How EU rules regulate the use of data and protect consumers

The European Union has established a comprehensive regulatory framework governing data and digital activities, with a strong emphasis on consumer protection as its core principle. Together with financial services and insurance-specific legislation, this broader set of rules requires companies to take full responsibility for how consumer data is used and how consumers are protected.

Under the current EU regulatory framework, insurers are required to embed a customer-centric approach at every stage of their operations, from the moment they collect consumer data, to sales and post-sale services. **This framework ensures that appropriate safeguards are in place to protect consumers and that their data must be treated in a fair and transparent manner.**

Transparency, privacy and potential risks of bias

The current EU regulatory framework is designed to **protect consumers' privacy and to ensure that their data is treated in a fair and transparent manner**, with a view to addressing potential risks of bias and discrimination.

General Data Protection Regulation (GDPR)

The **GDPR** provides consumers with strong protection to safeguard their personal data. This includes two of the core principles behind the GDPR: data minimisation and purpose limitation. These principles prevent insurers from being unduly intrusive in consumers' personal lives or putting their privacy at risk.

- The **data minimisation principle** requires insurers to limit data processing to what is strictly needed for the specific service. Collecting personal data that is not strictly needed would constitute a breach of the data minimisation principle. The data minimisation principle, therefore, guarantees the collection of data strictly related to the purposes of the processing and, together with principle of transparency, provides individuals with control over their personal data.
- **Purpose limitation** means that personal data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Before processing their personal data, insurers are required to provide consumers with key pieces of information, including who will carry out the processing and what is the purpose of such processing.

The GDPR requires that companies must use personal data in a way that is fair and transparent vis-à-vis consumers. This means that data must not be processed in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.

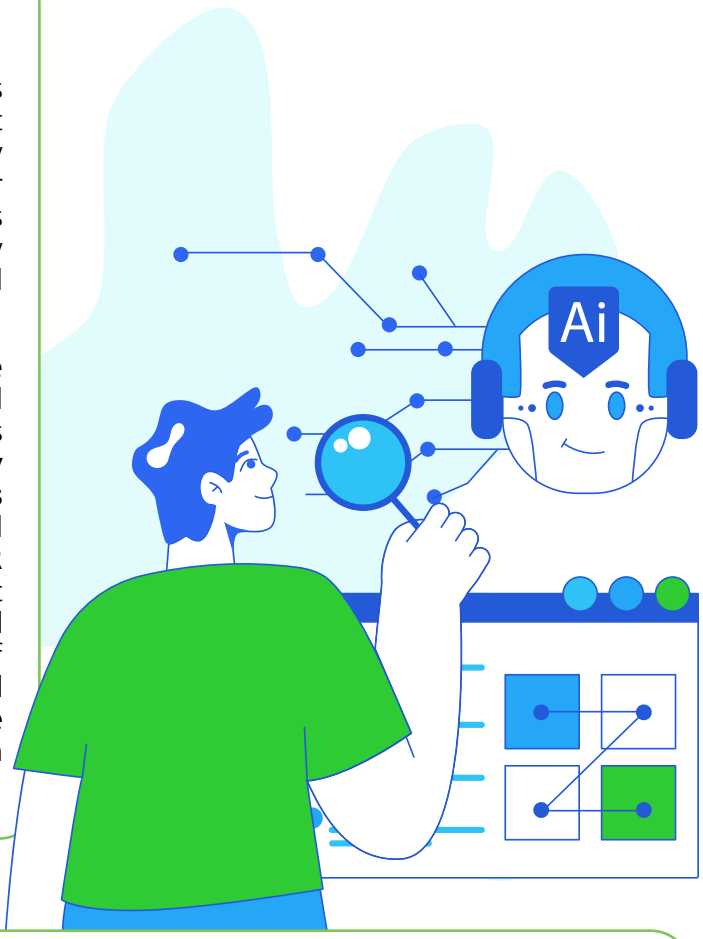
The GDPR also grants individuals the right to object to data processing in cases of automated decision-making and profiling. For instance, if a premium is calculated solely by automated means and consumers are not satisfied with the result, they have the right to ask for a human to review the decision.

© Insurance Europe aisbl, October 2025

Artificial Intelligence Act (AI Act)

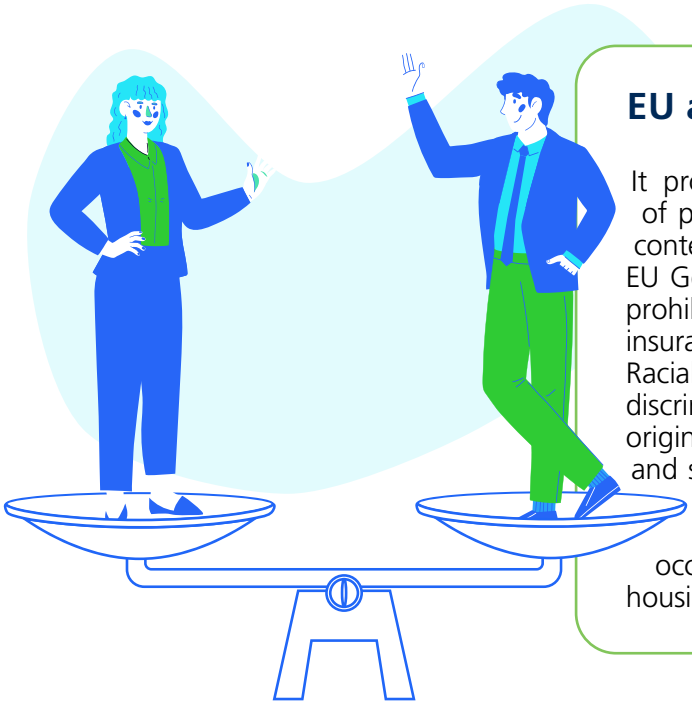
The **AI act** aims to ensure that all AI tools used within or impacting the European market are safe and trustworthy. One of its key objectives is to address potential risks of bias or discrimination by the use of AI. These systems are regulated based on the level of risk they pose to the health, safety and fundamental rights of a person.

Certain AI systems used on health and life insurance are classified as higher risk and therefore, they must meet higher standards including, among others, on **quality management, human oversight, robustness and transparency,** providing an additional layer of protection to consumers.The GDPR also grants individuals the right to object to data processing in cases of automated decision-making and profiling. For instance, if a premium is calculated solely by automated means and consumers are not satisfied with the result, they have the right to ask for a human to review the decision.



Solvency II Directive

This directive requires insurers to maintain strong governance and risk management practices to ensure financial stability and protect policyholders. In order to comply with the prudential regulations for risk management, insurers must base their pricing on **reliable data.**



EU anti-discrimination legislation

It 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 an insurance contract 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.

© Insurance Europe aisbl, October 2025

Product governance, advice and distribution

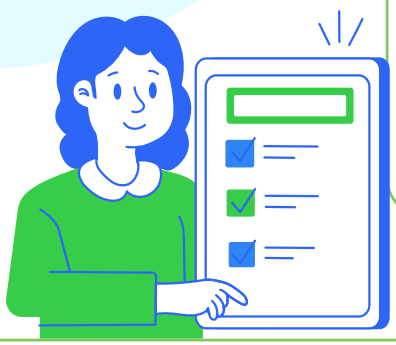
EU rules require that any insurance product that is proposed to a consumer must be consistent with their **demands and needs** and that they are provided with key pre-contractual information allowing them to compare offers in the market and choose the right product.

Insurance Distribution Directive (IDD)

The **IDD** regulates how insurance products are designed and sold in the EU. Its provisions on product oversight and governance regulate the design of new insurance products and ensure that all insurance products meet the demands and needs of their specific target market. These rules require distributors to make sure that products are consistent with customers' expectations thus addressing the risks of unsuitable products being sold to them. Insurers must ensure transparency in their offerings, providing clear and comprehensible information so that consumers can make informed decisions.

Packaged Retail and Insurance-based Investment Products (PRIIIPs) Regulation

The **PRIIPs Regulation** requires insurers to provide consumers with a standardised key information document (KID) to help them understand the main features of retail investment products.



Unfair Commercial Practices Directive (UCPD)

The **UCPD** 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. Together with the IDD, these Directives address the risks of poor and unfair selling practices which may be based on the misuse of data.

Insurance Europe is the European insurance and reinsurance federation. Through its 39 member bodies — the national insurance associations — it represents insurance and reinsurance undertakings active in Europe and advocates for policies and conditions that support the sector in delivering value to individuals, businesses, and the broader economy.

© Insurance Europe aisbl, November 2025