European Union Artificial Intelligence Act

Artificial intelligence (AI) is an emerging general-purpose technology: a highly powerful family of computer programming techniques. The uptake of AI systems has a strong potential to bring societal benefits, economic growth and enhance EU innovation and global competitiveness.

However, in certain cases, the use of AI systems can create problems. The specific characteristics of certain AI systems may:

- create new risks related to safety and security fundamental rights;
- accelerate the probability or intensity of the existing risks;
- make it hard for enforcement authorities to verify compliance with and enforce the existing rules.

This set of issues in turn leads to:

- legal uncertainty for companies;
- potentially slower uptake of AI technologies, due to the lack of trust, by businesses and citizens; and
- regulatory responses by national authorities to mitigate possible externalities that risk fragmenting the internal market.

The main objective of the EU Artificial Intelligence Act (“EU AI Act”) is to ensure that AI systems within the EU are safe and comply with existing laws on fundamental rights, norms and values.

The AIA defines AI systems broadly by including logic- or rule-based information processing (such as expert systems), as well as probabilistic algorithms (such as machine learning).

Like the GDPR, it applies to all firms wishing to operate AI systems within the EU, irrespective of whether they’re based in the EU or not.

The AIA adopts a risk-based approach to regulating AI systems. In terms of their perceived risk, some AI systems are banned outright, while others aren’t regulated at all.
Categories of AI system

First, there are ‘prohibited AI practices’, which are banned outright. This includes a very limited set of particularly harmful uses of AI that contravene EU values because they violate fundamental rights.

For example, social scoring by governments, exploitation of vulnerabilities of children, use of subliminal techniques, and – subject to narrow exceptions – live remote biometric identification systems in publicly accessible spaces used for law enforcement purposes).

Second, there are ‘high-risk AI systems’. In line with a risk-based approach, those high-risk AI systems are permitted on the European market subject to compliance with certain mandatory requirements and an ex-ante conformity assessment.

The classification of an AI system as high-risk is based on the intended purpose of the AI system, in line with existing product safety legislation.

Therefore, the classification as high risk depends not only on the function performed by the AI system, but also on the specific purpose and modalities for which that system is used, such as:

- Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning
- Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems.
- Statistical approaches, Bayesian estimation, search and optimisation methods.

Action Items

If you’re developing or using software that’s developed with one or more of these techniques, you might be in scope of the EU AI Act:

- Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning
- Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems.
- Statistical approaches, Bayesian estimation, search and optimisation methods.
<table>
<thead>
<tr>
<th>Area</th>
<th>AI System classified as ‘high-risk’</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biometric identification and categorisation of natural persons</td>
<td>Biometric identification and categorisation of natural persons</td>
</tr>
<tr>
<td>Management and operation of critical infrastructure</td>
<td>AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity</td>
</tr>
<tr>
<td>Education and vocational training</td>
<td>AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions</td>
</tr>
<tr>
<td>Employment, workers management and access to self-employment</td>
<td>AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests</td>
</tr>
<tr>
<td>Access to and enjoyment of essential private services and public services and benefits</td>
<td>AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, as well as to grant, reduce, revoke or reclaim such benefits and services</td>
</tr>
<tr>
<td>Law enforcement</td>
<td>AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences</td>
</tr>
<tr>
<td>Migration, asylum and border control management</td>
<td>AI systems intended to be used by competent public authorities as polygraphs and similar tools or to detect the emotional state of a natural person</td>
</tr>
<tr>
<td>Administration of justice and democratic processes</td>
<td>AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts</td>
</tr>
</tbody>
</table>

These also include safety components of products covered by sectoral Union legislation. They’ll always be high risk when subject to third-party conformity assessment under that sectoral legislation. Third, there are ‘limited-risk AI systems’. AI systems under this category are subject to transparency obligations to allow individuals interacting with the system to make informed decisions.
This is the case for a chatbot, where transparency means letting the user know they’re speaking to an AI-empowered machine. Further examples may include spam filters, AI-enabled video and computer games, inventory management systems or customer and market segmentation systems.

Providers need to ensure that natural persons are informed that they’re interacting with an AI system (unless this is obvious from the circumstances and the context of use).

Fourth, there are ‘low-risk AI systems’; they’re low risk because they neither use personal data nor make any predictions that influence human beings. According to the European Commission, most AI systems will fall into this category.

A typical example is industrial applications in process control or predictive maintenance. Here there’s little to no perceived risk, and as such no formal requirements are stipulated by the AIA.

It’s important to note that the requirements stipulated in the AIA apply to all high-risk AI systems. However, the need to conduct conformity assessments only applies to ‘standalone’ AI systems.

For algorithms embedded in products where sector regulations apply, such as medical devices, the requirements stipulated in the AIA will simply be incorporated into existing sectoral testing and certification procedures.

**Action Items**

It’s important to determine at an early stage what risk categories your AI system falls into. Depending on the classification there are different legal implications.

**Who needs to act**

The legal framework will apply to both public and private actors inside and outside the EU as long as the AI system is placed on the Union market or its use affects people located in the EU.

It can concern both providers (e.g. a developer of a CV screening tool) and users of high-risk AI systems (e.g. a bank buying this CV screening tool). It doesn’t apply to private, non-professional uses.
In general, the EU AI Act distinguished between the following roles:

- **Providers**: any person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark.

- **Importers**: any person established in the 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.

- **Distributors**: any person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market without affecting its properties.

- **Users**: any person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity.

The following table provides an overview of parties’ obligations:

<table>
<thead>
<tr>
<th>Legal Requirement</th>
<th>Providers</th>
<th>Importers</th>
<th>Distributors</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establishing a risk system</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirements regarding training, validation and testing data</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technical documentation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Record-keeping</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transparency and provision of information</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human oversight</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accuracy, robustness &amp; oversight</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality management system</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conformity assessment</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registration obligation</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information of national competent authority</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Affix CE marking</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Comply with instructions for use</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Consider relevance of input data</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Monitor operation of the system</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Record-keeping for automatically generated flags</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Execution of DPIA</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
It’s important to note that this role concept isn’t a fixed one. There might be situations where an importer, distributor or any other third party might be considered as a provider. In essence, this means that this party then also has to follow the obligations for providers. Such a change in role takes place when:

- they place on the market or put into service a high-risk AI system under their name or trademark
- they modify the intended purpose of a high-risk AI system already placed on the market or put into service
- they make a substantial modification to the high-risk AI system.

**Action Items**

**First**, you need to check whether your AI system affects people located in the EU.

**Second**, you need to check whether you’re considered as a provider, importer, distributor or just a user of the AI system.

**What is the risk for companies based in third-countries, such as the United States of America?**

The EU AI Act will likely have a significant impact on Swiss companies that provide or use AI systems, even if they don’t have a legal presence in the EU. In fact, similar to the EU General Data Protection Regulation (‘GDPR’), the draft EU AI Act has an extraterritorial effect and thus also applies to organisations outside the EU, essentially to:

- providers placing on the market or putting into service AI systems in the EU, irrespective of whether these providers are located within the EU or in a third country (e.g. Switzerland)
- users of AI systems who are located in the EU, and
- providers and users of AI systems who are located in a third country (e.g. Switzerland), where the output produced by the AI system is used in the EU.
Consequently, the AI Act in principle applies if an AI system or its output is used within the EU. As an example, the use of a chatbot to answer enquiries from EU-based individuals regarding a credit or the use of AI systems for checks on creditworthiness regarding individuals in the EU by a Swiss bank would likely trigger the application of the AI Act.

Conformity assessments: what needs to be done?

The EU AI Act requires providers of high-risk AI systems to conduct conformity assessments before placing their product or service on the European market. A conformity assessment is a process carried out to demonstrate whether specific consumer protection and product integrity requirements are fulfilled, and if not, what if any remedial measures can be implemented to satisfy such requirements. Occasionally, such conformity assessments may need to be performed with the involvement of an independent third-party body. But for most AI systems, conformity assessments based on ‘internal control’ will be sufficient. However, while the EU AI Act stipulates a wide range of procedural requirements for conformity assessments based on internal control, it doesn’t provide any detailed guidance on how these requirements should be implemented in practice.

If an AI system falls under the EU AI Act, then the actions needed are determined by the level of risk embedded in the respective system. The initial question for providers is therefore to determine that risk level in light of the types and categories set out in the EU AI Act.

In contrast, ‘standalone’ high-risk AI systems have to undergo an AI-specific conformity assessment before they can be placed on the EU market.

How to conduct a conformity assessment

There are two ways to conduct such conformity assessments: conformity assessment based on internal controls and, in some cases, a conformity assessment of the quality management system and technical documentation conducted by a third party, referred to as a ‘notified body’. These are two fundamentally different conformity assessment procedures.
The type of procedure required for a specific AI system depends on the use case, in other words the purpose for which it is employed.

In short, high-risk AI systems that use biometric identification and categorisation of national persons must conduct a third-party conformity assessment. For most high-risk AI systems, however, conformity assessment using internal controls will be sufficient.

The AIA itself doesn’t specifically stipulate how to execute a conformity assessment based on internal control. Only the following is stated:

- The provider verifies whether the established quality management system is in compliance with the AIA.
- The provider examines the information contained in the technical documentation in order to assess the compliance of the AI system with the relevant essential requirements of the AIA.
- The provider also verifies that the design and development process of the AI system and its post-market monitoring is consistent with the technical documentation.

Providers of AI systems that interact directly with humans – chatbots, emotional recognition, biometric categorisation and content-generating (‘deepfake’) systems – are subject to further transparency obligations. In these cases, the AIA requires providers to make it clear to the users that they’re interacting with an AI system and/or are being provided with artificially generated content. The purpose of this additional requirement is to allow users to make an informed choice as to whether or not to interact with an AI system and the content it may generate.

What are the penalties for non-compliance?

The penalties set out in the EU AI Act for non-conformance are very similar to those set out in the GDPR. The main thrust is for penalties to be effective, proportionate and dissuasive. The sanctions cover three main levels:

- Non-compliance with regard to prohibited AI practices and/or the data and data governance obligations set out for high-risk AI systems can incur a penalty of up to 30mEUR, or 6% of total worldwide turnover in the preceding financial year (whichever is higher).
- Non-compliance of an AI system with any other requirement under the AIA than stated above can incur a penalty of up to 20m EUR, or 4% of total worldwide turnover in the preceding financial year (whichever is higher).
- Supply of incomplete, incorrect or false information to notified bodies and national authorities in response to a request can incur a penalty of up to 10mEUR, or 2% of total worldwide turnover in the preceding financial year (whichever is higher).

It should be noted that the enforcement of the AIA sits with the competent national authorities. Individuals adversely affected by an AI system may have direct rights of action, for example concerning privacy violations or discrimination.

**How can AI & Partners help**

We can support you in particular in the following areas around the AIA:

**Designing a risk management system:**

For high-risk AI systems, a risk management system needs to be established. This system needs to consist of an iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating. It needs to include:

- identification and analysis of the known and foreseeable risks associated with each high-risk AI system
- evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse
- evaluation of other possible arising risks based on the analysis of data gathered from the post-market monitoring system
- adoption of suitable risk management measures

**Creating the technical documentation:**

This documentation for high-risk AI systems needs to be created before the system is placed on the market or put into service. It regularly needs to be kept up to date. The technical documentation needs to demonstrate how the AI system complies with the requirements of the AIA. It should enable national competent authorities as well as notified bodies with all necessary information to assess the compliance of the AI system.
Designing transparency and information requirements:

High-risk AI systems need to be designed in a way that their operation is fully transparent for users. Therefore, it should be possible for users to interpret the system’s output.

Information requirements include, for example, the instructions for use, identification of the provider as well as characteristics, capabilities and limitations of performance of the high-risk AI system.

**Designing a quality management system:**

Providers of high-risk AI systems need to put in place a quality management system. It needs to be documented in the form of written policies, procedures and instructions, including, for example, the following aspects:

- a strategy for regulatory compliance
- techniques, procedures and systematic actions to be used for the design, design control and design verification of the high-risk AI system
- examination, test and validation procedures to be carried out before, during and after the development of the high-risk AI system
- systems and procedures for data management, including data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation and data retention
- procedures related to the reporting of serious incidents and of malfunctioning
- systems and procedures for record keeping of all relevant documentation and information

**Conformity assessment procedure based on internal controls**

We support you with the execution of a conformity assessment procedure based on internal controls.

Besides that, our global Responsible Artificial Intelligence Toolkit is a suite of customisable frameworks, tools and processes designed to help organisations harness the power of AI in an ethical, unbiased and responsible manner – from strategy to execution.
With this offering, we can help you to ensure the responsible use of A.I. at different levels of technical depth by

- Defining A.I. control framework. Looking at the main areas of Governance, Robustness ad Security, and Performance will allow for a 360-degree view on the necessary controls.
- Cataloguing the use of A.I. across the organization. In order to answer the fundamental questions around the design and deployment of A.I., the organizations need to categorize and monitor the key risks.
- Reviewing the high-risk A.I. solutions. The appropriate validation of an A.I. model involves considering both the components of the model as well as the environment and processes that it is embedded in.
- Operationalizing trustworthy A.I. This step would involve considering the external influencers (regulation, standards, guidelines, think tanks) and mapping those onto the strategic direction of the company tied to the business outcomes.