Browne Jacobson

The EU AI Act: What does it mean for insurers?

24 April 2024

The European Union Artificial Intelligence Act (the Act) is the world's first comprehensive framework on Artificial Intelligence (AI). But what does the Act mean for insurers in the UK?

What does the Act do?

Risk based approach

The Act introduces an AI classification system that determines the level of risk an AI solution could present to individuals. The four levels of risk classifications are:

1. **Unacceptable risk** – Application of AI that is banned within the European Union (EU), for example social scoring and monitoring of people and AI which manipulates human behaviour or exploits people's vulnerabilities.
2. **High risk** – Examples include AI that controls access to financial services, critical infrastructure or employment. High risk AI systems are subject to strict conformity assessment and monitoring. AI systems that profile individuals, for example that process personal data to assess various aspects of a person's life such as health or economic situation, interests or behaviour.
3. **Limited risk** – Examples include chatbots. They are subject to specific transparency obligations. For example, users should be aware that they are interacting with AI. There are also requirements to ensure that AI generated content is identifiable.
4. **Minimal risk** – Examples include spam filters and AI enabled video games. Minimal risk is unregulated.

The majority of obligations under the Act relate to high risk AI systems.

The Act also establishes AI regulatory sandboxes for controlled innovation. Testing can also occur in the real world outside the sandbox with regulatory oversight.

It also limits the use of biometric identification systems by law enforcement.

High risk AI systems

There are a number of governance requirements for high risk AI systems, such as establishing risk management and quality management systems.

High risk AI systems must be designed:

- for record keeping so that certain events and substantial modifications are automatically recorded
- to allow for human oversight
- to achieve appropriate levels of accuracy, robustness and cybersecurity

Instructions for use must be provided to downstream deployers to enable their compliance.

The Act establishes a right for consumers to submit complaints about AI systems and receive explanations about decisions based on high risk AI that affect their rights.

General purpose AI

There are a number of requirements for general purpose AI (AI that has capability to serve a variety of purposes) such as providing information and documentation to downstream providers, establishing a policy to respect copyright and publishing a summary about the

content used to train the model.

Free and open licence general purpose AI model providers just need to comply with the copyright and training data summary requirements, unless they present a systemic risk.

Implementation

The Act will be implemented in stages, after entry into force:

- Six months for prohibited AI systems.
- 12 months for General Purpose AI.
- 24 months for high risk AI systems under Annex III.

What does this mean for EU insurers?

Some markets have been labelled high risk and some technologies closed off. Classification as high risk means that the use of AI will be subject to stricter requirements.

The Act lists the use of AI systems used for risk assessment and pricing in life and health insurance as high risk AI systems. This is because it could have a significant impact on a persons' life and health, including financial exclusion and discrimination.

However, the Act says systems used for the purpose of detecting fraud in financial services and for prudential purposes to calculate credit institutions' and insurances undertakings' capital requirements should not be considered high risk. AI systems used to evaluate creditworthiness are otherwise classified as high risk. However, the Act will still have an impact on how AI can be used to detect fraud. For example, biometric data use has been classified as high risk or completely prohibited.

Fundamental rights impact assessments are only required for bodies which are governed by public law, private actors providing public services and banking and insurance providers using AI systems listed as high risk. The aim of the fundamental rights impact assessment is for the deployer to identify the specific risks to the rights of individuals or groups of individuals likely to be affected and to identify measures to be taken in the case of a materialisation of those risk.

Financial service regulators are designated within their respective competences as competent authorities for the purpose of supervising and implementing the Act, unless member states decide to designate another authority to fulfil these market surveillance tasks.

What does this mean for the UK and UK insurers?

A number of businesses and insurers operate in both jurisdictions. The Act applies to those that intend to place on the market or put into service AI systems in the EU, regardless of whether they are based in the EU or a third country. It also applies to third country providers where AI system's output is used in the EU.

The UK currently relies on existing insurance laws and regulations, which are broad enough to apply to new technologies. It has implemented a cross-sector and outcome-based framework for regulating AI, underpinned by five core principles:

1. Safety, security and robustness
2. Appropriate transparency and explainability
3. Fairness
4. Accountability and governance
5. Contestability and redress.

With the Act the EU is hoping to play a leading role globally. The UK is holding off introducing legislation until the challenges and risks of AI are better understood, the Government says:

"We recognise the need to build a stronger evidence base before making decisions on statutory interventions. In doing so, we will ensure that we strike the right balance between retaining flexibility in our iterative approach and providing clarity to businesses"

Legislation in this this area is expected in the future. The EU example may influence future legal developments in the UK, particularly if it proves to be successful.

UK regulators such as the Financial Conduct Authority currently have a large amount of autonomy in how they approach AI. As a result, AI technologies are regulated through a complex patchwork of legal requirements. This current patchwork of legal frameworks is unlikely to sufficiently address the risks that AI can pose.

The Government says:

> *"Instead of giving responsibility for AI governance to a new single regulator, the government will empower existing regulators - such as the Health and Safety Executive, Equality and Human Rights Commission and Competition and Markets Authority - to come up with tailored, context-specific approaches that suit the way AI is actually being used in their sectors."*

In a White Paper dated March 2023 'A pro-innovation approach to AI regulation' the Government details its plans for implementing AI regulation (UK AI Paper).

The UK AI Paper says that the Government received feedback from industry that the absence of cross-cutting AI regulation creates uncertainty and inconsistency which can undermine business and consumer confidence in AI, and stifle innovation. It also acknowledges that some AI risks arise across, or in the gaps between existing regulatory remits.

The UK AI Paper says:

> *"Our framework is context-specific. We will not assign rules or risk levels to entire sectors or technologies. Instead, we will regulate based on the outcomes AI is likely to generate in particular applications. For example, it would not be proportionate or effective to classify all applications of AI in critical infrastructure as high risk. Some uses of AI in critical infrastructure, like the identification of superficial scratches on machinery, can be relatively low risk. Similarly, an AI-powered chatbot used to triage customer service requests for an online clothing retailer should not be regulated in the same way as a similar application used as part of a medical diagnostic process. A context-specific approach allows regulators to weigh the risks of using AI against the costs of missing opportunities to do so... To best achieve this context-specificity we will empower existing UK regulators to apply the cross-cutting principles. Regulators are best placed to conduct detailed risk analysis and enforcement activities within their areas of expertise. Creating a new AI-specific, cross-sector regulator would introduce complexity and confusion, undermining and likely conflicting with the work of our existing expert regulators."*

Following implementation of the UK's new framework to regulate AI, joint guidance on AI produced by the Financial Conduct Authority (FCA) and other relevant regulatory authorities is expected. This will increase clarity on the regulatory requirements relevant to AI and on how to satisfy those requirements in the context of insurance, including consumer services and products.

Annex A of the UK AI Paper sets out factors that the government believes regulators may wish to consider when providing guidance/implementing each of the five core principles. The FCA will be considering these factors in determining its approach to AI. A full list can be found from page 68 of the UK AI paper. We have selected some highlights as follows:

- "Set explainability requirements, particularly of higher risk systems, to ensure appropriate balance between information needs for regulatory enforcement (e.g. around safety) and technical tradeoffs with system robustness."
  Read our previous deep dive into explaining artificial intelligence use to insurance customers.
- "Interpret and articulate 'fairness' as relevant to their sector or domain."
- "Decide in which contexts and specific instances fairness is important and relevant (which it may not always be)."
- "Design, implement and enforce appropriate governance requirements for 'fairness' as applicable to the entities that they regulate."

- "Where a decision involving use of an AI system has a legal or similarly significant effect on an individual, regulators will need to consider the suitability of requiring AI system operators to provide an appropriate justification for that decision to affected parties."
- "AI systems should comply with regulatory requirements relating to vulnerability of individuals within specific regulatory domains. Regulators will need to consider how use of AI systems may alter individuals' vulnerability, pursuant to their existing powers and remits."
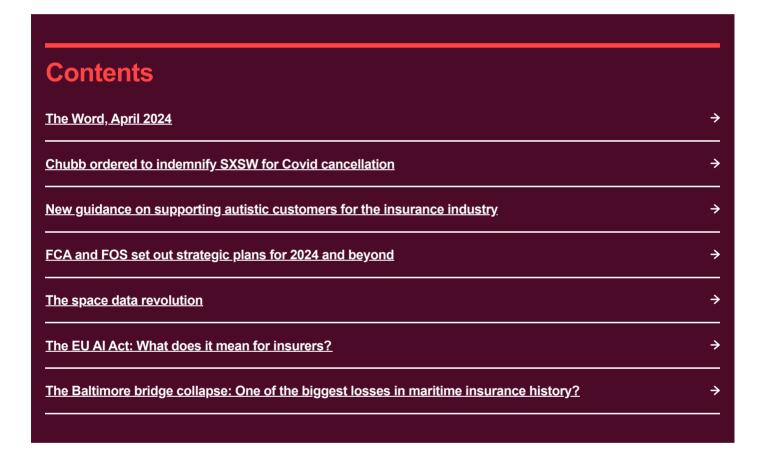
The Financial Times has recently reported that the Government may already be rethinking its approach and legislating AI following alarm over its potential risks.

Key contact

Tim Johnson

Partner

tim.johnson@brownejacobson.com

+44 (0)115 976 6557

Related expertise

AI regulation and governance

Artificial intelligence

Counter fraud for insurance

Cyber liability and data security insurance

Financial services and insurance advisory

Financial services regulation

Insurance distribution for financial services businesses

Regulatory