WILLIAM FRY

// PRIVACY SOURCE

Data and the Insurance Industry

May 2020

The EU General Data Protection Regulation (**GDPR**), which took effect on 25 May 2018, is one of the most ground-breaking pieces of EU legislation in the digital era.

The GDPR modernises the legal framework of data protection and privacy in Europe to ensure the consistent protection of personal data. The implementation of the GDPR brings about a number of sweeping changes and "data heavy" (re) insurance companies and intermediaries must review their data processes and procedures to ensure GDPR compliance.

Some key changes and impacts brought about by GDPR include:

PENALTIES & CLAIMS

Fines up to €20m or 4% of global annual turnover and the right to sue for material and non-material damage.

PROFILING	Stricter rules on automated decision making are likely to impact the various technologies deployed within the insurance sector to aggregate and analyse data such as big data analytics, profiling and telematics.
ONE-STOP SHOP	Organisations may be regulated by one data protection authority if the main establishment of the organisation is in the EU. In these circumstances, (re)insurance companies and intermediaries will deal with one data protection authority.
ENHANCED RIGHTS FOR POLICY HOLDERS/ CONSUMERS	Internal mechanisms for GDPR rights including the right to erasure, right to restriction of processing and right to data portability (eg to a new insurance provider) must be implemented.
MANDATORY DPO (DATA PROTECTION OFFICER)	Insurance businesses engaged in regular and systematic monitoring on a large scale OR large scale of processing of special categories of data such as health data require a DPO. SMEs (such as intermediaries) are exempt unless the processing is core to their business.
SECURITY BREACH REPORTING	Requirement to report to Data Protection Authority within 72 hours where risks to rights and freedoms of individuals.
VENDOR MANAGEMENT & DATA PROCESSORS	New liability principles and a requirement for more detailed contract terms with outsource service providers, distributors and other intermediaries.
EXTENSION OF LIABILITY	Responsibility for privacy breaches extends to data processors so both the data controller and data processor will be jointly liable for any damages on a statutory basis.

CONSENT

Higher threshold for consent. Consent must be specific, freely given, informed and unambiguous and explicit consent is required for processing special categories of data, such as health data.

DPIAS (DATA PRIVACY IMPACT ASSESSMENTS)

Mandatory for high risk data processing such as profiling and large-scale processing of special categories of personal data such as health data.

Contact Us

If you have any queries in relation to this, or would like to know more about our PrivacySource offering, please contact our Partners below, our your usual William Fry contact.

David Cullen
PARTNER
+353 1 639 5202
david.cullen@williamfry.com

Leo Moore
PARTNER
+353 1 639 5152
leo.moore@williamfry.com

John O'Connor
PARTNER
+353 1 639 5183
john.oconnor@williamfry.com

Contact our PrivacySource Team here

Follow us @WFIDEA