EU AI Act: Prohibited and Regulated Use Cases.

Could you run into issues under the EU AI Act with your use case? Check out the following for getting an indication.

1. Do we have an "AI system"?

- Machine-based system;
- it is designed to operate with varying levels of autonomy;
- it may exhibit adaptiveness after deployment;
- it, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions; *and*
- the output can influence physical or virtual environments

Covered separately: General purpose AI models (AI model with significant generality, able to perform many tasks, can be integrated in many apps)

2. Which role do we have?

The Act defines various roles, and our obligations under the Act vary depending on our role.

- **Provider:** We (i) develop an AI system or a general-purpose AI model (or have this done by a 3rd party) and (ii) have it placed on the EU market (i.e. make it available for distribution or use in the EU) or put into service in the EU (i.e. supply it for first use and intended purpose in the EU by ourselves or a deployer), and (iii) under our own name or trademark, **or** (iv) we put our name or trademark on a high-risk AI system (on the market/put into service) or made substantial changes to it, **or** (v) modified the intended purpose of a system to get high-risk
- **Deployer:** We use an AI system under our authority (except where used in the course of a personal non-professional activity)
- **Importer:** We are established or located in the EU and place on the EU market an AI system bearing the name of someone outside the EU
- **Distributor**: We make an AI system available on the EU market, but are neither the provider nor the importer
- **Product manufacturer:** We place on the market or put into service in the EU an AI system with our product under our own name

3. Are we within the scope of the Act?

The Act has a broad scope of applicability and extraterritorial reach. It in principle applies in the following cases (exceptions exist, for example, for scientific research, open source and purely personal use).

- **Provider:** We (i) place on the market or put into service AI systems in the EU, (ii) place on the EU market general-purpose AI models, [or (iii) the output of the AI system is to be used in the EU; the intention is to protect affected persons in the EU, but this may not be enforceable]
- **Deployer:** We (i) are established or located in the EU, or (ii) the output of the AI system is used in the EU
- **Importer, distributor, product manufacturer:** As defined above

4. Is our use case prohibited under the Act?

These use cases are considered prohibited under the Act as of February 2025, for those that place on the market or put into service AI systems for such cases and those who use AI systems for them (exceptions apply).

- Use of subliminal, purposefully manipulative or deceptive techniques, with the objective to or the effect of materially distorting behaviour or impairing the person's ability to make an informed decision, that may result in a decision that causes or is reasonably likely to cause significant harm
- Exploiting vulnerabilities of persons due to age, disability or a specific social or economic situation, to materially distort their behaviour in a manner that causes or is reasonably likely to cause significant harm
- Biometric categorisation to deduce or infer a person's race, political opinion, trade union membership, religious or philosophical belief, sex life or sexual orientation (i.e. based on biometric data)
- Evaluation or classification of persons over a period of time based on their social behavior or known, inferred or predicted personality characteristics with this social scoring leading to detrimental or unfavorable treatment that is unrelated to the original data context, or is unjustified or disproportionate to their social behavior or its gravity
- Real-time remote biometric identification in publicly accessible spaces for the purpose of law enforcement, except for certain targeted victim searches, prevention of certain specific, substantial and imminent threats or the localization or identification of suspects of certain defined categories of crimes (Annex II), subject to additional conditions (e.g., court approval, permission only to search for specifically targeted individuals)
- Profiling or assessment of personality traits or characteristics of persons to assess or predict the risk of them committing criminal offences, except for assisting human risk assessments of specific persons involved in a crime
- Creation or expansion of a facial recognition database based on untargeted scraping on the Internet or CCTV footage
- Inferring emotions (including intent) of persons in workplace areas or in education institutions except where intended for medical or safety reasons

5. Will our use case be a "high-risk" AI system?

The following use cases in principle result in a "high-risk" AI system under the Act (exceptions apply). As of August 2, 2027, they trigger various obligations for providers and (to a much lesser extent) deployers.

- A product that according to the EU law listed in Annex I has to undergo a third-party conformity assessment before being placed on the market or put into service, or is a safety component of such a product
- Remote biometric identification (beyond mere authentication) or biometric categorization based on sensitive or protected attributes or characteristics inferred from such attributes
- Inferring emotions/intentions based on biometrics (emotion recognition)
- AI is used as a safety component in the management and operation of critical digital infrastructure, road traffic or the supply of water, gas, etc.
- Use in education and vocational training, insofar (i) access, admission or assignment is to be determined by AI, (ii) AI is to evaluate learning outcomes or (for granting access) the educational level of persons, or (iii) AI is to be used to monitor or detect prohibited behavior during tests
- Employment, workers management and access to self-employment, insofar (i) AI is to be used for recruitment or selection of persons or (ii) AI is to be used to make decisions affecting the terms of employment, the promotion or termination of employment, to allocate work based on behavior or other personal characteristics, and to monitor and evaluate performance and behavior
- AI is to be used for evaluating (for or as a public authority) whether essential public assistance benefits and services, including healthcare, are or continue to be available to a particular person
- AI is to be used for evaluating the creditworthiness of a person or their credit score, except for the purpose of detecting financial fraud
- AI is to be used to evaluate and classify emergency calls by persons or in dispatching or triaging emergency first response or services or health care
- AI is to be used for risk assessments and pricing of life or health insurance
- Law enforcement use, where (i) AI is to be used for assessing the risk of a person becoming a victim of criminal offences, (ii) AI is to be used as a polygraph or similar tool or (iii) AI is to be used to detect the reliability of evidence (in each case, other than a prohibited practice above)
- Law enforcement use, where (i) AI is to assess the risk of a person offending or re-offending not solely based on their (automated) profiling, (ii) AI is to be used to assess personality traits, characteristics or past criminal behaviour of a person, or (iii) AI is to be used for profiling persons in the course of detection, investigation or prosecution of criminal offences
- Migration, asylum and border control management use, where (i) AI is to be used as a polygraph or similar tool, (ii) AI is to be used for assessing risks posed by persons entering the EU or intending to do so, (iii) AI is to be used to examine applications for asylum, visa, residence permits and related complaints, and assess related evidence, (iv) AI is to be used to detect, recognize or identify persons, except for the verification of travel documents
- AI is to be used by a judicial authority or on their behalf or in an alternative dispute resolution to assist the judicial authority in researching and interpreting facts and the law and applying it to a specific case
- AI is to be used to influence the outcome of an election or voting referendum or individual voting, but not where persons are not directly exposed to the output of AI (e.g., AI systems used for organising, optimising and structuring the administration or logistics of political campaigns)

Exceptions and distinctions may apply that are important in practice. Please obtain expert legal advice and consult the ful AI Act before proceeding.

6. Other cases that require providers to act

- A high-risk AI system as laid out above under Section 5, but the AI system at issue (i) poses no significant risk of harm (e.g., narrow procedural task, quality control of human activities or completed decision making) and (ii) does not perform any profiling: Likely not a high-risk AI system, but the Provider shall document the assessment and register the system
- An AI system directly interacts with individuals, except for those systems authorized by law to detect, prevent, investigate and prosecute criminal offences: Providers shall design the AI system so that individuals are informed that they are interacting with an AI system, unless obvious
- An AI system generates synthetic audio, image, video or text content: Providers must inter alia ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated, and that the solution is effective, interoperable, robust and reliable (with exceptions inter alia for AI systems used only in an assisting role for standard editing or that do not substantially alter the input data)
- General-purpose AI models: Providers must inter alia inform about their model, including its training content, and comply with EU copyright law
- A general-purpose AI model with a "systemic risk" because it (i) has high impact capabilities (including where its training has involved 10^25 FLOPS or greater) or (ii) it has been determined as being the foregoing: Providers must inter alia also perform model evaluations, do risk management, track and report serious incidents, ensure adequate cybersecurity

7. Other cases that require deployers to act

- AI systems inferring or detecting emotions and intents or does biometric categorization, except for those systems that are permitted by law to detect, prevent and investigate criminal offences: Deployers shall inform the persons that are exposed to it of the AI system's operation
- AI systems generating "deep fakes": Deployers shall disclose that the content has been artificially generated or manipulated (with exceptions inter alia for content used in artistic, creative, satirical and fictional or analogous work or programs)
- AI Systems generating or manipulating text published for the purpose of informing the public: Deployers shall disclose that the text has been artificially generated or manipulated, except inter alia for content that has undergone a process of human review or editorial control and where there is a human with editorial responsibility for the publication
- Obligation to train/ensure AI literacy of those dealing with AI systems

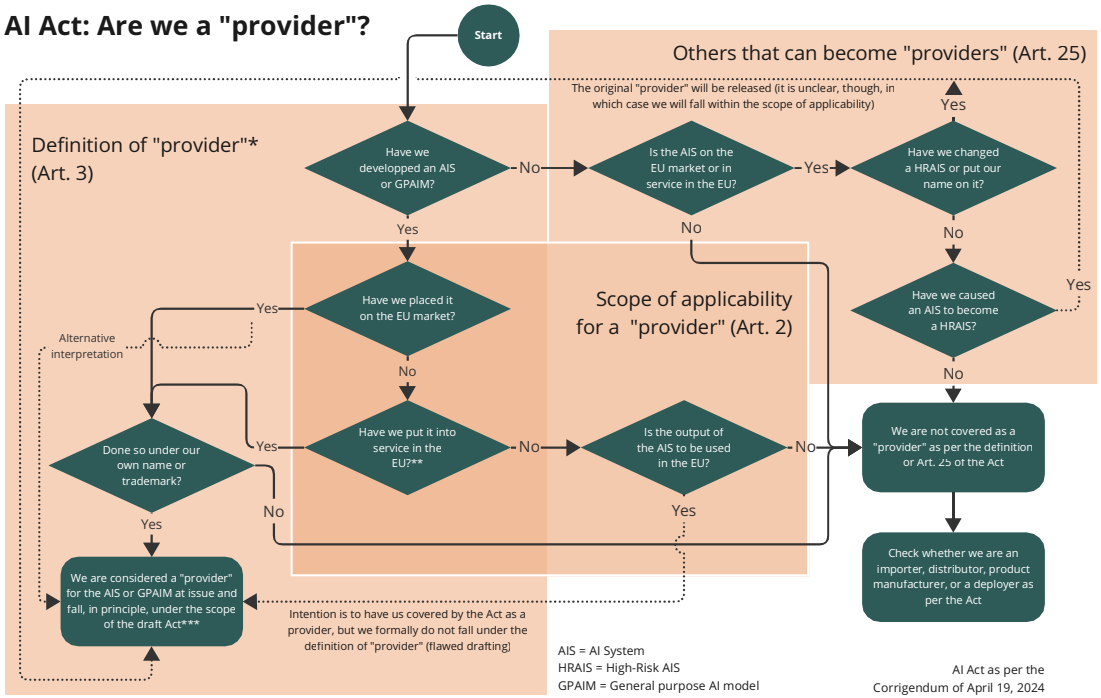
AI Act online (not VISCHER): https://vischerlnk.com/ai-act
Generative AI Risk Assessment: https://vischerlnk.com/gaira
Generative AI Risk Check: https://vischerlnk.com/ai-riskcheck

If you have any questions, contact us at ai@vischer.com or visit us at vischer.com/ai.

Author: David Rosenthal (david.rosenthal@vischer.com) 30.7.24 This document (incl. updates): vischerlnk.com/ai-act-uc

VISCHER SWISS LAW AND TAX

AI Act: Are we a "provider"?



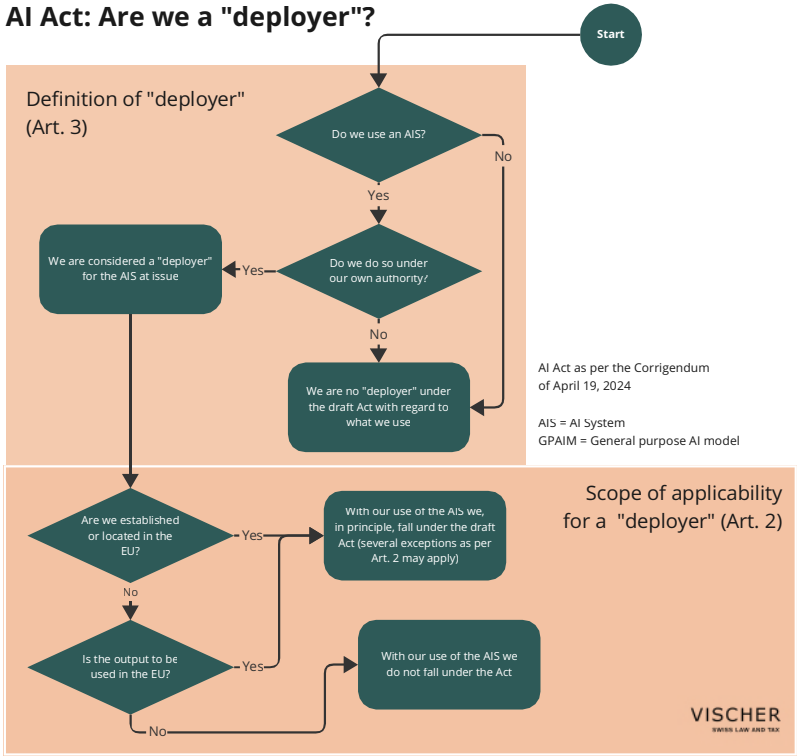
AIS = AI System
HRAIS = High-Risk AIS
GPAIM = General purpose AI model

AI Act as per the Corrigendum of April 19, 2024

* Including definitions of "placing on the market" and "putting into service"
** This applies only in the case of an AIS, not GPAIM in terms of the scope of the Act as per Art. 3
*** Several exceptions may apply as per Art. 2 (e.g., scientific research only, testing only)

VISCHER SWISS LAW AND TAX

AI Act: Are we a "deployer"?



AI Act as per the Corrigendum of April 19, 2024

AIS = AI System
GPAIM = General purpose AI model

VISCHER SWISS LAW AND TAX

Timeline EU AI Act