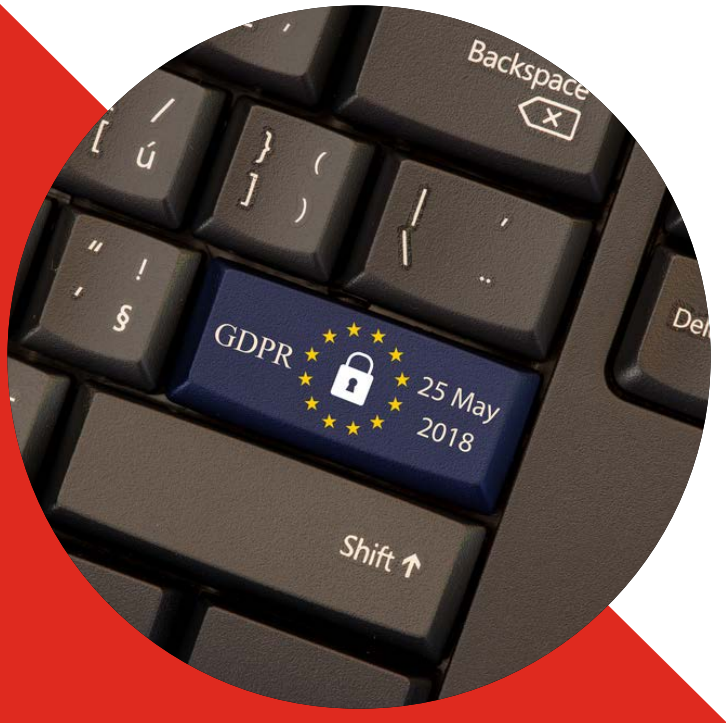
bsi.

...making excellence a habit.™

Aligning to GDPR

The date is finally upon us, now what do we do?

A Whitepaper



Background

The need for EU data protection reform

The current directive (Directive 95/46/EC) 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 with regards to personal data since 1995 – mobile phones and tablets are ubiquitous, and using a mobile phone or accessing the internet from any device is leaving a trail of "digital DNA" that can be linked back to you as 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 is long overdue.

Data protection compliance has never been as important as it is today. The EU General Data Protection Regulation (EU GDPR), set to take effect on 25 May 2018, will place significant responsibilities on organizations that collect, store or process data.

The aims of the reform

Reform of the data protection regulations has five fundamental aims that can be summarized 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

Fundamental rules – The six principles:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality

The potential impact

Upcoming GDPR requirements will affect all organizations who collect or process personal information, including SMEs and large organizations. While SMEs may not process or collect personal information at the same scale as large multinational organizations, they are still subject to the GDPR's requirements and as such, need to align accordingly.

Unfortunately, it is often the case that organizations have not taken existing data protection requirements seriously and as a result, the effort required to become compliant in advance of 25 May 2018 may be significant. This could expose the organization to fines, audits and inspections by the applicable supervisory authority and could massively affect the organization.

However, it is also important to note that while an SME may not have the resources or staff to match a large multinational organization's privacy framework, it is often the case that the scope of an SME's exposure to GDPR requirements and the distribution of personal information is greatly reduced and more manageable.

This means that while there will be an uphill battle at the start of the organization's GDPR alignment project, once the initial steps are completed it should become significantly easier to deploy and maintain on a continual basis.

This whitepaper will provide information on how an organization can begin to align to GDPR from an unprepared posture with an immature privacy framework and what timely action can be taken to address some of the more general requirements to having a defensible position.

Call: +44 345 222 1711 /+353 1 210 1711 Email: cyber@bsigroup.com Visit: bsigroup.com

Starting from scratch – Initial steps

Management engagement – Awareness and buy-in

In any effective information privacy programme, data protection needs to be embedded throughout the whole organization. To do this, senior management needs to drive the message from the top down and ensure the organization remains complaint on a continual basis. This is especially important if the organization's awareness of current data protection requirements is limited.

The first step to establishing an effective data privacy framework, is to ensure that management understand GDPR, it's requirements and impact. A presentation to the board and senior management outlining the requirements of GDPR and the potential impact of non-compliance can be one way of achieving this. Once senior management have this understanding, it will ensure that there is sufficient buy-in to enable the successful delivery of a GDPR alignment project.

Management engagement – Establishing oversight of GDPR alignment

Once the alignment project is underway, Key Perforamce Indicators and the status of the alignment project should be documented and presented to senior management on a regular basis. This ensures oversight of the project is maintained and any risks to the successful project delivery are identified and appropriately addressed.

Output

- Senior management understanding of their responsibility in maintaining GDPR compliance
- Buy-in from senior management to allocate the budget and resources to align the organization to GDPR compliance
- Senior management oversight of GDPR alignment project

Appointing a Data Protection Officer (DPO)

Under the GDPR, a DPO is a senior management leadership role responsible for overseeing data protection strategy monitoring compliance with GDPR requirements.

It should be noted that under the GDPR, there are a number of circumstances whereby you must appoint a DPO, namely:

- The organization is a public authority
- The core activities of the organization consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale
- The core activities of the organization consist of processing on a large scale of special categories of data or data related to criminal convictions

If your organization does not fall into one of these three categories, there is no obligation on the business to designate someone to this role.

Tasks of the DPO

1. Inform and advise organization and employees of obligations under GDPR
2. The DPO is the voice of data protection compliance within an organization
3. Monitor GDPR compliance for their organization
4. Interface with data subjects to inform them about how their data is being used, their rights to have their personal data erased, and what measures the company has put in place to protect their personal information
5. Training staff involved in safe data processing and data handling
6. Maintaining comprehensive records of all data processing activities conducted by the company
7. Data Privacy Impact Assessments
8. Liaison with supervisory authorities

The qualifications of the DPO will largely depend on the context of how information is processed within an organization. The GDPR is reasonably vague when it comes to the qualification requirements stating that, "The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices".

Outputs

- Dedicated resource for the management and reporting of GDPR compliance

Data discovery

An organization cannot truly begin to align to the GDPR until they understand their data. Without this, any project to align to GDPR runs a high risk of failure due to:

- Failure to identify all business process which collect or process personal data
- Failure to consistently protect personal data throughout the organization
- Failure to identify third parties where personal data is exchanged or processed
- Misallocation or waste of resources

Data discovery workshops are performed with business stakeholders to identify what business processes and associated data flows are within the organization and of these, which collect or process personal information.

Business stakeholders will walkthrough each of their processes and the data flows associated with them including:

- What data is collected and why it is needed
- Where it is stored
- How is it used
- Who does it get shared with
- How is it disposed of

As part of this walkthrough, the business will also identify what systems, applications, networks and assets support each of these business processes. This information will be documented as part of the workshop and the resultant information registers and data flow diagrams produced.

Outputs

This phase will essentially quantify the "scope" of an organization's exposure to GDPR. It will provide the organization with visibility of their business processes, information flows and what personal information they collect and process. Documents that will be created during this process may include:

- Information registers
- Data flow diagrams

From the summary alone, we can clearly see that once this exercise is performed, it is possible that an organization's exposure to GDPR requirements may be:

- Limited to a small number of business units which may require updated policies, processes and training
- Limited to a small number of third parties or partners where contract revisions and due diligence exercises need to be performed
- Limited to a small number of data repositories and devices where best practice security controls need to be designed and deployed

Recommended format for this exercise

- Workshop/Roundtable Exercise

Required staff

- Senior management for oversight
- Business unit leaders for overviews of the business function
- Business unit managers for detailed operational and day-to-day breakdowns of the information collected/processed
- IT to identify the systems and applications which process or store this data
- DPO/Privacy team for guidance

Call: +44 345 222 1711 /+353 1 210 1711 Email: cyber@bsigroup.com Visit: bsigroup.com

GDPR Gap analysis

Now that the scope of GDPR is understood and responsibility assigned, determining where the organization' current privacy posture is versus GDPR requirements. The most effective way to quantify this is to perform a gap analysis of the in-scope business processes, data flows and supporting assets versus GDPR requirements.

If performed correctly, the output of this exercise will determine which areas the organization is underperforming and identify any significant gaps. The true value of this exercise however, will be providing a risk prioritized roadmap. Through data discovery and accountability exercises, the scope of compliance is understood and accountability documented and agreed, the activities and projects required can be easily allocated and actioned to ensure timely resolution.

Outputs

- Quantification of the organization's GDPR posture
- Identification of GDPR gaps and deficiencies
- Prioritized roadmap of remediation activities to further align the organization to GDPR compliance

Recommended format for this exercise

- Onsite audit

Required staff

- DPO/Privacy team
- Business unit leaders
- HR
- Legal

Quick wins

Training

Training is key to the continued compliance of any organization to GDPR. "People" have long been considered the weakest link in the chain when it comes to IT security and this is no different with privacy. An organization can have all the required technical controls in place but will still result in non-compliance or breaches if the staff handling this information are not adequately trained.

Training will ensure that staff understand why personal data must be treated securely and arm staff with the opportunity to understand the organization's policies, processes and procedures in place to ensure this information is handled in line with GDPR requirements.

We recommend that the following is performed:

1. Annual staff awareness training is provided for all staff
2. GDPR requirements state that staff handling sensitive personal information are provided with specialized training tailored to the requirements of the role
3. Data protection and GDPR training is provided as part of the on-boarding process

In addition, we advise that a training log is kept as documented evidence to demonstrate that staff are regularly trained, should an incident, audit or inspection occur.

It is possible to meet this requirement through acquiring data privacy and GDPR training through an online training software solution or through engagement with a data protection and GDPR advisory firm.

Privacy champions

In addition to appointing a DPO, "privacy champions" can be nominated within the business units identified as in-scope for GDPR compliance. Privacy champions can maintain oversight of the business unit's day to day operations with regard to privacy and provide support to staff who have privacy concerns or queries and facilities the communication of any privacy concerns to the appropriate staff.

Contract review

Where data is shared with third parties, organizations need to ensure that appropriate security and privacy agreements are contractually agreed and enforced. Ideally, these contracts should include clauses to ensure that third parties are processing data in a safe and secure manner and permit you to perform audits and spot checks to ensure compliance.

In addition to security, there is a need to ensure that any third parties in scope understand the reasons for processing this information, verifying that processing is limited to this purpose and that documented procedures are in place to handle any privacy incidents or requests from data subjects. This is important as per GDPR, failure to process data subject requests is considered an issue of non-compliance and may open up an organization to audits or fines.

From the output of the data discovery exercise, a list of in-scope third parties and partners will be identified where contracts and agreements must be revised and updated to ensure that GDPR requirements are met and sufficient controls are in place to provide assurance of continual GDPR compliance.

Any third party reviews should verifying that:

- Contracts include clauses to ensure that third parties are processing data in a safe and secure manner and permit you to perform audits and spot checks to ensure compliance
- All applicable data protection requirements are mandated to all third parties
- Documented procedures are in place to address data protection non-compliance
- Documented procedures are in place to address data subject requests (subject access request, erasure, etc.) in a timely manner

Any gaps identified in this review should then be renegotiated and agreed with the in-scope third parties.

Data protection policy

An integral part of any GDPR project is producing appropriate documentation to demonstrate your compliance. As part of this, organizations will need to produce a data protection policy. Policies differ from procedures, as they are high-level documents that set principles, rather than details of how, what and when things should be done.

A data protection policy provides a valuable resource for everyone to understand the way in which data protection applies in their roles within the organization.

A GDPR complaint data protection policy should include:

- A general policy statement and acknowledgement of the importance attached to data protection compliance by the organization
- Outline the categories of personal data that the organization handles, including staff, customer and supplier personal data
- Describe the key data protection concepts, such as: data controller; data processor; data subject; personal data; sensitive personal data; and processing of personal data, to facilitate understanding of the policy
- Include a brief statement as to what the organization will do to comply, such as: putting in place adequate business compliance processes and procedures; providing staff awareness training; implementing technical and organizational data security measures; and ensuring that the organization has an appropriate legal basis for its data processing activities
- Specify who within the organization has overall responsibility for data protection compliance. Under the GDPR some organizations will need to appoint a data protection officer
- Acknowledge that data subjects of the personal data processed by the organization have rights to request access to their personal and requests must be responded to within 40 calendar days under the Data Protection Act. The GDPR reduces the timescale for responding to requests within one month
- Confirm the arrangements that the organization has in place with its third party service providers, including its professional advisers, marketing agencies and sponsors, within written agreements setting out parties' roles and responsibilities for data protection
- Provide high level details of the types of data security measures that the organization has in place

If a data protection policy is already in place, review the existing policy against the above points and ensure that the policy is updated to reflect these.

How BSI can help

Data protection implementation support

We'll work with your organization to develop a comprehensive understanding of the scope of your environment. This will include all flows of personal data and potential exposure to breaches or censure under the current regulation.

Once the scope has been defined and formally agreed, we establish the policies, procedures and lines of accountability necessary to meet regulatory demands.

Data protection and GDPR training

In addition to general awareness training we offer a number of detailed course offerings to arm DPOs and Privacy champions with the expertise to oversee and maintain GDPR compliance, these include:

- The Certified Information Privacy Professional Europe (CIPP/E) certification covers the pan-European and national data protection regulations as well as industry standard best practices for corporate compliance with these regulations. It is the first credential specific to european data protection professionals.
- The Certified Information Privacy Technologist (CIPT) credential imparts the necessary knowledge needed to build your organization's privacy structures from the ground up. With regulators worldwide calling for tech professionals to factor data privacy into their products and services, the need for privacy-trained IT pros has never been stronger.
- The Certified Information Privacy Manager (CIPM) is the worlds first and only certification in privacy program management and is a demonstrable measurement of privacy program administration. The CIPM training equips you with the skills on how to establish, maintain and manage a privacy programme across all stages of its lifecycle.

GDPR assessments

Our consultants can help you in identifying your data protection posture and establishing a prioritized roadmap to compliance. Our consultants provide:

- Workshops
- Awareness, Data Discovery and Accountability
- Questionnaire-based audits
- Onsite inspections
- Gap analysis

These services result in practical and policy-driven solutions in order to drive organizations to a positive audit outcome.

DPO as a service

Our outsourced DPO services enable organizations to implement a successful Data Protection programme so the business can continue to focus on its core activities. In addition to maintaining compliance, these services also deliver security, productivity, risk management and cost-efficiency benefits.

BSI Cybersecurity and Information Resilience

BSI Cybersecurity and Information Resilience helps you address your information challenges. We enable organizations to secure information, data and critical infrastructure from the changing threats that affect your people, processes and systems; strengthening your information governance and assuring resilience. Our cyber, information security and data management professionals are experts in:

Cybersecurity

Penetration testing, vulnerability management, incident response and cloud security services

Security awareness

Phishing and user awareness training, online solutions, social engineering and simulation testing

Information management and privacy

Information risk management, privacy, data protection, eDiscovery and forensics

Compliance and testing

PCI DSS services, Cyber Lab testing and product and software assessments (CC, CAS-T/CPA)

Our expertise is accredited by:

CREST

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR

CYBER ESSENTIALS

CREST STAR

CHECK IT Health Check Service

Find out more

UK

Call: +44 345 222 1711
Email: cyber@bsigroup.com
Visit: bsigroup.com

IE/International

+353 1 210 1711
cyber.ie@bsigroup.com
bsigroup.com

bsi.