



Helen Dixon was appointed as Data Protection Commissioner for Ireland in September 2014. Responsible for upholding the rights of individuals regarding how data about them is used, the role, among other things, requires regulation of a large number of US internet multinationals with European bases in Ireland

GDPR – the time to prepare is now

The General Data Protection Regulation (GDPR) is effective from 25 May 2018. All organisations should be preparing for compliance now, says Data Protection Commissioner Helen Dixon

The GDPR is a once-in-a-generation overhaul of Europe's Data Protection laws that will strengthen the rights of individuals and create a regulatory environment fit for purpose in the digital age.

Personal data is any data that can identify an individual – this includes names, contact details, health records, bank statements and so on, or indeed new types of data emerging alongside new technologies, such as your smartphone's location data or an IP address.

The GDPR will bring new responsibilities to organisations that use personal data and tough new penalties for non-compliance. Now is the time to get ready and review your handling of personal data.

Why GDPR?

The ways in which personal data are used have changed fundamentally since existing data protection laws were created. The Data Protection Acts were last amended in 2003 – at that time Google was in its infancy; Facebook not yet invented; and smartphones unheard of.

As society moves increasingly into the digital sphere, data protection and privacy concerns are coming to the fore.

For these reasons, the European Union has agreed a far-reaching reform of data protection laws effective from May 2018: the General Data Protection Regulation or GDPR.

It brings a set of clear, harmonised data protection rules that put the individual firmly in control. It benefits businesses and promotes growth and innovation by providing a safe, legal basis for using data, boosting consumer confidence in the digital economy, and replacing 28 differing sets of EU laws with a single EU-wide regulation.

Changes

The GDPR retains all of the familiar principles of data protection with which you are already acquainted. Namely, that information should be obtained fairly; used for one or more specific purposes; kept safe and secure; not excessive, out of date or irrelevant; retained for only as long as is necessary; and a copy of his or her data given to anyone that requests it.

However, it also adds two new principles of data integrity and accountability, reinforced by a number of new responsibilities.

Meanwhile, individuals will be empowered through new and more clearly defined personal data protection rights. The new law also introduces heavy new sanctions for non-compliance. The Irish data protection authority (DPC) will be responsible for driving compliance and enforcing the new law.

A new one-stop-shop provision allows multinational businesses to deal with a single lead supervisory authority in whichever country they are mainly established. This provision is particularly relevant in an Irish context – Ireland's Data Protection Commissioner will be lead regulator in Europe for many of the world's leading internet multinationals.

It's important to remember that there is no grace period after the 25th May 2018 – the new law will have direct, immediate effect, so the time to prepare is now.

How to prepare

Preparing for compliance with the GDPR can seem like an intimidating task, and it will certainly demand focus, resources and attention.

As a first step, organisations can consult the DPC's *12 steps to being prepared* document available on our new microsite, GDPRAndYou.ie. As May 2018 approaches, this site will be continuously updated with more in depth and sector-specific guidance.

The foundation underpinning any preparations should be an awareness of what data you hold. Can you identify all of the data that you hold? For what purpose do you hold that data? What is your legal basis for processing? What measures do you take to secure it? Keeping these records is both a requirement of the GDPR and an essential first step in preparing for compliance.

A role for Accountants

Certified Public Accountants are well suited to data protection. Your expertise in record keeping and processing sensitive information and commitment to ethics in the public interest, are highly compatible with the principles behind data protection and the GDPR. The DPC will be expecting high standards of compliance from the accountancy sector.

Indeed, there are many similarities between the role of an accountant and a Data Protection Officer, so a data protection qualification is something a certified public accountant might consider as the GDPR drives demand for appropriately skilled and qualified data protection practitioners.

Summing up

The digital economy is here to stay and Data Protection will become an ever more crucial element of how we safeguard people's rights. The GDPR is designed to facilitate this shift in our society, and provide a safe environment for the use of personal data.

The key message here is that by preparing now for the GDPR, you can be in a position not only to navigate the challenges ahead but also to prosper and thrive in the digital age as you retain the trust of your clients.

An Coimisinéir Cosanta Sonrai GDPR – what's new?

Enhanced Personal Rights

The Right to be informed – organisations collecting your data must provide privacy notices setting out how your data will be used.

The Right of access – organisations must provide you with a copy of your data within 30 days of a request, and cannot charge a fee for responding to access requests.

The right to rectification – Individuals can have inaccurate or incomplete information about them rectified.

The right to erasure – individuals can request that personal data which is no longer relevant be deleted.

The right to restrict processing – organisations must cease processing an individual's data once this right is exercised. Organisations should retain just enough data to ensure the restriction is respected.

The right to data portability – individuals should receive their data in a reusable format, and can transfer it from one service provider to another.

The right to object – individuals can object to data processing based on legitimate interests; direct marketing; and processing for the purposes of research and statistics.

The right not to be subject to automated decision-making, including profiling – the GDPR provides safeguards to protect individuals from potentially harmful decisions being made without human intervention.

New Responsibilities

Many organisations will be required to appoint a **Data Protection Officer**.

It will be mandatory to **report data breaches** within 72 hours.

New high-risk projects will require a **Data Protection Impact Assessment**. If this assessment finds residual risk that cannot be mitigated, consultation with the DPC is mandatory.

Data Protection by design and default, long advised as best practice, is now mandatory. This means services should be automatically privacy friendly, and should take account of privacy concerns from the outset.

The **transparency principle** has been strengthened and privacy notices will require additional information on how data will be used.

Organisations must **maintain records** of all data processing activities.

New Sanctions

Data Protection authorities will have heavy new sanctioning powers. Where offences occur, organisations can be liable for fines of **up to €4 million, or 20% of global turnover**, whichever is greater.

For further information, check out

GDPRandYOU.ie
@DPCIreland