As AI gains human traits, will it gain human trust?

An overview of the EU AI Act and its impact on the markets

The better the question. The better the answer.
The better the world works.

EY
Building a better working world

The AI Act

The European Commission has proposed and presented the Artificial Intelligence Act (AI Act) – an important milestone in the field of AI which will place the European Union at the frontier of AI regulation and innovation for the upcoming years. The proposal aims to harmonize rules for the development, placement on the market, use and adoption of AI, while addressing the risks posed by the technology. The AI Act proposes a risk classification categorization and is one of the most important first steps in the EU's approach to dealing with the societal and ethical implications of Artificial Intelligence. The finalized text is expected towards the end of 2023 and a two to three year implementation period is expected thereafter to comply with all requirements of the regulation.

Who will be affected?

- Operators* of AI systems located in the EU
- Operators of AI systems located outside the EU if they operate AI systems in the EU or the output produced by the AI systems is used in the EU
- Providers placing on the market or putting into service AI systems outside the Union where the provider or distributor of such systems is located within the EU

> “
>
> Success in creating AI would be the biggest event in human history. It might also be the last, unless we learn how to avoid the risks.
>
> Stephen Hawking

Penalties in case of non-compliance

The AI act lays down a strict liability regime for non-compliance. Therefore, compliance with the AI act is essential since enforcement can lead to significant fines. In this context, the AI act operates on the notion of three levels. Depending on the violation, the act gives the following fines:

Non-compliance case	**Proposed Fine**
Use of high-risk AI systems without solid data governance or violation of transparency requirements	Fines up to €20 million or 4% turnover, whichever is higher
Placing prohibited AI systems on the market	Fines up to €40 million or 7% turnover, whichever is higher
Other violations of the act, e.g. misleading information to the public	Fines up to €10 million or 2% turnover, whichever is higher

Actors defined in the AI Act

Provider
A governmental, legal, natural or other body that is or has developed an AI system to place on the market, or to put into service under its own name or trademark

User
Any natural or legal person using an AI system, including public authorities, agencies or other bodies

Importer
Any natural or legal person within the EU 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

Distributor
Any natural or legal person, not being the provider or importer, which gives access to an AI system in the EU market without affecting its properties

Product manufacturer
A manufacturer of an AI system that is put on the market or putting into service an AI system together with their product and under their own name or trademark

*Operator is an umbrella term for provider, user, authorized representative, importer and distributor

The proposed Risk Classification: a three tier model

The AI Act proposes a risk-based approach to consider and remediate the impact of AI systems on fundamental rights and user safety. The proposed approach entails different requirements per tier. Three types of risk are described for different types of AI practice:

Unacceptable Risk

- Systems with an unacceptable risk rating **are prohibited** by the European Commission:
  - AI systems that deploy **subliminal techniques** beyond a person's consciousness in order to materially influence one's behavior or opinions;
  - AI systems that **exploit vulnerabilities** of a specific group of persons, such as age, disabilities or specific economic or social situation;
  - AI systems used for the **evaluation or classification of natural persons** based on their social behavior or personality characteristics;
  - The use of **'real-time' remote biometric identification systems** in publicly accessible spaces for the purpose of law enforcement.

High Risk

- Systems with a high risk rating must comply with multiple requirements and undergo a conformity assessment:
  - AI systems used as a safety component covered by the Union harmonization legislation;
  - AI systems used for:
    - Biometric identification and categorisation of natural persons;
    - Management and operation of critical infrastructure;
    - Education and vocational training;
    - Employment, workers management and access to self-employment;
    - Access to and enjoyment of essential private/public services and benefits;
    - Law enforcement;
    - Migration, asylum and border control management;
    - Administration of justice and democratic processes.

Lower Risk: so called "Certain AI systems"

- Certain AI systems which do not meet the specified criteria for the other two tiers and still present limited risk are recommended to apply the same practices as high-risk AI systems and are subject to transparency obligations (which shall be clearly communicated at the latest at the time of first interaction or exposure):
  - Users must be informed that they are interacting with an AI system unless this is obvious from the circumstances;
  - Users must be informed when biometric categorization and emotion recognition systems are used unless they are permitted by law to detect, prevent and investigate criminal offences;
  - Content that has been artificially generated or manipulated to generate deep fakes must be disclosed.

Sample of the proposed requirements for high-risk AI systems:

Deployment of an appropriate risk management system

An appropriate risk management system shall be established, implemented, documented and maintained. In addition, an established continuous iterative process must run throughout the entire lifecycle of the AI systems.

Appropriate levels of accuracy, robustness and cyber security

High-risk AI systems shall be developed to consistently perform at an appropriate (i.e., relevant, representative, free of errors and complete) level of accuracy, robustness and cyber security, in line with each AI system's specific purpose. These must be clearly documented in the system's instructions of use.

Comprehensive instructions for use

To ensure AI systems are clear for natural persons, they shall be accompanied by instructions for use that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to users (i.e., the system's intended purpose, performance and any circumstances that may lead to risks to the health and safety or to fundamental rights).

Logging capabilities and human oversight

AI systems must be designed and developed to enable the automatic recording of events, ensuring traceability of the systems throughout their entire lifecycle. Also, AI systems shall be designed and developed in such a way to enable natural persons to effectively oversee their use.

Use of appropriate training, validation and testing data

Training, validation and testing datasets must be subject to appropriate data governance and management practices, including relevant design choices, data collection, data preprocessing, formulation of assumptions, prior assessment of availability and statement of biases and shortcomings.

Specific technical documentation

AI systems technical documentation must be developed and used to assess the compliance of each AI system to the regulation. The documentation must contain the general characteristics, capabilities and limitations of the system, algorithms, data, training, testing and validation processes, as well as risk management considerations.

How are models in Financial Services impacted by the Act?

AI systems are used throughout most of Financial Institutions. Refer below for examples of how implementations at Financial Institutions are currently expected to be classified under the proposed AI Act. It is recommended to classify implementations on a case-by-case basis against the Act*:

<table>
<tr><th></th><th>Banks (Retail, Commercial, Internet, Central, Investment)</th><th>Insurance Companies</th><th>Brokerage Firms</th><th>Public Finance</th></tr>
<tr><td>Unacceptable risk</td><td colspan="3">Real-time facial recognition systems in ATMs or physical buildings
Robo-advisory services or insurance premium calculations that apply subliminal techniques to influence customers or discriminate customers based on vulnerabilities of specific groups (e.g., age, specific economical or social situation)</td><td>Use of ‘real-time’ remote biometric identification in public spaces
Social scoring systems that assigns scores to persons and rewards good behavior</td></tr>
<tr><td rowspan="2">High risk **</td><td colspan="4">Human Resources AI systems used for screening and evaluation of candidates for recruitment/interview processes
Human Resources AI systems used for making decisions on promotion and termination of work -related contractual relationships
AI techniques used for task allocation or for assessing and monitoring employees’ behavior and performance
AI systems intended to be used for the ‘real-time’ and ‘post’ remote biometric identification of natural persons</td></tr>
<tr><td>Credit scoring AI systems used for evaluating the creditworthiness of customers or establishing their credit score</td><td>AI used for claims processing
AI systems used for premium calculations</td><td>n/a</td><td>AI systems used to evaluate the eligibility of natural persons for public assistance benefits and services, such as tax calculations and tax reductions</td></tr>
<tr><td rowspan="2">Lower Risk (so called “Certain AI systems”)</td><td colspan="4">Chatbots
AI systems used for biometric categorization of natural persons
AI systems used for emotion recognition
Deep fakes
Speech analytics
Social media check for feedback purposes</td></tr>
<tr><td>Customer experience improvement systems
AI systems used for regulatory compliance
AI systems used for customer pattern analysis
Money-laundering monitoring AI systems</td><td>Customer experience improvement systems
AI systems used for regulatory compliance
AI systems used for customer pattern analysis
Customer lifetime value prediction</td><td>Customer experience improvement systems
AI systems used for regulatory compliance
AI systems used for customer pattern analysis
AI systems used to classify and give rating to stocks</td><td>n/a</td></tr>
<tr><td rowspan="2">Other AI systems not in scope of the risk classification proposed by the AI Act</td><td colspan="4">AI systems used for data collection and (predictive) analysis
AI systems for process automation
AI systems used for operational efficiency and/or data driven decisions
Document processing automation
Automatic translation
Pricing and risk management decisions</td></tr>
<tr><td>Pricing algorithms used for credit line applications and acceptance
AI systems used for tracking market trends</td><td>Insurance premium calculations for compulsory protection products, such as home or car insurance
Fraud detection for claims</td><td>AI systems used for tracking market trends</td><td>Using AI to detect identity fraud</td></tr>
</table>

* The European Commission has not issued a finalized list of all possible AI systems per classification
** Boxes referring to multiple categories are used to capture examples overlapping between those sectors
*** Note that the above examples are based on the latest list as published on 3 November 2022

What can you start doing now?

It is often more costly and complex to ensure compliance when AI systems are operating than during the design phase.

Here are some practical steps you can start implementing now:

Establish a formal governance

Establish an AI Ethics committee with experienced professionals to decide on challenging AI Ethics disputes

Assess your risks

Ensure your organization has a comprehensive risk management framework in line with the AI Act requirements

Assign responsibility

Determine and enforce roles and responsibilities for the entire AI lifecycle and associated requirements

Design ethical systems

Promote a sustainable and ethical use of AI incorporating it in your organizational strategy

Raise awareness

Disseminate information and train your people with regards to the benefits and risks brought by AI

Stay up-to-date

Stay tuned to new regulatory developments to anticipate their impact on your organization and ensure timely compliance

Start preparing now!

Start designing and implementing strategic improvements to your AI lifecycle in order to decrease complexity and implementation costs

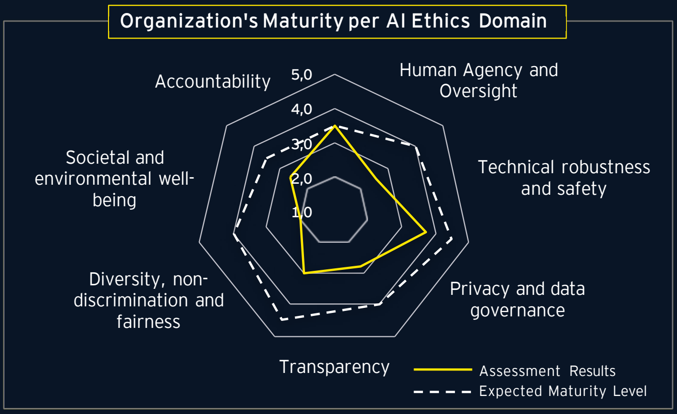
How can EY teams support you in preparing for the AI Act?

As regulators are finalizing the last changes of the AI Act, organizations will have a **two to three year period** after the final text's approval to comply with the requirements, and can face **fines of up to 40 million euros or 7% turnover** in case they fail to do it in time.

In our experience, systematically applying such changes is often a challenging and lengthy process. We believe **it is crucial to start acting as soon as possible** to comply with the timelines and enable sustainable change.

Therefore, EY teams developed the **AI Act Readiness Assessment** to:

- Help organizations navigate through the regulation's requirements
- Assess the use of AI systems and the extent to which the regulation applies
- Support organizations in understanding where they stand regarding the regulation's requirements and determine to what extent organizations are ready to comply with the regulation
- Assess organizational maturity and determine areas of prioritized focus
- Perform a deep dive on specific AI systems in view of the legal requirements set by the Act



If you are interested in finding out more about your organization's preparedness for the AI Act, **reach out to us!**

Swiss Financial Services Contacts

Adrian Ott

Partner
Chief Artificial Intelligence Officer
EY Switzerland
adrian.ott@ch.ey.com

Roger Spichiger

Partner
Responsible AI Leader in Financial Services
EY Switzerland
roger.spichiger@ch.ey.com

Konrad Meier

Senior Manager
Privacy Law Leader
EY Switzerland
konrad.meier@ch.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

ED None

In line with EY's commitment to minimize its environmental impact this document has been printed on FSC®-certified paper that consists of 60% recycled fibers.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com