New frontiers in data privacy

Personal data security is increasingly important, but many companies may not be ready to comply with tougher data protection laws.

Citizens around the world are growing increasingly concerned about what organisations do with their personal data. High-profile data breaches at some of the largest global firms have demonstrated the risks to individuals and businesses.

Despite this, many companies have been slow to wake up to the new data responsibilities required under the EU's tougher data protection laws, which must be implemented by May 2018. This may require a complete overhaul of how companies use, share and obtain consent to process personal data (see box below for more details).

For example, a survey of Irish companies by Mazars in Ireland and law firm McCann Fitzgerald (see box, right) found that only 16% had started a project to meet the compliance requirements of the General Data Protection Regulation (GDPR). Although this survey was conducted in August 2016 and the situation has evolved since then, there are still many major organisations that are just at the kick-off stage of their GDPR project.

All EU businesses that handle data will have to comply with the GDPR, which will require

THE GDPR: NEW DATA REQUIREMENTS

OBTAINING CONSENT
Companies must demonstrate that they have obtained appropriate consent from data subjects to process their data where this is a legal requirement.

INVENTORY OF PERSONAL DATA
Companies must maintain an inventory of personal data, including how it is used and shared.

THE RIGHT TO BE FORGOTTEN
An individual can request the deletion of personal data—where a company has publicised it, other data controllers can be required to comply with the request.

DATA PORTABILITY
Individuals have the right to receive personal data that they have provided to a company in a commonly used format and request that it is transferred to another company.

DATA PROTECTION OFFICER
Certain companies must appoint a Data Protection Officer (DPO) to monitor compliance with the GDPR. They must be experts in data protection laws and regulations, they must be independent and they must report to the highest level of management.

REPORTING DATA BREACHES
Companies must report data breaches to their local regulator within 72 hours of becoming aware of the event. The subject of the breach must also be informed where there is a high risk that their rights and freedoms will be affected.

Shutterstock

investment in systems and training for employees. This takes time and the stakes are high. Companies that fail to comply with the GDPR could face fines of up to 4% of global turnover or €20m, whichever is greater, in the case of a breach. Most importantly, the reputational damage of such a breach can have major consequences for a business.

However, smart companies should focus on the opportunities to maximise returns on investment, rather than focusing on the threat of sanctions. "The new GDPR requirements can be an opportunity for organisations to promote a data-responsible image," says Vincent Rezzouk-Hammachi, UK head of data privacy and data management at Mazars. "Companies need to find new ways to limit the amount of data they collect, and communicate the benefits to customers."

Boardroom awareness

For large international companies the harmonisation of the data protection rules across Europe is a positive step. The introduction of the "one stop shop" principle, for example, allows businesses to rely on only one regulator when they are a cross-border organisation.

However, the job of identifying every system and process that may not be in line with the GDPR is a major task. For a large, complex organisation with numerous different systems and a high volume of data, it can take many months to analyse all the programmes and systems that are used within the business. Some systems, for example, will communicate across different functions of the group and with subsidiaries; some will not. Sometimes IT is well coordinated at group level; sometimes it is not.

"The GDPR will affect many departments and goes beyond any border within an organisation, so the relevant level for accountability has to be at board level," says Rezzouk-Hammachi. "Often, the first question we are asked by companies is, 'how much will the remedies cost?'"

Board directors need to take a step back and use the GDPR as an opportunity to take a fresh look at what is going on inside the company's systems, says Rezzouk-Hammachi. The first step is to create a Core Privacy Team, composed of the organisation's main stakeholders which process personal data.

Know your systems

The best starting point is for companies to do a GDPR-readiness assessment. This provides an understanding of where the data is located and the operational needs of different departments of the business. It also involves a number of checks including: the purpose of the data processing; how consent was collected; and how long it takes to respond if an individual asks for access to their personal data. This results in a report giving an overview of the risks and where they are located, says Rezzouk-Hammachi.

The next stage is to perform a detailed gap analysis to identify any areas where the company falls short of the requirements in terms of its systems, processes or employees' awareness of the GDPR principles. This leads to an implementation action plan with specific recommendations, such as system adaptation or cyber-training programmes.

New projects

As the deadline for implementing GDPR approaches, data privacy is sure to rise up the agenda for senior management and board directors. However, companies must ensure that the strategic importance of data protection remains a boardroom issue long after the May 2018 deadline.

As a minimum, boards must ensure that their businesses remain compliant with the GDPR. Companies will have to constantly monitor their systems and processes against the regulation's requirements, avoid data breaches and manage the risks. Large companies may want to create privacy committees to improve oversight or link data privacy objectives to directors' performance management.

Boards also need to be aware of the GDPR principle of "privacy by design". This means that companies must consider data privacy at the outset of any new project or programme to ensure that personal data is only collected when there is a clear business or regulatory need.

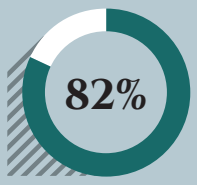
For example, does a bank need a customer's date of birth? Probably, yes, for regulatory and background checks. But what about a bookshop? The marketing department might argue that, yes, there is an operational need. Without it, the loyalty programme would not be able to send a voucher to customers on their birthdays.

Until now, these questions have not been asked, systematically leading to the collection of unnecessary data. "Businesses are starting to realise how important it is to limit the amount of data they collect to limit risks and ensure that systems work as smoothly as possible," says Rezzouk-Hammachi.

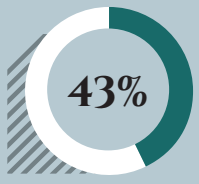
Data privacy is much more than a compliance process. It has become a key area where companies will be judged in terms of their engagement with customer concerns and their ability to adapt to technology challenges. That should be more than enough to make board directors take note. ●

Readiness for GDPR

What Irish businesses said

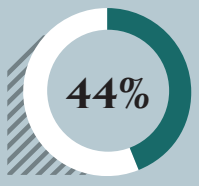


Complying with GDPR will be challenging or extremely challenging



The most challenging requirement will be creating and maintaining an inventory of personal data

do not have a Data Protection Officer (DPO) required to monitor compliance with the GDPR



meeting the requirement to notify the Data Protection Commissioner of a security breach within 72 hours will be very or extremely challenging

Source: General Data Protection Regulation survey, Mazars and McCann Fitzgerald, August 2016