Proposed EU Data Protection Regulation

A BSI factsheet for business

Data protection is already a priority for business. Now, the proposed EU Data Protection Regulation is set to raise the stakes even further. But the information security standard ISO/IEC 27001 can help address the challenge.

Snapshot

- Data protection is a major cause of concern for businesses
- Many organizations have suffered information security (IS) breaches, resulting in regulatory action, fines, commercial costs and reputational damage
- The EU is proposing a new Data Protection Regulation (EUDPR), imposing a tougher data protection regime across the EU
- The onus is on businesses to put adequate procedures in place to prevent IS breaches
- Help is at hand: the Information Security Management System (ISMS) Standard ISO/IEC 27001 responds to legal requirements with practical measures
- Companies can demonstrate best practice through independent certification to ISO/IEC 27001.

Why data protection matters

Data protection is a major issue for businesses of all sizes and across all sectors, with lapses in information security (IS) putting them at risk of fines, commercial costs and reputational damage.

Many organizations have already suffered IS breaches and concerns are growing.

Record number of data protection complaint cases.*

of large organizations suffered a security breach in the last year.**

For large organizations serious breaches typically cost between £600,000 and £1.15m.**

The scale and cost of IS breaches affecting UK businesses over the last year has almost doubled.**

The cost of breaches has shot up for the third consecutive year.**

**July 2014 - Information Commissioner's Office (ICO), the UK's chief data regulator.*

***Department for Business, Innovation and Skills (BIS) Information Security Breaches Survey 2014 (carried out by PwC).*

bsi.

...making excellence a habit.™

Regulation speculation

The coming months are likely to see the introduction of new European regulations ratchet up the stakes further. Specifically, the adoption of a new EU Data Protection Regulation (EUDPR) will set out to strengthen current data protection legislation. It is likely to impose onerous new responsibilities on organizations, putting them at greater risk of falling foul of the law and subject to heavier penalties if they do.

The EUDPR as currently proposed, will result in a single regulatory system across the EU, creating one of the world's most comprehensive and heavily enforced data breach notification regimes.

What is being proposed?

Possible outcomes of the proposed EUDPR will be that organizations:

- Must report data breaches promptly
- Must appoint a dedicated Data Compliance Manager, if they have more than 250 employees
- Will be legally as well as contractually obliged to keep personal information secure, if they are 'data processors' (for example, third-party payroll service providers)
- Must conduct an 'impact assessment' on data privacy for new projects
- Must maintain records
- Must gain individuals' consent to hold their data, in many circumstances
- Will be subject to a 'one-stop-shop' regulator with enforcement powers across the EU
- Will be liable to penalties of up to 2% of global turnover for failures and breaches

Under the current Data Protection Act, UK companies have been obliged to protect the personal data they hold on customers, employees, prospects and others – with the risk of penalties for any failure to do so. But, as Renzo Marchini, Special Counsel at law firm Dechert LLP, explains, the proposed EUDPR goes much further. "For example, in the UK there is currently no general obligation to report a data breach, while monetary penalties under the Act are limited to a maximum of £500,000, with a higher 'trigger level' for a large fine to be imposed."

Marchini continues, "The EU Regulation has not yet been finalized because member states have widely differing views. EU regulation is imposed centrally and should apply uniformly, with no differences between states, but the feeling is that various countries are trying to opt out of different proposals." The UK, for example, is resisting the idea of a dedicated Data Protection Officer for all companies with more than 250 employees, with the ICO arguing that this is not suitable for all companies in all sectors.

Some observers believe the end result may look more like an EU Directive – whereby individual states exercise discretion over how they translate EU legislation into local laws – as is the case now in the UK, where the original 1984 Data Protection Act was updated and replaced in 1998 in response to a 1995 EU Directive.

Marchini adds, "We are still some way from reform, so businesses don't need to panic, but they would be well-advised to look ahead and prepare themselves during the proposed two-year transition period."

Anticipated timescales for change

Autumn 2014	Early 2015	2015-2016	Early 2017
EU Council finalizes the EUDPR	Adoption of the EUDPR	Two-year transition period	The EUDPR comes into force

What it means for business

The onus is on businesses to put in place robust measures to manage and mitigate IS risks to comply with the new law – and also because it is in their best commercial interests. "The bottom line for businesses is that under the current law if you hold data you must keep it secure, and the new law will have the same objective," says Marchini.

Andrew Miller, Cyber Security Director at PwC, says that with data breaches becoming more sophisticated and their impact more damaging, boards need to be reviewing threats and vulnerabilities on a regular basis. "While investment in IS has increased in the last year, businesses must make sure that the way they are spending their money is effective," says Miller. "Organizations also need to develop the skills and capability to understand how the risk could affect them and what strategic response is required."

How standards can help

The international information security management system (ISMS) standard ISO/IEC 27001 is well established as the only certifiable international standard to define the requirements for an ISMS. Businesses of any size or sector can either choose to adopt the standard and self-declare compliance to it, or be independently certified to it by BSI.

ISO/IEC 27001 provides a framework for managing IS risks and easing compliance with regulations such as the proposed EUDPR. As one of many respected standards – including ISO 22301 for a business continuity management system – ISO/IEC 27001 provides businesses with a way to help meet legal and regulatory compliance, manage and protect valuable information and give confidence to stakeholders.

Adopting a systems approach for establishing an ISMS with ISO/IEC 27001 will enable businesses to address key issues, such as what do you do if your data has been breached. It can be built upon, for example, by cloud service providers with CSA STAR certification, or by any business with ISO 22301 to establish 'information continuity' and brings about greater organizational resilience if the confidentiality, integrity or availability of information is compromised.

Gigi Robinson, BSI's ISO/IEC 27001 scheme manager expands "ISO/IEC 27001 requires risks to information to be mitigated in a number of ways including the establishment of an awareness programme to ensure all members of staff understand their responsibilities around information security and the implementation of security measures. This covers areas such as classification and transfer of information; consideration of information security in the supply chain; reporting and management of incidents; and implementation of appropriate physical security controls. Finally, robust review through internal and independent assessment, governance and improvement processes are expected to ensure that the privacy and protection of personally identifiable information is in line with relevant legislation and regulation."

Protect and survive

Lisa Dargan, Business Development Director at Ultima Risk Management, a consultancy specializing in business resilience, says, "ISO/IEC 27001 is a fantastic framework because it looks at IS in the broadest sense, starting with the question, 'what information are you trying to protect and why?' and recognizing that a large part of the security solution lies in employee training and awareness."

BIS's Information Security Breaches Survey 2014

Experts agree that IS risks will, at times, become reality. "Sooner or later you will have a breach," stresses Alan Cook, Director of management consultancy Agenci Information Security. "Businesses don't realize it can come from anywhere – from their 'soup' of systems, their processes, and especially from their people. If everyone adopted ISO/IEC 27001 there'd be a fantastic improvement in IS across the UK."

Standard bearer: Capgemini

"If we fail to comply with regulation we risk heavy fines and severe damage to our reputation. Security has also become a major concern for clients. Without robust systems in place, we could lose business. That's why we went down the standards route. We wanted to prove best practice to ourselves, but we also wanted to demonstrate it to both commercial and government clients who are insisting on it."

Bill Millar, *Global Chief Information Security Officer for the UK Infrastructure Services division of Capgemini, BSI ISO/IEC 27001 certification client.*

Standard bearer: Fredrickson International

"Information security is fundamental to the success of our business, with much of our work involving receiving, analysing and storing sensitive consumer and business credit information. ISO/IEC 27001 has helped us ensure that we have appropriate policies, procedures and controls in place to protect our systems from criminals, and prevent personal information falling into the wrong hands."

Simon Jones, *Managing Director, Fredrickson International BSI ISO/IEC 27001 certification client.*

To find out more about ISO/IEC 27001 with BSI
Call: **0845 080 9000**
or visit: **bsigroup.com**

bsi.

BSI UK
Kitemark Court
Davy Avenue, Knowlhill
Milton Keynes, MK5 8PP
United Kingdom

T: +44 845 080 9000
E: certification.sales@bsigroup.com
bsigroup.com