Regulatory
Update

EU General Data Protection Regulation

Provided by **Crendon Insurance Brokers Ltd**

Quick Facts

- The data protection rules become effective on 25th May 2018.
- The new rules replace the 1995 and 2008 standards and directives.
- Fines for non-compliance can be up to €20 million or 4 per cent of annual global turnover.

The GDPR enables individuals to better control their personal data, regardless of where this data is sent, stored or processed.

EU Data Protection Reform

The EU's new data protection reform was published on 4th May 2016. The new rules become applicable on **25th May 2018**. Because of how the rules are set up, member states are not required to adopt local laws to incorporate the new data protection requirements into domestic legislation.

The EU enacted these rules to create uniform data protection rules for all member states. In its view, a unified set of rules and standards would allow EU citizens more control over their personal information. Organisations that trade in the EU, whether based there or not, must comply with these rules in regards to processing the data of their EU customers.

The new rules update and replace the current data protection rules, which are based on the 1995 Data Protection Directive and the 2008 Framework Decision for the police and criminal justice sector.

Data protection reform takes place through two major instruments:

- The General Data Protection Regulation (GDPR); and
- The Data Protection Directive.

Enforcement

A company that fails to comply with the new rules by the effective date may be subject to a fine of up to €20 million, or 4 per cent of the company's global annual turnover.

The GDPR

The GDPR enables individuals to better control their personal data, regardless of where this data is sent, stored or processed.

The GDPR has four provisions which provide:

- Individuals with more access to their own data—individuals will have more information on how their data is processed (this information must be provided in a clear and understandable way);
- A right to data portability—by making it easier for individuals to transmit their personal data between service providers;
- A 'right to be forgotten'—individuals have a right to have their personal data erased if there is no legitimate ground for retaining the data; and
- Individuals with the right to know when their information has been hacked—by creating an obligation for those who gather, store or process personal data to notify their respective national

Crendon Insurance Brokers

The GDPR will do away with the obligation for businesses to notify other national data protection authorities about the data they are processing, which costs businesses about €130 million per year, according to the European Commission.

supervisory authority of any data breaches that put them at risk (notifications should be given as soon as possible so that affected individuals can take appropriate measures).

Consent and Specific Purpose

The GDPR's 'right to be forgotten' is tied to two main concepts— **specific purpose** and **consent**.

The GDPR assumes that when an individual consents to the processing of his or her personal data, he or she does so because that data is intended for the individual's benefit or some other specific purpose.

For this reason, individuals have a right to request that their personal data be erased when processing this data is no longer required in order to meet the specific purpose for which consent was given.

However, an individual's right to be forgotten is not absolute. Data does not need to be erased if a legitimate purpose remains. Legitimate purposes include freedom of expression and scientific research.

Finally, the GDPR also recognises that a certain level of maturity and understanding is required in order to provide consent for a specific purpose. For this reason, one GDPR rule indicates that consent, for the processing of a child's personal information, must be given by whoever holds that child's parental responsibility, until the child is deemed sufficiently old enough to give consent. The GDPR allows member states to set their own age limit standard between 13 and 16 years of age.

Data Protection Directive

The Data Protection Directive applies to the police and criminal justice sectors. The directive was adopted to protect the personal data of victims, witnesses and suspects in a criminal investigation or law enforcement action.

The directive also facilitates the sharing of information and cross-border cooperation to combat crime and terrorism.

Impact on Businesses

The reforms create a more efficient business environment by cutting red tape and reducing the costs many businesses must endure if they process personal data across borders. Businesses may be able to capitalise on simpler, clearer and more unified standards as they restore or maintain consumer trust.

The reforms also make new data protection standards extraterritorial by requiring all businesses to comply while they do business in an EU member state. This ensures that all players within the EU are bound by the same rules, regardless of where they are established.

In addition, the rules streamline data safety by creating one central, single supervisory authority in each member state. It also promotes a risk-based approach to compliance requirements, recognising that businesses should have different obligations and operate under standards that more accurately represent the particular risk associated with their data processing.

Finally, the new rules call for data processors to implement data protection safeguards from the early stages of product and service development to ensure that data protection becomes the norm—by design and by default. This includes appointing a data protection officer (DPO) responsible for data protection compliance. Organisations must appoint a DPO if they are a public authority, they carry out large-scale systematic monitoring of individuals, or if they carry out large-scale processing of special categories of data or data relating to criminal convictions and offences.

Impact on Small and Medium Enterprises

The new rules also level the playing field for SMEs by requiring them to:

- Appoint DPOs only when the SMEs' core activities require regular and systematic monitoring, or if they process special categories of personal data (for example, data that reveals racial origin or religious belief);

The GDPR will establish a single, pan-European law for data protection, meaning that companies will only have to deal with one law, not 28. The new rules will bring benefits of an estimated €2.3 billion per year, according to the European Commission.

- Keep processing records only if processing is not occasional or is likely to put rights and freedoms at risk; and
- Report data breaches to individuals only if the breaches place their rights and freedoms at high risk.

In situations where SMEs must appoint DPOs, the new rules do not require that officers be full-time employees. The use of *ad hoc* and consultants is sufficient to satisfy this requirement.

Impact on Employers

Employers process a large amount of personal data from their employees. Often, processing employee information is necessary to comply with employment law and to provide adequate benefits.

For this reason, employers should evaluate how the GDPR affects their personal data processing practices, policies and procedures. In particular, employers should consider whether they have obtained consent for a specific purpose and delineate when and how this consent may lapse.

Preparing for the GDPR

Although the GDPR does not come into effect until 2018, the Information Commissioner's Office (ICO) has created a checklist of things businesses can do right now to prepare and ensure compliance:

1. **Awareness:** Ensure that all decision makers and key people in your organisation are aware of the GDPR—they need to appreciate its impact.
2. **Information You Hold:** Document what personal data you hold, where it came from and whom you share it with. Also, organise an information audit.
3. **Communication of Privacy Information:** Review your current privacy notices and put a plan in place for making any necessary GDPR changes.
4. **Individuals' Rights:** Check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.
5. **Subject Access Requests:** Update your procedures and plan how you will handle requests within the new timescales and provide any extra information.
6. **Legal Basis for Processing Personal Data:** Look at the various types of data processing you carry out, identify your legal basis for doing so and document it.
7. **Consent:** Review how you are seeking, obtaining and recording consent and whether you need to make any changes.
8. **Children:** Think about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.
9. **Data Breaches:** Ensure you have the right procedures in place to detect, report and investigate data breaches.
10. **Data Protection by Design and Data Protection Impact Assessments:** Familiarise yourself with the guidance the ICO has produced on Privacy Impact Assessments, and work out how and when to implement them.
11. **Data Protection Officers:** Designate a DPO, if required, or someone to be responsible for data protection compliance, and assess where this role will sit within your organisation's structure and governance arrangements.
12. **International:** If your organisation operates internationally, you should determine which data protection supervisory authority you fall under.

For a more detailed overview of your responsibilities under the GDPR, consult the ICO's guide for organisations located here: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr. And for more information on protecting your business and ensuring compliance, contact the insurance professionals at **Crendon Insurance Brokers Ltd** today.

Crendon Insurance Brokers