Callaghan Innovation Te Pokapū Auaha | Simply Privacy

4 EU AI Fact Sheet

High-risk AI systems

You'll notice this fact sheet is a bit longer than the others. That's because AI systems classified as 'high risk' have the most obligations in the EU AI Act. We've summarised below how to work out if your AI system is high risk and what the different obligations are for Providers and Deployers. Buckle up!

What makes an AI system 'high risk' under the AI Act?

AI systems that could have a significant negative impact on people's health, safety or fundamental rights are classified as 'high risk' in the AI Act. For example, where there is a risk of discrimination or exclusion from access to services, or an automated decision could affect the rights or opportunities of individuals or groups in a harmful way.

An AI system may be classified as 'high risk' in two key ways:

1. Where it's specifically identified in the AI Act as being high risk because it poses a high risk of harm (see below).
2. Where it's a product already covered by EU product safety legislation or a safety component of that kind of product. For example: medical devices, industrial machinery, lifts, toys, aircraft and cars.

Which AI systems are specifically identified as 'high risk'?

» Biometrics

Remote biometric identification systems, AI systems used for emotion recognition or biometric categorisation systems inferring sensitive characteristics that are not already prohibited.

– **Why?** Bias and discrimination risks.

» Critical infrastructure

Safety components in critical digital infrastructure, traffic and water, gas, heating and electricity supply.

– **Why?** Malfunctions could jeopardise the lives of many people and lead to significant disruption.

» Education

AI systems used to determine access to education/ training, evaluate progress or identify cheating.

– **Why?** Repeating historical patterns of discrimination in education could affect the course of someone's life and their earning capacity.

» Employment

AI systems used in recruitment and performance evaluation.

– **Why?** Potential negative impact on career prospects, earning ability and fundamental rights.

This document is a summary of key aspects of the EU AI Act and does not constitute legal advice.
You should seek specific expert advice on whether and how the EU AI Act might apply to your situation.

» Essential public services

AI systems used to evaluate eligibility for public benefits and services and to evaluate, classify and prioritise emergency services.

- **Why?** Potential for significant impacts on people's welfare and infringement of rights. AI systems in emergency contexts could make life and death decisions.

» Law enforcement

Includes AI systems to assess the risks of re-offending, personality characteristics, lie detection and to evaluate evidence.

- **Why?** These systems may involve significant power imbalances and could lead to surveillance, arrest or the discriminatory treatment of certain people.

» Border control

AI systems used to assess people's health or security risk when entering the EU and to examine asylum, visa etc. applications.

- **Why?** Impacts on people in vulnerable situations with potential for discrimination.

» Essential banking and insurance services

AI systems that establish creditworthiness and life and health insurance pricing and risk assessment (excluding fraud detection).

- **Why?** Impacts on access to financial resources and insurance impacts on health and income.

» Administration of justice and democratic processes

AI systems used by courts for researching, interpreting facts and applying the law, as well as to influence electoral outcomes or people's voting behaviour.

- **Why?** These systems could have a potentially significant impact on democracy, the rule of law, individual freedoms and the right to an effective remedy and a fair trial.

Case studies

These real-life case studies give a flavour of the types of risk that informed the development of the 'high risk' category in the AI Act.

» Simulated exam results

A UK government algorithm, used during COVID lockdowns to simulate university entrance exam results, penalised students from more disadvantaged schools while favouring those from wealthier schools.

» False identification

A black man from Detroit was wrongfully arrested in 2020 after facial recognition technology falsely identified him as a shoplifting suspect.

» Recruitment

Amazon scrapped its AI-powered CV review tool after the model learnt to prioritise male candidates over female ones because of historical hiring biases reflected in the training data.

» Visa applications

The UK Home Office scrapped an algorithm used to process visa applications following complaints it perpetuated institutional racism.

» Predicting benefit fraud

The Dutch tax authority used an algorithm that wrongly accused 20,000 families of childcare benefit fraud. As a result, several victims committed suicide, over 1,000 children were taken into foster care and the Dutch government was forced to resign.

» Credit card access

Women using the Apple Card were getting lower credit limits than their male partners, despite having higher credit scores. Although gender was not a data input, the model used data proxies correlated with gender, leading to unfair outcomes.

This document is a summary of key aspects of the EU AI Act and does not constitute legal advice.
You should seek specific expert advice on whether and how the EU AI Act might apply to your situation.

Provider obligations

Providers (aka ‘developers’) have strict obligations before, during and after the launch of a high-risk AI system.

- **Establish risk and quality management systems** across the AI lifecycle that include a compliance strategy, design, development and quality control processes and an accountability framework.
- **Implement data governance**, including ensuring training data is relevant, sufficiently representative and “to the best extent possible, free of errors and complete in view of the intended purpose”.
- **Create and maintain technical documentation** for each high-risk AI system and enable automatic logging to ensure traceability of functions and to facilitate monitoring of operations.
- **Provide instructions for use** to Deployers.
- **Design human oversight into AI systems** to enable people to understand their capabilities and limitations, to detect and address issues, avoid over-reliance and interpret AI system outputs.
- **Design and build accuracy, robustness and cybersecurity into AI systems** and let users know you’ve done so.
- **Pass a conformity assessment** to verify the AI system complies with EU requirements.
- **Develop and deploy AI systems transparently** with clear usage instructions; withdraw, disable or recall non-compliant AI systems, informing Deployers, Distributors and Importers; and register in an EU database.

Deployer obligations

Deployers (aka ‘users’) also have obligations relating to their use of high-risk AI systems.

- **Implement technical and organisational measures** so high-risk AI systems are used according to Providers’ instructions for use, including assigning human oversight to those with necessary competence and authority.
- **Ensure input data is relevant and sufficiently representative** to minimise the risk of unfair bias.
- **Monitor high-risk AI systems** in accordance with Provider instructions for use and suspend and report any serious malfunctions.
- **Maintain automatically generated logs** of AI systems for at least 6 months.
- **Conduct Data Protection Impact Assessments** (usually called Privacy Impact Assessments in New Zealand) where AI systems use personal information.
- **Ensure transparency** by informing people where AI systems make decisions affecting them.
- **Conduct a fundamental rights impact assessment**, when using high-risk AI systems in certain circumstances, to consider the impact on rights like equality and privacy, and to determine appropriate mitigants.

This document is a summary of key aspects of the EU AI Act and does not constitute legal advice. You should seek specific expert advice on whether and how the EU AI Act might apply to your situation.

Are there any exceptions?

AI systems are not 'high risk' if there's no risk to health, safety or fundamental rights.

That includes if they:

- **perform 'narrow procedural tasks'** e.g. an AI system that transforms unstructured data into structured data.
- **improve the results of previous human activity** e.g. improving a document's professional tone.
- **detect decision-making patterns**, provided they don't influence previous assessments without human review — e.g. an AI system that flags deviations from teachers' standard grading patterns.
- **do purely preparatory tasks** e.g. file handling solutions like indexing, searching or linking to other sources.

AI systems will always be considered high-risk if they're used to 'profile' people. The definition of 'profiling' is borrowed from Europe's privacy law, the General Data Protection Regulation (aka 'GDPR'). It means the automated processing of personal data to evaluate someone, including analysing or predicting their economic situation, health, personal preferences, behaviour or location.

Important note

Whether you're classified as a Provider or a Deployer is a big deal. Providers have the bulk of the obligations. **But be aware that your role classification isn't fixed and can change depending on your actions.**

- A Provider won't always be the organisation that developed the AI system. For example, a Deployer that integrates an AI tool like ChatGPT into its products can become a Provider — with many more obligations.
- If you're a Deployer and you make 'substantial modifications' to a high-risk AI system — or if you re-purpose a low-risk AI system for a high-risk purpose — then you will be classified as Provider.

This document is a summary of key aspects of the EU AI Act and does not constitute legal advice.
You should seek specific expert advice on whether and how the EU AI Act might apply to your situation.