What is the GDPR?

Network ROI, the Scottish IT services company, explains the key points of new Data Protection Regulations, which come into force in May. If you store and use customer data or information you may be affected.

THE EU General Data Protection Regulation (GDPR) will replace the Data Protection Act 1998 (the 1998 Act) when it comes into effect on May 25th this year. The GDPR has been designed to harmonise data privacy laws across Europe, to protect and empower all EU citizen's data privacy and to reshape the way organisations across the region approach data privacy.

Consideration has been given to new technologies, business processes and data usage that have become part of the digital economy in recent years.

Principles of the GPDR

Under the GDPR, the data protection principles set out the primary responsibilities for organisations. Personal data must be:

- *"processed lawfully, fairly and in a transparent manner in relation to individuals."*
- *"collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."*
- *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."*
- *"accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay."*
- *"kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed."*
- *"processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."*

Lawful basis for processing under the GDPR

Although not new, the lawful basis for processing under the GDPR places more emphasis on accountability and transparency relating to how your organisation processes data.

The six lawful bases are similar to the old conditions for processing, although there are some differences – the ICO website contains more information on lawful processing.

Individual rights

The GDPR provides the following rights for individuals.

- The right to be informed
- The right of access
- The right of rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights related to automated decision making and profiling

You can read more about individuals' rights on the ICO website.

Time to report a data breach

Under the 1998 Act, organisations have one month to report a data breach but once GDPR is enforceable, this period will reduce dramatically. Once a data breach has been detected, organisations will have 72 hours to investigate the violation, let the regulator know what's happened, figure out if personally identifiable information (pii) has been compromised and have a plan to manage the threat.

Unless there are technical controls and a robust information security policy in place to mitigate the threat of a data breach, many organisations will struggle to meet these demands.

Data Protection Officer

In some circumstances, organisations must appoint a Data Protection Office (DPO). You must appoint a DPO if you:

> "The GDPR has been designed to harmonise data privacy laws across Europe, to protect and empower all EU citizen's data privacy and to reshape the way organisations across the region approach data privacy."

- are a public authority (except courts acting in a judicial capacity)
- carry out large-scale systematic monitoring of individuals (e.g. behaviour tracking)
- carry out large-scale processing of special categories of data or data relating to criminal convictions or offences – at this time, there is no numerical definition of "large-scale processing."

You may appoint a data protection officer to act for a group of companies or a group of public authorities – depending upon size and data processing requirements.

Any organisation can appoint a DPO. Our Technical Director, Neil Douglas is a qualified GDPR Data Protection Officer and is always free to chat regarding your DPO or GDPR requirements.

Penalties

The maximum penalty for suffering a severe data breach under the Data Protection Act 1988 is £500,000. Mobile telecoms company, Talk Talk received a £400,000 fine for failing to prevent a serious data breach back in 2015.

Penalties under the GDPR are far more severe. A maximum fine of €20 million or 4% of global annual turnover for the most severe data breaches is on the cards. However, we don't expect the Information Commissioners Office (ICO), the UK's governing body to impose the maximum fine as it hasn't done so under the existing regulations – that's not to say they won't impose sizeable penalties.

To find out more about the GDPR, visit https://www.networkroi.co.uk/gdpr •