AI & Partners

Amsterdam - London - Singapore

The European Union Artificial Intelligence Act

Handbook

Articles 6-7 & Annex III (High-Risk AI Systems)

July 2024

About

AI & Partners

Amsterdam - London - Singapore

For more information on this publication, visit https://www.ai-and-partners.com/.

About AI & Partners

'AI That You Can Trust' - Your trusted advisor for EU AI Act Compliance. Unlock the full potential of artificial intelligence while ensuring compliance with the EU AI Act by partnering with AI & Partners, a leading professional services firm. We specialise in providing comprehensive and tailored software solutions for companies subject to the EU AI Act, guiding them through the intricacies of regulatory requirements and enabling responsible and accountable AI practices. At AI & Partners, we understand the challenges and opportunities that the EU AI Act presents for organisations leveraging AI technologies. Our team of seasoned experts combines in-depth knowledge of AI systems, regulatory frameworks, and industry specific requirements to deliver strategic guidance and practical solutions that align with your business objectives.

To find out how we can help you, email contact@ai-and-partners.com or visit https://www.ai-and-partners.com.

Business Integrity

AI & Partners defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots professional services, regulatory interventions, and participating in industry groups such as AI Commons, we fight for fundamental rights in the artificial intelligence age.

AI & Partners' publications do not necessarily reflect the opinions of its clients, partners and/or stakeholders.

Contents

AI & Partners

Amsterdam - London - Singapore

AI & Partners

Amsterdam - London - Singapore

What is the EU AI Act Handbook?

The EU AI Act Handbook is a comprehensive guide that outlines the legislative and other provisions made under the EU AI Act.

It is designed to ensure the safe and ethical development, deployment, and use of AI systems within the European Union. The Handbook provides detailed explanations of the Act's requirements, including prohibited AI practices, high-risk AI systems, and governance structures.

Content

High-Risk AI Systems: This section details AI practices that pose a high risk of harm to individuals health, safety, and fundamental rights due to their inherent characteristics. Examples include biometrics, critical infrastructure, education and vocational training, employment, workers' management and access to self-employment.

Under the [AI] influence

AI & Partners

Amsterdam - London - Singapore

Description (Including Legislative Reference)

- Legislative Reference: Article 6(1) of the EU AI Act
- Description: If an AI system meets both of the following conditions:
  - Condition (a): The AI system is intended to be used as a safety component of a product, or the AI system itself is a product, covered by the Union harmonisation legislation listed in Annex I.
  - Condition (b): The product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment before being placed on the market or put into service.

Factors to be Taken into Account

- Nature of Techniques: The use of audio, image, or video stimuli that are beyond human perception or other manipulative techniques that subvert or impair autonomy and decision-making.
- Vulnerable Groups: Special consideration for groups vulnerable due to age, disability, or specific social/economic situations.
- Degree of Control: The extent to which the AI system can control the stimuli presented to individuals, potentially through advanced interfaces like virtual reality or machine-brain interfaces.

Real-World Examples

- Example 1: An AI-driven advertising platform that uses imperceptible audio cues to influence consumer purchasing decisions without their conscious awareness.
- Example 2: A virtual reality application that subtly manipulates user emotions and decisions through controlled visual and auditory stimuli, leading to significant psychological impacts.
- Example 3: An AI system in social media that uses hidden algorithms to nudge users towards specific behaviours or opinions, potentially causing financial or psychological harm.

AI & Partners

Amsterdam - London - Singapore

Description (Including Legislative Reference)

- **Legislative Reference**: Annex III (1) of the EU AI Act
- **Description**: certain AI systems in the field of biometrics are classified as high-risk. These include:
  - **Remote Biometric Identification Systems**: AI systems used for identifying individuals from a distance based on biometric data, excluding systems used solely for biometric verification (e.g., authentication).
  - **Biometric Categorisation Systems**: AI systems that categorize individuals based on sensitive or protected attributes inferred from biometric data.
  - **Emotion Recognition Systems**: AI systems that infer emotions from biometric data.

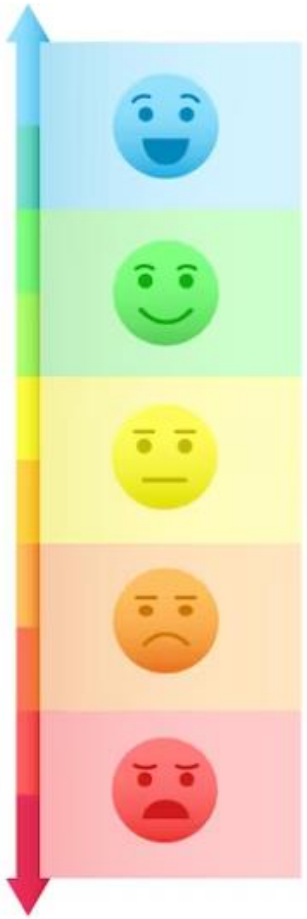
Factors to be Taken into Account

- **Intended Use**: The specific purpose for which the AI system is designed, particularly if it involves remote identification, categorization, or emotion recognition.
- **Union Harmonisation Legislation:** Compliance with relevant Union harmonisation legislation listed in Annex.
- **Risk of Harm**: The potential risk of harm to health, safety, or fundamental rights, including the risk of biased results.
- **Conformity Assessment**: The requirement for a third-party conformity assessment to ensure compliance with safety and performance standards.

Real-World Examples

- **Example 1: Remote Biometric Identification in Public Surveillance:** AI systems used by law enforcement agencies to identify individuals in public spaces through facial recognition technology.
- **Example 2: Biometric Categorisation in Access Control**: AI systems used in secure facilities to categorize individuals based on biometric data (e.g., fingerprint or iris scans) to grant or deny access.
- **Example 3: Emotion Recognition in Customer Service**: AI systems used in customer service applications to analyse facial expressions and voice tones to infer customer emotions and tailor responses.

Biometrics



Under pressure, AI aids

AI & Partners

Amsterdam - London - Singapore

Critical Infrastructure

Description (Including Legislative Reference)

- **Legislative Reference**: Annex III (2) of the EU AI Act
- **Description**: AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating, or electricity are classified as high-risk. These systems are crucial for ensuring the safety and reliability of essential services and infrastructure.

Factors to be Taken into Account

- **Intended Use**: The specific purpose for which the AI system is designed, particularly if it involves safety components in critical infrastructure.
- **Union Harmonisation Legislation**: Compliance with relevant Union harmonisation legislation listed in Annex I.
- **Conformity Assessment**: The requirement for a third-party conformity assessment to ensure compliance with safety and performance standards.
- **Risk of Harm**: The potential risk of harm to health, safety, or fundamental rights, including the risk of significant disruptions to social and economic activities.
- **Cybersecurity**: Ensuring the AI system is resilient against cyberattacks and other security vulnerabilities.

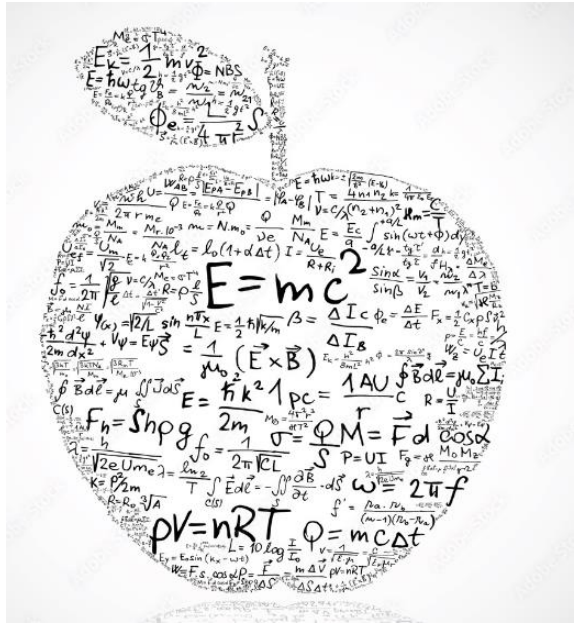
Real-World Examples

- **Example 1: AI in Smart Grids**: AI systems used in smart grids to manage and optimize the distribution of electricity, ensuring efficient and reliable power supply.
- **Example 2: AI in Traffic Management**: AI systems used in intelligent traffic management systems to monitor and control traffic flow, reduce congestion, and enhance road safety.
- **Example 3: AI in Water Supply Management**: AI systems used to monitor and control water pressure and quality in water supply networks, ensuring safe and reliable water distribution.

AI & Partners

Amsterdam - London - Singapore

Education and Vocational Training



Description (Including Legislative Reference)

- **Legislative Reference**: Annex III (3) of the EU AI Act
- **Description**: Certain AI systems used in education and vocational training including:
  - **AI systems for determining access or admission**: AI systems used to decide or assign individuals to educational and vocational training institutions at all levels.
  - **AI systems for evaluating learning outcomes**: AI systems used to assess learning outcomes, including those that influence the learning process.
  - **AI systems for assessing education levels**: AI systems used to determine the appropriate level of education an individual will receive or can access.
  - **AI systems for monitoring and detecting prohibited behaviour**: AI systems used to monitor and detect prohibited behaviour during tests.

Factors to be Taken into Account

- **Intended Use**: The specific purpose for which the AI system is designed, particularly if it involves critical decisions about access, evaluation, or monitoring.
- **Union and National Law**: Compliance with relevant Union and national laws governing the use of AI in education.
- **Risk of Harm**: The potential risk of harm to individuals' educational and professional opportunities, including the risk of biased or discriminatory outcomes.
- **Conformity Assessment**: The requirement for a third-party conformity assessment to ensure compliance with safety and performance standards.
- **Transparency and Accountability**: Ensuring that the AI system's decision-making processes are transparent and accountable to prevent misuse and ensure fairness.

Real-World Examples

- **Example 1: AI in University Admissions:** AI systems used by universities to evaluate applications and determine admissions based on various criteria such as grades, extracurricular activities, and personal statements.
- **Example 2: AI in Online Learning Platforms**: AI systems used in online learning platforms to evaluate students' learning outcomes and provide personalized learning paths based on their performance.
- **Example 3: AI in Exam Proctoring**: AI systems used to monitor students during online exams to detect prohibited behaviour such as cheating or using unauthorized materials.

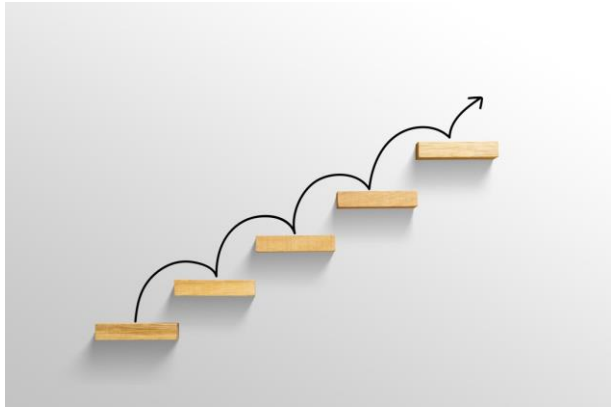
AI & Partners

Amsterdam - London - Singapore

Employment, Workers' Management and Access to Self-Employment

Description (Including Legislative Reference)

- **Legislative Reference**: Annex III (4) of the EU AI Act
- **Description**: Certain AI systems used in employment, workers' management and access to self-employment including:
  - **AI systems for recruitment or selection**: AI systems intended to be used for the recruitment or selection of natural persons, including placing targeted job advertisements, analysing and filtering job applications, and evaluating candidates.
  - **AI systems for work-related decisions**: AI systems intended to be used to make decisions affecting terms of work-related relationships, such as promotion or termination, task allocation based on individual behaviour or personal traits, or monitoring and evaluating performance and behaviour.



Factors to be Taken into Account

- **Intended Use**: The specific purpose for which the AI system is designed, particularly if it involves critical decisions about recruitment, selection, or work-related relationships.
- **Union and National Law**: Compliance with relevant Union and national laws governing the use of AI in employment 6.
- **Risk of Harm**: The potential risk of harm to individuals' career prospects, livelihoods, and fundamental rights, including the risk of biased or discriminatory outcomes.
- **Conformity Assessment**: The requirement for a third-party conformity assessment to ensure compliance with safety and performance standards.
- **Transparency and Accountability**: Ensuring that the AI system's decision-making processes are transparent and accountable to prevent misuse and ensure fairness.

Real-World Examples

- **Example 1: AI in Job Application Screening:** AI systems used by companies to screen job applications, filter resumes, and rank candidates based on predefined criteria.
- **Example 2: AI in Employee Performance Monitoring**: AI systems used to monitor employee performance and behaviour, providing real-time feedback and evaluations based on data collected from various sources.
- **Example 3: AI in Task Allocation**: AI systems used to allocate tasks to employees based on their individual behaviour, skills, and performance metrics.

Emergency AIssistance

AI & Partners

Amsterdam - London - Singapore

Description (Including Legislative Reference)

- **Legislative Reference**: Annex III (5) of the EU AI Act
- **Description**: Certain AI systems used in the context of essential private and public services and benefits including:
  - **AI systems for public assistance benefits**: AI systems used by public authorities or on their behalf to evaluate eligibility for essential public assistance benefits and services, including healthcare, and to grant, reduce, revoke, or reclaim such benefits.
  - **AI systems for creditworthiness evaluation**: AI systems used to evaluate the creditworthiness of natural persons or establish their credit score, excluding those used solely for detecting financial fraud.
  - **AI systems for insurance risk assessment**: AI systems used for risk assessment and pricing in life and health insurance.
  - **AI systems for emergency call evaluation**: AI systems used to evaluate and classify emergency calls, dispatch emergency first response services, or establish priority in dispatching, including police, firefighters, medical aid, and emergency healthcare triage.

Access to and enjoyment of essential private services and essential public services and benefits

Factors to be Taken into Account

- **Intended Use**: The specific purpose for which the AI system is designed, particularly if it involves critical decisions about public assistance, creditworthiness, insurance, or emergency response.
- **Union and National Law**: Compliance with relevant Union and national laws governing the use of AI in these contexts.
- **Risk of Harm**: The potential risk of harm to individuals' access to essential services, financial stability, and safety, including the risk of biased or discriminatory outcomes.
- **Conformity Assessment**: The requirement for a third-party conformity assessment to ensure compliance with safety and performance standards.
- **Transparency and Accountability**: Ensuring that the AI system's decision-making processes are transparent and accountable to prevent misuse and ensure fairness.

Real-World Examples

- **Example 1: AI in Public Assistance Benefits:** AI systems used by government agencies to determine eligibility for social welfare programs, such as unemployment benefits, healthcare subsidies, and housing assistance.
- **Example 2: AI in Credit Scoring**: AI systems used by financial institutions to evaluate the creditworthiness of individuals applying for loans, mortgages, or credit cards.
- **Example 3: AI in Emergency Response**: AI systems used by emergency services to classify and prioritize emergency calls, dispatch appropriate response units, and manage emergency healthcare triage.

AI & Partners
Amsterdam - London - Singapore

Law enforcement

Description (Including Legislative Reference)

- **Legislative Reference**: Annex III (6) of the EU AI Act
- **Description**: Certain AI systems used in the context of law enforcement including:
  - **AI systems for assessing victim risk**: AI systems used by or on behalf of law enforcement authorities to assess the risk of a natural person becoming the victim of criminal offenses.
  - **AI systems as polygraphs or similar tools**: AI systems used by or on behalf of law enforcement authorities as polygraphs or similar tools.
  - **AI systems for evaluating evidence reliability**: AI systems used by or on behalf of law enforcement authorities to evaluate the reliability of evidence during investigations or prosecutions.
  - **AI systems for assessing re-offending risk**: AI systems used by or on behalf of law enforcement authorities to assess the risk of a natural person offending or re-offending, not solely based on profiling as per Article 3(4) of Directive (EU) 2016/680.
  - **AI systems for profiling in criminal investigations**: AI systems used by or on behalf of law enforcement authorities for profiling natural persons during the detection, investigation, or prosecution of criminal offenses as per Article 3(4) of Directive (EU) 2016/680.

Factors to be Taken into Account

- **Intended Use**: The specific purpose for which the AI system is designed, particularly if it involves critical decisions about victim risk, evidence reliability, or profiling.
- **Union and National Law**: Compliance with relevant Union and national laws governing the use of AI in law enforcement.
- **Risk of Harm**: The potential risk of harm to individuals' fundamental rights, including the risk of biased or discriminatory outcomes, and the impact on procedural rights such as the right to a fair trial.
- **Conformity Assessment**: The requirement for a third-party conformity assessment to ensure compliance with safety and performance standards.
- **Transparency and Accountability**: Ensuring that the AI system's decision-making processes are transparent and accountable to prevent misuse and ensure fairness.

Real-World Examples

- **Example 1: AI in Predictive Policing:** AI systems used by law enforcement agencies to predict areas where crimes are likely to occur and allocate resources accordingly.
- **Example 2: AI in Lie Detection**: AI systems used as polygraphs or similar tools to assess the truthfulness of individuals during interrogations.
- **Example 3: AI in Evidence Evaluation**: AI systems used to evaluate the reliability of digital evidence, such as video footage or digital documents, during criminal investigations.

AI & Partners

Amsterdam - London - Singapore

Description (Including Legislative Reference)

- **Legislative Reference**: Annex III (7) of the EU AI Act
- **Description**: Certain AI systems used in the context of migration, asylum, and border control including:
  - **AI systems as polygraphs or similar tools**: AI systems used by or on behalf of competent public authorities or Union institutions to assess the truthfulness of individuals.
  - **AI systems for risk assessment**: AI systems used to assess various risks, including security, irregular migration, or health risks, posed by individuals entering or within a Member State.
  - **AI systems for examining applications**: AI systems used to assist in the examination of applications for asylum, visas, or residence permits, including assessing the reliability of evidence.
  - **AI systems for detecting and identifying persons**: AI systems used to detect, recognize, or identify individuals in the context of migration, asylum, or border control management, excluding travel document verification.

Migration, asylum and border control management, in so far as their use is permitted under relevant Union or national law

Factors to be Taken into Account

- **Intended Use**: The specific purpose for which the AI system is designed, particularly if it involves critical decisions about risk assessment, application examination, or identification.
- **Union and National Law**: Compliance with relevant Union and national laws governing the use of AI in these contexts.
- **Risk of Harm**: The potential risk of harm to individuals' fundamental rights, including the risk of biased or discriminatory outcomes, and the impact on procedural rights such as the right to a fair trial.
- **Conformity Assessment**: The requirement for a third-party conformity assessment to ensure compliance with safety and performance standards.
- **Transparency and Accountability**: Ensuring that the AI system's decision-making processes are transparent and accountable to prevent misuse and ensure fairness.

Real-World Examples

- **Example 1: AI in Asylum Application Processing**: AI systems used by immigration authorities to assist in processing asylum applications, including evaluating the reliability of evidence provided by applicants.
- **Example 2: AI in Border Security Risk Assessment**: AI systems used to assess the security risk posed by individuals attempting to enter a Member State, including identifying potential threats based on behavioural analysis.
- **Example 3: AI in Biometric Identification at Borders**: AI systems used to detect and identify individuals at border crossings using biometric data such as facial recognition or fingerprint scanning.

AI & Partners

Amsterdam - London - Singapore

Administration of justice and democratic processes

Description (Including Legislative Reference)

- **Legislative Reference**: Annex III (8) of the EU AI Act
- **Description**: Certain AI systems used in the context of administration of justice and democratic processes are classified as high-risk. These include:
  - **AI systems for judicial assistance**: AI systems intended to be used by a judicial authority or on their behalf to assist in researching and interpreting facts and the law, and in applying the law to a concrete set of facts or used similarly in alternative dispute resolution.
  - **AI systems for influencing elections**: AI systems intended to be used to influence the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote. This excludes AI systems whose output natural persons are not directly exposed to, such as tools used to organize, optimize, or structure political campaigns from an administrative or logistical point of view.

Factors to be Taken into Account

- **Intended Use**: The specific purpose for which the AI system is designed, particularly if it involves critical decisions about judicial processes or influencing democratic outcomes.
- **Union and National Law**: Compliance with relevant Union and national laws governing the use of AI in these contexts.
- **Risk of Harm**: The potential risk of harm to individuals' fundamental rights, including the risk of biased or discriminatory outcomes, and the impact on procedural rights such as the right to a fair trial and the integrity of democratic processes.
- **Conformity Assessment**: The requirement for a third-party conformity assessment to ensure compliance with safety and performance standards.
- **Transparency and Accountability**: Ensuring that the AI system's decision-making processes are transparent and accountable to prevent misuse and ensure fairness.

Real-World Examples

- **Example 1: AI in Legal Research and Interpretation**: AI systems used by courts to assist judges in researching legal precedents, interpreting laws, and applying them to specific cases.
- **Example 2: AI in Alternative Dispute Resolution**: AI systems used in mediation or arbitration to assist in resolving disputes by analysing facts and legal principles.
- **Example 3: AI in Political Campaigns**: AI systems used to influence voter behaviour by targeting specific demographics with tailored political messages during elections.

Thank you!

AI & Partners

Amsterdam - London - Singapore

AI & Partners

Amsterdam - London - Singapore

Email

contact@ai-and-partners.com

Phone

+44(0)7535 994 132

Website

https://www.ai-and-partners.com/

Social Media

LinkedIn: https://www.linkedin.com/company/ai-&-partners/
Twitter: https://twitter.com/AI_and_Partners

Disclaimer

AI & Partners

Amsterdam - London - Singapore

This Presentation may contain information, text, data, graphics, photographs, videos, sound recordings, illustrations, artwork, names, logos, trade marks, service marks, and information about us, our lines of services, and general information may be provided in the form of documents, podcasts or via an RSS feed (“the Information”).

Except where it is otherwise expressly stated, the Information is not intended to, nor does it, constitute legal, accounting, business, financial, tax or other professional advice or services. The Information is provided on an information basis only and should not be relied upon. If you need advice or services on a specific matter, please contact us using the contact details for the relevant consultant or fee earner found on the Presentation.

The Presentation and Information is provided “AS IS” and on an “AS AVAILABLE” basis and we do not guarantee the accuracy, timeliness, completeness, performance or fitness for a particular purpose of the Presentation or any of the Information. We have tried to ensure that all Information provided on the Presentation is correct at the time of publication. No responsibility is accepted by or on behalf of us for any errors, omissions, or inaccurate information on the Presentation. Further, we do not warrant that the Presentation or any of the Information will be uninterrupted or error-free or that any defects will be corrected.

Although we attempt to ensure that the Information contained in this Presentation is accurate and up-to-date, we accept no liability for the results of any action taken on the basis of the Information it contains and all implied warranties, including, but not limited to, the implied warranties of satisfactory quality, fitness for a particular purpose, non-infringement, compatibility, security, and accuracy are excluded from these Terms to the extent that they may be excluded as a matter of law.

In no event will we be liable for any loss, including, without limitation, indirect or consequential loss, or any damages arising from loss of use, data or profits, whether in contract, tort or otherwise, arising out of, or in connection with the use of this Presentation or any of the Information.