CRC Group
Wholesale & Specialty

GDPR – General Data Protection Regulation

PURPOSE OF GDPR – BECOMES ENFORCEABLE ON MAY 25TH, 2018

The GDPR establishes one single set of rules across Europe, which will make it simpler and cheaper for organizations to do business across the EU and ensure that the rights of EU residents to a private life is enforced and maintained. This replaces the Data Protection Directive of 1995 (Directive 95/46/EC), which had recently come under criticism for the increasing lack of harmonization across the EU member states as well as the increased data flow between them without boundaries and proper regulation.

Notification of a Personal Data Breach

In the case of a personal data breach, the controller must notify the supervisory authority of the personal data breach no later than 72 hours after having become aware of it.

Expanded Definition of Personal Data

The GDPR applies to "personal data," whose definition has been expanded. Information such as an online identifier, like an IP address, can be personal data. This expanded definition reflects the changes in technology and the way organizations collect information about people. Additionally, the GDPR applies to both automated personal data and to manual filing systems.

Role of Data Processors

One of the key changes is that data processors have direct obligations for the first time to maintain a written record of processing activities carried out on behalf of each controller, designate a data protection officer when required, and make sure that the data controller will be able to demonstrate that "explicit" consent was given when processing personal data.

Increased Territorial Reach

The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU. This means that a company outside the EU which is targeting consumers in the EU will be subject to the GDPR – this is not the case currently.

Fines & Penalties

The GDPR mandates two levels of fines – the first is up to €10M or 2% of the company's global annual turnover of the previous financial year, whichever is higher. The second is up to €20M or 4% of the company's global annual turnover of the previous financial year, whichever is higher.

GDPR's Effect on Cyber Policies

LEGAL - FINES & PENALTIES

The GDPR itself does not prohibit the insurance of fines. However, the law surrounding the legal insurability of fines arises out of public policy and will depend on each member state of the EU. Most carriers' Regulatory Fines and Penalties coverage should broadly include international data protection laws. Non-compliance penalties are not specifically excluded from the definition of Regulatory Fines and Penalties.

DEFINITION OF PERSONAL IDENTIFIABLE INFORMATION (PII)

Make sure that the definition of PII is broad enough to trigger 1st and 3rd party coverage – usually it is broad enough to encompass GDPR's expanded definition.

Additionally, coverage should be extended to the Insured and all of their outsourced partners (controllers and processors) to encompass the scope of the GDPR territorial scope.

EXCLUSIONS

Gross negligence and intentional acts are not covered (if the Insured willfully non-complies with GDPR), but could get a carve-back for acts by "rogue" employees.

Unauthorized collection of personal data is excluded. As mentioned above, explicit consent is a requisite under the GDPR, thus if the Insured fails to get consent, then there is no coverage.