Artificial Intelligence Act (AI Act)

Contents

1. Description

The Artificial Intelligence Act, also known as AI Act, is an AI law by the European Union. The Act was proposed by the European Commission on April 21, 2021 with an aim to establish a unified regulatory and legal framework for all sectors and types of artificial intelligence. The AI Act adopts a risk-based approach where the obligations for a system are proportionate to the level of risk that the system poses.

The Act distinguishes the following categories of systems:

Unacceptable systems that are prohibited in the EU.

High-risk systems that are subject to stricter obligations and conformity assessment requirements.

Generative AI and general-purpose models are subject to transparency requirements and compliance with copyright law, with the exception of high-impact general-purpose AI models that might pose systemic risk. Such systems must undergo thorough risk assessment, incident reporting, testing and evaluation, ensure cybersecurity and provide information on energy consumption.

Providers of AI systems that interact with natural persons or create synthetic content, and deployers of emotion recognition, biometric categorisation, deepfake systems, as well as certain AI systems manipulating text are subject to transparency obligations.

The AI Act is currently in its final phase, the trilogues have been concluded, and political agreement has been made. The final version of the AI Act is expected to be published in early 2024. The AI Act will transition in the following stages:

The ban on prohibited AI practices apply after 6 months of the AI Act coming into force.

Obligations concerning general-purpose AI models apply after 12 months of the AI Act coming into force.

Requirements and obligations concerning providers of standalone high-risk systems listed in Annex III apply 24 months after the AI Act comes into force.

Transparency obligations of providers of AI systems that interact with natural persons or create synthetic content, and deployers of emotion recognition, biometric categorisation, deepfake systems, as well as certain AI systems manipulating text, apply after 24 months of the AI Act coming into force.

Deployers of high-risk systems developed by third-party providers apply after 24-36 months of the AI Act coming into force.

Providers of high-risk systems subject to Union harmonisation legislation listed in Annex II apply 36 months after the AI Act comes into force.

2. Scope

The Act regulates AI systems placed or put into service in the EU market and places its main obligations on providers and deployers of AI systems. The AI Act applies to providers who place on the EU market or put into services AI systems. This means that also providers who are not established or located in the European Union can be subject to the Act if their systems are made available in the EU. Deployers who are established or located in the EU are also subject to the Act. Furthermore, it is also important to note that providers and deployers who are established or located outside the EU fall under the scope of the AI Act in case the output, outcomes, or results produced by the AI system are utilised in the EU.

Providers cover natural and legal persons, including public authorities and agencies developing AI systems to place them on the market under their name or trademark - in practical terms, these are the entities that develop an AI tool. Deployers, on the other hand, cover similar entities using AI systems under its authority, with the exception of use for personal and non-professional activities - deployers are the entities that buy and take into use the tool developed by the provider. In addition to providers and deployers to whom the majority of the obligations under AI Act are directed at, the AI Act also places certain obligations to importers, distributors, and authorised representatives of AI systems.

The Act defines an AI system as a machine-based system created to operated with different degrees of autonomy and that learns and adjusts its behaviour over time. Its purpose is to produce outputs, whether explicitly or implicitly intended, such as predictions, content, recommendations, or decisions that can have an impact on physical or virtual environments.

The AI Act's requirements do not apply to research, development, and prototyping activities before the AI system is placed on the market, taken into use. Moreover, AI systems used solely for military, defense, or national security purposes are not subject to this regulation, no matter who operates them. Lastly, creators of free and open-source AI models are mostly free from the duties that typically apply to AI system providers. However, this exemption does not cover those who provide general-purpose AI models that carry significant systemic risks - providers of such AI systems must still fulfil certain obligations.

3. Key Information

Most of the regulatory obligations in the Act are directed towards high-risk AI systems. The Act classifies certain standalone AI systems as high-risk AI systems, as well as AI systems used as safety components of products, AI systems embedded in products, or systems that are products subject to a third-party assessment under sectoral legislation. The list of standalone high-risk AI systems includes biometric identification and categorisation of natural persons, management and operation of critical infrastructure, educational or vocational training, employment, including workers management and access to self-employment, access to essential private and public services, law enforcement, migration, asylum, and border control management, as well as administration of justice and democratic processes.

The high-risk AI systems will be subject to mandatory requirements both before and after they are introduced to the market. These requirements encompass various aspects, including the development of a risk management process for identifying and mitigating risks (Art 9), the implementation of appropriate data governance and management practices (Art 10), the creation of technical documentation that facilitates the assessment of the system's compliance (Art 11), the establishment of ongoing system monitoring throughout its lifecycle (Art 12), the provision of transparency to empower users in understanding and confidently utilising the products (Art 13), the facilitation of human oversight of the system's operations (Art 14), the assurance of an adequate level of accuracy, robustness, and cybersecurity (Art 15), and the implementation of a quality management system, comprising written policies, procedures, and instructions, to ensure compliance with the regulation (Art 17). Furthermore, providers of high-risk systems are subject to conformity assessment obligations (Art. 43), post-market monitoring obligation (Art. 61) and various administrative obligations.

The AI Act also places specific obligations to providers of general purpose AI modelsand providers of general purpose AI models with systemic risks. These obligations include requirement to draft technical documentation, provide transparency to downstream AI system providers, comply with EU copyright law, as well as document and make publicly available summaries of model training data. Providers of general purpose AI models with systemic risks are subject to additional supplementary technical documentation obligations, as well as obligations concerning model evaluation and testing, risk assessment and mitigation, incident tracking, and cybersecurity.

Furthermore, general purpose AI systems, including general-purpose AI models are subject to certain transparency and information obligations with other AI systems posing transparency risk. Such system posing transparency risk cover AI systems designed to interact with natural persons, systems capable of emotion recognition or biometric categorisation, as well as systems that generate or manipulate image, audio, or video content, and deepfakes.

Lastly, all other systems not falling into the scope of unacceptable systems, high-risk systems, general purpose AI models or systems with transparency risk are categorised as minimal or no risk systems. In the AI risk-based framework, the majority of AI systems are categorised as minimal to no risk.

4. Penalties

Operators, including providers, deployers, product manufacturers, authorised representatives, importers, and distributors, can be subject to penalties under the AI Act for non-compliance with the requirements and obligations mentioned in the Act.

The relevant authorities will consider the nature and gravity of the violation and other circumstances when imposing a fine. The following non-compliance can be subject to penalties:

Non-compliance with the ban on prohibited AI practices. Such violation can be subject to fines up to 35 million EUR, or where the offender is a company, up to 7% of its total global annual turnover for the previous financial year.

Provider's non-compliance with most of their obligations (incl. requirements for high-risk AI systems, quality management system, conformity assessment, registration to EU database and other obligations) can be subject to fines up to 15 million EUR, or where the offender is a company, up to 3% of its total global annual turnover of the previous financial year.

Deployers, authorised representatives, importers, and distributors' non-compliance with most of their obligations can be subject to fines up to 15 million EUR, or where the offender is a company, up to 3% of its total global annual turnover of the previous financial year.

Non-compliance with transparency obligations of providers of AI system that interacts with natural persons or creates synthetic content, and deployers of emotion recognition, biometric categorisation, deepfake systems, as well as certain AI systems manipulating text can be subject to fines up to 15 million EUR, or where the offender is a company, up to 3% of its total global annual turnover of the previous financial year.

Non-compliance of providers of general-purpose AI models with their requirements and obligations can be subject to fines up to 15 million EUR, or where the offender is a company, up to 3% of its total global annual turnover of the previous financial year.

Provision of false, incomplete, or misleading information to notified bodies or authorities can result in a fine of up to 7.5 million EUR, or where the offender is a company, up to 1% of its total global annual turnover of the previous financial year.

5. Roles

5.1 Provider

An AI provider refers to an individual or entity, whether natural or legal, including public authorities, agencies, or other organisations, who either develops an AI system or a general-purpose AI model or commissions the development of an AI system or general-purpose AI model and places them on the market or puts it into service it under their own identity or brand, regardless of whether this is done for a fee or without charge.

Reference

AI Act, Art 3(2)

5.2 Deployer

Deployer refers to any natural or legal person, public authority, agency or other body that is using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity.

Reference

AI Act, Art. 3(4)

5.3 Importer

Importer refers to any natural or legal person established or located in the European Union that places on the market or puts into service an AI system that bears the name or trademark of a natural or legal person established outside the Union. Therefore, importer brings in an AI system from outside the EU and introduces it to the EU market.

Reference

AI Act, Art. 3(6)

5.4 Distributor

Distributor refers to any natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market.

Reference

AI Act, Art. 3(7)

5.5 Authorised representative

Refers to any natural or legal person established or located in the Union who has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to perform and carry out on behalf of the provider the obligations and procedures laid down in the AI Act to ensure that the AI system or general-purpose AI model complies with the AI Act.

Reference

AI Act, Art. 3(5)

6. Policy Coverage

6.1 Prohibited AI practices

Certain particularly harmful AI practices are prohibited as they contravene the European Union values. Such prohibited practices include AI systems that violate fundamental rights or use subliminal techniques to manipulate people. The Act also prohibits AI-based social scoring and biometric categorisation based on biometric data.

6.1.1 Systems using subliminal or purposefully manipulating or deceptive techniques

Systems using subliminal or purposefully manipulating or deceptive techniques are AI systems that employ subliminal (not noticed by the conscious mind) or intentionally manipulative and deceptive techniques with the aim of substantially altering an individual's or a group's behavior. These types of systems are prohibited from being placed on the market, put into service, or used in the EU because they impair a person's capacity to make informed decisions, decisions done knowingly and willingly, leading them to make choices they would not have otherwise made, which can result in significant harm to the individual, others, or a group.

Reference

AI Act, Art. 5(1)(a)

6.1.2 Systems exploiting vulnerabilities

AI systems that exploit vulnerabilities based on age, disability, or social or economic situations are systems that specifically target and leverage the weaknesses of individuals or groups due to their particular circumstances. These types of systems are prohibited from being placed on the market, put into service, or used in the EU because they aim or result in significantly distorting the behaviour of a person or someone associated with that group in a way that causes or is reasonably likely to result in significant harm to that person or another individual.

Reference

AI Act, Art. 5(1)(b)

6.1.3 Biometric categorisation

Biometric categorisation systems are AI systems that categorise individually people based on their biometric data to deduce or infer characteristics like race, political opinions, trade union affiliations, religious or philosophical beliefs, or details about their sex life or sexual orientation. The placing on the market, putting into service for this reason, to use of such systems in the EU is prohibited.

This prohibition does not apply to the labeling or filtering of biometric datasets obtained legally, such as images, when based on biometric data, nor does it apply to the categorisation of biometric data in the context of law enforcement activities.

Reference

AI Act, Art. 5(1)(ba)

6.1.4 Social scoring systems

Social scoring systems are AI systems that evaluate or classify individuals or groups of individuals over time. This evaluation or classification is based on their social behaviour or known, perceived or predicted personal or personality characteristics. The placement on the market, putting into service or use of such systems is prohibited in the EU where the social score provided by the systems leads to either of both of the following:

Detrimental or unfair treatment of individuals or groups in situations unrelated to where their data was initially gathered.

Detrimental or unfair treatment of individuals or groups that is unjustified or excessive compared to their actual behavior or its gravity.

Reference

AI Act, Art. 5(1)(c)

6.1.5 “Real-time” remote biometric identification systems

The use of ‘real-time’ remote biometric identification systems is prohibited in publicly accessible spaces for the purposes of law enforcement. The prohibition does not apply in situations where the use of real-time remote biometric identification is strictly necessary for one or more of the following objectives:

Targeted search of specific victims of abduction, human trafficking, sexual exploitation, and search for missing persons.

Prevention of specific, severe, and immediate threats to life, physical safety, and present and genuine, or genuine and foreseeable threat of terrorist attack.

Localisation or identification of suspects in serious crimes for investigation, prosecution, or execution of criminal penalty for offences referred to in Annex IIa.

Reference

AI Act, Art. 5(1)(d)

6.1.6 Predictive policing systems

Predictive policing systems are AI systems that make risk assessments of individuals with the purpose of assessing or predicting the risk of an individual committing a criminal offence. Such assessment or prediction is based solely on profiling of an individual or assessing their personality traits or characteristics. The placing on the market, putting into service for this specific purpose, and use of such systems is prohibited in the EU.

The prohibition does not apply to AI systems that assist human assessment of a person's involvement in a criminal activity, provided the assessment is grounded in objective and verified facts directly related to the criminal activity.

Reference

AI Act, Art. 5(1)(da)

6.1.7 Creating or expanding facial recognition databases through untargeted scraping of facial images

The placement in the market, putting into service for this specific purpose, or use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage is prohibited.

Reference

AI Act, Art. 5(1)(db)

6.1.8 Emotion recognition systems

The placement in the market, putting into service for this specific purpose or use of AI systems that infer the emotions of natural persons is prohibited, where such systems are used in workplaces or education institutions.

The prohibition does not apply where the emotion recognition system is intended to be put into place or into the market for medical or safety reasons.

Reference

AI Act, Art. 5(1)(dc)

6.1.9 Prohibitions coming from infringements of other Union law

In addition to the prohibitions listed in the AI Act, also AI practices that violate other Union law are prohibited.

Reference

AI Act, Art 5(1a)

6.2 High-risk

Certain AI systems that negatively affect safety or fundamental rights are considered high risk. High-risk systems are subject to various obligations under the AI Act and are required to undergo conformity assessment. Such high-risk systems include two different types of systems:

AI systems that are intended to be used as a safety component of a product, or the AI system is itself a product that falls under European Union's harminosation legislation.

AI systems that fall into specific areas listed in the AI Act.

AI systems are not considered high-risk if they do not pose a significant risk of harm to the health, safety, or fundamental rights of individuals and do not significantly impact decision-making outcomes. This exemption applies when any of the following criteria are met:

The AI system is intended to perform a limited procedural task.

The AI system aims to enhance the outcome of a task already performed by humans.

The AI system is intended to identify patterns or changes in decision-making but is not intended to override or sway the earlier human evaluation without appropriate human oversight.

The AI system is designed to carry out a preparatory task related to an assessment important for the use cases outlined in Annex III.

AI systems that perform profiling of natural persons are always considered high risk and the above exemptions do not apply to such systems.

6.2.1 Machinery and related components

AI systems that are products or are intended to function as safety components for products governed by Directive 2006/42/EC of the European Parliament and the Council, dated May 17, 2006, concerning machinery and amending Directive 95/16/EC (OJ L 157, 9.6.2006, p. 24) [repealed by the Machinery Regulation], fall within the category of high-risk AI systems. This Directive applies to the following products:

Machinery

Interchangeable equipment

Safety components

Lifting accessories

Chains, ropes, and webbing

Removable mechanical transmission devices

Partly completed machinery.

Reference

AI Act, Annex II, Section A; Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC, Art. 1

6.2.2 Toys

AI systems that are products or are intended to function as safety components for products governed by Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (OJ L 170, 30.6.2009, p. 1), fall within the category of high-risk AI systems. This Directive regulates toys, referred to as products designed or intended, whether or not exclusively, for use in play by children under 14 years of age.

Reference

AI Act, Annex II, Section A; Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys, Art. 2

6.2.3 Recreational craft, personal watercraft, and related components

AI systems that are products or are intended to function as safety components for products governed by Directive 2013/53/EU of the European Parliament and of the Council of 20 November 2013 on recreational craft and personal watercraft and repealing Directive 94/25/EC (OJ L 354, 28.12.2013, p. 90), fall within the category of high-risk AI systems. This Directive applies to the following products:

Recreational craft and partly completed recreational craft

Personal watercraft and partly completed personal watercraft

The following components listed in Annex II of the Directive when placed on the Union market separately:

Ignition-protected equipment for inboard and stern drive petrol engines and petrol tank spaces

Start-in-gear protection devices for outboard engines

Steering wheels, steering mechanisms and cable assemblies

Fuel tanks intended for fixed installations and fuel hoses

Prefabricated hatches, and port lights

Propulsion engines which are installed or specifically intended for installation on or in watercraft

Propulsion engines installed on or in watercraft that are subject to a major engine modification

Watercraft that are subject to major craft conversion.

Reference

AI Act, Annex II, Section A; Directive 2013/53/EU of the European Parliament and of the Council of 20 November 2013 on recreational craft and personal watercraft and repealing Directive 94/25/EC, Art. 2, Annex II

6.2.4 Lifts and safety components for lifts

AI systems that are products or are intended to function as safety components for products governed by Directive 2014/33/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to lifts and safety components for lifts (OJ L 96, 29.3.2014, p. 251), fall within the category of high-risk AI systems. This Directive applies to lifts permanently serving buildings and constructions as well as safety components of lifts used in such lifts.

Lifts permanently serving buildings and constructions and intended for the transport of:

Persons

Persons and goods

Goods alone, provided that the carrier is easily accessible, meaning that an individual can enter it without encountering any obstacles, and equipped with controls located inside the carrier or within reach of an individual inside the carrier.

Safety components of lift used in the above-listed lifts:

Devices for locking landing doors

Devices to prevent falls to prevent the car from falling or uncontrolled movements

Overspeed limitation devices

Energy-accumulating buffers:

Non-linear, or

With damping of the return movement.

Energy-dissipating buffers

Safety devices fitted to jacks of hydraulic power circuits where these are used as devices to prevent falls

Electric safety devices in the form of safety circuits containing electronic components.

Reference

AI Act, Annex II, Section A; Directive 2014/33/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to lifts and safety components for lifts, Art. 1, Annex III, Annex I (3.2)

6.2.5 Equipment and protective systems intended for use in potentially explosive atmospheres

AI systems that are products or are intended to function as safety components for products governed by Directive 2014/34/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to equipment and protective systems intended for use in potentially explosive atmospheres (OJ L 96, 29.3.2014, p. 309), fall within the category of high-risk AI systems. The Directive applies to the following products:

Equipment and protective systems intended for use in potentially explosive atmospheres

Safety devices, controlling devices and regulating devices intended for use outside potentially explosive atmospheres but required for or contributing to the safe functioning of equipment and protective systems with respect to the risks of explosion

Components intended to be incorporated into equipment and protective systems intended for use in potentially explosive atmospheres.

Reference

AI Act, Annex II, Section A; Directive 2014/34/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to equipment and protective systems intended for use in potentially explosive atmospheres, Art. 1

6.2.6 Radio equipment

AI systems that are products or are intended to function as safety components for products governed by Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (OJ L 153, 22.5.2014, p. 62), fall within the category of high-risk AI systems. The Directive applies to radio equipment.

Reference

AI Act, Annex II, Section A; Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC, Art. 1

6.2.7 Pressure equipment

AI systems that are products or are intended to function as safety components for products governed by Directive 2014/68/EU of the European Parliament and of the Council of 15 May 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of pressure equipment (OJ L 189, 27.6.2014, p. 164), fall within the category of high-risk AI systems. The Directive applies to pressure equipment and assemblies with a maximum allowable pressure PS greater than 0,5 bar.

Reference

AI Act, Annex II, Section A; Directive 2014/68/EU of the European Parliament and of the Council of 15 May 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of pressure equipment, Art. 1

6.2.8 Cableway installations

AI systems that are products or are intended to function as safety components for products governed by Regulation (EU) 2016/424 of the European Parliament and of the Council of 9 March 2016 on cableway installations and repealing Directive 2000/9/EC (OJ L 81, 31.3.2016, p. 1), fall within the category of high-risk AI systems. The Regulation applies to new cableway installations designed to transport persons, to modifications of cableway installations requiring a new authorisation, and to subsystems and safety components for cableway installations.

Reference

AI Act, Annex II, Section A; Regulation (EU) 2016/424 of the European Parliament and of the Council of 9 March 2016 on cableway installations and repealing Directive 2000/9/EC, Art. 2

6.2.9 Personal protective equipment

AI systems that are products or are intended to function as safety components for products governed by Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment and repealing Council Directive 89/686/EEC (OJ L 81, 31.3.2016, p. 51), fall within the category of high-risk AI systems. The Regulation applies to personal protective equipment, defined as:

Equipment designed and manufactured to be worn or held by a person for protection against one or more risks to that person's health or safety

Interchangeable components for such equipment which are essential for its protective function

Connexion systems for such equipment that are not held or worn by a person, that are designed to connect that equipment to an external device or to a reliable anchorage point, that are not designed to be permanently fixed and that do not require fastening works before use.

Reference

AI Act, Annex II, Section A; Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment and repealing Council Directive 89/686/EEC , Art. 2, 3(1)

6.2.10 Appliances burning gaseous fuels and related safety devices

AI systems that are products or are intended to function as safety components for products governed by Regulation (EU) 2016/426 of the European Parliament and of the Council of 9 March 2016 on appliances burning gaseous fuels and repealing Directive 2009/142/EC (OJ L 81, 31.3.2016, p. 99), fall within the category of high-risk AI systems. The Regulation applies to the following appliances and fittings:

Appliances burning gaseous fuels used for cooking, refrigeration, air-conditioning, space heating, hot water production, lighting or washing, and also forced draught burners and heating bodies to be equipped with such burners

Fittings, meaning safety devices, controlling devices or regulating devices and sub-assemblies thereof, designed to be incorporated into an appliance or to be assembled to constitute an appliance.

Reference

AI Act, Annex II, Section A; Regulation (EU) 2016/426 of the European Parliament and of the Council of 9 March 2016 on appliances burning gaseous fuels and repealing Directive 2009/142/EC, Art. 1, 2(1)(2)

6.2.11 Medical devices

AI systems that are products or are intended to function as safety components for products governed by 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 (OJ L 117, 5.5.2017, p. 1), fall within the category of high-risk AI systems. The Regulation applies to medical devices for human use and accessories for such devices, including also the following:

Contact lenses or other items intended to be introduced into or onto the eye.

Products intended to be totally or partially introduced into the human body through surgically invasive means for the purpose of modifying the anatomy or fixation of body parts with the exception of tattooing products and piercings.

Substances, combinations of substances, or items intended to be used for facial or other dermal or mucous membrane filling by subcutaneous, submucous or intradermal injection or other introduction, excluding those for tattooing.

Equipment intended to be used to reduce, remove or destroy adipose tissue, such as equipment for liposuction, lipolysis or lipoplasty.

High intensity electromagnetic radiation (e.g. infra-red, visible light and ultra-violet) emitting equipment intended for use on the human body, including coherent and non-coherent sources, monochromatic and broad spectrum, such as lasers and intense pulsed light equipment, for skin resurfacing, tattoo or hair removal or other skin treatment.

Equipment intended for brain stimulation that apply electrical currents or magnetic or electromagnetic fields that penetrate the cranium to modify neuronal activity in the brain.

Reference

AI Act, Annex II, Section A; 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, Art. 1(2), Annex XVI

6.2.12 In vitro diagnostic medical devices

AI systems that are products or are intended to function as safety components for products governed by Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176), fall within the category of high-risk AI systems. The Regulation applies to in vitro diagnostic medical devices for human use and accessories for such devices.

Reference

AI Act, Annex II, Section A; Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU, Art. 1

6.2.13 Civil aviation security

AI systems that are products or are intended to function as safety components for products governed by Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72), fall within the category of high-risk AI systems. The Regulation aims to ensure the security of civil aviation and applies to the following:

All airports or parts of airports located in the territory of a European Union Member State that are not exclusively used for military purposes

All operators, including air carriers, providing services at airports in EU Member States.

All entities applying aviation security standards that operate from premises located inside or outside airport premises and provide goods and/or services to or through airports in EU Member States.

Reference

AI Act, Annex II, Section B; Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002, Art. 1,2

6.2.14 Two- or three-wheel vehicles and quadricycles

AI systems that are products or are intended to function as safety components for products governed by Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles (OJ L 60, 2.3.2013, p. 52), fall within the category of high-risk AI systems. The Regulation applies to two- or three-wheel vehicles and quadricycles intended to travel on public roads, designed and constructed in one or more stages, and to systems, components and separate technical units, as well as parts and equipment, designed and constructed for such vehicles. Additionally, the Regulation also applies to enduro motorcycles, trial motorcycles, and heavy all-terrain quads.

Reference

AI Act, Annex II, Section B; Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles, Art. 2

6.2.15 Agricultural and forestry vehicles

AI systems that are products or are intended to function as safety components for products governed by Regulation (EU) No 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles (OJ L 60, 2.3.2013, p. 1), fall within the category of high-risk AI systems. The Regulation applies to agricultural and forestry vehicles, designed and constructed in one or more stages, and to systems, components and separate technical units, as well as parts and equipment, designed and constructed for such vehicles.

Reference

AI Act, Annex II, Section B; Regulation (EU) No 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles, Art. 2

6.2.16 Marine equipment

AI systems that are products or are intended to function as safety components for products governed by Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC (OJ L 257, 28.8.2014, p. 146), fall within the category of high-risk AI systems. The Directive regulates marine equipment placed on board of EU ships.

Reference

AI Act, Annex II, Section B; Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC, Art. 1

6.2.17 Rail systems

AI systems that are products or are intended to function as safety components for products governed by Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (OJ L 138, 26.5.2016, p. 44), fall within the category of high-risk AI systems. The Directive regulates the European Union rail system and parts of it, covering the following elements:

Network:

Specially built high-speed lines equipped for speeds generally equal to or greater than 250 km/h

Specially upgraded high-speed lines equipped for speeds of the order of 200 km/h

Specially upgraded high-speed lines which have special features as a result of topographical, relief or town-planning constraints, to which the speed must be adapted in each case. This category includes interconnecting lines between high-speed and conventional networks, lines through stations, accesses to terminals, depots, etc. travelled at conventional speed by 'high-speed' rolling stock

Conventional lines intended for passenger services

Conventional lines intended for mixed traffic (passengers and freight)

Conventional lines intended for freight services

Passenger hubs

Freight hubs, including intermodal terminals

Lines connecting the abovementioned elements

The network includes traffic management, tracking and navigation systems, technical installations for data processing and telecommunications intended for long-distance passenger services and freight services on the network in order to guarantee the safe and harmonious operation of the network and efficient traffic management.

Vehicles likely to travel on all or part of the Union's network:

Locomotives and passenger rolling stock, including thermal or electric traction units, self-propelling thermal or electric passenger trains, and passenger coaches

Freight wagons, including low-deck vehicles designed for the entire network and vehicles designed to carry lorries

Special vehicles, such as on-track machines

The list of vehicles shall include those which are specially designed to operate on the different types of high-speed lines.

Reference

AI Act, Annex II, Section B; Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (recast), Art. 1, Annex I

6.2.18 Motor vehicles and their trailers

AI systems that are products or are intended to function as safety components for products governed by Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC (OJ L 151, 14.6.2018, p. 1), and Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such

vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (OJ L 325, 16.12.2019, p. 1) , fall within the category of high-risk AI systems.

The Regulations apply to motor vehicles of categories M and N and their trailers of category O and to systems, components and separate technical units, as well as to parts and equipment, designed and constructed for such vehicles and their trailers.

Reference

AI Act, Annex II, Section B; Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC, Art. 2; Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166, Art. 2

6.2.19 Products, parts and equipment for remote control of an aircraft

AI systems that are products or are intended to function as safety components for products concerning unmanned aircraft and their engines, propellers, parts and equipment to control them remotely, governed by Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1), fall within the category of high-risk AI systems. The Regulation applies to:

The design and production of products, parts, and equipment for remotely controlling aircraft, provided they are under the oversight of the Agency or a Member State and are not covered by the following point.

The design, production, maintenance, and operation of aircraft, including engines, propellers, parts, non-installed equipment, and remote control equipment, if the aircraft is registered in a Member State, a third country but operated by an operator in the EU, or an unmanned aircraft operated within the EU territory.

The operation of aircraft by third-country operators into, within, or out of the EU territory.

The design, production, maintenance, and operation of safety-related aerodrome equipment used at specific aerodromes and the provision of ground handling services and apron management services (AMS) at those aerodromes.

The design, maintenance, and operation of aerodromes, including the safety-related equipment used at those aerodromes, in the EU territory that are open to public use, serve commercial air transport, and have paved instrument runways of 800 meters or more, or exclusively serve helicopters using instrument procedures.

Safeguarding the surroundings of the aerodromes, with consideration for environmental and land-use planning laws.

The provision of Air Traffic Management and Air Navigation Services (ATM/ANS) in the Single European Sky airspace, as well as the design, production, maintenance, and operation of systems and components used in these services.

The design of airspace structures in the Single European Sky airspace, while recognizing the responsibilities of Member States regarding airspace under their jurisdiction.

Reference

AI Act, Annex II, Section B; Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91, Art. 2

6.2.20 Biometrics permitted under Union or national law

High-risk biometric AI systems cover the biometric systems which use is allowed under European Union law or under national law of an EU Member State. This covers biometric categorisation, identification, and emotion recognition systems that are not considered prohibited practices under the AI Act. The following biometric systems are considered high-risk:

Remote biometric identification systems. Biometric identification refers to the automated process of recognising an individual's physical, physiological, behavioural, and psychological characteristics to determine their identity by matching their biometric data with stored data in a database. This does not include biometric verification systems whose sole purpose is to confirm that an individual is the person they claim to be.

AI systems intended for biometric categorisation. Such systems categorise individuals according to sensitive or protected attributes or characteristics based on deducing or inferring those attributes or characteristics.

AI systems intended to be used for emotion recognition.

It is important to make a distinction between biometric systems considered as high-risk and prohibited biometric categorisation and emotion recognition systems.

Reference

AI Act, Annex III, 1, Art. 3(33a)

6.2.21 Critical infrastructure

High-risk AI systems used in critical infrastructure encompass AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, and the supply of water, gas, heating and electricity.

Critical infrastructure refers to an asset, a facility, equipment, a network or a system, or any part of these, that is necessary for the provision of an essential service. Essential services are understood as a service that is crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment.

Reference

AI Act, Annex III, 2, Art. 3(44h); Directive (EU) 2022/2557, Art. 2(4)

6.2.22 Education and vocational training

High-risk AI systems in the context of education and vocational training include:

AI systems intended to be used for making decisions about an individual's access, admission, or assignment to educational and vocational training institutions at all levels.

AI systems intended to be used for evaluating learning outcomes, including their use to guide the education and training process of individuals in educational and vocational training institutions at all levels.

AI systems intended to be used for assessing the suitable education level that an individual will receive or will be able to access in educational and vocational training institutions.

AI systems intended to be used for monitoring and detecting prohibited behavior by students during tests within educational and vocational training institutions.

Reference

AI Act, Annex III, 3

6.2.23 Employment, workers management and access to self-employment

High-risk AI systems within the realm of employment and workforce management include the following:

AI systems intended to be used for tasks such as recruitment or selection of individuals particularly for placing targeted job advertisements, analysing and filtering job applications, and to evaluate candidates.

AI systems intended to be used for tasks that make decisions impacting terms of employment, promotion or ending work-related contracts, assigning tasks based on behaviour or personal traits, and monitoring and evaluating the performance and behaviour of individuals in work-related contexts.

Reference

AI Act, Annex III, 4

6.2.24 Essential private services and essential public services and benefits

High-risk AI systems included in the category of essential private services and essential public services include the following:

AI systems used by or on behalf of public authorities to assess the eligibility of individuals for essential public assistance, benefits and services, including healthcare services as well as to grant, reduce, revoke, or reclaim such benefits and services.

AI systems used to evaluate individuals' creditworthiness or establish their credit score, excluding those used for the purpose of detecting financial fraud.

AI systems intended to evaluate and classify emergency calls from individuals or dispatch emergency first response services, such as police, firefighters, and medical aid, as well as emergency healthcare patient triage systems.

AI systems intended to be used for risk assessment and setting prices for life and health insurance policies for individuals.

Reference

AI Act, Annex III, 5

6.2.25 Law enforcement, permitted under Union or national law

High-risk AI systems in the context of law enforcement encompass the following:

AI systems for assessing the risk of an individual becoming a victim of criminal offenses, intended for use by or on behalf of law enforcement authorities, or by EU institutions, agencies, offices, or bodies in support of law enforcement activities.

AI systems functioning as polygraphs and similar tools, intended to be used by or on behalf of law enforcement authorities or by EU institutions, bodies, and agencies in support of law enforcement authorities.

AI systems for evaluating evidence reliability, intended for use by or on behalf of law enforcement authorities, or by EU institutions, agencies, offices, or bodies in support of law enforcement activities.

AI systems for assessing the risk of an individual committing or re-committing a crime, intended for use by or on behalf of law enforcement authorities, or by EU institutions, agencies, offices, or bodies supporting law enforcement. The assessment provided by the system must not be solely based on profiling as defined in Article 3(4) of Directive (EU) 2016/680, or used to evaluate personality traits, characteristics, or past criminal behavior of individuals or groups.

AI systems for profiling individuals as defined in Article 3(4) of Directive (EU) 2016/680, intended for use by or on behalf of law enforcement authorities, or by EU institutions, agencies, offices, or bodies in support of law enforcement activities during the detection, investigation, or prosecution of criminal offenses.

Reference

AI Act, Annex III, 6

6.2.26 Migration, asylum and border control management, permitted under Union or national law

High-risk AI systems in the category of migration, asylum, and border control include the following:

AI systems are utilised by competent public authorities as polygraphs, and similar tools.

AI systems intended to be used by or on behalf of competent public authorities, or EU agencies, offices, or bodies, to evaluate risks such as security, irregular migration, or health risks presented by individuals planning to enter or already within a Member State's territory.

AI systems intended to be used by or on behalf of competent public authorities or EU agencies, offices, or bodies to assist competent public authorities in reviewing applications for asylum, visas, and residence permits, along with related complaints. These systems assist in determining the eligibility of applicants and evaluating the reliability of supporting evidence.

AI systems intended to be used by or on behalf of competent public authorities, including EU agencies, offices, or bodies, in managing migration, asylum, and border control. These systems aim to detect, recognise, or identify individuals. AI systems for verifying travel documents are exempted from this and not considered high risk.

Reference

AI Act, Annex III, 7

6.2.27 Administration of justice and democratic processes

High-risk AI systems used in the administration of justice and democratic processes encompass the following:

AI systems intended to be used by a judicial authority or on their behalf to support a judicial authority in researching and interpreting facts and the law, as well as in applying the law to specific cases, or used in a similar way in alternative dispute-resolution processes.

AI systems employed to influence election or referendum outcomes or the voting behavior of individuals during elections or referenda. However, this excludes AI systems whose output is not directly presented to individuals, such as tools utilised to organise and optimise political campaigns from an administrative and logistical perspective.

Reference

AI Act, Annex III, 8

6.3 General purpose AI

The AI Act lays down obligations to providers of general-purpose AI models and general-purpose AI systems. It should be noted that high-impact foundation models are distinguished from this group due to the potential systemic risks such models can pose.

These foundation models and general-purpose AI systems are subject to certain transparency requirements and requirements related to copyright law..

6.3.1 General-purpose AI models

General-purpose AI model is an AI system that has been extensively trained on a large amount of data using self-supervision. General-purpose AI models display significant generality and are capable of effectively performing a wide variety of tasks irrespective of the way the model is placed on the market. General-purpose AI models can also be integrated into variety of downstream, systems or applications.

The definition of general-purpose AI model does not cover AI models used before their release on the market for research, development, and prototyping activities,

Reference

AI Act, Art. 3(44b)

6.3.2 General-purpose AI system

A general-purpose AI system refers to an AI system that is based on a general-purpose AI model. Such general-purpose AI system has the capability to serve various different purposes and that can be used directly as well as for integration in other AI systems.

Reference

AI Act, Art. 3(44d)

6.4 General purpose AI models with systemic risk

General purpose AI models with systemic risk are general-purpose AI models that have capabilities that match or exceed the capabilities recorded in the most advanced general-purpose models. General purpose AI models with systemic risk can greatly influence the internal market because of their extensive scope. They have the potential, or a reasonable likelihood, to adversely affect public health, safety, security, fundamental rights, or society at large. These negative impacts can spread widely across the value chain, posing a systemic risk at the Union level.

Such general-purpose AI models are subject to stricter requirements in the AI Act than other general purpose AI models, and the providers of such models must assess and mitigate risks, report serious incidents, conduct state-of-the-art tests and model evaluations, ensure cybersecurity and provide information on the energy consumption of their models.

6.4.1 General-purpose AI models with systemic risk

General-purpose AI models with systemic risk AI models are general-purpose AI models that have capabilities that match or exceed the capabilities recorded in the most advanced general-purpose models. Such general-purpose AI models can greatly influence the internal market because of their extensive scope. They have the potential, or a reasonable likelihood, to adversely affect public health, safety, security, fundamental rights, or society at large. These negative impacts can spread widely across the value chain, posing a systemic risk at the Union level.

General-purpose AI model is classified as general-purpose AI models with systemic risk if it meets any of the following criteria:

General-purpose AI model has high impact capabilities determined by technical methodologies and tools, including indicators and benchmarks

General-purpose AI model is designated by the Commission to be a general-purpose AI model with systemic risk due to their equivalent impact A presumption of high impact is made when the AI model's training compute exceeds 10^25 FLOPs. The Commission may update these criteria to align with technological advancements.

Reference

AI Act, Art. 3(44d)(44c), 52a

6.5 Transparency risk

Systems with transparency risk include an exhaustively defined list of systems that possess a limited risk on the life of a user. Such systems are subject to information and transparency obligations such as disclosures or labelling.

6.5.1 Systems interacting with natural persons

AI systems intended to directly interact with individuals include systems such as chatbots. Such systems may pose specific risks of impersonation or deception, and thus are subject to transparency obligations.

Reference

AI Act, Art. 52(1)

6.5.2 Systems generating synthetic audio, image, video or text content

AI systems, including GPAI systems, that generate synthetic audio, image, video or text content are subject to transparency obligations.

Reference

AI Act. Art. 52(1a)

6.5.3 Emotion recognition and biometric categorisation systems

An emotion recognition system refers to an AI system designed to identify or deduce the emotions or intentions of individuals by analysing their biometric data. A biometric categorisation system refers to an AI system designed to classify individuals into specific categories based on their biometric data, except when it is a secondary component of another commercial service and strictly required for objective technical purposes.

Biometric categorisation and emotion recognition systems are not subject to limited risk obligations when use is lawful and for the purpose of detection, prevention, and investigation of crimes, provided that adequate measures are in place to protect the rights and freedoms of third parties and in accordance with EU law.

Reference

AI Act, Art. 3(34)(35), 52(2)

6.5.4 Systems generating or manipulating content (deepfakes)

AI system that generates or manipulates image, audio or video content . Deepfake content is generated or manipulated images, audio, or video content that closely resemble real individuals, objects, locations, or events in a way that could mislead a person into thinking it is genuine or accurate when it is not.

Deepfake is not subject to limited risk obligations when its use is allowed by law for purposes such as detecting, preventing, investigating or prosecuting criminal offences. For content that is clearly intended for artistic, creative, satirical, or fictional purposes, the obligation to inform about the artificial nature of the content is confined to making a disclosure that the content has been generated or altered. This disclosure should be done in a manner that does not interfere with the audience's experience or the integrity of the work.

Reference

AI Act, Art. 52(3), Recital 70b

6.6 Minimal or no risk

The category of minimal or no risk AI systems include all other AI systems not falling into other categories of AI systems under the AI Act and present minimal risk or no risk at all to people's safety and fundamental rights. Such AI systems that present only low or minimal risk could be developed and used in the EU without conforming to any additional legal obligations.

6.6.1 Minimal or no risk AI system

An AI system that possesses no risk or only minimal risk to the safety and fundamental rights of individuals. Such AI system is a machine-based system created to operate with different degrees of autonomy and can learn and adjust its behaviour over time. Its purpose is to produce outputs, whether explicitly or implicitly intended, such as predictions, content, recommendations, or decisions that can have an impact on physical or virtual environments.

Reference

AI Act, Art. 3(1)

6.7 Open source

AI systems released under free and open source license are exempted from the majority of the requirements under AI Act. However, this does not apply to open source AI system classified as prohibited AI systems, high-risk AI systems, or general purpose AI models with systemic risks.

Furthermore, certain obligations of general purpose AI models apply to providers of open source AI systems.

6.7.1 AI systems under free and open source license

AI systems released under free and open source license that are not placed into service as prohibited AI systems, high-risk AI systems, or general purpose AI models with systemic risks.

General purpose AI models released under free and open source license are subject to certain obligations applicable to general purpose AI models.

Reference

AI Act, Art. 2(5g)

7. Policy Requirements

7.1 Exemption from high-risk system classification

AI systems are not categorised as high-risk if they pose no significant risk of harm to the health, safety, or fundamental rights of an individual and do not substantially affect decision-making outcomes. This exemption is applicable when the system either:

Executes a defined procedural function.

Enhances the results of previously completed human tasks.

Identifies trends or deviations in decision-making, provided it does not replace or influence previous human assessments without adequate human review.

Performs initial tasks essential for evaluations relevant to the use cases specified in Annex III.

These exemptions do not extend to AI systems engaged in the profiling of individuals, as such systems are always classified as high-risk.

Exempted high-risk AI system referred to in Annex III must document the assessment of exemption before the system is placed on the market or put into service. This documentation must be provided to the national competent authority upon their request. Such providers must also register the exempted high-risk system to the EU database for high-risk systems.

Role

Provider

References

AI Act, Art. 6(2b)

7.1.1 Assessment of exemption from high-risk classification

A provider who considers that an AI system referred to in Annex III is not high-risk according to the derogations referred to in Art. 6(2a) must document its assessment of the exemption before the system is placed on the market or put into service.

Reference

AI Act, Art. 6(2b)

7.1.2 Registration to EU or national database

Prior to introducing a standalone high-risk AI system, as mentioned in Annex III, to the market or putting it into use, the provider or their authorised representative must register the system in the EU database.

High-risk AI systems used in the area of critical infrastructure (point 2, Annex III) are exempted from the EU database registration. Instead, such systems must be registered at a national level.

This registration obligation also applies to providers who have concluded that their system is not high-risk by using the procedure under Article 6(2a). Either the provider or the authorised representative must register the system.

Providers will input the data specified in Annex VIII that contains the following information required:

Details of the provider (name, address, contact information).

Where submission of information to the database is handled by someone else, the name, address and contact details of that person.

Information (name, address, and contact details) on the authorised representative, if applicable.

AI system trade name and a unique reference for identification.

Description of the AI system's intended purpose and the components and functions supported through the AI system.

Simple and concise description of the information used by the system (data, inputs) and the system's operating logic.

The status of the AI system (e.g., on the market, in service, recalled).

Certificate details (type, number, expiry date, notified body's name/ID), if applicable.

A scanned copy of the certificate issued by notified body, if applicable.

List of Member States where the AI system has been placed on the market or put into service.

Copy of the EU declaration of conformity.

Electronic instructions for use (excluding high-risk AI systems in the areas of law enforcement and migration, asylum and border control management).

Optional URL for additional information.

The information in the database will be publicly accessible but will only contain necessary personal data, such as the names and contact details of individuals authorised to represent the provider.

Reference

AI Act, Art. 51(1)(1d), 60, Annex VIII Section A

7.1.3 Cooperation with national competent authority

Upon request, the provider must make the assessment of the high-risk AI system's exemption from high-risk classification available to the national competent authority.

Reference

AI Act, Art 6(2b)

7.2 Risk management system

Establish, implement, document, and maintain a risk management system for AI systems. This system should encompass a continuous risk management process that spans the entire lifecycle of the AI system. It involves the identification and analysis of known and foreseeable risks pertaining to health, safety, and fundamental rights. Additionally, risks identified through post-market monitoring should be evaluated. Appropriate risk management measures must be adopted, including designing and developing the system to eliminate or reduce risks whenever possible. For risks that cannot be eliminated, suitable mitigation and control measures must be implemented. The risk management system should ensure transparency and, if necessary, provide training to system users. Testing procedures are an integral part of the risk management system, serving to identify the most appropriate risk management measures and ensuring that high-risk systems perform as intended.

Role

Provider

References

AI Act, Art. 9

7.2.1 Risk management system policies and processes

Risk management system must be established, implemented, documented and maintained for high-risk AI systems. The risk management system consists of policies, procedures, and instructions.

Reference

AI Act, Art. 9(1)

7.2.2 Risk identification and evaluation process

High-risk AI systems must have a continuous iterative process for risk identification, analysis, estimation, and evaluation in place for the whole lifecycle of the AI system. The process must be planned and run throughout the entire AI system lifecycle and regularly reviewed and updated. This process must cover:

Identification and analysis of known and reasonably foreseeable risks to health, safety, and fundamental rights when the AI system is used according to its intended purpose;

Estimation and evaluation of the risks that may emerge when the system is used in accordance with its intended purpose and under reasonably foreseeable misuse;

Evaluation of other risks that could potentially arise based on the analysis of data gathered from the post-market monitoring system.

Reference

AI Act, Art. 9(2)(a)(b)(c)

7.2.3 Risk management measures adoption

High-risk AI systems must implement appropriate and targeted risk management measures to address and reduce all identified risks. It should be noted that the risks mentioned here are those that can be feasibly reduced or removed through the design, and development of the high-risk AI system, or by providing adequate technical information. The chosen risk management measures for high-risk AI systems should account for how different requirements for high-risk AI systems influence each other. The providers should aim to lower risks efficiently and ensure that the measures are applied in a balanced way to satisfy all the necessary requirements.

The adopted risk management measures shall ensure that any relevant residual risk associated with hazards, as well as the overall residual risk of high-risk AI systems, is deemed to be acceptable. The risk management measures must ensure:

Eliminating or reducing identified risks through adequate design and development, as far as technically feasible.

Implementing control and mitigation measures to address risks cannot be fully eliminated.

Providing the required information about risks that can emerge when the system is used as intended or under reasonably foreseeable misuse (as outlined in Article 13), and offering user training to deployers when necessary.

When eliminating or reducing risks, factors such as deployers' technical knowledge, experience, education, training, and the system's presumed usage context should be taken into account.

Reference

AI Act, Art. 9(2)(d),9(2a) 9(3), 9(4)

7.2.4 Risk testing procedures

High-risk AI systems must undergo testing to determine the most effective and targeted risk management measures. The testing must ensure that the AI systems perform consistently their intended functions and comply with all the requirements relevant to high-risk AI systems. The testing procedures may include testing in real world conditions in accordance with Art. 54a. High-risk AI systems must be tested at various stages during development and always before being placed on the market or put into service. Testing should be based on predefined metrics and probabilistic thresholds that are appropriate to the system's intended purpose.

Reference

AI Act, Art. 9(5),9(6),9(7)

7.2.5 Assessment of impacts on children and vulnerable groups of people

Providers must consider whether the system is likely to adversely impact children, persons under 18, and other vulnerable groups and consider this when implementing risk management system.

Reference

AI Act, Art. 9(8)

7.2.6 Integrated risk management under relevant sectorial Union law

Providers of high-risk AI systems, already governed by sector-specific EU laws for internal risk management, can integrate or align the risk management system with their existing risk management practices as established by those sectorial laws.

Reference

AI Act, Art. 9(9)

7.3 Data and data governance

To ensure the quality and integrity of data used in AI systems, it is essential to establish a robust data management and governance framework. This framework should encompass the entire lifecycle of AI systems and include practices such as relevant design choices, transparent data collection processes, meticulous data preparation processing operations, formulation of assumptions, assessment of data availability and suitability, examination of biases, identification of data gaps and shortcomings, and adherence to dataset quality requirements (relevant, representative, free of errors, complete).

Role

Provider

References

AI Act, Art. 10

7.3.1 Data governance and management practices

High-risk AI systems using data-trained models must be developed using training, validation, and testing datasets that adhere to the quality standards laid down in the Data and data governance requirement. For high-risk AI systems not based on model training, only the testing datasets must comply with these requirements.

These datasets must undergo suitable data governance and management practices tailored to the AI system's intended use, covering in minimum:

The relevant design choices;

Data collection processes, origin of data, and for personal data, the initial purpose of collection;

Data preparation processing operations, such as annotation, labelling, cleaning, updating, enrichment and aggregation;

Formulation of assumptions concerning the data, importantly, what the data is supposed to measure and represent;

Assessment of the availability, quantity and suitability of the datasets needed;

Examination of possible biases likely to affect health and safety of individuals, negatively impact fundamental rights or lead to discrimination prohibited by Union law, particularly when data outputs shape future inputs;

Appropriate measures to detect, prevent and mitigate possible identified biases;

Identification of relevant data gaps or shortcomings that prevent compliance with the AI Act, and how these should be addressed.

Reference

AI Act, Art. 10(1),(2),(6)

7.3.2 Dataset representativeness and completeness

Training, validation and testing data sets shall be relevant, sufficiently representative, free of errors to the best extent possible, and complete considering the intended purpose of the AI system. The datasets must possess relevant statistical properties and metrics, also regarding the persons or groups of persons in relation to whom the AI systems are intended to be used. These data characteristics can be fulfilled either within individual data sets or by combining multiple datasets.

Reference

AI Act, Art. 10(3)

7.3.3 Dataset relevancy and applicability

Datasets must consider the unique elements and characteristics of the specific geographical, contextual, behavioral, or functional environment within which the high-risk AI system is intended to be used.

Reference

AI Act, Art 10(4)

7.3.4 Special categories of personal data

For the purposes and to the extent strictly necessary for ensuring bias detection and correction in high-risk AI systems (as laid down in data governance and management practices), providers may exceptionally process sensitive personal data. The sensitive personal data that falls into the scope of this requirement covers sensitive personal data under GDPR (Regulation (EU) 2016/679), Law Enforcement Directive (Directive (EU) 2016/680)), and the Regulation on the processing of personal data by EU institutions (Regulation (EU) 2018/1725)).

This processing is subject to strict safeguards to protect individuals' fundamental rights. In addition to the conditions set out in the above mentioned regulations and directive, the following conditions must be met for processing:

Bias detection and correction cannot be effectively achieved using other data types, like synthetic or anonymised data.

Special categories of personal data used for bias detection must have technical restrictions on reuse, state-of-the-art security, and privacy measures, including pseudonymisation.

Special categories of personal data must be securely stored, protected, and accessible only to authorised individuals under strict controls and confidentiality agreements to prevent misuse.

The special categories of personal data should not be shared, transferred, or accessed by third parties.

The special categories of personal data processed must be deleted after bias correction or at the end of its retention period, whichever comes first.

The records of processing activities must include a justification for using special personal data for bias detection and correction, affirming that this objective could not be met with other data.

Reference

AI Act, Art. 10(5), General Data Protection Regulation, Art. 9(1); The Law Enforcement Directive, Art.10; Regulation on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, Art. 10(1)

7.4 Technical documentation

AI systems must be accompanied by comprehensive and up-to-date technical documentation before the system is introduced to the market or put into service. This documentation serves as evidence of the system's compliance with the requirements outlined in the relevant regulations and provides national competent authorities and notified bodies with the essential information needed to assess its compliance. The technical documentation required can be found from Annex IV.

SMEs and start-ups can submit the technical documentation outlined in Annex IV in a simplified form. The Commission will create a specific form for this, designed for small and micro enterprises. Where an SME or start-up chooses to use this simplified approach, it must use the provided form, which notified bodies will accept for conformity assessment purposes.

Role

Provider

References

AI Act, Art. 11, 18, Annex IV

7.4.1 General description of the AI system

The general description of the AI system should include the following information:

Intended purpose of the system, the name of the provider, and the version of the system, reflecting its relation to previous versions.

AI system interaction with hardware or software, including other AI systems that are not part of the system.

Software or firmware versions and requirements relevant to version updates.

Form(s) of the AI system or service to be placed in the market (e.g. software package embedded into hardware, downloadable, API etc.).

Description of the hardware on which the AI system will operate.

Photographs or illustrations of AI system used as a component.

Description of the user interface provided to the deployer.

Instructions of use for AI system deployer and a basic description of the user-interface provided to the deployer.

Reference

AI Act, Art. 11, Annex IV(1)

7.4.2 Description of AI system elements and its development process

The description of AI system elements and its development process should include the following information:

Methods and steps taken for the development of the AI system (including recourse to pre-trained systems or tools by third parties, their use, and potential integrations or modifications).

The design specifications of the AI system (the general logic of the system and of the algorithms; key design choices including the rationale and assumptions made, also regarding persons or group of persons the system is intended to be used; the relevant classification choices; system's designed optimisation and relevance of the different parameters; the expected outputs and output quality of the system; potential

decisions regarding trade-offs to ensure that the system complies with the high-risk AI system requirements under the AI Act).

System architecture explanation, including a description of relevant software components and their relation, connection, and integration to overall system processing; the relevant computational resources for developing, training, testing, and validating the AI system.

Datasheet containing the data requirements, including descriptions of training methodologies and techniques and training datasets used, a general description of the dataset and information on the provenance of the used datasets, as well as their scope and main characteristics; information on data selection and obtention, data labelling procedures and data cleaning methodologies.

Human oversight measures and their assessment, including assessment of needed technical measures for facilitation of interpretation of AI system outputs to the deployers.

Description of pre-determined changes to the AI systems and its performance, including adopted technical measures ensuring system compliance with the requirements for high-risk AI systems.

Description of used validation and testing procedures, including used validation and testing data and its characteristics; metrics used to measure system accuracy, robustness, discriminatory impacts, and compliance with requirements applicable to high-risk AI systems; dated and signed test logs and test reports, including potential pre-determined changes.

Description of cybersecurity measures put in place.

Reference

AI Act, Art. 11, Annex IV(2)

7.4.3 Information on monitoring, functioning, and control of the AI system

The information on monitoring, functioning, and control of the AI systems should include the following information:

AI system limitations and capabilities regarding the system performance, including degrees of accuracy for specific persons or groups of persons on which the AI system will be used, and overall expected level of accuracy relevant to the system’s intended purpose.

Foreseeable unintended outcomes and sources of risk to health, safety, and fundamental rights, as well as foreseeable discrimination in accordance with the system’s intended purpose.

The necessary human oversight measures required to comply with the requirement of human oversight contained in Article 14 of the AI Act, including necessary technical measures to facilitate deployer's understanding of the system’s outputs.

Appropriate specifications on system input data.

A description of the appropriateness of the performance metrics for the specific AI system

Reference

AI Act, Art. 11, Annex IV(3)

7.4.4 Risk management

The information on risk management should include detailed description of the risk management system in accordance with the requirement of risk management system contained in Article 9 of the AI Act.

Reference

AI Act, Art. 11, Annex IV(4)

7.4.5 Change management

The information on changes should include a description of the relevant changes made by the provider to the system throughout its whole lifecycle.

Reference

AI Act, Art. 11, Annex IV(5)

7.4.6 Harmonised standards

The harmonised standards should include the following information:

List of harmonised standards published in Official Journal of the European Union and that are applied in part or in full.

Where no such harmonised standards have been applied, a detailed description of the solutions adopted to meet the requirements for high-risk AI system, including a list of technical specifications and other relevant standards applied.

Reference

AI Act, Art. 11, Annex IV(6)

7.4.7 EU declaration of conformity

The EU declaration of conformity should include copy of the high-risk AI system's EU declaration of conformity.

Reference

AI Act, Art. 11, Annex IV(7)

7.4.8 Post-market monitoring plan

The post-market monitoring plan should include a description of the system put in place to evaluate AI system performance after it has been put on the market or put into service, and the post-market monitoring plan referenced in Article 61 of the AI Act.

Reference

AI Act, Art. 11, Annex IV(8)

7.5 Record-keeping

AI systems should technically allow the automatic recording of events ('logs') during their operation. These logs enable traceability of the AI system's functioning throughout its lifecycle, aligning with the system's intended purpose. They should facilitate monitoring of the system's operation and obligations of deployers, identifying situations that may present risks or lead to substantial modifications.

Role

Provider

References

AI Act, Art. 12

7.5.1 Logging for system lifecycle and risk monitoring

High-risk AI systems must have the capability to automatically log events throughout their lifespan. These logs should ensure traceability that matches the system's intended purpose by recording events relevant for:

Identifying situations that may result in the AI system presenting a risk according to the meaning of Art. 65(1). Such risk refers to the system's potential to harm health and safety, including at workplace, consumer protection, the environment, public security, and other public interests under EU legislation. It includes harm that goes beyond what is acceptable, considering the product's intended use, duration of use, and any installation and maintenance needs.

Identifying situations that may result in a substantial modification. Substantial modification refers to any unplanned or unforeseen change made to an AI system after its market introduction that has not been foreseen in the initial conformity assessment, and thus impacts the system's compliance with the high-risk AI system requirements in Title III, Chapter 2 of the AI Act, or alters its originally assessed intended purpose.

Supporting the post-market monitoring, referred to in Art. 61.

Facilitating the deployer's monitoring of high-risk AI system operation, referred to in Art. 29(4).

Reference

AI Act, Art. 12(1)(2), 65(1), 3(23), 29(4); Regulation (EU) 2019/1020, Art. 3(19)

7.5.2 Logging requirements for remote biometric identification systems

AI systems intended to be used for remote biometric identification of natural persons are subject to following minimum logging capabilities:

Recording the period of each use of the system (start date and time, and end date and time).

Documenting the reference database used for input verification.

Maintaining a record of the input data that resulted in a match.

Identifying the natural persons involved in the verification of system results, as per Art. 14(5).

Reference

AI Act, Art. 12(4)

7.6 Transparency and provision of information to deployers (Instructions for use)

AI systems should be designed and developed in a manner that ensures transparency in their operation, allowing deployers to interpret the system's outputs and use them appropriately. An appropriate level of transparency should be maintained, taking into account the respective obligations of deployers and providers. Instructions for use, in a suitable digital format or otherwise, should accompany AI systems and provide deployers with concise, complete, correct, and clear information that is relevant, accessible, and easily understandable.

Role

Provider

References

AI Act, Art. 13

7.6.1 Provider contact details

The instructions of use should include information about the identity and the contact details of the provider and where applicable, of its authorised representative.

Reference

AI Act, Art. 13(3)(a)

7.6.2 Characteristics, capabilities, and limitations of performance of the system

The instructions of use should include information on the characteristics, capabilities, and limitations of performance of the high-risk AI system, including:

System's intended purpose.

Level of accuracy, including system's accuracy metrics, robustness, and cybersecurity against which the system has been tested and validated and that can be expected from the system. This should also include any known of foreseeable circumstances that may impact the expected levels of accuracy, robustness, and cybersecurity.

Any known and foreseeable circumstances which may lead to risks to health and safety or fundamental rights under the system's intended use or under foreseeable misuse, as referred to in Art. 9(2).

Where relevant, the AI system's technical features and capabilities to provide information that is relevant to clarify and explain its results.

Where relevant, performance regarding the specific persons or groups of persons on which the system is intended to be used.

Where relevant, specifications on input data or any other relevant information related to the training, validation, and testing datasets used.

Where relevant, information that helps deployers understand the system's output and to correctly use the system.

Reference

AI Act, Art. 13(3)(b)

7.6.3 Pre-determined changes

The instructions of use should include information on the pre-determined changes to the system and its performance. These are the changes, if any, that have been determined by the provider at the moment of the system's initial conformity assessment.

Reference

AI Act, Art. 13(3)(c)

7.6.4 Human oversight measures

The instructions of use should include information on the human oversight measures, as referred to in Art. 14, including the technical measures put in place to support the interpretation of the AI system outputs by deployers.

Reference

AI Act, Art. 13(3)(d)

7.6.5 Computational and hardware resources, expected lifetime and necessary maintenance measures

The instructions of use should include information of the computational and hardware resources needed by the AI system, its expected lifetime, as well as any necessary maintenance and care measures put in place, covering also software updates, including their frequency to ensure the proper functioning of the AI system.

Reference

AI Act, Art. 13(3)(e)

7.6.6 Log management

The instructions of use should include, where applicable, a detailed explanation of the features and mechanisms within the AI system that enable users to efficiently collect, store, and interpret the logs, as specified in Art.12.

Reference

AI Act, Art. 13(3)(ea)

7.7 Human oversight

AI systems must be designed to enable effective human oversight. Human-machine interfaces and appropriate measures should be implemented to prevent or minimise risks to health, safety, and fundamental rights. Oversight measures can include built-in capabilities within the AI system or measures identified by the provider and implemented by the user. Human oversight allows operators to understand system capabilities, detect anomalies, mitigate automation bias, interpret outputs correctly, make independent decisions, and intervene or stop the system.

Role

Provider

References

AI Act, Art. 14

7.7.1 Effective oversight

High-risk AI systems must be designed and developed to enable effective human oversight while the system is in use, inlcuding through suitable human-machine interfaces. High-risk AI system human oversight should focus on preventing or reducing health, safety, and fundamental rights risks that might arise when the system is used as intended or in reasonably foreseeable misuse conditions, especially when these risks persist despite adherence to other high-risk AI requirements under the AI Act.

Reference

AI Act, Art. 14(1)(2)

7.7.2 Human oversight measures

Human oversight measures should correspond to the risks, autonomy level, and usage context of the AI system. Human oversight must be achieved through either one or all of the following measures:

Measures identified and built into the high-risk AI system by the provider, if technically feasible, before the system is placed on the market or put into service.

Measures identified by the provider before market placement or service initiation that are appropriate measures that the high-risk AI system users can implement.

These measures must, as appropriate and proportionate to the circumstances, enable individuals responsible for human oversight to:

Properly understand the AI system's relevant capacities and limitations and monitor its operation, including identifying and addressing anomalies, dysfunctions, and unexpected performance.

Be and remain aware of the potential for 'automation bias' – excessive reliance on the AI system's output, particularly when these systems are used to provide information or recommendations for people to make decisions.

Correctly interpret the AI system's output considering for example the available interpretation methods and tools.

Make decisions to not use the AI system or disregard, override, or reverse its output in specific situations.

Intervene or interrupt the AI system's operation through a "stop" button or a similar procedure that ensures the system halts safely.

Reference

AI Act, Art. 14(3)(4)

7.7.3 Human oversight measures for biometric identification systems

AI systems intended to be used for the biometric identification of natural persons, the human oversight measures must ensure that the deployer takes no action or decision based on the identification resulting from the system, unless this has been separately verified and confirmed by at least two natural persons who have the necessary competence, training, and authority to do such verification and confirmation.

The rule that at least two people must check the system's work does not apply to high-risk AI used in law enforcement, migration, border control, or asylum situations if EU or national laws find this rule to be unnecessary.

Reference

AI Act, Art.14(5)

7.8 Accuracy, robustness and cybersecurity

AI systems should be designed and developed to ensure an appropriate level of accuracy, robustness, and cybersecurity throughout their lifecycle. Accompanying instructions of use should declare accuracy levels and relevant metrics. Resilience against errors, faults, and inconsistencies, including interactions with humans or other systems, is essential. Robustness can be achieved through technical redundancy solutions while addressing biases resulting from feedback loops is crucial for continuously learning AI systems. Unauthorised attempts to alter system use or performance must be resisted, requiring suitable cybersecurity measures. Technical solutions should address AI-specific vulnerabilities, including data poisoning, model poisoning, adversarial examples or model evasion, confidentiality attacks and model flaws.

Role

Provider

References

AI Act, Art. 15

7.8.1 Performance and accuracy assurance

High-risk AI systems must be designed and developed to ensure an appropriate levels of accuracy, robustness, and cybersecurity. These qualities and system's performance should be consistent throughout the AI system's lifecycle. These levels of accuracy and associated accuracy metrics must be provided in the instructions for use.

The Commission will collaborate with relevant stakeholders and organisations, like metrology and benchmarking authorities, to develop benchmarks and measurement methodologies for assessing the accuracy, robustness, and other relevant performance metrics.

Reference

AI Act, Art. 15(1)(1a)(2)

7.8.2 Resilience and robustness

High-risk AI systems must be as resilient as possible, to be able to handle errors, faults, and inconsistencies that may arise in their environment or due to interactions with people or other systems. Providers are required to undertake technical and organisational measures to achieve this requirement.

The AI robustness of AI system can be achieved through technical redundancy measures like backup or fail-safe plans. For AI systems that continue learning after deployment, steps must be taken to address potential biases stemming from feedback loops with appropriate mitigation measures. High-risk AI systems that continue learning after deployment should be developed to eliminate or to reduce as far as possible the risk of biased outputs affecting future inputs ('feedback loops'), ensuring these risks are properly managed with effective mitigation measures.

Reference

AI Act, Art. 15(3)

7.8.3 Cybersecurity resilience

High-risk AI systems must be able to resist unauthorised attempts to manipulate their use, outputs, or performance by exploiting vulnerabilities. The technical cybersecurity solutions must be suitable for the specific circumstances and risks.

These technical solutions should also address AI-specific vulnerabilities, where appropriate, including measures to prevent, detect, respond to, resolve, and control attacks such as:

Manipulating the training data (data poisoning), or pre-trained components used in training (model poisoning).

Providing misleading inputs causing the model to make a mistake (adversarial examples or model evasion).

Confidentiality attacks or model flaws.

Reference

AI Act, Art 15(4)

7.9 Quality management system

Providers of AI systems should establish a comprehensive quality management system to ensure compliance with the regulations. This system should be documented in written policies, procedures, and instructions, covering various aspects such as regulatory compliance strategy, design control and verification, development, quality control and assurance, examination, testing, and validation procedures, technical specifications, data management, risk management, post-market monitoring, incident reporting, communication protocols, record keeping, resource management, and an accountability framework.

The implementation of these aspects should be proportionate to the size of the provider's organisation. However, providers must always maintain the necessary diligence and protection level to guarantee their AI systems comply with the AI Act.

Role

Provider

References

AI Act, Art. 17

7.9.1 Strategy for compliance

The quality management system shall include a strategy that ensures the compliance with the AI Act. This shall include plan for compliance with AI system conformity assessment procedures and procedures for the management of modifications to the system.

Reference

AI Act, Art.17(1)(a)

7.9.2 Design, control, and verification procedures

The quality management system shall encompass processes, techniques, and systematic measures for designing, controlling, and verifying the high-risk AI system.

Reference

AI Act, Art 17(1)(b)

7.9.3 Development and quality assurance procedures

The quality management system shall include techniques, procedures, and systematic processes for developing, ensuring quality control, and providing quality assurance for the high-risk AI system.

Reference

AI Act, Art 17(1)(c)

7.9.4 Examination, testing, and validation procedures

The quality management system shall comprise examination, testing, and validation procedures to be conducted prior to, during, and following the development of the high-risk AI system, specifying their required frequency.

Reference

AI Act, Art 17(1)(d)

7.9.5 Technical specifications and compliance assurances

The quality management system shall encompass technical specifications, including standards. In cases where complete adherence to relevant harmonised standards is not achieved or they do not cover all the relevant requirements for high-risk AI systems set in Title III, Chapter II, the system should detail the methods to ensure compliance with the requirements for high-risk AI systems.

Reference

AI Act, Art 17(1)(e)

7.9.6 Data management systems and procedures

The quality management system shall include data management systems and procedures, covering data acquisition, collection, analysis, labelling, storage, filtration, mining, aggregation, retention, and any other data-related operations conducted prior to and for the purpose of introducing high-risk AI systems to the market or putting them into service.

Reference

AI Act, Art 17(1)(f)

7.9.7 Risk management system

The quality management system shall include the risk management system as detailed in Article 9 of the AI Act.

Reference

AI Act, Art 17(1)(g)

7.9.8 Establishment and maintenance of post-market monitoring system

The quality management system shall encompass the establishment, execution, and continuous maintenance of a post-market monitoring system, compliant with the requirements of Article 61.

Reference

AI Act, Art 17(1)(h)

7.9.9 Procedures for reporting serious incidents

The quality management system shall cover procedures regarding the reporting of serious incidents, as stipulated in Article 62.

Reference

AI Act, Art 17(1)(i)

7.9.10 Communication and management with regulatory authorities and relevant stakeholders

The quality management system shall cover the management of communication with national competent authorities, other relevant authorities, including those offering or facilitating data access, notified bodies, other stakeholders, customers, and interested parties

Reference

AI Act, Art 17(1)(j)

7.9.11 Record keeping systems and procedures

The quality management system shall cover processes and procedures for the maintenance and organisation of all relevant documentation and information.

Reference

AI Act, Art 17(1)(k)

7.9.12 Resource management

The quality management system shall include resource management, which also encompasses measures for ensuring supply security.

Reference

AI Act, Art 17(1)(l)

7.9.13 Accountability framework

The quality management system shall establish an accountability framework that outlines the roles and responsibilities of management and other personnel concerning all the aspects required from the quality management system.

Reference

AI Act, Art 17(1)(m)

7.9.14 Providers subject to quality management system under sectorial Union law

Providers of high-risk AI systems already under sector-specific EU laws for quality management systems or similar functions can incorporate the requirements into their existing quality management systems as dictated by those laws.

Reference

AI Act, Art. 17(2a)

7.9.15 Integrated quality management system - Directive 2013/36/EU

Financial institution providers subject to internal governance, arrangements, or process requirements under EU financial services legislation are considered to have met most of the quality management system obligation by adhering to the internal governance rules under the relevant EU financial laws. Within this framework, any harmonised standards mentioned in Article 40 of the AI Act should also be considered.

Excluded from this are the following quality management system obligations:

Risk management system.

Establishment and maintenance of post-market monitoring system.

Procedures for reporting serious incidents.

Reference

AI Act, Art 17(3)

7.10 Conformity assessment

To demonstrate compliance with the requirements of the AI Act, providers of high-risk AI systems must follow a conformity assessment process based on internal control or based on the assessment of the quality management system and the technical documentation by a notified body. Furthermore, for high-risk AI systems listed in Annex II, section A, providers are obligated to follow the conformity assessment as required by the relevant act.

Role

Provider

References

AI Act, Art. 43, Annexes VI, VII

7.10.1 Presumption of conformity with certain requirements

High-risk AI systems trained and tested on data that accurately represents the environment they are meant to operate in are assumed to meet the Data and data governance's dataset relevance and applicability requirement referred to in Art. 10(4).

Similarly, high-risk AI systems that have received a cybersecurity certification or conformity statement under The Cybersecurity Act (Regulation (EU) 2019/881), with references published in the EU Official Journal, are assumed to comply with Accuracy, robustness, and cybersecurity requirement referred to in Art. 15, as far as the certification or conformity statement encompasses these requirements.

Reference

AI Act, Art. 42

7.10.2 Harmonised standards and common specifications

High-risk AI systems that align with established harmonised standards detailed in the Official Journal of the European Union, are considered compliant with the high-risk AI system requirements detailed in Chapter 2 of the AI Act or where relevant, with the requirements concerning GPAI models, as long as these standards address those requirements. The Commission will issue requests for AI standardisation to improve resource efficiency and energy use in high-risk and general-purpose AI systems, consulting with key stakeholders and ensuring alignment with EU values and safety legislation.

If no harmonised standards exist, they are deemed to be insufficient or lacking consideration of specific safety or fundamental rights, the Commission can establish common specifications. If high-risk AI systems meet these common specifications they are also deemed compliant with the high-risk AI system requirements detailed in Chapter 2 of the AI Act, as long as these common specifications address those requirements. If providers deviate from these specifications, they must adequately justify equivalent technical solutions.

Following consultations with the Advisory Forum, referred to in Art. 58a, the Commission can establish common specifications for AI systems, in line with Chapter 2's requirements for high-risk AI systems, or for requirements for GPAI models, provided the following conditions are met:

The Commission's request for harmonised standards under Regulation 1025/2012 is either not accepted, not met by the deadline, inadequately addresses fundamental rights, or fails to comply.

No harmonised standards for Chapter II high-risk AI system requirements have been or are expected to be published in the EU Official Journal within a reasonable timeframe.

If high-risk AI systems meet these common specifications they are also deemed compliant with the high-risk AI system requirements detailed in Chapter 2 of the AI Act, as long as these common specifications address those requirements. If providers deviate from these specifications, they must adequately justify equivalent technical solutions that meet the requirements for high-risk AI systems in Chapter II at an equivalent level.

Reference

AI Act, Art. 40, 41

7.10.3 Conformity assessment procedure based on internal control

The self-certification process is suitable for most standalone high-risk AI systems, with the exception of biometric systems to which additional criteria apply.

As part of the internal control assessment, the provider of the high-risk AI system performs a self-evaluation to verify that the AI system's quality management system, technical documentation, and post-market monitoring plan adhere to the requirements stipulated in the AI Act.

The internal conformity assessment consists of the following steps:

The AI system provider confirms that the quality management system in place adheres to the standards specified in Article 17 of the AI Act.

The AI system provider assesses the information within the technical documentation to ensure the AI system complies with the essential requirements outlined in the requirements for high-risk systems in Chapter 2 of the AI Act.

Additionally, the AI system provider ensures that the AI system's design, development process, and post-market monitoring, as defined in Article 61, align with the technical documentation.

In the case of biometric systems referred to in Annex III point 1, the provider of such biometric system must follow the conformity assessment procedure based on third-party assessment under the following conditions:

There are no harmonised standards under Art. 40 or common specifications under Art. 41 available.

The provider did not fully apply the harmonised standards.

The provider has not applied existing common specifications.

The common specifications exist but were not applied by the provider.

Where any harmonised standard mentioned has been published with restrictions, but only concerning the restricted parts.

However, in situations where the biometric identification systems either apply harmonised standards or common specifications, such systems can be certified in accordance with the conformity assessment based on internal control.

Reference

AI Act, Art. 43(1)(2), Annex VI

7.10.4 Conformity based on third-party assessment

The third-party conformity assessment is applicable to safety components of products or systems specified in Annex II of the AI Act, as well as certain biometric systems referred to in Annex III point 1.

In conformity based on third-party assessment, an independent third party, a notified body, conducts the conformity assessment, evaluating both the quality management system and the technical documentation as per the procedures detailed in Annex VII of the AI Act. This procedure involves several steps, including the following:

Overview: The provider's quality management system for AI system design, development, and testing is assessed and monitored. Technical documentation of the AI system is also evaluated.

Quality Management System Assessment: The provider's application must include various details, and the quality management system is examined to determine if it meets the necessary requirements referred to in Art. 17. Any intended changes to the system require notification and reassessment by the notified body.

Technical Documentation Control: The technical documentation related to the AI system is reviewed by the notified body. The provider must provide full access to the training, validation, and testing datasets, including when appropriate and subject to security protections, through APIs or other relevant technical means and tools. This access must be granted to the notified body when this is relevant to their duties and is within the scope of their duties. When reviewing the technical documentation, the notified body can request additional evidence or tests from the provider to thoroughly assess the AI system's compliance with Title III, Chapter 2 requirements. If the tests provided by the provider are insufficient, the notified body will conduct the necessary tests directly. Lastly, if after trying all other reasonable methods to verify compliance and finding them inadequate, upon a reasoned request, the notified body must be given access to the AI system's training and trained models, including relevant parameters, to assess conformity with high-risk AI system requirement in Title III, Chapter 2. This access must respect EU laws on intellectual property and trade secret protection.

Assessment Outcome: Based on the assessment of the quality management system and the technical documentation, an EU technical documentation assessment certificate is either issued if the AI system meets requirements or refused if it does not meet the necessary requirements. Where the system needs retraining due to data issues, a new conformity assessment is required. Furthermore, any changes to the system that could affect the system's compliance after it has obtained the certificate of conformity assessment, require approval from the notified body.

Surveillance of the Quality Management System: Periodic audits that may include additional testing of the system, are conducted to ensure the provider maintains and applies the quality management system correctly. This entails the provider granting the notified body access to the facilities where AI systems are

designed, developed, and tested, and the provider must also provide the notified body with all required information.

Reference

AI Act, Art. 43(1), Annex VII

7.10.5 Conformity assessment of high-risk AI systems in Annex II, section A

For high-risk AI systems listed in Annex II, section A, providers are obligated to follow the conformity assessment as required by the relevant act. However, this assessment must include:

The AI system's compliance with requirements for high-risk AI systems specified in Chapter 2 of the AI Act.

Evaluation of the high-risk AI system's technical documentation as specified in points 4.3, 4.4, and 4.5 in Annex VII (Technical Documentation Control).

If the legal acts in Annex II, section A permit providers to opt-out of the conformity assessment, they can only do so if they meet the criteria outlined in those acts and have applied harmonised standards or common specifications confirming the high-risk AI system requirements in Chapter II of the AI Act.

Reference

AI Act, Art. 43(3), Annex II, Section a, Annex VII points 4.3, 4.4, 4.5

7.10.6 Requirement to undergo new conformity assessment

High-risk AI systems that have already been subject to conformity assessment procedure, are required to undergo a new conformity assessment if they are substantially modified, whether they are intended for further distribution or remain in use by the current deployer. Substantial modification refers to any unplanned or unforeseen change made to an AI system after its market introduction that has not been foreseen in the initial conformity assessment, and thus impacts the system's compliance with the high-risk AI system requirements in Title III, Chapter 2 of the AI Act, or alters its originally assessed intended purpose.

In situations where a high-risk AI system continues learning after being put on the market, any predetermined changes to the system's performance, specified by the provider during the initial conformity assessment and included in the technical documentation, are not considered substantial modifications if implemented post-market placement.

Reference

AI Act, Art. 43(4), 3(23)

7.10.7 Certificate of conformity

Certificates issued by notified bodies for conformity based on third-party assessment are drawn in a language easily understandable by the relevant authorities in the Member State of the notifying body.

These certificates are valid for a maximum of five years for AI systems covered in Annex II, and extendable for a maximum of 5 years upon the provider applying for extensions. For AI systems covered by Annex III, the certificated are valid for a maximum of four years, extendable for a maximum of 4 years upon the provider applying for an extension. The extension of the certificate will be determined through a re-assessment of the conformity. Any supplement to the certificate will remain valid as long as the main certificate itself is valid.

If an AI system no longer meets the requirements for high-risk AI systems determined in Chapter 2 of the AI Act, the notified body can suspend or withdraw the certificate, with reasons provided, unless the provider takes corrective action within a specified deadline.

Providers will be able to appeal against decisions of the notified bodies, including on issued conformity certificates.

Reference

AI Act, Art. 44

7.10.8 EU declaration of conformity

The provider must create an EU declaration of conformity for each AI system, keeping it accessible to national competent authorities for 10 years post-market placement. The EU declaration of conformity must be written machine-readable and physically or electronically signed.

This declaration must state the AI system's compliance with high-risk AI system requirements in Chapter 2 of the AI Act, and include the following information:

AI system name, type, and identifiable reference;

Provider's name and address (or their authorised representative's);

A statement confirming the AI system provider's sole responsibility of the EU declaration;

A statement confirming that the AI system is in conformity with the AI Act and with other relevant Union legislation that requires issuing of EU declaration of conformity;

A statement confirming that the AI system complies with the GDPR (Regulation (EU) 2016/679), Law Enforcement Directive (Directive (EU) 2016/680)), and the Regulation on the processing of personal data by EU institutions (Regulation (EU) 2018/1725)), where the system involves the processing of personal data.

References to applicable harmonised standards or common specifications to which the system conforms;

Where relevant, the name and identification number of notified body, description of conformity assessment procedure, and certificate of conformity information;

Declaration of conformity details, including place, date, signer's name and function, and indication of the entity represented, with a signature.

This declaration must be translated into a language that is easily understood by the national competent authorities of the Member State(s) in which the high-risk system is placed on the market or made available.

When high-risk AI systems are subject to multiple Union harmonisation legislation requiring an EU declaration of conformity, a consolidated declaration covering all applicable legislations is required. By drawing up the declaration, the provider assumes responsibility for the system's compliance with high-risk AI system requirements referred to in Chapter 2 of the AI Act and is responsible for keeping the declaration up-to-date.

Reference

AI Act, Art. 48, Annex V

7.10.9 CE marking of conformity

The CE marking of conformity must comply with the general principles outlined in Art. 30 of Regulation (EC) 765/2008:

The CE marking must be applied exclusively by the manufacturer or their authorised representative.

It should only be affixed to products specified by EU harmonisation legislation.

Applying the CE marking signifies the manufacturer's commitment to comply with all relevant EU legislation requirements.

The CE marking is the only mark that indicates a product's conformity with applicable EU standards.

Misleading markings that could confuse the meaning or appearance of the CE marking are not allowed. Other markings can be added as long as they do not affect the CE marking's visibility or interpretation.

EU Member States are responsible for ensuring the proper use of the CE marking, including implementing penalties for misuse, which can range from fines to criminal sanctions for serious violations. These penalties are designed to be proportional and act as a deterrent.

High-risk AI systems offered digitally must feature a digital CE marking that is easily accessible either through the system's interface or via machine-readable code or other electronic means. For physical high-risk AI systems, the CE marking must be visible, legible, and permanent, placed on the packaging or accompanying documentation if direct affixing is not feasible. Additionally, where relevant, the CE marking shall include the identification number of the notified body responsible for conformity assessment. The identification number of the notified body is affixed by the notified body itself, or by the provider or by its authorised representative based on the instructions of the notified body. This identification number must also be included in any promotional material that states the high-risk AI system meets the CE marking requirements.

If a high-risk AI system falls under other Union laws requiring a CE marking, this marking will also confirm compliance with those laws.

Reference

AI Act, Art. 49; Regulation (EC) 765/2008, Art. 30

7.11 Obligations of providers of high-risk AI systems

Providers of high-risk AI systems are subject to obligations in relation to automatically generated logs, corrective actions, risk notification, cooperation with authorities, EU database, post-market monitoring plan, as well as incident and malfunction reporting.

Role

Provider

References

AI Act, Art. 16, 18, 20, 21, 23, 51, 60, 62

7.11.1 Identification and contact information

Providers are required to display their name, registered trade name or trademark, and contact address on the high-risk AI system itself, or where that is not possible, on its packaging or accompanying documentation, as appropriate.

Reference

AI Act, Art. 16(aa)

7.11.2 Document retention

The provider of high-risk AI system must retain, for 10 years after the AI system is placed on the market or put into service, and make available to national competent authorities:

Technical documentation, referred to in Art. 11.

Documentation on the quality management system, referred to in Art. 17.

Documentation of the changes approved by notified bodies, if applicable.

Decisions and other documents issued by notified bodies, if applicable.

The EU declaration of conformity, referred to in Art. 48.

Member States will set conditions for keeping documentation available to national authorities if a provider goes bankrupt or stops operations before the period ends.

Providers that are financial institutions subject to requirements concerning their internal governance, arrangements, or processes under Union financial services legislation must integrate technical documentation into their records as required by the relevant EU financial services legislation.

Reference

AI Act, Art. 18

7.11.3 Automatically generated logs

Providers of high-risk AI systems must retain the logs automatically generated by their systems, referred to in Art. 12(1), as far as these logs are under their control. In accordance with Union or national law, and specifically considering laws on personal data protection, logs must be stored for a duration suitable for the high-risk AI system's intended use, for a minimum of six months, unless otherwise specified by relevant laws.

Financial institutions governed by EU financial services legislation regarding internal governance and processes, are required to retain automatically generated logs from their high-risk systems within the documentation required by relevant EU financial services laws.

Reference

AI Act, Art. 20

7.11.4 Corrective actions and duty of information

Providers of high-risk AI systems, upon recognising or having a reason to believe that a system does not conform to requirements established by the AI Act, must without delay take corrective measures to ensure compliance. This involves bringing the system into conformity, withdrawing it, disabling it, or recalling it, as deemed necessary. AI system providers must also inform relevant distributors of it, and, where applicable, also deployers and authorised representatives.

In a situation where a high-risk AI system provider becomes aware that the high-risk AI system poses a risk to the health or safety or to the protection of fundamental rights of persons, the AI system provider must immediately investigate the causes in collaboration with the deployer, and where relevant, inform the market surveillance authorities in the Member States where the system is available. Providers must also notify the notified body that granted a certificate of conformity, referred to in Art. 44 , for the high-risk AI system. This notification should include information about the nature of non-compliance and any corrective actions that have been taken.

The risk for which notification must be submitted refers to a product that has the potential to harm people's health and safety, including at workplace, consumer protection, the environment, public security, and other public interests protected by Union harmonisation legislation. This refers to harm that goes

beyond what is acceptable based on the product's intended purpose and typical usage conditions, including how long it is used, as well as any installation and maintenance requirements.

Reference

AI Act, Art. 21, 65(1); Regulation (EU) 2019/1020, Art. 3(19)

7.11.5 Cooperation with authorities

Upon a reasoned request by a competent national authority, providers of high-risk AI systems must provide them all necessary information and documents to demonstrate that the AI system complies with the requirements for high-risk AI system.

Where the authority requests, providers must also allow access to the system's logs,, referred to in Art. 12(1) as long as these logs are controlled by the AI system provider.

All information gathered by a national competent authority must be handled according to the confidentiality requirements specified in Article 70.

Reference

AI Act, Art. 16(j), 23

7.11.6 Accessibility requirements

Providers are responsible for making sure their high-risk AI system meets the accessibility standards set by Directive 2019/882 on product and service accessibility and Directive 2016/2102 on the accessibility of public sector websites and mobile applications.

Reference

AI Act, Art. 16(ja); Directive 2019/882; Directive 2016/2102

7.11.7 Registration to EU or national database

Prior to introducing a standalone high-risk AI system, as mentioned in Annex III, to the market or putting it into use, the provider or their authorised representative must register the system in the EU database.

High-risk AI systems used in the area of critical infrastructure (point 2, Annex III) are exempted from the EU database registration. Instead, such systems must be registered at a national level.

This registration obligation also applies to providers who have concluded that their system is not high-risk by using the procedure under Article 6(2a). Either the provider or the authorised representative must register the system.

Providers will input the data specified in Annex VIII that contains the following information required:

Details of the provider (name, address, contact information).

Where submission of information to the database is handled by someone else, the name, address and contact details of that person.

Information (name, address, and contact details) on the authorised representative, if applicable.

AI system trade name and a unique reference for identification.

Description of the AI system's intended purpose and the components and functions supported through the AI system.

Simple and concise description of the information used by the system (data, inputs) and the system's operating logic.

The status of the AI system (e.g., on the market, in service, recalled).

Certificate details (type, number, expiry date, notified body's name/ID), if applicable.

A scanned copy of the certificate issued by notified body, if applicable.

List of Member States where the AI system has been placed on the market or put into service.

Copy of the EU declaration of conformity.

Electronic instructions for use (excluding high-risk AI systems in the areas of law enforcement and migration, asylum and border control management).

Optional URL for additional information.

The information in the database will be publicly accessible but will only contain necessary personal data, such as the names and contact details of individuals authorised to represent the provider.

Reference

AI Act, Art. 51(1)(1d), 60, Annex VIII Section A

7.11.8 Reporting of serious incidents

Providers of high-risk AI systems must report serious incidents to the market surveillance authorities in the Member State where the incident occurred. Market surveillance authorities will further notify relevant national public bodies after receiving information from the provider.

A serious incident refers to any situation or malfunction involving an AI system that directly or indirectly causes one or more of the following outcomes: the death of an individual or severe harm to a person's health; significant and irreversible disruption to the functioning and management of critical infrastructure; a breach of obligations laid out by EU legislation designed to safeguard fundamental rights; or considerable damage to property or the environment.

As a general rule, the period for reporting a serious incident must take into account the severity of the serious incident. To ensure prompt reporting, the provider or deployer can first submit an incomplete initial report, followed by a detailed complete report later. The reporting of the incident must be made as soon as the provider links the AI system to the incident or determines a reasonable likelihood of such a link, but no later than 15 days after either the provider's or deployer's awareness of the incident. However, the following exceptions apply:

The reporting of the serious incident must be done immediately or no later than two days after the provider or deployer becomes aware of the incident where the incident is a widespread infringement as referred to Art. 3(44e). Widespread infringement refers to a violation of EU law that negatively impacts people's rights in at least two Member States other than where the violation occurred or where the responsible provider, its authorised representative, or deployer is located. This includes actions that harm, or could harm, groups of people across three or more Member States, involving similar illegal activities, affecting the same rights, and carried out by the same operator at the same time.

In the event of death of person, serious incident must be reported immediately after the provide or deployerhas established or suspects a link between the high-risk AI system and serious incident. The reporting of the incident must be made no later than 10 days after the provider of deployer has become aware of it.

After reporting a serious incident, the provider must immediately investigate the incident and the AI system involved. This includes assessing the risks and planning corrective actions. The provider must work with the relevant authorities and, if applicable, the notified body during the investigation. They should

not alter the AI system in any way that could impact the analysis of the incident's causes without first informing the authorities.

For high-risk AI systems listed in Annex III placed on the market or put into service by providers already subject to similar reporting requirements under different union legislation, reporting of serious incidents is only necessary for those defined in Article 3(44)(c). Furthermore, if the high-risk AI systems are safety components or devices under Medical devices regulation (Regulation (EU) 2017/745) and In-vitro diagnostic medical devices regulation (Regulation (EU) 2017/746), incident reports should also focus on Article 3(44)(c) events and be directed to the national authority selected by the Member State where the incident took place.

Reference

AI Act, Art. 62, 3(44), 3(44e)

7.12 Post-market monitoring

Providers of high-risk AI systems must establish a post-monitoring system, consisting of proactive actions and measures conducted by AI system providers to gather and assess insights gained from the usage of their systems after it has been placed on the market or put into service. The aim of the post-market monitoring is to promptly identify and implement any necessary corrective or preventive actions.

Role

Provider

References

AI Act, Art. 61

7.12.1 Post-market monitoring plan

Providers of high-risk AI systems must establish and document a post-market monitoring system, consisting of actions, policies, procedures, and instructions that matches the complexity and risks associated with their AI technology. A post-market monitoring plan must be created and is considered part of the technical documentation. The Commission will provide a template for the post-market monitoring system plan six months before the AI Act enters into application.

The post-market monitoring system must actively collect and analyse data on the AI system's performance throughout its entire lifecycle to ensure ongoing compliance with the requirements of high-risk AI systems set out in Chapter 2 of the AI Act. The data for the post-market monitoring system can be provided by deployers of the AI system or collected from other sources.

When applicable, post-market monitoring should examine how the AI system interacts with other AI systems. However, this requirement does not extend to the sensitive operational data held by deployers who are law enforcement authorities.

Providers of AI systems under existing EU harmonisation legislation regulating post-market monitoring rules (Annex II, Section A) may integrate AI Act monitoring obligations into their current post-market monitoring systems if equivalent protection levels are maintained. This option extends also to financial institutions offering high-risk AI systems (Annex III, point 5) related to essential services, provided they are subject to internal governance, arrangements, and processes under EU financial services legislation.

Reference

AI Act, Art. 61

7.13 Enforcement by market surveillance authorities

Providers and deployers, and other operators, where relevant, must grant access to AI system documentation, technical information, as well as in certain cases, to system data and source code. Furthermore, all operators are required to cooperate with market surveillance authorities as they enforce the compliance with AI Act.

Role

Provider,Deployer,Importer,Distributor,Authorised representative

References

AI Act, Chapter 3, Art. 63-68

7.13.1 Application of Regulation (EU) 2019/1020 on Market Surveillance and Compliance of Products

The Regulation (EU) 2019/1020 on Market Surveillance and Compliance of Products applies to all operators and AI systems that fall into the scope of the AI Act. The Regulation strengthens the market

surveillance of products and lays down rules and procedures for economic operators, establishing a system for their cooperation with supervisory authorities.

Under the Regulation 2019/1020, the market surveillance authorities have broad powers to ensure compliance with EU legislation, including:

Requesting documents, technical details, data, compliance information, and access to embedded software from economic operators.

Demanding information on supply chains, distribution networks, product quantities, and similar models for compliance purposes.

Requiring details to verify website ownership related to investigations.

Conducting unannounced inspections and product checks.

Entering business premises to detect non-compliance and gather evidence.

Initiating investigations to identify and address non-compliance.

Ordering economic operators to correct non-compliance or mitigate risks.

Enforcing measures against non-compliance, including market restrictions or product recalls.

Imposing penalties.

Obtaining product samples covertly for inspection and evidence.

In cases of serious risk, demanding online content removal or warnings and restricting access to online interfaces.

Utilising any form of information or evidence obtained during investigations.

Reference

AI Act, Art. 63(1); Regulation (EU) 2019/1020 on Market Surveillance and Compliance of Products, Art. 14(4)

7.13.2 Access to high-risk AI system documentation, data, and source code

The providers of high-risk AI systems must provide the relevant market surveillance authorities complete access to the documentation, training, validation, and testing data for the high-risk AI system, where appropriate and subject to security measures, via APIs or other technical methods that allow for remote access.

Furthermore, providers must grant the market surveillance authorities access to the source code, when the following conditions are met:

Access to source code is necessary for assessing high-risk AI system's compliance with requirements set in Title III, Chapter 2 of the AI Act.

The market surveillance authority's other methods, including testing/auditing procedures and verifications based on the documentation and data have been exhausted or proven insufficient to verify compliance.

All obtained information must be handled according to confidentiality (Art. 70).

Reference

AI Act, Art. 63(7a)(7b)(7c)

7.13.3 Monitoring and information access for general-purpose AI systems

When a provider develops both a general purpose AI model and the AI system that uses it, the AI Office has the authority to monitor and supervise the AI system's compliance with AI Act. The AI Office has the same powers as market surveillance authorities under the Regulation (EU) 2019/1020 on Market Surveillance and Compliance of Products, including, for example, the right to request access to relevant documents, technical details, data, compliance information, and embedded software.

If market surveillance authorities suspect a general purpose AI system, usable directly for high-risk applications, is not compliant with the relevant requirements under the AI Act, they must collaborate with the AI Office for a compliance review and notify the EU AI Board and other market surveillance authorities authorities.

Where a national authority, when investigating high-risk AI system's compliance, face challenges in accessing necessary information on the general-purpose AI model used in the high-risk AI system for its investigation, it can request assistance from the AI Office. The AI Office will provide relevant information on the general-purpose AI model within 30 days while maintaining confidentiality (Art. 70).

Reference

AI Act, Art. 63a

7.13.4 Supervision of AI system testing in real-world conditions

Market surveillance authorities are tasked with ensuring that real-world testing of AI systems complies with this Regulation.

The market surveillance authorities are responsible for verifying compliance with Art. 54a for AI systems for which testing in real-world conditions is conducted within a regulatory sandbox in accordance with Art. 54.

If the authority is informed of a serious incident or it suspects non-compliance with sandbox conditions, the authority can either suspend or terminate the testing, or modify the aspects of the real-world testing. Decisions or objections made by authorities will explain their reasoning and how providers can contest them. Additionally, if a decision impacts testing, authorities must share their reasons with counterparts in other Member States where the AI system was tested.

Reference

AI Act, Art. 63b

7.13.5 Access of authorities protecting fundamental rights to high-risk AI system documentation

National public authorities or bodies safeguarding fundamental rights, including non-discrimination, have the right to request and access all documentation created and maintained under the AI Act for standalone high-risk AI systems specified in Annex III. Access in an accessible format and language must be granted when necessary in order for the public authorities to fulfil their responsibilities effectively. All information will be treated confidentially (Art. 70).

In case the provided documentation is insufficient to determine whether a breach of Union law safeguarding fundamental rights has occurred, the relevant public authority or body can request technical testing of the high-risk system, organised by the market surveillance authority.

Reference

AI Act, Art. 64

7.13.6 Non-compliant AI systems presenting a risk at the national level

AI systems presenting a risk to health, safety, and fundamental rights are understood as systems that have the potential to harm people's health and safety, including at the workplace, consumer protection, the environment, public security, and other public interests protected by Union harmonisation legislation. This refers to harm that goes beyond what is acceptable based on the product's intended purpose and typical usage conditions, including how long it is used and any installation and maintenance requirements.

Where a Member State's market surveillance authority believes an AI system poses such risks, it will evaluate the system's compliance with the AI Act, paying special attention to potential impacts on vulnerable groups. Where risks to fundamental rights are identified, the relevant operators must cooperate with market surveillance authorities and public authorities and bodies protecting fundamental rights.

Where the market surveillance authority finds out, based on the evaluation that the system does not comply with the AI Act, the relevant operators must take corrective actions without undue delay, including possible market withdrawal or recall within period of time no later than 15 days. The authority will inform both the notified body and, if risks extend beyond national borders, the Commission and other Member States.

Failure to take adequate corrective actions may lead to provisional national measures to limit the AI system's availability, which will be communicated across Member States for further action or objection. Measures taken are subject to review and, if unchallenged within 3 months (or 30 days for non-compliance with prohibited AI practices), are considered justified.

If a market surveillance authority from one Member State disagrees with another's decision about an AI system, or if the European Commission thinks the decision breaks EU law, the Commission will quickly discuss it with the involved Member State and the AI system's operators. They will review the decision and decide if the original decision was correct within six months (or just 60 days for certain serious violations). This decision will be shared with all Member States. If the Commission agrees with the decision, every Member State must take steps like removing the AI system from sale. If the Commission disagrees, the Member State that made the original decision must cancel it. Also, if the problem was due to issues with the standards or specifications the AI system was supposed to meet, the Commission will handle it according to specific EU procedures.

Reference

AI Act, Art. 65, 66; Regulation (EU) 2019/1020, Art. 3(19)

7.13.7 Compliant AI systems presenting risk at the national level

AI systems presenting a risk to health, safety, and fundamental rights are understood as systems that have the potential to harm people's health and safety, including at the workplace, consumer protection, the environment, public security, and other public interests protected by Union harmonisation legislation. This refers to harm that goes beyond what is acceptable based on the product's intended purpose and typical usage conditions, including how long it is used and any installation and maintenance requirements.

Where a Member State's market surveillance authority believes an AI system poses such risks, it will evaluate the system's compliance with the AI Act, paying special attention to potential impacts on vulnerable groups. Where risks to fundamental rights are identified, the relevant operators must cooperate with market surveillance authorities and public authorities and bodies protecting fundamental rights.

Where the market surveillance authority finds out, based on the evaluation, that the high-risk AI system is compliant with the AI Act, but the system poses risks to health, safety, fundamental rights, or the public interest, the operator is required to take appropriate measures. These appropriate measures must be taken without undue delay and within the timeframe provided by the authority to ensure that the system, when placed on the Union market or put into service, no longer presents a risk. The AI system provider or other relevant operators must ensure that the necessary corrective actions are implemented for all concerned AI systems throughout the Union.

Member States are required to notify the Commission and other Member States, detailing the AI system's information, including data for identification, the origin of the system and its supply chain, as well as the nature of the risk it poses and the nature and duration of national measures. The Commission will review these national actions, decide on their appropriateness, and, if needed, suggest further measures. This decision and any proposed actions will be communicated promptly to all concerned Member States and operators.

Reference

AI Act, Art. 65, 67; Regulation (EU) 2019/1020, Art. 3(19)

7.13.8 AI systems classified as not high-risk AI systems

Where a market surveillance authority has sufficient reason to suspect that an AI system, classified as non-high-risk in Annex III by the provider, is actually high-risk under Annex III, the market surveillance authority will evaluate the system's classification.

In the situation where the market surveillance authority finds that the AI system concerned is high-risk, the provider will be required to comply with the AI Act and take appropriate corrective actions. Where the system's use extends beyond national borders, the authority will notify the Commission and other Member States about the evaluation and required actions.

Providers must correct any non-compliance or face penalties as outlined in Article 71. Failure to take timely corrective action triggers further actions such as prohibiting or restricting the AI system's availability on the market and service or withdrawing or recalling it from the market.

Where the authorities find that the AI system was misclassified to evade requirements for high-risk AI systems under AI Act, the provider will be subject to fines in accordance with Art. 71.

To exercise their power and monitor the classification of AI systems, the authorities will conduct checks, including reviewing data in the EU database, to enforce compliance.

Reference

AI Act, Art. 65a, 65(5-9)

7.13.9 Formal non-compliance

Where a Member State's market surveillance authority identifies any of the following issues, it will require the provider to correct the non-compliance within a set timeframe:

Incorrect CE marking

Missing CE marking,

Missing EU declaration of conformity,

Incorrect EU declaration of conformity,

Failure to register in the EU database,

Failure to appoint an authorised representative, if needed,

Lack of technical documentation.

Should the non-compliance continue, the authority will take necessary actions to either limit the availability of the high-risk AI system on the market or require system recall or removal promptly.

Reference

AI Act, Art. 68

7.14 Appointment and obligations of authorised representative

Providers from outside the EU must appoint an authorised representative within the EU. The authorised representative is responsible for ensuring the system's conformity with EU regulations, maintaining essential documentation, collaborating with authorities to mitigate risks, and fulfilling registration requirements, and has the authority to terminate the mandate if the provider fails to meet its obligations.

Role

Provider,Authorised representative

References

AI Act, Art. 25

7.14.1 Appointment and mandate of the authorised representative

Before making their systems available in the EU market, providers established outside the EU must appoint an authorised representative, which is established in the EU, through a written mandate. Providers are also responsible for ensuring that their authorised representative can fulfil their duties and tasks under the AI Act.

Reference

AI Act, Art. 25(1)(1b)(2)

7.14.2 Tasks of the authorised representative

The authorised representative, appointed by the provider, must fulfil tasks outlined in their mandate and present a copy of it to market surveillance authorities upon request. The copy of the mandate must be presented in one of the official languages of the EU which will be determined by the national authority.

The tasks of the authorised representative include:

Verifying that the EU declaration of conformity and technical documentation are properly prepared by the provider, and a conformity assessment by the provider has been conducted.

Keeping at the disposal of national authorities for 10 years after the AI system is placed on the market or put into service, the provider's contact details, a copy of the EU declaration of conformity, technical documentation, and a certificate issued by the notified body, where relevant.

Providing necessary information and documentation to national competent authorities upon reasoned request, to demonstrate system's compliance with high-risk AI system requirements in Chapter 2, Title III. Information that must be provided includes access to the AI system's logs, as far as these are under the provider's control.

Cooperating with competent authorities on actions the authority takes concerning the high-risk AI system, in particular, to reduce and mitigate the risk posed by the high-risk AI system.

Where relevant, fulfilling registration obligations to the EU database (Art.51(1), or ensuring the accuracy of the information if registration is completed by the provider.

The mandate allows competent authorities to contact the authorised representative regarding compliance issues instead of or in addition to the provider.

Reference

AI Act, Art. 25(2)

7.14.3 Termination of mandate by authorised representative

Where the authorised representative considers or has reason to consider that the provider is not meeting its obligations under the AI Act, the authorised representative must terminate the mandate giving it the authority to act as authorised representative. When the authorised representative terminates the mandate, it must immediately notify the market surveillance authority in its Member State and, if relevant, the notified body, about termination of the mandate and the reasons for the termination.

Reference

AI Act, Art.25(2b)

7.15 Importer obligations

Importers of high-risk AI systems are subject to a set of pre-market placement requirements. Importers must also ensure the system's compliance with AI Act is not compromised when the system is under their responsibility. Importers are also required to cooperate with national authorities.

Role

Importer

References

AI Act, Art. 26

7.15.1 Pre-market placement obligations

Before placing a high-risk AI system on the market, importers of high-risk AI systems must verify that:

The system has undergone the appropriate conformity assessment procedure by the AI system provider, as set in Art. 43.

The provider has prepared the technical documentation, as set in Art. 11 and Annex IV.

The system bears the CE marking and has the accompanying EU declaration of conformity and instructions of use.

The provider has appointed an authorised representative, as set in Art. 25(1).

Where an importer has sufficient reason to consider that the system does not comply with the AI Act, its compliance is falsified, or the system is accompanied with falsified documentation, they must ensure that the system complies with the AI Act before placing it into market. Where the high-risk system presents a risk to people's health and safety, and fundamental rights the importer must inform the system provider, its authorised representative, and the market surveillance authorities of these.

Reference

AI Act, Art. 26(1)(2)

7.15.2 Identification and contact information

Importers of high-risk AI systems must display on the system and in the system packaging or in the accompanying documentation the following information of the importer:

Name

Registered trade name or trademark

Contact address.

Reference

AI Act, Art. 26(3)

7.15.3 Compliance assurance

Importers must ensure that storage and transportation conditions, while the high-risk AI system is under their responsibility, do not compromise its compliance with the requirements high-risk AI systems are subject to in Chapter 2, Title III of the AI Act.

Reference

AI Act, Art. 26(4)

7.15.4 Document retention

Importers are required to retain a copy of the certificate issued by the notified body (if applicable), the instructions for use, and the EU declaration of conformity for a period of 10 years after the AI system is placed on the market or put into service.

Reference

AI Act, Art. 26(4a)

7.15.5 Information provision and collaboration

Importers must, upon a reasoned request, provide the national authorities with all necessary information and documentation in a language that can be understood easily, including the certification issued by the notified body, instructions for use, and EU declaration of conformity to demonstrate the system's compliance with high-risk AI system requirements set in Chapter 2, Title III of the AI Act. Importers must also ensure that the technical documentation of the high-risk AI system can be made available to those authorities.

Reference

AI Act, Art. 26(5)

7.15.6 Cooperation with national authorities

Importers must work together with national authorities on any measures they implement, especially those aimed at reducing and mitigating the risks posed by the high-risk AI system.

Reference

AI Act, Art. 26(5a)

7.16 Distributor obligations

Distributors of high-risk AI systems are subject to set of pre-market placement requirements. Distributors must also ensure that system compliance is not compromised and undertake corrective actions where system may not meet the necessary requirements. Distributors are also required to cooperate with national authorities upon requests.

Role

Distributor

References

AI Act, Art. 27

7.16.1 Pre-market verification

Distributors of high-risk AI systems are required to ensure that the systems they plan to offer on the market carry the necessary CE conformity marking, are accompanied by a copy of the EU declaration of conformity and instructions for use, and obtain confirmation from both the provider and importer that they have adhered to their relevant obligations.

The relevant obligations that the distributor must verify for the provider are the provider's obligation to:

Indicate its name, registered trade name or registered trade mark, and the address at which the provider can be contacted on the high-risk AI system. Where this is not possible, this information must be indicated in the AI system's packaging or accompanying documentation. (Art. 16(aa)).

Have in place a quality management system that complies with Art. 17. (Art. 16(b)).

The relevant obligation that the distributor must verify for the importer is the importer's obligation to:

Display on the system and in the system packaging or in the accompanying documentation the name, registered trade name or trademark, and the address for contact for the importer.

Where a distributor considers or has reason to consider non-compliance with the high-risk requirements set in Chapter 2, Title III of the AI Act, on the basis of the information it possesses, they must ensure that the system complies with the AI Act before placing it into market. Where the high-risk system presents a risk to people's health and safety, or fundamental rights, the distributor must inform the system provider or the importer of the system.

Reference

AI Act, Art. 27(1)(2)

7.16.2 Compliance assurance

Distributors must ensure that storage and transportation conditions, while the high-risk AI system is under their responsibility, do not compromise its compliance with the requirements high-risk AI systems are subject to under Chapter 2, Title III of the AI Act.

Reference

AI Act, Art. 27(3)

7.16.3 Post-market corrective actions

If a distributor considers or has reason to consider on the basis of the information the distributor has in its possession that a high-risk AI system placed on the market does not comply with the high-risk AI system requirements under Chapter 2, Title III of the AI Act, they must take corrective actions to ensure conformity, withdraw, or recall the system, or the provider, importer, or other relevant operator takes those corrective actions.

If the system poses a risk to the health, safety, and fundamental rights of individuals, the distributor must promptly inform provider or importer of the system and the relevant national authorities in the Member State in which the product has been made available, detailing the system's non-compliance and any corrective actions taken.

Reference

AI Act, Art. 27(4)

7.16.4 Information provision and collaboration

Upon a reasoned request, high-risk AI system distributors must provide national authorities with all necessary information and documentation regarding the distributors activities that is necessary to demonstrate the system's compliance with Chapter 2, Title III of the AI Act.

Reference

AI Act, Art. 27(5)

7.16.5 Cooperation with national authorities

Distributors must work together with national authorities on any measures they implement, especially those aimed at reducing and mitigating the risks posed by the high-risk AI system.

Reference

AI Act, Art. 17(5a)

7.17 AI value chain responsibilities and provider obligation transfer

Any distributor, importer, deployer, or other third-party, will be subject to the provider's obligations under the AI Act, if they meet any of the pre-specified criteria under the Act. The AI Act also places obligations to product manufacturers of safety components of products as well as supplies who supply AI systems, tools, or other components that are used by or integrated to high-risk AI system.

Role

Provider,Deployer,Distributor,Importer

References

AI Act, Art. 28

7.17.1 Transfer of provider obligations

Any distributor, importer, deployer, or other third-party, will be considered a provider of high-risk system under the AI Act and will be subject to the provider's obligations under any of the following situations:

Distributor, importer, deployer, or other third-party puts their name or trademark on a high-risk AI system that is already placed on the market or puts it into service under their name or trademark. This applies without prejudice to contractual arrangements stating that obligations are allocated otherwise.

Distributor, importer, deployer, or other third-party makes a substantial modification to the high-risk AI system that has already been placed on the market or service. This applies where substantial modification has been done in a way that the high-risk AI system remains as high-risk AI system.

Distributor, importer, deployer, or other third-party modifies the intended purpose of an AI system, including a general-purpose AI system that has already been placed on the market or put it into service. This applies where the modification of intended purpose is done in a manner that results the AI system to become high-risk AI system.

In the situations where the distributor, importer, deployer, user, or other third party will be considered a provider, the initial provider who introduced the AI system to the market or put it into service will be no longer considered a provider of that specific AI system.

The former provider must work closely with the new provider, sharing and making available essential information and providing the technical access and support needed to meet the regulatory requirements and obligations under the AI Act, especially for conformity assessments of high-risk AI systems. However, this requirement does not apply if the former provider has explicitly excluded and stated that their system

would not be converted into a high-risk system, thus exempting them from the obligation to transfer documentation. This is done without prejudice to the need to respect and protect intellectual property rights and confidential business information or trade secrets in accordance with Union and national law.

Reference

AI Act, Art. 28(1)(2)

7.17.2 Provider obligations of manufacturers of safety components of products

For high-risk AI systems that are safety components of products covered by the legal acts in Annex II, section A, the product's manufacturer will be treated as the AI system's provider and are subject to provider's obligations under the following situations:

The high-risk AI system is placed on the market along with the product that is branded with the product manufacturer's name or trademark.

The high-risk AI system is put into service under the product manufacturer's name or trademark after the product has been placed o the market.

This is done without prejudice to the need to respect and protect intellectual property rights and confidential business information or trade secrets in accordance with Union and national law.

Reference

AI Act, Art. 27(2a)

7.17.3 Supplier obligations

Any third-party that supplies an AI system, tools, services, components, or processes that are used or integrated in a high-risk AI system, are required to together with the providers of such high-risk AI system to specify in a written agreement the necessary information, capabilities, technical access, and assistance needed for the high-risk AI system provider to meet the obligations under AI Act. This does not apply to third-party sharing tools or services under a free and open license, except for general-purpose AI models.

The AI Office may create and suggest optional contract templates for these relationships, considering sector-specific or business-specific needs. These templates will be published online for free in a user-friendly format.

Reference

AI Act, Art. 28(2b)

7.18 Deployer obligations

Deployers of AI systems are subject to certain obligations when taking in to use high-risk AI systems. These include requirements to use the system in accordance with the instructions of use, implement human oversight measures, ensure input data relevance, ensure monitoring, reporting, and record-keeping of the AI system. Furthermore, deployers of certain high-risk AI systems are subject to further obligations under the AI Act, such as fundamental rights impact assessment.

Role

Deployer

References

AI Act, Art. 29

7.18.1 Measures to comply with the instructions of use

Deployers of high-risk AI systems are required to use high-risk AI systems in accordance with the AI system's instructions of use provided by the high-risk AI system provider.

In order to do this, the deployers must implement appropriate technical and organisational measures.

Reference

AI Act, Art. 29(1)

7.18.2 Implement human oversight

Deployers of high-risk AI systems are required to assign human oversight to natural persons and must ensure that these individuals have the necessary competence, training, authority, and support to ensure system oversight.

These duties do not affect other legal obligations deployers may have under EU or national laws, nor do they limit how deployers manage their resources and activities to apply the provider's suggested human oversight measures.

Reference

AI Act, Art. 29(1a)(2)

7.18.3 Ensure input data relevance and representativeness

Deployers of high-risk AI systems are required to ensure that the input data of the high-risk AI system is relevant and sufficiently representative, and aligns with the intended purpose of the high-risk AI system.

This obligation applies to the extent to which the deployer has control over the input data.

Reference

AI Act, Art. 29(3)

7.18.4 Monitoring and reporting obligations

Deployers of high-risk AI systems are required to monitor the system operations as per the provided instructions of use. Furthermore, and where relevant, deployers are required to inform providers in accordance with post-market monitoring obligations in Art. 61. According to post-market monitoring, the post-market monitoring system will collect, document and analyse relevant data that can be provided by deployers.

If the deployer suspects that the use of the high-risk AI system in accordance with the instruction of use may present potential risks to individuals' health, safety, and fundamental rights, they must, without undue delay, inform the provider or distributor and the relevant market surveillance authority and suspend the system use. The notification requirement applies to risk that has the potential to harm

people's health and safety, including at the workplace, consumer protection, the environment, public security, and other public interests protected by Union harmonisation legislation. This refers to harm that goes beyond what is acceptable based on the product's intended purpose and typical usage conditions, including how long it is used, as well as any installation and maintenance requirements.

Additionally, when deployers identify any serious incidents, they must immediately first inform the providers, then the importer or distributor and relevant market surveillance authorities. Where the deployer cannot contact the provider, the incidents must be reported to the market surveillance authority in the Member State where the incident or breach occurred, per Art. 62.

Deployers that are financial institutions subject to requirements under EU financial services laws, meet the monitoring obligations by adhering to their internal governance, arrangements, and processes as required by those financial regulations, if subject to such requirements.

Reference

AI Act, Art. 29(4), 61(2)

7.18.5 Record-keeping

Deployers of high-risk AI systems must retain the system-generated logs to the extent the deployer has control over them. The logs must be kept for a period that is appropriate to the system's intended purpose, at least for 6 months, unless provided otherwise by Union or national law, particularly laws concerning personal data protection.

Deployers that are financial institutions subject to internal governance, arrangements, and processes under EU financial services laws are required to maintain logs as part of the documentation kept according to the relevant legislation.

Reference

AI Act, Art. 29(5)

7.18.6 Workplace deployment notification

Deployers who are employers and put into service or use high-risk AI systems at work must inform worker representatives and the affected employees that they will be subject to the system. This information should be shared, where applicable, following EU and national laws and practices regarding worker and representative notification.

Reference

AI Act, Art. 29(5a)

7.18.7 Registration to EU or national database by public authorities or persons acting on their behalf

Public authorities and EU institutions, bodies, offices, and agencies, or persons acting on their behalf deploying high-risk AI systems must register these systems to EU database, as outlined in Art. 51. Where the deployer finds that the system they plan to take in use is not registered in the EU database by the provider, as outlined in Art. 60, the deployer must not use the system and must notify the provider or distributor about this.

High-risk AI systems used in the area of critical infrastructure (point 2, Annex III) are exempted from the EU database registration. Instead, such systems must be registered at a national level.

The deployers must provide and update to the EU database the following details:

Deployer's name, address, and contact information.

Name, address, and contact details of the person submitting the information on behalf of the deployer.

A summary of the fundamental rights impact assessment results, as required by Article 29a of AI Act.

The URL for the AI system's entry in the EU database, as provided by its provider.

A summary of the data protection impact assessment, in line with Article 35 of the GDPR (Regulation (EU) 2016/679) or Article 27 of the Law Enforcement Directive (Directive (EU) 2016/680), as detailed in Article 29(6) of AI Act. where applicable.

Reference

AI Act, Art. 29(5b), 51(1b)(1d), Annex VIII Section B

7.18.8 Compliance with data protection impact assessment obligations

Deployers of high-risk AI systems are required to use the information provided in the user instructions of use to comply, where relevant, with their potential obligations to carry out data protection impact assessments, as required in Art. 35 of the GDRP (Regulation (EU) 2016/679), and Art. 27 of the Law Enforcement Directive (Directive (EU) 2016/680).

Reference

AI Act, Art. 29(6)

7.18.9 Judicial authorisation for exempted use of post-remote biometric identification

For investigations seeking a convicted or suspected criminal, deployers of AI systems used for post-remote biometric identification must obtain prior authorisation from a judicial or administrative authority without undue delay, no later than 48 hours, unless the system is used for initial suspect identification based on objective and verifiable facts linked to the crime.

The authorisation is crucial and must be specific to the crime under investigation. If authorisation is denied, the system's use must cease immediately, and related personal data must be deleted. Such AI systems cannot be used indiscriminately for law enforcement without a connection to a specific crime, proceeding, threat, or search for a missing person. Deployers must ensure that decisions affecting individuals cannot solely rely on these systems' outputs.

Usage must comply with EU directives on biometric data processing and be documented for oversight by relevant authorities, with annual reports on use submitted to market surveillance and data protection authorities, ensuring sensitive law enforcement data remains confidential. Member States can introduce stricter regulations on the usage of these systems.

Reference

AI Act, Art. 29(6a)

7.18.10 AI decision transparency disclosure

Deployers of standalone high-risk AI systems listed in Annex III, used for making or assisting decisions about individuals, must notify these individuals about the system's use.

For systems employed in law enforcement, the notification requirements of Article 13 from the Law Enforcement Directive (Directive 2016/680) will apply.

Reference

AI Act, Art. 29(6b)

7.18.11 Cooperation with national authorities

Deployers are required to work with relevant national competent authorities on any measures related to the high-risk system they deploy to ensure compliance with the AI Act.

Reference

AI Act, Art. 29(6c)

7.18.2 Fundamental rights impact assessment

Certain deployers are required to conduct a fundamental rights impact assessment before deploying a standalone high-risk AI system listed in Annex III of the AI Act. This requirement to conduct fundamental rights impact assessment applies to the following deployers:

Deployers that are bodies governed by public law, with the exception of AI systems used in the area of critical infrastructure (point 2, Annex III).

Private operators providing public services, with the exception of AI systems used in the area of critical infrastructure (point 2, Annex III).

Operators deploying high-risk systems that are intended to evaluate the creditworthiness of natural persons to establish credit score and/or AI systems intended to be used for risk assessment and pricing for life and health insurance (point 5 (b) and (ca), Annex III).

The fundamental rights impact assessment must consist of the following:

Description of the processes where the system is used and its intended purpose.

Description of system usage period and frequency.

Categories of individuals and groups likely to be affected by the system.

Description of potential risks to these groups, taking into account the information provided in the instructions of use by the provider.

Description of the implementation of human oversight measures, as per the instructions of use.

Measures to be taken in case the identified risks materialise, including internal governance processes and complaint mechanisms.

The fundamental rights impact assessment is mandatory for the system's first use, but deployers can reference previous assessments conducted by the deployer or existing assessments by the system provider for similar cases. Changes in any assessed factors require an update on the fundamental rights impact assessment.

Deployers must inform the market surveillance authority of the assessment outcomes by submitting a filled template (the template will be developed by the AI Office). Exemptions apply under certain conditions.

If the deployer has conducted a data protection impact assessment (DPIA) under GDPR (Art. 35 Regulation (EU) 2016/679) or the Law Enforcement Directive (Art. 27 Directive (EU) 2016/680), the fundamental rights impact assessment can be carried out together with the DPIA.

Reference

AI Act, Art. 29a

7.19 Transparency obligations of certain AI systems

Certain AI systems, particularly those posing specific manipulation risks, will be subject to transparency obligations. This includes systems interacting with humans, those detecting emotions or determining associations based on biometric data, and systems generating or manipulating content. Additionally, disclosure obligations apply to AI systems generating or manipulating content to resemble authentic content (deep fakes). This ensures individuals can make informed choices in relevant situations. The disclosures must be clearly presented to the relevant individuals no later than their first interaction or exposure to the system. The disclosures must also comply with relevant accessibility standards. The AI Office will support the creation of EU-wide codes of practice to help implement rules for identifying and labeling artificial content.

Role

Provider,Deployer

References

AI Act, Art. 52

7.19.1 AI interaction transparency

Providers must ensure that AI systems directly interacting with individuals are designed and developed so that the concerned individuals are informed of the AI system's nature, unless it is clear to a reasonably informed, observant, and cautious person, considering the situation and how the system is used.

The information must be clearly presented to the relevant individuals no later than their first interaction or exposure, complying with accessibility standards.

AI systems authorised by law to detect, prevent, investigate, and prosecute criminal offences are exempted from these obligations, provided that they protect third-party rights and freedoms. The exemption does not apply to systems available to the public for reporting criminal offences.

Reference

AI Act, Art. 52(1),(3a)

7.19.2 Synthetic content disclosure and marking requirement

Providers of AI systems that create synthetic audio, images, videos, or text, including providers of GPAI systems, must ensure that the outputs produced by the AI systems are labelled and marked as artificially generated or manipulated in a machine-readable format.

Providers must ensure that their technical methods are effective, interoperable, robust, and reliable across systems, as current technology allows, considering content variety, cost, and generally acknowledged state-of-the-art.

The information must be clearly presented to the relevant individuals no later than their first interaction or exposure, complying with accessibility standards.

This requirement does not apply to AI systems that aid in routine editing without significantly modifying the deployer's provided data or its meaning, or to systems legally used for detecting, preventing, investigating, and prosecuting crimes.

Reference

AI Act, Art. 52(1a),(3a)

7.19.3 Emotion recognition and biometric categorisation transparency

Deployers using emotion recognition or biometric categorisation systems must notify the individuals affected by these systems and handle their personal data according to GDPR (Regulation (EU) 2016/679), Regulation on the processing of personal data by EU institutions (Regulation (EU) 2018/1725), and the Law Enforcement Directive (Directive (EU) 2016/280), as relevant.

The information must be clearly presented to the relevant individuals no later than their first interaction or exposure, complying with accessibility standards.

This requirement does not apply to biometric categorisation and emotion recognition AI systems legally used for detecting, preventing, and investigating crimes, provided they ensure the protection of third-party rights and freedoms in line with EU law.

Reference

AI Act, Art. 52(2),(3a)

7.19.4 Disclosures of AI-generated deep fake content

Deployers of AI systems that create or manipulate image, audio, or video content constituting a deep fake must disclose that the content is artificially generated or manipulated.

The information must be clearly presented to the relevant individuals no later than their first interaction or exposure, complying with accessibility standards.

This rule does not apply if the use is legally authorised for crime detection, prevention, investigation, or prosecution.

When the generated content is clearly for artistic, creative, satirical, or fictional purposes, the transparency requirement should be applied in an appropriate manner, ensuring it does not interfere with how people experience or enjoy the work.

Reference

AI Act, Art. 52(3),(3a)

7.19.5 Disclosure of AI-generated public interest text

Deployers of AI systems that generate or manipulate text used for informing the public on matters of public interest, must indicate if the text is artificially produced.

The information must be clearly presented to the relevant individuals no later than their first interaction or exposure, complying with accessibility standards.

The rule does not apply when the use is authorised by law to detect, prevent, investigate, and prosecute criminal offences or where the AI-generated content has undergone a process of human review or editorial control, with a person or entity taking responsibility for its publication.

Reference

AI Act, Art. 52(3),(3a)

7.20 Obligations for general purpose AI models

Providers of general purpose AI models are subject to certain requirements under the Act. Provider must ensure compliance with these obligations prior to its placement on the market. The requirements apply irrespective of the form of the model (standalone, embedded, service).

Providers of general-purpose AI models with systemic risk can use codes of practice as per Article E for early compliance demonstration until a harmonized standard is available, which then offers a presumption of conformity. Those not following an approved code must show the Commission other sufficient compliance methods.

Open-source models are exempted from the majority of the obligations, except from compliance with copyright law and the documentation and publishing of training data.

Role

Provider

References

AI Act, Art. 28(b)

7.20.1 GPAI technical documentation

Providers of general-purpose AI models are required to draw up and regularly update technical documentation, covering the model's training, testing, and evaluation outcomes. This documentation must include, at a minimum, the key details specified in Annex IXa and be made available to the AI Office and relevant national authorities upon request.

The technical documentation for general-purpose AI models, as required by Annex IXa, must include information suited to the model's size and risk profile, such as:

A general overview of the AI model, covering:

Intended tasks of the model and potential AI system integrations, including their type and nature.

Acceptable use policies.

Release date and distribution methods.

Architecture and number of parameters.

Input and output modalities and formats.

Licensing information.

Detailed description of the elements of the model and the development processes, including:

Technical integration requirements (use instructions, infrastructure, tools) required for the AI model to be integrated into an AI system.

Model design specifications and training process, including training methodologies and techniques, key design choices, including the rationale and assumptions made. In addition to these, information on the optimisation and the relevance of different parameters.

Information on the data used for training, testing, and validation: type, provenance curation methods (e.g. cleaning, filtering, etc.), number of data points, their scope and main characteristics. The information should also include how data was obtained and selected, as well as detection measures unsuitability of the data sources and bias detection measures.

Computational resources for training the model (e.g. number of floating point operations (FLOPS)), including training time and other details related to training.

Energy consumption estimates of the model. In case not known, this could be based on information about computational resources used.

Reference

AI Act, Art. 52c(1)(a), Annex IXa Section 1

7.20.2 Downstream provider transparency and instructions of use

Providers of GPAI models are required to draw up, regularly update, and make available instructions of use for the model. The documentation and instructions enable the downstream providers to integrate the GPAI model into their AI system. The documentation should help the downstream AI system providers clearly understand the general-purpose AI model's capabilities and limitations, and enable them to comply with the requirements the AI Act places on them. This documentation must include, at a minimum, the elements specified in Annex IXb.

The technical documentation for downstream providers integrating the general purpose AI model into their AI system should include, at minimum, the following:

General description of the AI model, including:

The tasks the model is intended to perform and the type and nature of AI systems it can be integrated into.

Policies for acceptable use.

Release date and distribution methods.

Potential interactions with external hardware or software, including how it interacts or can be used to interact.

Versions of related software, if relevant.

The model's architecture and number of parameters.

The modality (e.g., text, image) and format of data inputs and outputs.

Licensing information for the model.

A detailed explanation of the model's elements and its development process, including:

The necessary technical resources (such as usage instructions, infrastructure, and tools) for integrating the general-purpose AI model into AI systems.

The modality (e.g., text, image) and format of the inputs and outputs, along with their maximum size (e.g. the length of the context window, etc.).

Details on the data used for training, testing, and validation, if applicable, covering the data's type, provenance, and curation methodologies.

Reference

AI Act, Art. 52c(1)(b), Annex IXb

7.20.3 Compliance with copyright law

Providers of general-purpose AI models must put in place a policy to comply with EU copyright law. Specifically, the policy should detail how the provider identifies and respects, including through the use of advanced technologies, copyright exceptions and limitations for text and data mining, as outlined in Article 4(3) of the Directive on Copyright in the Digital Single Market (Directive (EU) 2019/790).

Reference

AI Act, Art. 52c(1)(c); Directive (EU) 2019/790, Art. 4(3)

7.20.4 Documentation and publishing of training data

Providers of general-purpose AI models must document and make publicly available a sufficiently detailed summary of the content used for training the general-purpose AI model.

This documentation must be done by using a template that will be provided by the AI Office.

Reference

AI Act, Art. 52c(1)(d)

7.20.5 Cooperation with authorities

Providers of general-purpose AI models are required to cooperate with the Commission and relevant national authorities as needed, to support their duties under the AI Act.

Reference

AI Act, Art. 52c(2)

7.21 Obligations for general purpose models with systemic risk

Providers of general purpose AI models with systemic risks are subject to certain additional requirements under the Act. Provider of models with systemic risks must ensure compliance with these obligations prior to its placement on the market. The requirements apply irrespective of the form of the model (standalone, embedded, service).

Providers of general-purpose AI models with systemic risk can use codes of practice for compliance demonstration until a harmonised standard is available, which then offers a presumption of conformity. Those not following an approved code must show the Commission other sufficient compliance methods.

Open-source models classified as general purpose models must also fulfill these obligations.

Role

Provider

References

AI Act, Art. 52d

7.21.1 Supplementary technical documentation

In addition to the information the providers of general purpose models with systemic risks must provide under the GPAI technical documentation requirement, the providers of GPAI models with systemic risks must provide certain supplementary information.

This information includes the following:

Comprehensive strategies for evaluation, detailing results using public evaluation protocols and tools or other evaluation methodologies. This should cover evaluation criteria, metrics, and methodology on how limitations are identified.

Where relevant, an in-depth explanation of measures for internal and/or external adversarial testing (such as red teaming), and any model adaptations, including alignment and fine-tuning processes.

When applicable, a thorough description of the system's architecture, illustrating the interaction and integration of software components within the overall processing framework.

Reference

AI Act, Art. 52c(1)(a), Annex IXa Section 2

7.21.2 Standardised model evaluation and adversarial testing

Providers of general purpose AI models with systemic risks must conduct and document model evaluations using up-to-date standardised protocols and tools, including adversarial testing, to identify and mitigate systemic risks.

Reference

AI Act, Art. 52d(1)(a)

7.21.3 Risk assessment and mitigation

Providers of general purpose AI models with systemic risks must assess and mitigate potential systemic risks at the EU level, including their sources, that could arise from development, placing on the market, or using the model.

Systemic risk at the EU level refers to a risk that is unique to the high-impact capabilities of general-purpose AI models that significantly affect the internal market because of the model's reach. This risk has real or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or society at large and can spread widely across the value chain.

Reference

AI Act, Art. 52d(1)(b), 3(44d)

7.21.4 Incident and corrective measure tracking, documenting, and reporting

Providers of general purpose AI models with systemic risks must keep track of, document, and inform without undue delay the AI Office and, when relevant, the national authorities about serious incidents and potential corrective measures the provider has undertaken.

A serious incident refers to any situation or malfunction involving an AI system that directly or indirectly causes one or more of the following outcomes: the death of an individual or severe harm to a person's health; significant and irreversible disruption to the functioning and management of critical infrastructure; a breach of obligations laid out by EU legislation designed to safeguard fundamental rights; or considerable damage to property or the environment.

Reference

AI Act, Art, 52d(1)(c), 3(44)

7.21.5 Cybersecurity protection

Providers of general purpose AI models with systemic risks must guarantee a sufficient level of cybersecurity for both the general-purpose AI model with systemic risk and the model's physical infrastructure.

Reference

AI Act, Art. 52d(1)(d)

7.22 Appointment and obligations of authorised representatives for GPAI

Providers of general-purpose AI models from outside the EU must appoint an authorised representative within the EU before placing the model in the Union market. The authorised representative is responsible for ensuring the performance of the tasks relevant to them. The authorised representative is authorised via a written mandate that authorises the representative to carry out their tasks.

The obligations concerning authorised representatives do not apply to certain open-source models.

Role

Provider,Authorised representative

References

AI Act, Art. 52ca

7.22.1 Appointment and mandate of the GPAI authorised representative

Before making their systems available in the EU market, providers of general purpose AI models established outside the EU must appoint an authorised representative established in the EU, through a written mandate. This written mandate authorises the representative to carry our their tasks.

Reference

AI Act, Art 52ca(1)

7.22.2 Tasks of the GPAI authorised representative

The authorised representative, appointed by the provider, must fulfil tasks outlined in their mandate and present a copy of it to the AI Office upon request. A copy of the mandate must be presented in one of the official languages of the institutions of the Union.

The mandate shall empower the authorised representative to carry out the following tasks:

Verify that the technical documentation, as detailed in Annex IXa, is properly prepared by the provider. Additionally, verify that the general purpose AI system provider, and where applicable, the provider of general purpose AI model with systemic risks is fulfilling all their obligations as specified in Articles 52c and 52d.

Keep technical documentation and provider's contact details at the disposal of the AI Office and national competent authorities for 10 years after the AI system is placed on the market.

Provide all necessary information and documentation, including technical documentation and information on the provider's fulfilment of their obligations to the AI Office upon reasoned request, to demonstrate compliance with obligations under the AI Act.

Cooperate with AI Office and national competent authorities, upon reasoned request, on actions the authority takes concerning the general-purpose AI models with systemic risks. This includes also situations where the general-purpose AI models with systemic risks is integrated into an AI system that is placed on the market or put into service in the Union.

The mandate allows competent authorities to contact the authorised representative regarding compliance issues instead of or in addition to the provider.

Reference

AI Act, Art. 52ca(2)(3)

7.22.3 Termination of mandate by GPAI authorised representative

Where the authorised representative considers or has reason to consider that the provider of the general purpose AI model, including general purpose AI model with systemic risks, is not meeting its obligations under the AI Act, the authorised representative must terminate the mandate giving it the authority to act as the authorised representative.

When the authorised representative terminates the mandate, it must immediately notify the AI Office about termination of the mandate and the reasons for the termination.

Reference

AI Act, Art. 52ca(4)

7.23.1 Codes of conduct

Codes of conduct are designed to prompt providers of non-high-risk AI systems to voluntarily adopt the mandatory requirements applicable to high-risk AI systems outlined in the AI Act. Providers of non-high-risk AI systems have the flexibility to create and implement these codes, which may cover voluntary commitments, such as environmental sustainability, accessibility for persons with disabilities, stakeholder participation in AI system design, development, and fostering diversity within development teams.

Role

Provider

References

AI Act, Art. 69

7.23.2 Voluntary codes of conduct

The AI Office and Member States aim to encourage and facilitate the creation of codes of conduct for AI systems and related governance mechanisms. These codes aim to foster voluntary application of high-risk AI system requirements, set out in Title III, Chapter 2, for system not classified as high risk. The codes fo conduct will consider technical solutions and industry best practices. Additionally, these codes will address:

Ethical guidelines for trustworthy AI.

Minimising AI's environmental impact through energy efficiency and sustainable design and use.

Enhancing AI literacy among those involved in AI's development, operation, and usage.

Ensuring AI systems are inclusively designed, advocating for diverse development teams and stakeholder participation.

Protecting vulnerable individuals or groups from AI's adverse effects, including improving accessibility and promoting gender equality.

Codes of conduct can be developed by AI providers, deployers, their organizations, or jointly, involving various stakeholders like civil society and academia, and may cover multiple AI systems with similar purposes. The AI Office and Member States will also consider the unique needs of SMEs and startups in these initiatives.

Reference

AI Act, Art. 69