

Existing legislative provisions relevant for AI

The proposed new legislative framework for AI is complemented by a wide body of existing EU legislation that addresses many of the potential risks and challenges associated with the development and use of AI in the insurance sector, which is further complemented by national regulatory frameworks. The EU regulatory framework covers general cross-sectoral areas of relevance, such as fundamental rights, privacy and data protection.

Financial services and insurance-specific legislation also ensures a robust regulatory framework in the insurance sector when it comes to AI use. The Solvency II framework, for example, contains provisions addressing the governance mechanisms put in place by insurers, while principles such as transparency, fairness and ethics are also addressed by rules on conduct of business and disclosure, such as the Insurance Distribution Directive (IDD).

Sector-specific legislation

Financial services legislation ensures a robust regulatory framework, with many provisions that are particularly relevant to tackle some of the risks identified in relation to the use of AI. In the insurance sector, relevant governance principles are set out in the Solvency II framework.

- **Solvency II framework**

In the context of organisational and prudential requirements, for example, there are requirements to establish and operate sound internal control mechanisms, effective procedures for risk assessment and effective control and safeguard arrangements for information processing systems. Articles 41, 44 and 46 of Solvency II require all insurance and reinsurance undertakings to have in place an **effective system of governance** which provides for **sound and prudent management** of the business.

Articles 38 and 49 of the Solvency II Directive also sets out the requirements regarding the **outsourcing** of functions and activities (eg collaboration with data vendors). Insurers are required to take appropriate arrangements to mitigate the risks related to the use of third-party service providers and ensure that the outsourcing does not impair the quality of their internal control and the ability of the competent authorities to monitor compliance with all their obligations, while remaining fully responsible for discharging all their obligations under legislation (even when several third-party providers are involved).

Furthermore, Article 19 of the Delegated Regulation (EU) 2015/3546 containing implementing rules for Solvency II establishes detailed **data accuracy/quality requirements**, in particular in relation to the data used in the calculations of the technical provisions.

- **Insurance Distribution Directive (IDD)**

The **product oversight and governance (POG)** requirements under the Insurance Distribution Directive (IDD) are also relevant for the use of AI, in particular in relation to the identification of the target market and the design/placing on the market of products. These provisions regulate the design of new insurance products and ensure that all insurance products meet the needs of their specific target market, regardless of the techniques used in said products.

Moreover, the IDD also requires (Article 20) that any insurance product that is proposed to a customer shall be consistent with their **demands and needs**, which addresses the risks of unsuitable products being sold to customers.

In addition, rules on **advice** (Article 20) apply wherever a personal recommendation is provided to a customer, regardless of whether that recommendation is provided by a human or AI actor.

Article 17(1) of the IDD also requires insurance distributors to **act honestly, fairly and professionally** in accordance with the best interests of their customers.

There are also requirements on insurers to establish fair and efficient claims and **complaints handling** processes (Article 14).

Horizontal cross-sectoral legislation

- **GDPR**

Many of the provisions of the EU General Data Protection Regulation (GDPR) are relevant and already address the use of AI applications.

Article 5 GDPR contains important principles regarding the processing of personal data, including for example the principle of **purpose limitation**, which requires insurers to inform individuals about the specific purposes for the processing of their data and ensures that any further processing must be compatible with the original purpose. Insurers must also only collect and process the personal data that is necessary to fulfil that purpose (principle of **data minimisation**).

Article 5 GDPR also comprises the principle of integrity and confidentiality: insurers must install appropriate technical and organisational safeguards that ensure the security of the personal data. Furthermore, they must also ensure the personal data is stored for no longer than necessary for the purposes for which it was collected (principle of **storage limitation**) and that the personal data used is accurate and up-to-date (principle of **data accuracy**).

Insurers must always treat consumers fairly and transparently when processing their data (principle of **fairness and transparency**) and must be responsible for and be able to demonstrate compliance with the above-mentioned principles (principle of **accountability**). Moreover, insurers must have in place the adequate governance measures that ensure the protection of consumer's privacy right from the start of the processing (principle of data protection by design and by default).

According to the GDPR, consumers have a right (i) to exercise the **right of access to their data**, in order to verify the accuracy of the data and the lawfulness of the processing (Article 15), (ii) to **request modifications** (Article 16), or even (iii) to **object to processing** in certain circumstances (Article 18). Moreover, consumers should be informed in advance, if data about them is to be used in an automated decision-making process, including profiling, and should be given information about the consequences of such processing.

According to Article 22 of GDPR, consumers will also be able to (i) ask insurers that a **human intervene** in the profiling, to (ii) express their point of view and (iii) contest a decision based on profiling. Consumers should also be given access to their "profiles" and to the logic of the decision-making that led to the development of their "profile".

A **data protection impact assessment** (DPIA) (Article 35) also provides for an evaluation of the impact on rights and freedoms of individuals before launching any new data processing activities. DPIAs examine considerations relating to the accuracy of the data, both in terms of new data being received, how that data is matched to any existing customer records and how it can be assured the outcome is also accurate.

It is also important to mention that the Article 9 GDPR introduces some restrictions concerning the processing of personal categories of data. These restrictions are in line with Article 21(1) of the European Union Charter of Fundamental Rights, which establishes that 'any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.' According to Article 21(2), discrimination on grounds of nationality shall also be prohibited.

- **Anti-discrimination legislation**

In addition to the overarching protections offered by the European Union Charter of Fundamental Rights, users of AI systems are also protected by existing EU and national equality legislation. The EU acquis prohibits discrimination based on a number of protected grounds in various settings. In the context of the sale of goods and services, the EU Gender Directive (2004/113/EC), for example, prohibits varying premium or benefits under a contract for insurance on the basis of gender. The Racial Equality Directive (2000/43/EC) prohibits discrimination on the ground of racial or ethnic origin in a broad range of fields, including goods and services offered to the public. Various other EU legislation prohibits discrimination in other settings such as employment and occupation, or access to education or social housing. Most European member states similarly have additional national provisions to protect against discrimination in the context of the provision of insurance. In some markets, this means for instance that certain factors cannot be taken into account when determining premium or benefits under a contract for insurance. This could be prohibiting the use of genetic information or family medical history (as opposed to individual medical history).

- **Unfair commercial practices Directive (UCPD)**

Article 5(2) of the Unfair Commercial Practices Directive defines unfair commercial practices as those that are contrary to the requirements of professional diligence and are likely to distort the economic behaviour of an average consumer. Furthermore, Article 5 (3) of the same Directive specifies that special consideration should be given to vulnerable consumers.