GDPR is around the corner: time for final checks by insurers

An overview of insurers' obligations under the General Data Protection Regulation

Data processing lies at the heart of the insurance business. Insurers collect and process personal data for several reasons. These include analysing risks that customers wish to cover, paying claims and benefits, and detecting and preventing fraud.

The new European data protection regulatory framework — the General Data Protection Regulation (GDPR) — applies from 25 May 2018. It introduces new requirements for insurers, provides enhanced rights for individuals, strengthens data authorities' powers and establishes high upper limits for fines in cases of non-compliance. As such, the GDPR will have an impact on both insurers and their customers.

What are insurers' main obligations?

Under the GDPR, when insurers process personal data in a situation in which they determine the means and purposes for which the data is processed, they become data controllers and need to comply with several obligations.

Lawful processing

Insurers must always rely on an appropriate legal basis when processing consumers' personal data. The GDPR provides six legal grounds, such as the consent of the individual or a contractual or legal obligation.

In addition, specific, more restrictive rules apply for the processing of special categories of data, such as health data. For example, the performance of an insurance contract cannot be used as a legal basis to process special categories of data.

Keeping consumers informed

Before processing personal data, insurers must provide their customers with certain information, such as who is processing their data and for what purpose. This also applies when insurers obtain personal data from third parties: for example, the personal data of a traffic accident victim in order to process a claim or if an insurer collects data from public sources.

Responding to consumers exercising their rights

The GDPR reinforces individuals' rights regarding their personal data, and insurers must be prepared to comply with these rights.

For instance, when insurers process data based on the consumer's consent or the contract, if the consumer requests it, an insurer must provide the consumer with their data in a machine-readable format or transmit the format to another company.

Additional safeguards for data processors

If an external company processes personal data on behalf of an insurer — for instance, a cloud service provider — then the insurer must ensure the external company has appropriate measures in place that demonstrate that its processing operations meet GDPR requirements.

Data Protection Officer

If an insurer's core activities involve regularly monitoring individuals or the processing of special categories of data, such as health data, on a large scale, it must appoint a data protection officer (DPO).

The DPO is responsible for advising the insurer and its employees about their obligations. The DPO will also monitor an insurer's compliance with the GDPR and cooperate with the supervisory authority on issues related to the processing of personal data.

Privacy by design and default

This requires insurers to consider data protection rules when designing products: for example, incorporating the encryption of personal data. They must also take appropriate measures to ensure that — by default — only personal data necessary for a specific purpose is processed.

For example, an insurer might opt to delete data using automated means once the period for which the data needs to be retained is over.

Data Protection Impact Assessment

When processing data entails a high risk to an individual's rights and freedoms, insurers must assess the risks and take measures to mitigate them before processing the data.

For instance, if an insurer processes health data on a large scale, it will need to conduct a data protection impact assessment (DPIA) to assess the risk posed to consumers from processing that data.

It is important for insurers to check whether their national supervisory authority has published a list that includes the processing operations that require a DPIA, as well as a list that refers to processing operations that do not require a DPIA.

International transfers

When transferring personal data to a company outside the EU/EEA, insurers must ensure the company is based in a country that the European Commission has recognised as having adequate data protection rules.

Alternatively, the insurer must ensure the company uses one of the appropriate safeguards listed in the GDPR to ensure a high level of data protection, such as standard contractual clauses or binding corporate rules. In exceptional circumstances, insurers can rely on derogations, such as the consumer's consent, for cross-border data transfers.

Notification requirements in case of a data breach

When personal data is either unlawfully or accidentally disclosed to unauthorised participants or is temporarily unavailable or altered, insurers must notify their supervisory authority within 72 hours of detecting the breach.

If the data breach entails high risks to the rights and freedoms of individuals, insurers must also notify all those individuals. Insurance Europe has developed a data breach notification template, that can help to comply with reporting requirements.

Last, but not least

Accountability
Along with complying with the GDPR, insurers must demonstrate their commitment to being compliant. They must implement processes in a way that actively demonstrates their compliance with the GDPR.

Awareness
It is vital for insurers to raise awareness within their company, so that staff involved in data processing activities are well aware of data protection rules.

It is important to note that national data protection authorities can impose fines of up to €20m or 4% of a company's global turnover if it is found to be non-compliant with GDPR rules.

For further information about insurers' obligations under the GDPR, please check:

- European Commission Q&As
- European Commission online guidance
- European Commission infographic for data controllers
- General Data Protection Regulation text
- Article 29 Working Party guidelines

or consult your Data Protection Authority