...making excellence a habit.™

EU General Data Protection Regulation (GDPR)

20 steps to GDPR compliance – A methodical, systematic and logical approach

A whitepaper

Executive summary

The General Data Protection Regulation (GDPR) is set to replace the Data Protection Directive 95/46/EC in May 2018. While many organizations have already aligned processes and procedures with the Directive, the GDPR will enforce a number of new requirements on organizations that were not applicable in the past. With the fines for non-compliance with the GDPR being increased up to €20 million or 4% of global worldwide turnover, the price of non-compliance could be costly for your business. This whitepaper outlines 20 practical steps that you can take to ensure that your organization can adopt a defensible position and implement and maintain an effective GDPR compliance programme.

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 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

Rules evolve into principles

To meet the above aims, the current eight rules of data protection are evolving into a set of principles and subject access rights. However, although this appears to be a significant change, the fundamental intent of the requirements stays the same; effectively this is a structural or cosmetic change.

The following table highlights how the rules and principles relate to each other:

1. Obtain and process the information fairly
2. Keep it only for one or more specified and lawful purposes
3. Process it only in ways compatible with the purposes for which it was given to you initially
4. Keep it safe and secure
5. Keep it accurate and up-to-date
6. Ensure that it is adequate, relevant and not excessive
7. Retain it no longer than is necessary for the specified purpose or purposes
8. Give a a copy of his/her personal data to any individual on request

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

Rec.59; Art.12(2)

- Controllers have a **legal obligation to give effect to the rights of data subjects**

At a high level, the new principles and rights mandated by the GDPR can in effect be summarized as three high level “underlying principles”: Transparency, Clarity, and Accountability.

- **Transparency:** Being fully transparent about the data processing activities undertaken. Nothing should happen to data that the data subjects are not fully aware of
- **Clarity:** Being clear about what those data processing activities are. It is no longer acceptable to obscure the details of your processing using “legalese” or complex terminology. Information on data processing must be presented in clearly written, understandable plain language
- **Accountability:** It should be clear both within the organizational structures and to the data subjects themselves who is responsible for oversight and management of their data and enforcement of data subject rights

Compliance “now” vs Compliance under GDPR

With the above in mind, if organizations are currently broadly in compliance with the existing Data Protection Acts, it is not unfair to say that they should similarly be broadly compliant with the clarifications and new requirements of the GDPR.

However, conversely, if an organization has not taken its current and existing data protection obligations seriously to date then the effort required to become compliant in advance of May 2018 may be significant.

In either of the above cases, whether compliant with the existing acts or not, following the methodical and systematic approach suggested in this document will be of benefit to both categories of organizations.

20 steps to GDPR compliance – BSI approach

A sequential and prioritized approach – BSI suggest that the following steps should be followed sequentially from step 1 to step 20; in many cases the outputs from the early steps will be used as inputs to the later steps. For example, the information flows and information registers.

Grouping of the steps

BSI groups the suggested 20 steps into four complimentary categories, as follows:

- **Governance** (6 steps)
- **Technical** (4 steps)
- **Operational** (6 steps)
- **Communicative** (4 steps)

Considerations before you begin

Before completing the following 20 steps, BSI have made an assumption that you understand your organizations place in the GDPR ecosystem. Ensure that your organization clearly understands whether you are a data processor, data controller, or even both.

Further, it may be similarly useful to consider in advance what governance structures already exist within your organization. These can perhaps be utilized and leveraged to make compliance with the GDPR a more streamlined process.

Similarly, we assume some degree of governance already exists (i.e. establishment of a risk management framework for maintaining on-going assurance over the effectiveness of the compliance efforts, change management frameworks, project management frameworks, etc.). As such, these steps are designed to integrate with existing structures; for example, output from the suggested Privacy Impact Assessment steps (steps 13 and 14 below) could for example feed into existing Risk Management Committees, where the DPO would now have a seat.

Governance steps

Step 1:
Data Protection Officer (DPO)

The primary step is to appoint a DPO. In fact, most organizations will need to formally determine whether they have a mandatory requirement for appointing a DPO based on the processing that they undertake. Irrespective of whether the formal role is required, accountability for data protection and privacy should be formally allocated. For example, a large law firm does not necessarily need a "DPO" but would still require appointment of someone to be responsible for data protection.

This can be achieved by:

- Assigning the DPO role to an existing employee
- Hiring as a newly defined position
- Outsourcing the DPO role to a 3rd party DPO provider

Irrespective of the way this requirement is met, organizations have two obligations, which are to:

- Ensure that DPO meets all training and competency requirements
- Ensure that appointed DPO has no other operational conflicts of interest

Meeting those requirements will be challenging for many organizations due to the shortage of skills in the area, resulting in high pay demands for those with both certifications and on the job experience as a DPO. Similarly, the cost of outsourcing the DPO role is likely to be at a premium for the next 18 months.

Meeting the skills shortfall by training an existing staff member may also prove costly due to the risk of receiving bad advice from an inexperienced DPO, as well as the opportunity cost of that staff member in many cases no longer being able to continue their day to day activities should an operational conflict of interest be judged to exist.

Step 2:
Accountability

Accountability now must be clearly assigned, understood, and demonstrated for all data processing activities across an enterprise.

The best way to achieve this is to assign data ownership responsibility to business unit heads/representatives of those business areas where data is processed.

Luckily, most organizations will already understand who is accountable within each business unit, at least on an informal basis. The key aspect of this step will be ensuring that responsibility and accountability becomes enmeshed in the data owners' roles. This can be achieved by mandating the data owners be responsible for completing Data/Information Registers and Data/Information Flow diagrams (see step 3 and step 4).

Step 3:
Data/Information registers

The most important thing to remember when beginning a data protection programme is the maxim that "you can't protect what you don't understand". This begins the process of understanding your data.

A data register format and structure should be agreed upon and all personal data that the organization holds or processes should be recorded on that register.

The Data (or Information) register will need to detail at least:

- The names of systems which holds personal data
- How the data is classified
- Purpose for processing the data
- Legal basis for processing the data
- How long is data retained for
- Specific fields or types of data contained therein
- The data owner
- If data is shared with 3rd parties and who they are

As per step 2, this should be completed by the data owner and reviewed by the DPO on a "challenge" basis.

Step 4:
Data flow diagrams

As part of your organization's efforts to ensure you avoid the "you can't protect what you don't understand" pitfalls, it's important to ensure that stakeholders across the organization can obtain a clear, quick, and concise understanding of their data processing activities. The data registers created at step 3 will be of limited use to achieve this.

As a balance, a diagrammatic representation is typically the best way to achieve understanding on a direct basis.

For each data processing activity or business unit, a diagram showing the flow of information into and out of the organization should be produced.

Diagrams should include:

- Customer data details
- How and where data is received
- Where it is stored
- Where it is transferred to internally
- Name of the systems in which it is held
- Details of 3rd parties to whom the data may be transferred (include security measures such as encryption)
- How and when the data is scheduled to be destroyed

As per steps 2 and 3, this should be completed by the data owner and reviewed by the DPO on a "challenge" basis.

An additional real tangible benefit of these diagrams is to be able to determine quickly where data resides. This should facilitate an efficient delivery of Subject Access Requests and Right to Erasure Requests (see steps 9 and 10).

Step 5:
Adequacy and non-excessiveness of data

Now that you understand what data you have, you can consider the adequacy of the information and the extent of the information that you have collected.

On a "challenge" basis, review all data on information registers/data flows. In practice, this means reviewing all of the data and asking the questions: "Do we really need this?" and "Have we obtained this and are we using this fairly?"

If data is not absolutely required, delete and stop collecting it. The less data you maintain, then the smaller the effort involved in maintaining compliance on an ongoing basis.

Step 6:
3rd party suppliers and processors

Where data is shared with 3rd parties ensure appropriate security and privacy agreements are contractually agreed and enforced.

Ideally the contracts will include contractual clauses to ensure that 3rd parties are processing data in a safe and secure manner, in line with privacy regulations, and further permit you to perform audits and spot checks to ensure compliance.

It is also becoming common practice for controllers to ask for evidence that the processor is certified to or at least aligned to an information security standard such as ISO/IEC 27001.

Technical steps

Step 7:
Consent management

Wherever possible, the lawful basis on which you process data should not be solely consent based. However, BSI recognizes that this is not always possible.

As such, where consent is used as basis for processing personal data, there will be a number of requirements to ensure that compliance is achieved:

- Ensure that the consent currently held will meet the requirements under the GDPR; if not, re-obtain consent
- Ensure that all consents can be immediately demonstrated; if not, re-obtain consent and maintain a consent record
- Where sensitive data (i.e. medical data/health data/ insurance claim data, etc.), ensure that additional explicit consent has been obtained
- Ensure the process for removal of consent is clearly communicated at all points where data is collected and in a privacy notice
- Identify any data relating to under 18s; ensure consent from a guardian has been provided; if not, re-obtain consent

Step 8:
Data retention

As part of your new understanding obtained from the previous steps, the reasons for processing and the length of time data should be retained will now be understood. Now the process of enforcing that retention period can begin.

Review your data registers and data flow diagrams and where any data has passed agreed retention deadlines you must now securely remove it.

Step 9:
Data subject rights (governance)

A number of data subject rights have been clarified or introduced. These will require both governance and technical approaches to build compliant response processes.

First from a governance perspective, organization should agree and document governance policy and processes for responding to these requirements.

- Subject access requests
- Right to restriction of processing/objection
- Right to rectify
- Right to erasure
- Right not to be subject to automated decision making/ right to not be profiled
- Data portability

Step 10:
Data subject rights (technical)

Secondly, from a technical perspective, organizations should agree and document their technical approach to responding to the clarified and new requirements for invocations of data subject rights.

- Subject access requests
- Right to restriction of processing/objection
- Right to rectify
- Right to erasure
- Right not to be subject to automated decision making/ right to not be profiled
- Data portability

Operational steps

Step 11:
Data breach response

The GDPR introduces a new mandatory breach reporting requirement, whereby breaches must be reported to the relevant supervisory authority (and in turn affected data subjects) within 72 hours. This 72 hour window will prove challenging at the best of times; without a well understood and regularly tested data breach response process, organizations will almost certainly fall short of this obligation.

Organizations should agree and document their data breach/data security incident response process. This should be tested on a periodic basis to ensure that it remains fit for purpose in the event of a real life data breach event. Conducting a data breach simulation exercise, will identify gaps in the response process and ensure that the organization is in a ready state to respond to a breach effectively.

Step 12:
Keep data safe and secure

As part of your new understanding obtained from the previous steps, the data being processed and the parties the data is shared with will now be understood.

Review your data registers and data flow diagrams and where any data is received, shared or transferred review the security provisions in place. Where there may be any potential security concern, flag it for review and remedial action, if appropriate. Ideally, this can be done in conjunction with your internal information security function or your external security consultants.

This should be completed for all data sets and data flows diagrams that were produced (i.e. both data at rest and also data in transit).

Step 13:
Baseline Privacy Impact Assessment (PIA)

One of the new GDPR requirements is the idea of implementing "Privacy by Design and Default"; what was historically best practice has now become a legal mandate to complete.

To put this principle into practice, organizations are now required to complete Data Privacy Impact Assessments (DPIAs).

A DPIA is a process of reviewing data processing activities from a risk perspective. Effectively, it is a risk assessment specific to the nature of privacy risk to the data subjects whose information is being processed.

For this step, BSI suggests completing a baseline privacy impact assessment; all data currently being stored or processed should be reviewed to ensure that any potential privacy risk is identified and where concerns are noted that they are presented to management for review.

To be clear, completion of retroactive privacy impact assessment is NOT a specific legal requirement under GDPR...

BUT!

In the event of a data breach or complaint about non-compliance being upheld by a supervisory authority, if the vulnerability or process deficiency is one that would have been uncovered by completion of a retroactive privacy impact assessment, then the fine for such an occurrence would be expected to be significantly higher. In this regard, completion of a baseline PIA could be viewed as an insurance policy against such an occurrence.

Step 14:
Operational Privacy Impact Assessment (PIA)

A part of the new GDPR requirements for implementing "Privacy by Design and Default" is that privacy impact assessments must be carried out in the following two circumstances:

- New collection or processing of personal data
- New usage or purposes being introduced for personal data already in an organization's possession

Organizations should agree and document a consistent, systematic, and repeatable approach for ongoing privacy impact assessments when the above circumstances occur.

In BSI's experience, this can be best achieved by embedding gateways or triggers into other pre-existing processes, i.e.

- SDLC
- Project management
- Change management
- Procurement, etc

So for example, from a change management perspective we would suggest that a gateway question be added to the Change Request form which asks: "Will this change result in new collection of personal data or new usage of existing personal data?" Should the answer be yes, this will signal and invoke the PIA process.

Step 15:
Management engagement

Management oversight of data processing activities has always been best practice; under the GDPR it will now be a legal requirement. Those who sit at a management or board of director level will now be required to demonstrate engagement and understanding of data processing within their organizations.

To achieve that, the DPO should be allocated time to present on the organizations current data protection profile as a standing item at board meetings.

In order to properly engage with management and arm them with the understanding they now require, relevant information and key performance indicators should be agreed and presented to the management and board audience.

BSI suggests that the KPIs should include at least the following:

- Incidents
- Near misses
- Access requests
- Privacy risks to be monitored/Outputs from PIAs
- Data shared with 3rd parties and plans to monitor compliance

Step 16:
Maintenance of detailed processing records

As per article 30 of the GDPR, it is now a legal mandate for organizations to maintain detailed records of processing operations.

As per our earliest steps where data registers and data flow diagrams were produced, organizations following our sequence of suggested steps will already be meeting the fundamentals of this requirement. However, some additional records should also be maintained.

BSI suggests that records should include at least the following:

- Information register
- Data retention register
- Third party transfer register
- Subject access request register
- Right to erasure register
- Complaints register
- Third party register, etc

Communicative steps

Step 17:
Training

Understanding the importance of data protection has always been important to organizations. This remains the case. Under the GDPR it will now be a legal mandate to ensure that all staff receive training appropriate to their role within the organization.

In practice, this means that all staff should receive training on data protection practices within the organization, both at induction and on at least an annual basis. Further, should staff handle personal data as part of their day to day roles they will be expected to receive appropriate training on proper and secure data handling practices. This will often require tailored training specific to the jobs that they carry out.

Step 18:
Data protection policy

From an internal perspective the organization should redefine its current data protection policy to account for outputs of all the above processes.

The policy should highlight how it operationally meets the principles of the GDPR and provide guidance to staff on proper data protection practices.

Additionally, BSI suggests that to meet their transparency and clarity obligations that the organizations data protection policy should also act as an internal privacy notice to staff; the policy should clearly address the processing of personal data belonging to staff as part of their employment (i.e. what staff personal data is stored or processed and the reasons for doing so, how long it will be retained for, how to invoke their data subject rights, etc.).

Step 19:
Privacy notice

From an external perspective the organization should redefine its privacy notice to account for outputs of all the above processes.

The privacy notice should clearly explain to customers or other 3rd parties whose information you store or process exactly what the nature of the data processing carried out.

To meet transparency and clarity obligations the organizations privacy notice should be available (or at least referred to) at every point that data is collected. The notice should make it clear to all external stakeholders:

- This is the data we have
- This is why we have it
- This is what we do with it
- This is where we store it
- This is how long we'll hold it for
- This is how you can exercise your rights
- This is who it is shared with
- This is who you contact if you have a privacy query

Step 20:
Communication

Publish and distribute updated data protection policy and updated privacy notice to all appropriate stakeholders (internal and external).

All affected data subjects – internal and external - can now be considered informed of the data protection practise of the organization and how to invoke their data subject rights.

It should be noted that this degree of transparency is expected to result in increased engagement from data subjects; more subject access requests or right to erasure requests will likely be received, resulting in an increased administrative burden on organizations. This is very much by design of the GDPR. However, on the assumption that all of the previous steps suggested in this whitepaper have been adopted, organizations should have nothing to fear; response processes should be resilient and any potential disruption should be minimized.

Target market

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

- Recently appointed DPOs
- Human Resource Managers
- Sales and Marketing Managers
- Information Security professionals
- Compliance and Audit Managers
- Healthcare professionals
- Small business owners where those businesses process personal data
- Senior Management looking to understand the path to compliance

Conclusion

We understand the value of data to your business and the serious implications of a data breach. We help organizations to apply best practice in managing and maintaining compliance to EU data protection standards, while still retaining the ability to use data for the benefit of the business. 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. By following the above 20 steps, organizations will be positioned in compliance with the requirements as currently understood in advance of May 2018.

Cybersecurity and Information Resilience

BSI Cybersecurity and Information Resilience help you address your information challenges. We enable organizations to secure information, data and critical infrastructure from the changing threats that effect 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, SaaS solutions, social engineering and simulation testing

Data management and privacy

GDPR services, information lifecycle management and 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

UKAS TESTING 8237

Disclaimer
BSI is an accredited Certification Body for Management System Certification and Product certification. No BSI Group company may provide management system consultancy or product consultancy that could be in breach of accreditation requirements. Clients who have received any form of management system consultancy or product consultancy from any BSI Group company are unable to have BSI certification services within a 2 year period following completion of consultancy.

bsi.

Find out more
Call UK: +44 345 222 1711
Call IE: +353 1 210 1711
Email: cyber@bsigroup.com
Visit: bsigroup.com