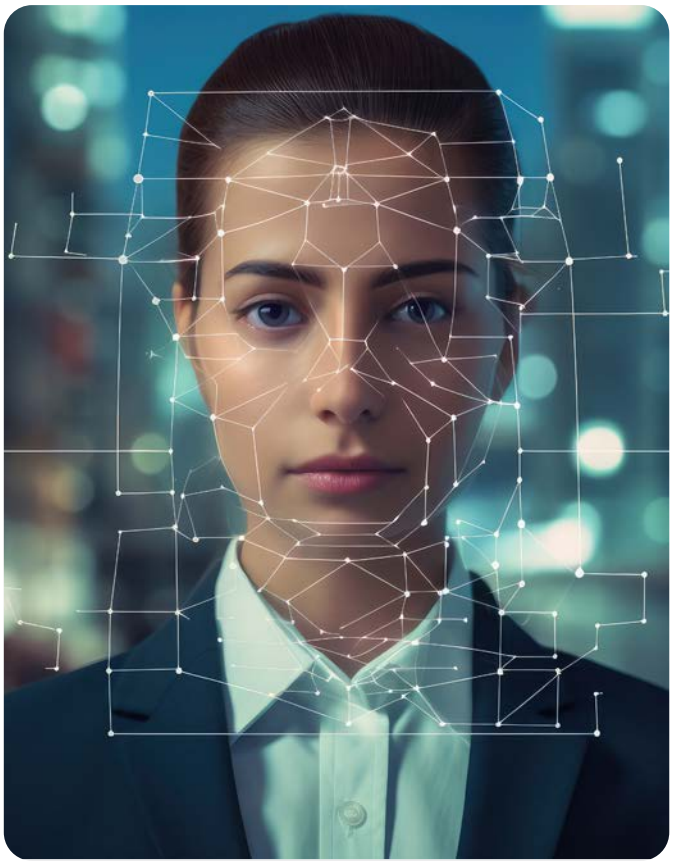
- Example: *"A doll with an integrated voice assistant encourages a minor to engage in progressively dangerous behaviour or challenges in the guise of a fun or cool game."*[28]

3 **AI systems used for social scoring purposes for public and private purposes- in particular, to classify the reliability of people based on their social behaviour or personality traits.[29]**

- Example: *"An AI system identifies at-risk children in need of social care based on insignificant or irrelevant social 'misbehaviour' of parents, e.g. missing a doctor's appointment or divorce."*[30]

4 **Biometric categorization of natural persons based on biometric data to deduce or infer their race, political opinions, trade union, membership, religious or philosophical beliefs, sex life or sexual orientation.[31]**

- Example: *"AI systems that infer 'criminality' based on data about people's facial structure or biological characteristics, for example, the colour of the skin."*



5 **Real-time remote biometric identification in publicly accessible spaces by law enforcement.[32]**

- Example: *"All faces captured live in a public space by video cameras checked, in real time, against a database to identify a criminal in the crowd."*

6 **Individual predictive policing; except for law enforcement if based on objective and verifiable facts.[33]**

- Example: *"AI-predicted behaviour based solely on their profiling, personality traits or characteristics, such as nationality, place of birth, place of residence, number of children, debt, their type of car, without a reasonable suspicion of that person being involved in a criminal activity based on objective verifiable facts and without human assessment thereof."*[34]

24 See recital 28 of AI Act
25 See 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. See https://cor.europa.eu/en/events/Documents/SEDEC/FINAL%20PDF%20AI%20Presentatiofor%20COR%20Sedec%20Committee%20meeting%2023%2006%2021.pdf
27 See Article 5(1)(b) of AI Act
28 See https://cor.europa.eu/en/events/Documents/SEDEC/FINAL%20PDF%20AI%20Presentatiofor%20COR%20Sedec%20Committee%20meeting%2023%2006%2021.pdf
29 See Article 5(1)(c) of AI Act
30 See https://cor.europa.eu/en/events/Documents/SEDEC/FINAL%20PDF%20AI%20 Presentatiofor%20COR%20Sedec%20Committee%20meeting%2023%2006%2021.pdf
31 See Article 5(1)(g) of AI Act
32 See Article 5(1)(h) of AI Act
33 See Article 5(1)(d) of AI Act
34 See Recital 42 of AI Act

7 **Emotion recognition in the workplace and education institutions, unless for medical or safety reasons (i.e. AI systems used in detecting the state of fatigue of professional pilots or drivers for the purpose of preventing accidents).**[35]

- Example*: "AI recruitment tools that assess a candidate's emotional state or truthfulness through analysis of facial expressions, voice modulation, or body language during interviews."*

8 **AI systems using indiscriminate scraping of biometric data from the internet or CCTV footage to create facial recognition databases.**[36]

- Example: *"AI system that collects facial images from social media without any specific targeting or consent, amassing a vast database of faces."*

However, it is important to mention that the use of real-time remote biometric identification in point 5 above has some exceptions related to the safety of society as a whole. In particular, the use of real-time remote biometric identification systems (such as facial recognition) in public spaces for law enforcement purposes will be allowed when the use of such systems can be justified by "three exhaustively listed and narrowly defined situations." These narrowly defined exceptions cover a rather broad range of situations:

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

- the *"prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or (...) of a terrorist attack."*[38]

- the *"localisation or identification"* of a person suspected of having committed a crime[39] with a maximum sentence of at least 4 years that would allow for the issuing of a European Arrest Warrant.[40]

Therefore, if the above is fulfilled, real-time biometric identification by law enforcement authorities may be permitted, if it is accompanied by safeguards for fundamental rights, including the ex-ante involvement of judicial authorities and prior fundamental rights impact assessment (unless in duly justified situations of urgency).

These safeguards will also be mandatory for the usage of AI systems for post remote biometric identification of persons under investigation.[41] An example of this would be the use of biometric surveillance to analyse footage during a protest to identify an individual that has committed a crime.

It is important to state that the above prohibition does not ban actors from using remote biometric identification for non-law enforcement purposes. This means that private entities may use such systems (e.g. marketplaces, public transport and even schools) if they go through a third-party conformity assessment or comply with harmonized European standards that are to be published later on.

35 See Article 5(1)(f) of AI Act
36 See Article 5(1)(e) of AI Act
37 See Article 5(1)(h)(i) of AI Act
38 See 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 See Article 5(1)(h)(iii) of AI Act
41 See Article 26 (10) of AI Act

Moving on to the next category under the **AI Act, "high-risk AI systems"** are those systems that create adverse impact on people's health and safety or their fundamental rights in a number of defined applications, products and sectors. This is the main focus of the regulation.

Before going into more detail, it is important to clarify that AI systems can be used on a stand-alone basis or as a component of a product, irrespective of whether the system is physically integrated into the product (embedded) or serve the functionality of the product without being integrated therein (non-embedded).[42]

The high-risk regime is based on the intended purpose of the AI system, in line with the New Legislative Framework (NLF), a common EU approach to the regulation of certain products such as machinery, lifts, medical devices, personal protective equipment and toys.[43]

The AI Act distinguishes between two categories of high-risk AI systems:

1 **AI systems that are products or safety components of products covered by certain Union health and safety harmonization legislation (such as toys, machinery, lifts, or medical devices) and are required to undergo a third party conformity assessment.[44]**

2 **Stand-alone AI systems deployed in eight specific areas:[45]**

   a. biometric identification, categorization and emotion recognition (outside prohibited categories);
   Example: AI systems used for facial recognition.

   b. management and operation of critical infrastructure;
   Example: AI systems used in road traffic, the supply of water, gas, heating, and electricity.

   c. educational and vocational training;
   Example: AI systems used in evaluating students on tests required for university admission.

   d. employment, worker management and access to self-employment;
   Example: AI systems used to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates.

   e. access to and enjoyment of essential services and benefits;
   Example: AI systems used for creditworthiness evaluation of natural persons.

   f. law enforcement;
   Example: AI systems used for detection, investigation, or prosecution of criminal offenses.

   g. migration, asylum and border management;
   Example: AI systems that identify a person who, during an identity check, either refuses to be identified or is unable to state or prove his or her identity.[46]

   h. administration of justice and democracy;
   Example: AI systems aimed at helping analyse and interpret facts regarding judicial authority.

The above list of high-risk AI systems may be updated over time as the EU Commission may modify or add additional use cases if they pose similar risks to the uses currently on the list. However, it can remove areas if they do no longer pose a significant risk to health, safety and fundamental rights.[47]

A stand-alone AI system can be classified as high-risk if it falls under any of the eight specific areas. However, as always, the AI Act has exceptions. If the system does not pose significant harm to the health, safety, or fundamental rights of people, including not materially influencing the outcome of decision-making, it may be exempt. This would be the case of the following systems:[48]

- Intended to perform a narrow procedural task.[49]
- Intended to improve the result of a previously completed human activity.[50]

42 See Recital 12 of AI Act
43 See New legislative framework - European Commission (europa.eu)
44 See 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 See the list in AI Act
46 See recital 33 of AI Act
47 See Articles 7 and AI Act
48 See Article 6 (3) of AI Act
49 See Article 6 (3) of AI Act
50 See Article 6 (3) of AI Act

- Intended to detect decision-making patterns or deviations from prior decision-making patterns.[51]

- Intended to perform a task that is only preparatory to an assessment relevant for the purpose of the high-risk use cases in Annex III.[52]

It is important to note that an AI system will always be considered at a minimum high-risk if the AI system performs profiling of natural persons.[53]

The next type of AI system risk level is "limited risk". **These are systems that have special disclosure obligations due to their particular interaction with humans given that they may pose the risk of manipulation**. These include AI systems that generate or manipulate image, audio or video content (i.e. deep fakes[54]), AI systems that are intended to interact with people (e.g. chatbots), and AI-powered emotion recognition systems and biometric categorization systems.

With this inclusion, the AI Act ensures that EU customers make informed decisions as they are aware that they are interacting with a machine.[55]

Finally, the last category is "minimal risk". **These AI systems do not fit in any of the other categories and present only low or minimal risk.** They can be developed and used within the EU without conforming to any additional legal requirements. However, the AI Act envisages the creation of codes of conduct to encourage providers of non high-risk AI systems to voluntarily apply the mandatory requirements for high-risk AI systems. These codes of conduct should be based on clear objectives and key performance indicators to measure the achievement of those objectives.[56] This could include elements around inclusiveness, fairness, transparency, confidentiality, and environmental sustainability.

The Commission and Member States will encourage the creation and voluntary compliance with these codes.[57]

It is important to underline that existing EU law, such as the GDPR, still applies when the use of AI systems falls within the scope of that law, no matter if classified as no risk under the AI Act.

51 See Article 6 (3) of AI Act
52 See Article 6 (3) of AI Act
53 See Article 6 (3) of AI Act
54 See Article 3(6) of of AI Act
55 See Article 50 of AI Act
56 See Recital 165 of AI Act
57 See Article 95 of AI Act

AI systems falling under other EU legislation.

Given the horizontal nature of the AI Act, **all AI systems across sectors are subject to the same risk-assessment criteria and legal requirements**. The AI Act interrelates with other EU legal instruments, for example rules on data protection, privacy, civil liability or sectorial law such as the Machinery Regulation or the Medical Devices Regulation (MDR). This horizontal approach prevents companies from "shopping around" between sectors and thus ensuring that all players conform to the same legal requirements. This approach might seem preferable as it is uniform, stable, and fair across industries. However, it is important to say that, if this approach is not properly addressed, it may lead to conflicting obligations and procedures for AI providers.

The AI Act draws on the New Legal Framework (NLF) regime,[58] designed to improve the EU internal market, and increase the quality of conformity assessment of certain products such as medical devices, machinery, or toys. As described by Veale and Zuiderveen Borgesius,[59] *"under NLF regimes, a manufacturer must undertake pre-marketing controls undertaken to establish products' safety and performance, through conformity assessment to certain essential requirements laid out in law. Manufacturers then mark conforming products with "CE"; marked products enjoy EU freedom of movement."*

The AI Act acknowledges that a single AI system may be affected by different Union Harmonization legislation.[60] [61] For example, a medical device product incorporating AI might present risks not addressed by the Medical Devices Regulation (MDR).[62] **This calls for a simultaneous and complementary application of several EU laws.**

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 See 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).

The NLF legal acts are built on the legal concept that **whenever a matter is regulated by two rules, the more specific one should be applied first.**[63] With this, it is ensured that products incorporating AI are not subject to a double regulatory burden. This was the intention of the Commission when it proposed the AI Act:

"To achieve those objectives, this proposal presents a balanced and proportionate horizontal regulatory approach to AI that is limited to the minimum necessary requirements to address the risks and problems linked to AI, without unduly constraining or hindering technological development or otherwise disproportionately increasing the cost of placing AI solutions on the market."[64]

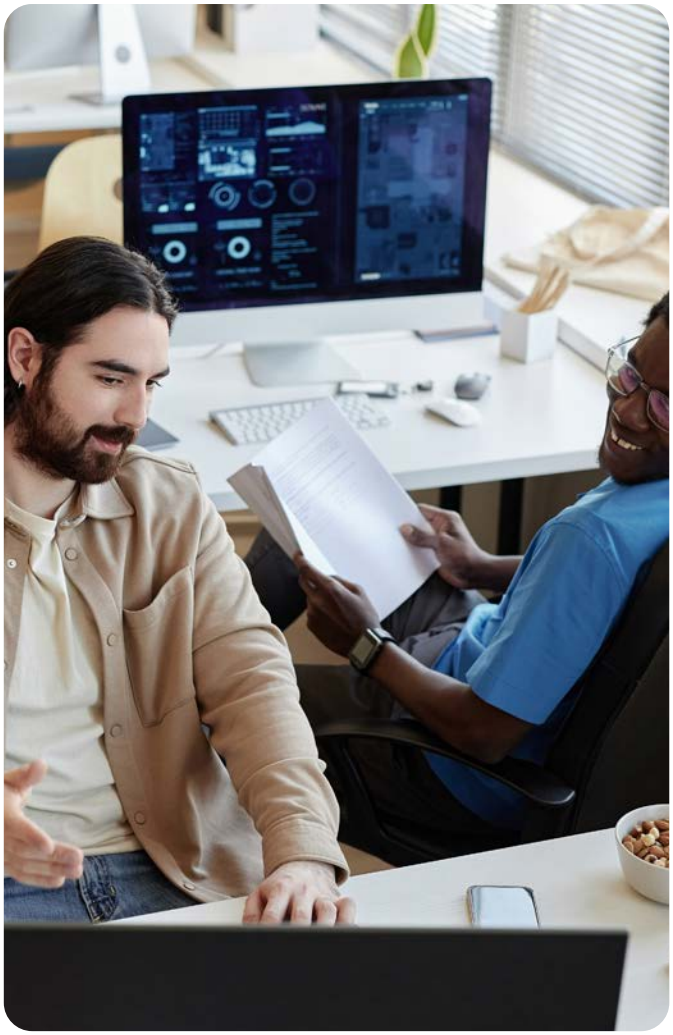
If we take AI-enabled medical devices as an example, the **AI Act tries to ensure consistency**, avoid duplications, and minimize additional burdens associated with the cumulative application of the AI Act and MDR. It allows AI providers to integrate the necessary measures to comply with the AI Act into the procedures and documents already required under MDR.[65] In practice, this means that the AI-enabled medical device manufacturer would be allowed to integrate the testing and reporting processes, information and documentation required under the AI Act into the already existing documentation and procedures required under the MDR. This is because the MDR is considered the more specific rule and, therefore, will take precedence.

However, as previously mentioned, there are certain tensions and inconsistencies that make it difficult to apply the AI Act in conjunction with other Union harmonization laws.

For example, as seen in the previous section, the **AI Act categorizes as high-risk AI systems those that are products or safety components of products already covered by Union harmonization legislation.** For AI-enabled medical devices both, the AI Act and MDR, would be applicable to the same product. The problem here is that there is no definition of "safety component" under the MDR and it is not clear for a medical device what a 'safety component' is.[66]

Additionally, the AI Act interplays not only with Union Harmonization law, but also with other horizontal legislation, such as the GDPR.[67]

The AI Act makes several references to the GDPR throughout the text and assures that it is without prejudice and complements the GDPR. Accordingly, both regulations apply side by side. In practice, this means that **all AI systems must strictly adhere to the GDPR** if they use personal data belonging to EU citizens, or plan to be deployed for usage within the EU. However, again there are some tensions when it comes to an AI system processing personal data.



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 See 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)

For example, the **AI Act states that it does not provide legal grounds for processing personal data and refers back to the GDPR to find a justifiable ground for this processing.**[68] However, it does not give clarity on how to apply the GDPR's requirements for collecting and processing personal data.

In this context, it is difficult to find a legal ground for the processing of personal data by Large Language Models (LLMs) as there is no controller/data subject relationship (e.g. contract), nor can the data subject expect their data to be used as training data for an app, and there is no possibility for the data subject to object to such processing (e.g. no explicit consent). In some cases, AI can handle personal data based on the justified grounds of "legitimate interest."[69] Nevertheless, this needs to be balanced to ensure that the data subject's rights are not compromised.

It is expected that the **Commission will issue guidelines clarifying how to train AI models** without violating personal data protection rules, including the Data Act, Data Governance Act and the Copyright Directive. Regarding the GDPR, legal grounds for the processing of personal data might require a significant rethink for AI systems.

On the cybersecurity side, the AI Act also overlaps with the EU Cybersecurity Act[70], including a presumption of conformity in Article 42(2) of the AI Act. The clause acknowledges that high-risk AI systems that have been certified under a cybersecurity scheme created according to the process provided by the Cybersecurity Act *"shall be presumed to be in compliance with the cybersecurity requirements set out in Article 15 of this Regulation."*[71] Article 15 and recital 49 of the AI Act state that high-risk AI systems should perform consistently throughout their lifecycle and meet an appropriate level of accuracy, robustness and cybersecurity in accordance with the generally acknowledged state of the art.

It is fair to say that Article 15 of the AI Act is very general and does not cover the entirety of potential cyberthreats to AI-powered systems such as those identified by ENISA[72] in its *"Artificial intelligence and Cybersecurity Challenges"* report.[73] Therefore, if AI developers want to ensure the highest level of cybersecurity for their AI system, they will need to either rely on the available cybersecurity schemes or, most likely, apply the harmonized standards[74] or common specifications defined by the Commission,[75] which are not available at this time.

On another note, but still within the EU cybersecurity framework, **the AI Act will also interplay with the new Cyber Resilience Act (CRA).**[76] Like the AI Act, this regulation is expected to enter into force in 2024. In the CRA,[77] we find a presumption of conformity with the AI Act. It states that products with digital elements classified as high-risk AI systems under the AI Act should comply with the essential cybersecurity requirements set out under the CRA.[78]

68 See Recital 63 of AI Act
69 See 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 See 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 See Article 40 of AI Act
75 See Article 41 of AI Act
76 Regulation 2022/0272 (CRA).
77 See Article 8 of Regulation 2022/0272 (CRA).
78 Essential cybersecurity requirements are in Article 10 and Annex I of Regulation 2022/0272 (CRA).

If those high-risk AI systems fulfil the CRA's cybersecurity essential requirements, they should be deemed compliant with the cybersecurity requirements set out in Article 15 of the AI Act, as long as those requirements are covered by the EU declaration of conformity issued under the CRA.[79]

Moreover, the **CRA clearly states that the AI Act is the reference act and that the AI Act's conformity assessment procedures are the ones to be followed**. In addition, the CRA clarifies that AI Notified Bodies under the AI Act can also control the conformity of high-risk AI systems with the CRA essential requirements.[80] However, there is an exception to this: if a high-risk AI system also falls under the CRA's scope as a 'critical product with digital elements' and to which internal control of the AI Act applies, then the conformity assessment to follow is the one under the CRA insofar as the essential cybersecurity requirements are concerned. The other aspects of the product can still follow the AI Act's internal control procedure. The reason behind this is that 'critical products with digital elements' create greater cybersecurity risks and, therefore, the conformity assessment should always involve a third-party conformity assessment body.

Finally, something important to mention is that high-risk AI providers also need to comply with accessibility requirements, including the EU directives 2016/2102 and 2019/882. The AI Act intends to ensure equal access to technology for all persons with disabilities. Therefore, AI providers will need to ensure compliance with these requirements by design.

All the above points have shown that, before placing in the EU market or putting into service a high-risk AI system, AI providers will need to consider multiple horizontal and sector-specific laws if they want to guarantee a holistic compliance of their products to EU law. Despite the contradictions and overlaps between the AI Act and other horizontal and sectorial laws, it is expected that the Commission will perform an in-depth gap analysis where it will provide clarification about the relationship between those laws.

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

Requirements & Obligations

For AI systems falling under the high-risk classification, there are stringent requirements. **The legal act does not specify how to fulfill its requirements at technical level –** therefore, the AI Act will be supported by a series of technical specifications produced by European Standardization Organizations (ESOs)[81] following a mandate by the Commission. The standards will translate the AI Act's requirements into actionable steps. Although these standards are not mandatory, AI providers that follow harmonized standards adopted by CEN/CENELEC will benefit from the "presumption of conformity" with the AI Act. There are still a greater number of AI-specific standards under development.

The AI Act lists requirements for high-risk AI systems in Chapter III, Section 2 (articles 9 to 15). **Compliance with the requirements should take into account the AI system's intended purpose and what is generally acknowledged as State of the Art (SotA).** Table 1 provides a high level summary of Chapter III requirements.

SotA is not a well-defined term, neither in the AI Act nor under other relevant NLF legislations. However, we can find multiple references to the SotA in the AI Act – harmonized standards, common specifications, technical standards, and codes of practice.[82]

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

Table 1: High-risk AI systems requirements[83]

Requirement	Summary
Risk management (RM) system	**The RM system planned and run throughout the entire lifecycle shall comprise of:** • Identification and analysis of the known and foreseeable risks to health, safety, or fundamental rights. • Evaluation of risks, including the analysis of data gathered from the post-market monitoring system. • Adoption of appropriate and targeted RM measures. Most appropriate RM measures shall reduce risks as far as technically feasible, with a view to minimizing risks effectively so that each residual risk as well as the overall residual risk are acceptable, considering the context and the deployer's technical knowledge, experience, education, and training. Specific considerations are made for vulnerable persons and those under the age of 18.
Data and data governance	**Data governance practices shall concern:** • Design choices. • Data collection processes and the original purpose of data collection. • Data-preparation processing operations such as annotation, labelling, cleaning, updating, enrichment, and aggregation. • Relevant assumptions on information that the data are supposed to measure. • Prior assessment of the availability, quantity, and suitability of the needed datasets. • Biases affecting health and safety or leading to discrimination. • Being free of errors and complete, to the best extent possible. **Training, validation and testing data sets shall:** • To the best extent possible free of errors and complete, and having the appropriate statistical properties at the level of individual data sets (or a combination thereof), including in regards to the persons or groups on which the system is intended to be used. • Take into account the intended purpose, the characteristics, or the elements that are particular to the specific geographical, behavioral, or functional setting within which the system is intended to be used.

83 See chapter III, Section 2 of AI Act

Requirement	Summary
Technical documentation	**Technical documentation shall:** • Be drawn up before placing on the market or put into service and shall be kept up-to date. • Provide national competent authorities and notified bodies with all the necessary information in a clear and comprehensive form to assess the compliance of the AI system with requirements. • Contain, at a minimum, the elements set out in Annex IV (amendable by Commission's delegated acts). In the case of small and medium-sized enterprises (SMEs), including start-ups, any equivalent documentation should meet the same objectives, unless deemed inappropriate by the competent authority. Where a high-risk AI system is placed on the market or put into service, one single technical document shall be drawn up containing all the information required under those legal acts listed in Annex I. Annex IV describes the required content of the technical documentation.
Record-keeping	**AI systems shall technically allow for the automatic recording of events ('logs') over their lifecycle. Logging capabilities shall enable:** • The recording of events relevant for identification of situations that may result in risks to health or safety or fundamental rights of persons. • Post-market monitoring. • Monitoring of the operations. • Recording of each use period of the system. • The reference database against which input data has been checked by the system. • The input data for which the search has led to a match. • The identification of the natural persons involved in the verification of results.
Transparency and provision of information to deployers	AI systems shall be designed and developed to ensure sufficiently transparent operation, achieving compliance with the relevant obligations, and enabling deployers to understand and use the system appropriately. It shall be accompanied by instructions for use (IFU) in an appropriate digital format or otherwise including concise, complete, correct, and clear information, which is relevant, accessible, and comprehensible to deployers.

Requirement	Summary
Human oversight	AI systems shall be designed to be effectively overseen by natural persons, aiming at preventing or minimizing the risks to health, safety, or fundamental rights. Human oversight shall be ensured through “pre” built-in measures (by the provider) and “post” measures (identified by the provider, but implemented by the user), and be enabled to understand capacities and limitations, automation bias, the system’s output, as well a the ability to override or reverse the output and interrupt the system. For remote biometric identification systems, two natural persons separate verification and confirmation is required.
Accuracy, robustness and cybersecurity	AI systems shall be designed and developed to achieve an appropriate level of accuracy, robustness, and cybersecurity, and to perform consistently in those respects throughout their lifecycle. Levels of accuracy and accuracy metrics shall be declared in instructions for use. High-risk AI systems shall be resilient as regards errors, faults, or inconsistencies due to their interaction with natural persons or other systems. The robustness may be achieved through technical redundancy solutions (backup or fail-safe plans). Learning AI systems shall be developed to eliminate or reduce as far as possible the risk of possibly biased outputs influencing input for future operations (‘feedback loops’). Appropriate cybersecurity solutions to address AI specific vulnerabilities shall include measures to prevent and control for attacks trying to manipulate the training dataset (‘data poisoning’), inputs designed to cause the model to make a mistake (‘adversarial examples’), or model flaws.

The AI Act goes further than other NLF legislations, as it details obligations not only for economic operators (e.g., providers, importers, distributors), but also obligations for deployers, providers, and deployers of certain AI systems (Chapter IV), providers of GPAI models (Chapter V, Section 2) and GPAI models with systemic risk (Chapter V, Section 3). These obligations are detailed in Table 2.

Table 2: AI Act obligations

Obligations per economic operators	Summary
Obligations of providers of high-risk AI systems[84]	Providers shall ensure compliance with AI Act requirements, indicate in the AI system the provider information, comply with Article 17 (QMS), keep Article 18 documentation available for 10 years, keep automatic generated logs for at least six months, follow appropriate conformity assessment procedures, comply with registration obligations (Article 49), affix CE and draw up an EU declaration of conformity, ensure compliance with accessibility requirements, and investigate and inform non-conformities and corrective actions to appropriate stakeholders.
Authorized representatives of providers of high-risk AI systems[85]	European Union providers shall mandate authorized representatives for specific tasks - namely, an EU declaration of conformity and technical documentation verification, keeping the prementioned plus the issued certificate and providing contact details for 10 years, provide national competent authorities with documentation and access to logs, cooperating to reduce/mitigate risks, and where applicable complying with registration obligations.
Obligations of importers[86]	Importers shall ensure their systems are in conformity with the AI Act, verifying that a conformity assessment according to Article 43 has been carried out, technical documentation, CE marking, EU declaration and IFUs are in place, and that the authorized representative is assigned. Packaging or documentations should indicate the importer's details. Importers should cooperate with national competent authorities and keep the relevant documentation for 10 years.
Obligations of distributors[87]	Distributors shall verify the required CE marking, EU declaration of conformity and instruction of use, and that provider and importer have complied with their obligations. They shall inform providers or importers of risks to the health or safety or to fundamental rights of persons, take the corrective actions necessary to bring system into conformity or ensure provider, importer or, operator do, and inform national competent authorities of the non-compliance or any corrective actions taken. Distributors shall cooperate and provide national competent authorities, upon reasoned request, information and documentation.

84 See Article 16 of AI Act
85 See Article 22 of AI Act
86 See Article 23 of AI Act
87 See Article 24 of AI Act

Obligations per economic operators	Summary
Obligations of deployers of high-risk AI systems[88]	Deployers shall use the system in accordance with the instructions of use, assign human oversight to natural persons with the necessary competence, training, and authority, and ensure input data is relevant and sufficiently representative. They shall inform the provider or distributor in case of risks or serious incidents and interrupt the use of the system, fulfill rules on internal governance arrangements, processes, and mechanisms pursuant to the relevant financial service legislation in case of financial institutions, and keep logs for at least six months. They are required to comply with the registration obligations, carry out data protection impact assessment (GDPR) and cooperate with national competent authorities.
Transparency obligations for providers and deployers of certain AI systems[89]	AI systems intended to interact directly with natural persons, should be designed to inform interaction with AI, unless this is obvious. Obligations are not applicable to AI systems authorized by law to detect, prevent, investigate, or prosecute criminal offences. AI systems, generating synthetic audio, image, video, or text content shall ensure outputs are marked as AI generated or manipulated. Deployers of an emotion recognition or biometric categorization system, excluding systems permitted by law to detect, prevent, or investigate criminal offences shall inform the natural person on the exposure to the system.
Obligations for providers of general-purpose AI models[90]	Providers of GPAI models, other than those which are free & open license, should draw and maintain technical documentation according to Annex XI, and draw up information/documentation to be provided to other AI system providers intending to integrate the GPAI model into their system.
Obligations for providers of general-purpose AI models with systemic risk[91]	In addition to GPAI providers obligations, systemic risk GPAI providers need to perform model evaluation including adversarial testing, assessing & mitigating systemic risks at the EU level, reporting appropriate incidents, and ensurng cybersecurity protection of the model and the physical infrastructure.

Any distributor, importer, deployer or other third-party that makes a substantial modification of a high-risk AI system OR changes the intended purpose of a non-high risk AI turning it into a high risk one, it will be considered the provider and will be subject to the AI Act providers' obligations.[92]

88 See Article 26 of AI Act
89 See Article 50 of AI Act
90 See Article 53 of AI Act
91 See Article 55 of AI Act
92 See Article 25 of AI Act

AI Act ecosystem

The AI Act's regulatory framework introduces a structured ecosystem of entities entrusted with the assessment, certification, and oversight of AI systems. **This framework aims to harmonize approaches, ensuring the safe and ethical deployment of AI systems.** To unpack this regulatory landscape, we explain and clarifying the definitions of the involved stakeholders:

National Level	**Conformity Assessment Body (CAB):**[93] A separate legal entity that performs third-party conformity assessment activities including testing, certification, and inspection. The primary objective of a CAB is to ascertain that AI systems meet requirements of the relevant applicable standards.
	Notified Body (NB):[94] A specialized form of CABs, NBs undergo formal notification in accordance with the EU AI Act and relevant EU harmonization legislation. Their tasks include conducting conformity assessment activities for high-risk AI systems, adhering to organizational, quality management, resource, process, and cybersecurity requirements. NBs maintain independence from evaluated AI system providers, ensuring impartiality and confidentiality. Articles 31 to 34 of the EU AI Act delineate specific obligations and operational criteria for NBs.
	Notifying Authority (NA):[95] Designated within each Member State, NAs manage the procedural framework for assessing, designating, and notifying CABs, alongside ongoing supervision. Operating under a mandate to prevent conflicts of interest, NAs uphold principles of objectivity and impartiality. They are structured to separate decision-making from assessment activities, explicitly prohibiting any commercial or competitive offerings. NAs ensure their personnel are highly qualified in relevant fields, including information technologies, artificial intelligence, and law.
	Market Surveillance Authority (MSA):[96] Designated as the national authority responsible for overseeing market activities to ensure compliance with legal requirements, particularly for high-risk AI systems. They enforce the regulation by monitoring, identifying non-compliance, and oversight of the corrective actions implemented by the AI providers to protect public interests, health, safety, and fundamental rights.
	National Competent Authority (NCA):[97] It includes the NA and the MSA. It represents the authoritative entities designated by EU member states to oversee the regulation and compliance of AI systems within their jurisdictions, focusing on ensuring the safety, security, and rights compliance of AI technologies.
EU Level	**Artificial Intelligence Office (AIO):**[98] An office within the European Commission tasked with monitoring and supervising AI systems, general-purpose AI models, and AI governance. The AIO plays a central role in fostering a coherent regulatory framework for AI across the EU, ensuring compliance with legislative mandates, facilitating enforcement, and overseeing AI governance to safeguard public interest and uphold standards.
	European Artificial Intelligence Board (AIB):[99] An advisory and coordinating body established to support the consistent and effective application of the AI Act across the EU. It functions to enhance cooperation among national competent authorities tasked with the Regulation's enforcement, share technical and regulatory expertise, and promote best practices among Member States.

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

The AI Act lists the responsibilities of Notified Bodies (NBs):[100]

01. Conformity Assessment[101]:

- NBs, or CABs acting on their behalf, impartially evaluate the quality management system (AI management system)[102] implemented by the provider of a high-risk AI system and the technical documentation[103], submitted by that provider. These assessments aim to verify compliance with the AI Act's harmonized standards and common specifications, focusing on applicable requirements. Each assessment is completed with an audit report[104] detailing the outcomes, identifying areas of compliance, and highlighting non-compliant areas (so-called "non-conformities") with the AI Act's regulatory framework.

- NBs are granted necessary and relevant access to the training, validation, and testing datasets utilized by AI systems, potentially through application programming interfaces (APIs) or other mechanisms facilitating remote access, underpinned by adequate security safeguards. NBs are also granted access to the training and trained models of the AI system, including relevant parameters (e.g., weights, architecture), after alternative conformity verification methods and finding them inadequate. NBs must conduct direct testing if they find the tests provided by the high-risk AI system provider inadequate.[105]

02. Issuance of Certificates:[106]

- Upon successful conformity assessment, NBs issue certificates to AI system providers, signifying compliance with the AI Act and associated requirements.

03. Continuous Monitoring and Surveillance:[107]

- Following a successful conformity assessment, NBs undertake ongoing surveillance of EU conformity certificates issued to AI system providers. This surveillance focuses on ensuring continual compliance with the AI Act and includes regular audits of quality management system to verify continuous compliance with applicable regulatory and technical requirements (harmonized standards, common specifications, and industry practices, in the absence of harmonized standards and common specifications).

- NBs must be informed by providers of high-risk AI systems of any proposed changes to the AI management system or AI system itself[108] that could impact compliance (and/or intended purpose) and NBs review the relevant documentation to approve changes where compliance is maintained.

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

04. Cooperation among Notified Bodies:

- NBs communicate with other NBs regarding any refusals, suspensions, or withdrawals of quality management system or EU technical documentation approvals. **Additionally, upon request, the NB must provide information regarding quality system approvals it has issued.**[109]

05. Documentation and Reporting:

- NBs maintain records and associated evidence of all assessments, decisions, and certifications, which are made accessible to NCAs for oversight purposes.[110]

The key responsibilities of NCAs[111] within the regulatory framework under the AI Act entail diverse roles essential for ensuring effective governance and oversight of the national-level implementation of the AI Act:

01. Regulatory Oversight:

- NCAs can request and review documentation from providers of non-high risk AI systems and general-purpose AI models (GPAI), ensuring transparency and compliance with AI Act regulatory requirements.[112] NCAs also request technical documentation from providers of high-risks AI systems (when the NB is not involved).[113]

- NCAs may support the provision of high-quality data for AI system training, which aims to support innovations, as well as the transparency and reliability of the data framework.[114]

- NCAs serve as primary points of contact, facilitating communication, regulatory, and technical compliance.[115]

- NCAs support the European Commission and exchange information between NCAs.[116]

02. Support for Innovations:

- NCAs establish national-level AI regulatory sandboxes to foster innovation and enable testing of AI systems and inform the AIO about the progress. Collaboration between NCAs, the AIO, and other relevant authorities facilitates knowledge exchange and best practices dissemination.[117]

- NCAs can offer SMEs and startups guidance on the AI Act, aligned with the Board and Commission position. For AI systems under other EU laws, relevant authorities must be consulted.[118]

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

03. Enforcement Actions:[119]

- NCAs (specifically MSA) are responsible for oversight of corrective actions implemented by the AI model providers to address incidents with involved AI systems, issuing warnings, imposing fines, and mandating compliance measures to uphold regulatory integrity. NCAs also act as the single point of contact.

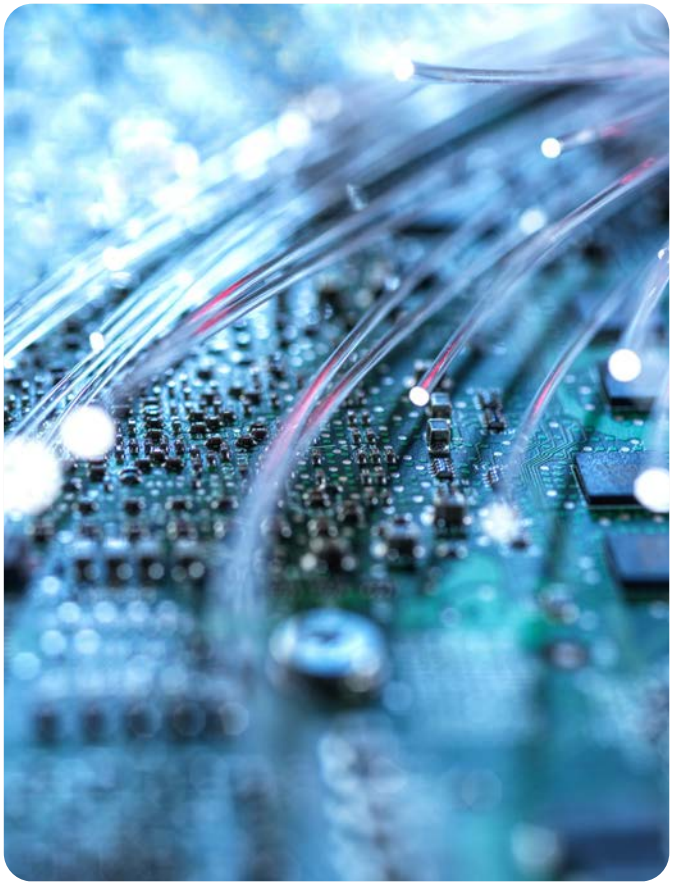
04. Designation, Monitoring, and Coordination of Notified Bodies (NBs):[120]

- NCAs designate NBs and ensure their qualifications comply with the AI Act's requirements for conducting conformity assessments. NCAs monitor and audit NBs, ensuring their compliance with the AI Act's requirements, which include the maintenance of competence, impartiality, and other legal, regulatory, and technical requirements applicable to the NBs[121].

The essential duties of the AIO within the regulatory framework established by the AI Act and its official website[122] **are outlined as follows:**

01. Central Coordination, Governance, and Oversight of GPAI:

- The AIO serves as the central coordinating body among EU member states, providing guidance and support for consistent AI Act implementation. It facilitates best practice exchange and ensures alignment across the EU. The AIO leverages its expertise in establishing EU-level advisory bodies (such as the Artificial Intelligence Board) fostering collaboration to ensure coherent AI Act application across all Member States.[123]



- The AIO supervises GPAI (requirements for providers, authorized representatives, deployers) to ensure compliance with the AI Act, standards, and associated requirements. **It develops tools, methodologies, and benchmarks for evaluating the capabilities and reach of GPAI models, classifying models with systemic risks.** The AIO also provides oversight of corrective actions taken by GPAI provider in case of non-compliance. The AIO has the power to request documentation and information from the GPAI provider and its authorized representatives, conduct evaluation of GPAI-models and request measures (including to restrict making GPAI available on the market, or to withdraw or recall the model). It also monitors fulfilment of obligations by the providers of GPAI.[124]

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

- **The AIO provides coordination support for joint investigations in case of market surveillance with involvement of specific categories of high-risk AI system(s), supervises and monitors the compliance of GPAI,** as well as taking necessary action(s) to monitor effective implementation and continuing compliance for providers of GPAI models with the AI Act.[125]

02. Policy Development:

- The AIO provides standardized templates for the areas required by the AI Act (e.g., summary of content used for training of the GPAI, summary of the content used codes of practice, questionnaire for deployers).[126]

- The AIO advises on best practices, facilitates access to AI testing environments, and promotes innovative ecosystems to boost EU competitiveness.[127]

- The AIO ensures the regulatory framework adapts to technological advancements and societal needs by engaging with diverse stakeholders, including AI developers, SMEs, and experts. It fosters continuous dialogue to inform policy formulation and develop codes of practice aligned with the AI Act.[128]

03. Cooperation with stakeholders:

- **The AIO collaborates with a diverse range of stakeholders, such as NCAs, providers of GPAI, scientific panels** (including independent experts), institutions, the European Artificial Intelligence Board, and the European Centre for Algorithmic Transparency (ECAT), to gather and share technical and regulatory expertise, including knowledge gathered from the establishment, running, and oversight of AI sandbox.[129]

The European Artificial Intelligence Board[130] plays a major role in robust oversight and the application of the AI Act by the Commission and Member states. It achieves this through several key activities:

1 Facilitating coordination among NCAs responsible for enforcing the AI Act and endorsing joint market surveillance activities.[131]

2 Maintaining technical expertise and best practices across EU Member States, as well as contributing to a cohesive understanding and application of the AI Act.

3 Delivering strategic advice on the regulation's enforcement, focusing on GPAI models and aiming to standardize approaches and interpretations.

4 Emphasizing the importance of consistent conformity assessments, the effective use of regulatory sandboxes, and the value of testing AI systems in real-world scenarios.

5 Playing a critical role in advising on the regulation's implementation and offering recommendations on various fronts including codes of conduct, the evolution of AI standards, and the integration of emerging technologies.

6 Engaging in broad educational efforts to boost AI literacy and fostering the public's awareness of AI's benefits and risks, while facilitating cross-sectoral and international cooperation to enhance the regulation's global relevance and effectiveness.

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

AI Act timelines

The development process of the AI Act has been characterized by significant complexity and anticipation over the past several months, as this period was fraught by a series of strategic discussions, uncertainties, and widespread speculations regarding the outcome. Nevertheless, the legislative journey succeeded with the final political agreement and the adoption of the Act on 13th March 2024. This result indicates a procedural timeline which is anticipated to take approximately up to two months for the formal publication of the legislation in the Official Journal of the EU. The legislation's entry into force, the significant milestone for the new AI Act, will be twenty days after its publication in the Official Journal.

To operate within the timelines in practical perspective, we analysed associated key milestones and relevant actions to be completed. The results of this analysis are presented in *Table 3*.

Table 3 – Key timelines of the AI Act implementation

Timeline	Relevant Action
13 March 2024	• Adoption on the EU Artificial Intelligence Act in the European Parliament's plenary.
22–25 April 2024	• Approval of the AI Act corrigenda in the plenary of the parliament
Entry into force[132] **1 August 2024**	• 20 days after publication in the Official Journal of the EU.
Entry into force + Three months[133] **2 November 2024**	• Member States must list, publish, and keep up to date list of public authorities and/or bodies.
Entry into force + Six months[134] **2 February 2025**	• Date of application for prohibited AI systems to be available on the market (Chapter II) • Date of application of general provisions (Chapter I)
Entry into force + Nine months[135] **2 May 2025**	• Readiness of codes of practices to be published by the AIO.
Entry into force + 12 months **2 August 2025**	• Chapter III (High-Risk AI Systems) Section 4, Chapter V (GPAI Models), Chapter VII, and Chapter XII, except Article 101.[136] • If the AI Office finds the code of practice insufficient or unfinalized 12 months after Entry into Force, the Commission, via implementing acts, may establish common rules for obligations in Articles 53 and 55, aligning with the examination process of Article 98(2).[137] • Member states to have implemented rules on penalties, including administrative fines.[138] • Readiness of NBs and governance structure, including conformity assessments.[139] • If no code of practice is finalized within 12 months after entry into force, or if deemed inadequate by the AIO, the Commission may issue implementing acts for Articles 53 and 55 obligations, following Article 98(2)'s examination procedure.[140] • Member States must inform the Commission of NAs and MSAs, including their tasks, and provide publicly accessible information on how NCAs (in a form of single point contact) can be contacted.[141] • The Commission will provide guidance for high-risk AI system providers to comply with obligations of reporting of serious incidents to MSAs.[142] • Member States must inform the Commission about their NCA's financial and human resources, assessing their sufficiency, with this being repeated every two years afterwards. The Commission will share this data with the AI Board for analysis and potential advice.[143] • Following the entry into force and until the delegated powers in Article 97 expire, the Commission is tasked with annually evaluating the necessity for updates to Annex III's list and Article 5's catalogue of banned AI practices. The outcomes of these assessments will be systematically presented to both the European Parliament and the Council.[144]

132 See Article 113 of AI Act
133 See Article 77 of AI Act
134 See Article 113 of AI Act
135 See Recital 179 and Article 56, Section 9 of AI Act
136 See Recital 179 and Article 113 of AI Act
137 See Article 56, Section 9 of AI Act
138 See Recital 179 of AI Act
139 See Recital 179 of AI Act
140 See Article 56 of AI Act
141 See Article 70, 59 of AI Act
142 See Article 73 of AI Act
143 See Article 70 of AI Act
144 See Article 112 of AI Act

Timeline	Relevant Action
Entry into force + 18 months **2 February 2026**	• The Commission, as well as the consulting AI Board, are to provide guidelines for the AI Act's entry, including examples of high/non-high risk AI use cases as required by Article 96.[145]
Entry into force + 24 months **2 August 2026**	• Application of the AI Act, which includes obligations on high-risk AI systems specifically listed in Annex III, inlcuding AI systems in biometrics, critical infrastructure, education, employment, access to essential public services, law enforcement, immigration, and the administration of justice to comply with the AI Act. It applies when significant design changes occur from that timeframe, aligning with Article 5 under Article 113(3)(a).[146] • Member States are mandated to create at least one national AI regulatory sandbox. Implementation of this requirement can be a collaborative effort among different Member States. The EU Commission offers support for sandbox development and operation. States may also join existing sandboxes, provided they ensure equivalent national coverage.[147]
Entry into force + 36 months **2 August 2027**	• Applicability of Article 6(1) (classification rules for Annex I Union harmonization legislation) and correlated obligations of the AI Act.[148] • GPAI model providers with products placed on the EU market 12 months prior to the AI Act's entry into force are required to undertake essential measures to meet the relevant obligations of GPAI model providers.[149]
Entry into force + 48 months[150] **2 August 2028**	• Every 48 months starting from the AI Act's entry into force, the Commission will analyse and inform the European Parliament and Council on potential amendments to Annex III, Article 50's AI system transparency requirements, and improvements to supervisory and governance frameworks. • Every 48 months from the AI Act's entry into force, the Commission will report its evaluation to the Parliament and Council, focusing on enforcement structure and the potential for an EU agency to address gaps. Amendments may be proposed based on these insights. All reports shall be made publicly available. • The Commission will assess the AI Office's performance, examining if it possesses adequate powers and competences for its duties, and if needed enhancing its role and enforcement capabilities, along with increasing its resources. The evaluation report will be submitted to the European Parliament and Council. • Every 48 months from the AI Act's entry into force, the Commission reports on the advancement of standardisation in energy-efficient development of general-purpose models. This includes assessing the necessity for additional measures, which are potentially binding. The final evaluation report will be submitted to the European Parliament and the Council and made publicly available. • The Commission is mandated to assess the influence and efficacy of voluntary codes of conduct every three years afterwards. These evaluations are aimed to optimize adoption of Chapter II, Section 2's requirements for providers of AI systems not classified as high-risk and to explore the potential for integrating additional mandates, notably concerning environmental sustainability.[151]
Entry into force + 60 months[152] **2 August 2029**	• The Commission is tasked with conducting a review of the AI Act, at intervals of four years and to report the findings to the European Parliament and the Council. An annual assessment is to be provided by the Commission to evaluate potential revisions to the lists of high-risk AI systems and prohibited practices.
Entry into force + 72 months **2 August 2030**	• Providers and deployers of high-risk AI systems designated for public authority use shall comply with AI Act's requirements.[153]

145 See Article 6 of AI Act
146 See Articles 111 and 113 of AI Act
147 See Article 57 of AI Act
148 See Article 113 of AI Act
149 See Article 111 of AI Act
150 See Article 112 of AI Act
151 See Recital 174 of AI Act
152 See Recital 174 of AI Act
153 See Article 111 of AI Act

Timeline	Relevant Action
31 December 2030	• AI systems integrated within large-scale IT frameworks, as specified in Annex X, and operational 36 months before the AI Act's entry into force must comply with the AI Act. Evaluations of these large-scale IT systems, mandated by the legal acts in Annex X, will incorporate the AI Act's requirements, especially when these acts undergo revisions or updates.[154]
Entry into force + 84 months[155] **2 August 2031**	• The Commission is required to execute an assessment of its enforcement. This analysis will be reported to the European Parliament, the Council, and the European Economic and Social Committee, reflecting on the initial years of the AI Act's application. Based on findings, if and when necessary, the final report shall be accompanied by a proposal for AI Act's amendment regarding the structure of enforcement and changes needed to be implemented by the EU agency to resolve any identified negative findings.

154 See Article 111 of AI Act
155 See Article 112, Section 13 of AI Act

AI products already on the market

The AI Act introduces the term "substantial modification", referring to a change to an AI system already placed on the market or put into service which is not foreseen in the initial conformity, and may affect compliance or modify its intended purpose.[156] **The AI Act also introduces the term "predetermined changes", a term used to describe predefined changes subject to an initial conformity assessment** of AI systems which are not static but continue to learn or evolve following placement on the market.[157]

For high-risk AI systems that have been placed on the market prior to the application of the AI Act, the AI Act applies only if following the AI Act's application date there are significant changes in the design or intended purpose. Furthermore, the AI Act makes no distinction for the prementioned purpose between the terms "significant change" and "substantial modifications". [158]

The AI Act makes an exemption for AI systems which are components of the large-scale IT systems and high-risk AI systems intended to be used by public authorities – compliance of those systems with the AI Act requirements is required by end of 2030, or by six years after the entry into force.

However, it is not immediately clear when a high-risk AI system falls under another EU legislation – as in the case of Annex I section A products – which legislation prevails in terms of substantial modifications. The answer to this question can be found in the recitals of the AI Act.[159] If a change is not considered significant under a more specific EU legislation (e.g., Regulation 2017/745 MDR), then the change should not trigger substantial modification under the relevant clauses of the AI Act.

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

Understanding AI Act conformity

The AI Act brings scrutiny also to sectors that were not previously subject to regulation. Due to its horizontal nature and levels of risk, the AI Act has different obligations for AI providers and deployers to ensure conformity of AI systems. The principal mechanisms of compliance within the AI Act are:

The use of a quality management system (QMS):[160] Although the recently published standard ISO/IEC 42001:2023 Information Technology Artificial Intelligence Management System (AIMS) is not yet harmonized with the AI Act, it is expected to be the reference standard for conformity with the relevant requirements. The AIMS should cover a strategy for compliance, processes on design, development, data governance, testing and validation of AI systems, risk management, post-market monitoring, and incident reporting. Providers and deployers of high-risk AI systems are obliged to use AIMS, with this also being an obligation for AI providers that are required to follow conformity routes stated in Annex VI (internal control) and Annex VII (assessment of QMS and Technical Documentation). When AI systems are subject to obligations for a QMS under other sectorial EU legislations, AIMS aspects may be covered as part of the sectorial QMS standard.

The creation and maintenance of technical documentation:[161] High-risk AI systems that may follow the conformity routes of Annex VI (internal control) and Annex VII (assessment of QMS and technical documentation (TD)), and providers of general-purpose AI models, will require putting in place TD for assessing compliance with the AI Act Chapter III, Section 2 requirements. Annex XI (TD for providers of general-purpose AI models, Article 53(1))) and Annex IV (TD referred to in Article 11(1)), describe the content of the TD. TD will need to be drawn up before placing the AI system on the market. When the AI system is subject to obligations of TD under other sectorial EU legislations, AI Act aspects may be covered as part of the sectorial TD.

Conformity with high-risk AI system requirements:[162] Chapter III, Section 2, lists high-risk AI systems requirements. Although the ISO/IEC JTC 1/SC 42 committee has already published multiple standards, none has as of yet been harmonized with the AI Act. The legislation clearly states (Article 40) that conformity with the AI Act's harmonized standards is a presumption of conformity with AI Act requirements.

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

Transparency obligations:[163] Providers of AI systems, including general-purpose AI systems, as well as deployers of certain AI systems, need to comply with transparency obligations set in Chapter IV, Article 50.

Sandboxes:[164] Sandboxes are established by members states, competent authorities. Sandboxes are controlled environments to facilitate development, training, testing, and validation of innovative AI systems. AI systems might use sandboxes prior to being placed on the market or put into service. The output (exit reports) of the sandboxes may be used to demonstrate compliance with the AI Act, as part of documentation provided for the conformity assessment process, or provided to relevant market surveillance authorities.

Routes to conformity:[165]

- When a high-risk AI system is subject to other sectorial EU legislations (Annex I, section A) the provider shall follow the relevant conformity assessment procedure as required under those legal acts. Requirements set out in the AI Act apply to these AI systems, and Notified Bodies may request datasets and the AI model for carrying out additional testing (Annex VII).

- Internal control (Annex VI) is available as a conformity assessment route to Annex III high-risk AI systems, however, Annex III point 1 AI systems (Biometric identification) may opt for (or be forced to follow) Annex VII conformity assessments which require the Notified Body's involvement for the assessment of AIMS and TD.

General-purpose AI (GPAI) models: The main oversight authority for GPAIs is the AI Office. Article 53 states obligations for GPAI providers and Annex XI describes technical documentation requirements for GPAIs models. Obligations are not applicable for free and open-license providers. There are additional obligations for GPAI models with systemic risks, including model performance evaluation, mitigation measures of systemic risks, and cybersecurity protection.[166] Compliance with codes of practice[167] will be considered sufficient for GPAIs systemic risk obligations, until harmonized standards are released.

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

Conclusion

The AI Act is en route to the Official Journal of the European Union, and the world is watching. What started out as conjecture has evolved into an emerging and impactful industry, not without its risks. It is evident in the legislative text that not one person or one group of persons can manage this new landscape on its own. It will take the collective effort of providers, deployers, the Commission, the AI Office, the AI Board, member states, National Competent Authorities, the public, and others to ensure the predictability and deployment of these systems is effectively controlled.

The momentum of the AI Act has left many wondering what the next steps are to prepare themselves for its impact. We anticipate that this paper will support organizations to take the firsts steps to determine if and how AI systems or models affect their organization, identifying the organization's role and obligations, supporting understanding of AI systems classification, and shedding light on the requirements need to be fulfilled, as well as the methods those requirements are met. Organizations should be able to understand conformity routes for their products, allowing them to proactively seek accredited or designated organizations under the schemes of interest to consolidate assessments where possible.

The AI Act encourages providers of high-risk AI systems to start the compliance journey on a voluntary basis during the transitional period.[168] BSI shares this view; all stakeholders will face a steep learning curve. BSI deeply values the AI Act and the approach adopted by the community engaged in the development of this regulation, recognizing that the publishing of the AI Act by legislators and achieving compliance are not end goals. Instead, they represent a journey of ongoing enhancement of the regulatory framework, evolving in tandem with technological advancements.

168 See Recital 178 of AI Act