GDPR

The General Data Protection Regulation (GDPR) will come into force on 25th May this year and will set the global standards for data protection and privacy rights. This is the biggest change in data privacy regulation in over 20 years and GDPR will replace the outdated 1995 Data Protection Directive, which was adopted to help regulate the processing of personal data.

Effective across all EU member states, GDPR will strengthen and harmonise data protection for all EU citizens. Unlike the previous Directive, GDPR will impact every business and public sector organisation and require everyone to be compliant, transparent and accountable when handling personal data.

Before 25th May, organisations will need to review their current approach to data processing, privacy and compliance and start putting new processes and systems in place to comply or risk heavy penalties.

The Key Changes of GDPR

Many of the key principles from the 1995 Directive will still apply with some new regulations added, including extended territorial scope, improved individual personal data rights, increased accountability and tougher sanctions for all organisations when handling EU citizens' personal data.

Within GDPR both the data processor and data controller are liable when it comes to processing personal data. A data controller is a person or a business which decides the purposes and ways that the data is processed whereas data processors consist of third parties such as IT services providers that process personal data on behalf of the data controllers.

Extended Territorial Scope

One of the biggest changes of GDPR is the expanded territorial scope. GDPR applies to all organisations that process the personal data of individuals in the EU.

Any organisation that offers goods or services to or monitors the behaviour of EU citizens will also observe the new regulation even if they are based outside the EU. These organisations will need to take the necessary steps to ensure compliance and in some cases may need to appoint an EU representative.

Personal Data and Consent

All data subjects are the legal owners of their personal data. Personal data refers to any data that will identify the person such as name, address, phone number, email address, bank details etc. Any business or organisation that collects this personal data will need the individual's permission and consent to collect and process it.

The areas around consent have been strengthened with GDPR and all organisations will be required to be transparent in their communications with all individuals. Examples of this required consent would be positive opt-ins, unticked boxes and use of clear and concise language. GDPR also requires that it must be easy for the individual to withdraw consent.

Improved Data Protection Rights

Under GDPR, individuals will have increased rights, including:

Right to access: Any person will have the right to receive confirmation from the data controller as to whether or not their personal data has been processed and for what purpose, and where it's located. Under GDPR the data controller will be obliged to provide a copy of the personal data undergoing processing.

Data portability: Any person will have the right to obtain their personal data and reuse it for their own purposes. The data controller will be requested to send a readable format to the individual or send on the data to another controller if requested.

Right to be forgotten: The right to be forgotten, also known as right of erasure, entitles the person to have the organisation's data controller remove or delete their personal data when requested. There are many reasons for erasure; data is no longer relevant to original purposes or the person withdraws their consent for processing.

Privacy by design is a new introduction with GDPR and requires that the subject of data protection and privacy are included during the design stages of new products. Both the data controller and processor will need to ensure personal data is protected when introducing new products.

Increased Accountability

For many years we have heard of data breaches happening and personal information becoming lost or sent to the wrong people. Under GDPR legislation , organisations will not only be required to ensure that personal data collection is done in a legal and fair way but they will also be expected to protect it from misuse, thereby respecting the rights of the data owners.

When a data breach occurs which could result in a risk to the rights and freedoms of an individual, the data controller will be required to inform the supervisory authority and the individual. As part of GDPR requirements all data controllers are required to document any personal data breaches detailing the facts and action taken. These documents will verify compliance for the supervisory authority. The supervisory authority is an independent public authority in each member state that will monitor the application of GDPR.

Some organisations may need to appoint a Data Protection Officer (DPO). Public authorities, organisations that monitor data subjects on a large scale, or process sensitive personal material on a large scale will require a DPO. A DPO may be someone in the organisation or an external individual that will be responsible for recording data processing activities and ensure data protection compliance.

Tougher Sanctions

Any organisation that is found to be in breach of GDPR after 25th May 2018 will face heavy penalties. There are two levels of fines and both the controller and the processor are liable for non-compliance. Fines for infringements will be considered on a case-by-case basis and will take a number of criteria into consideration.

For the most serious infringements, the maximum fine is up to 4% of annual global turnover or €20 million, whichever is greater. Serious infringements by GDPR include not having sufficient customer consent to process data and the transfer of data to third parties.

The second level fine is up to 2% or €10 million. Examples of these infringements include not having records in order and not notifying the supervisory authority and data subject when a data breach occurs.

Impact of GDPR

The introduction of GDPR gives EU citizens more control over how their personal data is processed. For businesses GDPR provides a clear legalised structure for data protection rights but will also create a significant amount of work ahead of the live date on 25th May. The serious penalties involved will certainly encourage compliance although it remains to be seen how effective the policing of such a massive undertaking can be. The only certainty at this stage is that GDPR will be at the top of many to-do lists for many months yet!