bsi.

...making excellence a habit.™

EU data protection reform

Background and insight

A Whitepaper

Executive summary

The Irish Data Protection Acts 1988 and 2003 gave effect to the European Data Protection Directive 95/46/EC. The existing legislation provides a balance between individual rights and organizational necessity by providing a framework within which to process data fairly and lawfully.

On 21 October 2013, Civil Liberties MEPs voted on implementing a reform of current EU Data Protection rules which aims to put people back in control of their personal data, enhance and build trust in social media and online shopping, and upgrade the protection of personal data processed by police and judicial authorities.

Following years of deliberation and debate on these proposed regulations, the European Parliament gave final approval to the enactment of the new EU Data Protection legislation on 14th April 2016 and it entered into force 20 days later. The regulations shall apply unilaterally in all EU member states within 2 years of publication, with the official compliance date being 25th May 2018.

The implications for business are significant. This paper discusses the nature and scope of the planned reforms, the considerable cross-business challenges they represent and how best to address them. It is therefore of relevance both to security and compliance professionals, and also to functional managers in Sales, Marketing and HR.

Background

The need for EU data protection reform

Unfortunately, the 1995 Data Protection Directive has been interpreted differently within different countries across the EU, with the result that the enforcement regime can differ significantly from country to country and, in some cases, even within the same country.

Much has changed since 1995: mobile phones and tablets are ubiquitous, and using a mobile phone or accessing the Internet from any device is leaving a digital trail that can be linked back to an individual. The rise of social media and the proliferation of apps that track every detail of our digital lives mean that the need for a comprehensive reform of the data protection regulations has never been more important.

The aims of reform

Reform of the data protection regulations has five fundamental aims that can be summarised as follows:

- To reinforce individuals' rights – privacy by design and by default
- To strengthen the EU internal market through new, clear and robust rules for the free movement of data
- To ensure consistent enforcement of the rules
- To set global data protection standards
- To ensure a high level of data protection across all industries

The pillars of EU data protection reform

The European Commission refers to the following four 'pillars' of the regulation:

Pillar One: one continent, one law with effective sanctions

The regulation will apply uniformly throughout individual EU member states without the requirement for any national implementing legislation to give it legal effect. The implications are as follows:

This brings a much-needed harmonisation of data protection law across the single European market.

- It provides a level playing field for business through one single law applicable to any business across the EU.
- This is expected to save businesses up to €2.3 billion per year.

There are significant fines for breaches of the regulations. These fines are presented in two tiers:

- Tier one - Up to €10 million or up to 2% of annual worldwide turnover, whichever is higher

This level of fine will be imposed for infringements of the regulations where, for example; no written contract is in place between the controller and the processor of data.

It is now the responsibility of organizations that possess and control a subject's personal or sensitive data to have a clear and concise written contract in place if passing to a third party (a Data Processor).

- Tier two – Up to €20 million or up to 4% of annual worldwide turnover, whichever is higher

This level will apply where, for example; a company doesn't obtain explicit consent from a data subject for the processing of sensitive personal data.

Pillar two: Non-European companies will have to stick to European data protection law if they operate on the European market.

This provides for wider territorial scope as follows:

- The regulation will apply to organisations outside the EU
- If organizations outside the EU process personal data in connection with the provision of services to, or monitoring of, individuals located in the EU, they're in scope
- Individuals will have the right to refer all cases to their home country national data protection authority, even if the data is processed outside of their home country

Pillar three: The right to be forgotten/ the right to erasure

When an individual no longer wishes their data to be processed and there are no legitimate grounds for retaining it, the data must be deleted. This is about empowering individuals, not about erasing past events or restricting freedom of the press. More specifically:

- "Right to be forgotten" is now being referred to as a "right to erasure"
- The onus will be on data controllers to prove that they need to keep the data, not on the data subject

Some additional clarifications:

- Where a particular type of storage technology does not allow for erasure, then the data subject has a right to have the data "restricted" as opposed to erased
- To strengthen the right to be forgotten... Every individual will have the right not to be profiled
- Profiling = any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability, or behavior

Pillar Four: a "one-stop-shop" for businesses and citizens

The concept of a one-stop shop has been discussed. The idea is that organisations would have a single

supervisory/regulatory authority overseeing their data processing activities across all EU Member States. However:

- This is now likely to be a "lead authority" which would be required to consult with all other competent authorities
- It is likely there will be significant further discussion on this point in order to clarify specific supervisory requirements

What This Means for Individuals

The primary aim of the data protection reforms is to strengthen citizens' rights. Enhanced data protection rules will strengthen the control an individual has over their personal data. The following elements will be significantly improved for the data subject:

- **Freely given consent**
  Putting the data subject in control when consent is required to process personal data, the subject must be asked to give it explicitly. It cannot be assumed. Businesses and organizations will also need to inform the data subject without undue delay about data breaches that could adversely affect them
- **Easier access to your data**
  A right to data portability will make it easier for the data subject to transfer their personal data between service providers
- **Disclosure to third party authorities**
  Data subjects will have the right to know if his/her personal data has been disclosed to a public authority at the authority's request. Such transfer of personal data required by a third country court decision or by an administrative authority will be (mostly) prohibited. This will change the current exemptions in place for frequent or large-scale data transfer and use of traffic and location data by public authorities for national security and law enforcement activities

- **'Privacy by design' and 'privacy by default'**
  These will become essential principles in EU data protection rules. This means that data protection safeguards should be built into products and services from the earliest stage of development, and that privacy-friendly default settings should be the norm – for example on social networks.

  Privacy settings are set at a high level by default. Data protection Impact Assessments (Article 33) have to be conducted when specific risks occur to the rights and freedoms of data subjects. Risk assessment and mitigation is required and a prior approval of the DPA for high risks.

Business challenges

There are a number of significant changes that businesses should start to prepare for now.

Mandatory notification of data breach

- Currently the conditions under which a breach must be reported are not clearly defined
- Under the new regulations, there are mandatory notification requirements to data subjects and other relevant authorities
- This may potentially lead to the requirement for notification within 72 hours

As any business unfortunate enough to have suffered a data breach can attest, in a crisis situation, being organized enough to provide a detailed notification to affected customers (or indeed regulators) is a difficult task on its own. When this is combined with required incident response processes, identifying the cause of the breach and attempting to close the vulnerability that allowed the breach to happen, all while determining the extent of the damage, it becomes exponentially more difficult.

A 72-hour data breach reporting window will prove enormously challenging for organizations. Without ready-prepared response and communications plans and procedures, it may prove impossible for organizations to notify within a compliant timeframe.

Mandatory appointment of a Data Protection Officer

Organizations will be required to appoint a dedicated Data Protection Officer (DPO) if their core activities involve regular and systematic monitoring of data or processing of data relating to

- sensitive personal data, including biometric or genetic data
- or data relating to criminal convictions or criminal records

there shall be a requirement to make such an appointment. Additionally, any public authority or body, will also be expected to appoint someone to the role. In the above circumstances, the following conditions must be met when hiring or appointing to the position:

- The Data Protection Officer must demonstrate professional competency and experience
- The Data Protection Officer must be appointed for a minimum term and must also have certain minimum qualifications
- DPO must be independent
- Monitoring of DPOs will be the responsibility of the Regulator rather than the Board of Directors

Appointment of a suitably qualified and experienced individual will be a challenge for most organizations. The pool of adequately experienced data protection professionals is currently small. Even those currently employed in the area may not have the required or appropriate certifications to meet the regulatory expectations.

Many organizations may plan on appointing an existing staff member to the role. However, the DPO must be demonstrably independent of the organization ("in the company, but not of the company"), and will be answerable externally to the Lead Authority. (In Ireland, this will be the Office of the Data Protection Commissioner). Management

of any perceived conflict of interest will be difficult. As a result, it is expected that an outsourced model will be employed by many organizations to address the above concerns.

Sanctions with more teeth

The increased financial impact of fines and the expected frequency of their enforcement will be a concern for most organizations. While the cost of implementing data protection / privacy measures may be a significant outlay, they must be considered justifiable in respect of the potential cost that may be accrued in their absence or in the event of a data breach.

Initial cost of compliance

Some of the new requirements will require organizations to refresh or realign their practices. The impact of this may be costly:

- Changes to how consent is explicitly obtained will require changes at a business level, particularly for companies that engage in direct marketing or plan on continued engagement with their customers
- Technical measures to ensure consent is explicitly obtained will also result in development cost. For example, updating web-based forms, cookie pop-ups and marketing emails will all require some measure of development to become compliant.
- Organizations that rely on analysis of personal data, user activity tracking or monitoring may, in a worst case scenario, lose fundamental capability in the event that the data subjects analysed refuse consent to be profiled. As a result, the business model may need to be refined to remain viable.
- To ensure new portability of data measures are met, some organizations may need to fundamentally change their approach to how data is structured to ensure swift response to any data movement requests received.
- Responding to data subject requests may incur both time and financial expense. The process by which data subjects can engage with and request modification /removal of their data will be made simpler; organizations can expect to see an increase in the requests made by data subjects. Providing subject access responses already takes time – responding to right to erasure measures, for example, will also be a drain on company resources.
- Where the right to be forgotten is enacted by a data subject, organisations will need to fully demonstrate that this has been completed at a defensible technical level. Ensuring removal of data across systems to meet that level will often by time consuming and costly.

Implementation

For the many businesses that must comply with the proposed data protection regulation reform legislation, the best way to prepare is to implement a solid data protection strategy and process that ideally should include best practice security controls.

Our certified data protection specialists have unrivalled experience in the planning, execution and maintenance of Data Protection programs across a wide range of industry verticals. As Information Security experts, we can advise on solutions and best practice security controls to safeguard your data.

The proposed legislation does not require any specific type of technical controls. However, best practice would be to implement state of the art technical controls to render personal data unintelligible to users not explicitly authorised to access it. Controls could include:

- User access control mechanisms
- Encryption
- Redacting data where full access is not required

Our team of expert consultants work with businesses to provide insights and solutions on a range of data protection issues. Services include:

- Data protection implementation support
- Data Protection Officer services (onsite and/or virtual)
- Data protection /privacy impact assessments
- Training
- Data protection audit support (internal and/or external)
- Subject access request preparation support

Benefits

It should be noted that the data protection reforms are not entirely bad news for organisations. Whilst not necessarily wholly self-evident, there are many benefits to compliance with the new reforms.

Reducing the likelihood of a breach means avoidance of fines associated with non-compliance.

- Avoidance of reputational damage from adverse publicity.
- Reinforcement of customer focus and governance rigour amongst stakeholders.
- Reassurance to both customers and regulators that best practice has been followed.
- Completion of privacy impact assessments can help ensure that problems are identified at an early stage: addressing them early will often be simpler and less costly

The new compliance requirements may also be a driver for business process re-engineering. An organization may take the opportunity to save money and reduce compliance cost by minimising the amount of information being collected or used where this is possible. This may result in more straightforward processes for staff.

Target Market

This paper is relevant to - and will benefit - all those involved in the processing, storage and management of personal information. This includes:

- Data Protection Officers
- Human Resource Managers
- Sales and Marketing Managers
- Information Security Professionals
- Compliance and Audit Managers
- Healthcare Professionals

Conclusion

We understand the value of data to your business and the serious implications of a data breach. We help organisations to apply best practice in managing and maintaining compliance to EU data protection standards. We strongly advocate a risk-based approach to help promote responsible data use. The bottom-line message is that, if you want to be ready for the Data Protection Regulation reform, you should start developing and implementing a data protection programme.

Additional Information

- **Q&A on European Data Protection reform**
  http://www.europarl.europa.eu/news/en/news-room/content/20130502BKG07917/html/QA-on-EU-data-protection-reform
- **European Commission – Data Protection**
  http://ec.europa.eu/justice/data-protection/index_en.htm
- **Putting the consumer at the centre: More freedom, more rights, more choice**
  http://ec.europa.eu/commission/2014-2019/jourova/announcements/putting-consumer-centre-more-freedom-more-rights-more-choice

Cybersecurity and Information Resilience Services

Our Cybersecurity and Information Resilience Services enable organizations to secure information from cyber-threats, strengthening their information governance and in turn assuring resilience, mitigating risk whilst safeguarding them against vulnerabilities – in their critical infrastructure.We can help organizations solve their Information challenges through a combination of:

Research

Commercial research and horizon scanning projects

Training

Specialist training to support personal development

Consulting

Cybersecurity and information resilience strategy, security testing and specialist support

Technical solutions

Managed service solutions to support your organization

Our expertise is supported by:

CREST

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR

CYBER ESSENTIALS

CSA cloud security alliance SM

bsi.

Find out more
Call: +44 (0)845 050 1711
Email: cyber@bsigroup.com
Visit: bsigroup.com