YOUR TOP QUESTIONS ABOUT GDPR, ANSWERED

The EU General Data Protection Regulation (GDPR) is the biggest reform to European Union (EU) data protection laws in twenty years. At its core, its aim is to give control back to citizens and residents over their personal data as well as to simplify the regulatory environment by unifying the regulation within the EU. It became enforceable on 25 May 2018.

The GDPR governs how entities collect and process personal data – i.e. any information relating to an identified or identifiable person (data subject) who resides in the EU. The GDPR sets out principles for how organisations treat data collection and processing and it also requires them to demonstrate how they comply with these principles. Furthermore, the GDPR requires organisations to identify a 'lawful basis' for processing personal data before doing so (and documentation of it). One example of lawful basis is explicit (not inferred) consent given by the data subject.

To ensure compliance with the GDPR, any organisation that is involved with the collection of personal data will need to make significant changes to the way they collect and/or process that data or, at the very least, how they document it. These organisations will be expected to implement comprehensive governance measures, and whereas some privacy tools and procedures have previously been seen as good practice, they will now become legally required. Fines for non-compliance can reach up to €20m or 4% of an organisation's group worldwide turnover.

With the GDPR now in force, we've addressed your most pressing questions to help you and your clients understand the complexities of the regulation.

DOES THE GDPR APPLY TO ME?

More than likely. The GDPR applies to "controllers" and "processors". A controller determines the purposes and means of processing personal data. Controllers can be any entity that collects data from an individual data subject – hospitals, retail stores, and law firms, for example, can all be classed as controllers. Processors are responsible for processing personal data on behalf of a controller and will typically be passed that data by the controller – cloud providers, data hosts, and other technology companies can all be classed as processors.

The GDPR applies to all data processing activities within the EU (carried out either by controllers or processors) and also to organisations outside the EU that offer goods or services to individuals in the EU. So, if your company is based outside the EU but you have customers who reside in the EU, you fall under the GDPR.

And don't forget about your partners, especially if you're a data processor. If you use sub-processors or contractors, they'll need to comply with your contractual data protection obligations too. For more information on how the GDPR impacts data processors, view our quick guide.

IS THE GDPR JUST ABOUT DATA BREACHES?

No – data breach is just one area that the GDPR addresses. But it is important.

Under the GDPR, all organisations will have a duty to report certain types of data breach to the relevant supervisory authority, and in some cases to the affected individuals themselves. A personal data breach will include any breach of security which leads to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

The relevant supervisory authority only needs to be notified where it is likely to result in a risk to the rights and freedoms of individuals. This essentially means that the breach has the potential, if not properly addressed, to cause harm to affected individuals, be that through financial loss, reputational damage, discrimination, or by leading to other negative outcomes. A notifiable breach has to be reported to relevant supervisory authority within 72 hours of the organisation becoming aware of it. If a breach is likely to result in a high risk to the rights and freedoms of individuals, then they must be notified directly and this must be done without undue delay.

In addition to the penalties related to data breaches, organisations can also be penalised for other infringements of the regulation such as failing to seek consent from data subjects before collecting their data and neglecting to maintain written records in relation to data processing activities. Generally speaking, infringements which directly impact the rights of individual data subjects will likely attract higher fines and penalties than more procedural breaches of the regulation.

ARE FINES UNDER THE GDPR INSURABLE?

Probably – at least until a court with relevant jurisdiction rules otherwise. There is nothing within the regulations themselves expressly preventing insurance against the proposed fines. Equally, the Information Commissioner's Office (who will be enforcing the regulation in the UK) has said nothing about them being uninsurable either.

In order for a fine to be deemed legally uninsurable, it would need to be mandated as such by a court of law, which means an individual or entity would need to legally contest the ability of an insurer to pay it. As a result, insurers will have the ability to pay GDPR fines and penalties until a court order states otherwise. The same goes for third party liability actions.

WILL MY CYBER / TECH INSURANCE POLICY COVER THE GDPR?

Most technology E&O policies, like CFC's, provide cover for regulatory costs and fines arising directly out of a policyholder's business activities. This would encompass GDPR fines, regardless of the reasoning behind them being imposed (subject to certain exclusions). However, in many cyber policies, cover for regulatory costs is often only triggered if they are levied as the result of a cyber event. With the GDPR, this may not always be the case as it possible that regulatory fines will be levied in cases of companies misusing customer data, for example. If you're unsure whether you're covered, check your policy or talk to your insurance broker.

Do you have more questions about the GDPR and insurance? If so, get in touch with us today at GDPR@cfcunderwriting.com.