

EU General Data Protection Regulation (GDPR)

Achieving compliance



GDPR - Key information

1. Introduction of significant fines

- Tier One: Up to €10 million or up to 2% of annual worldwide turnover of the parent company, the higher amount
- Tier Two: Up to €20 million or up to 4% of annual worldwide turnover of the parent company, the higher amount

2. The right to erasure

When an individual no longer wishes for their data to be processed and there are no legitimate grounds for retaining it, the data must be deleted. The onus will now be on data controllers to prove that they need to keep the data, not on the data subject (the individual).

3. The concept of consent has been revised to ensure transparency

Data subjects must be fully and specifically informed at the point of collection on all purposes for which data is used. Data subjects may now also remove their consent at any time, and for any reason.

4. Mandatory notification of a data breach

Organizations will now be required to report a data breach to their Supervisory Authority and to affected data subjects, within 72 hours of becoming aware of the breach.

5. Portability of data

The regulations propose the right that data subjects will be able to transfer their personal data in a commonly-used electronic format from one data controller to another without hindrance from the original controller.

6. Privacy by design

This is one of the fundamental ideas of the new regulation and one that aims to change the overall attitude and organizational planning towards Data Protection. Article 23 stipulates that Data Protection should be designed into the development of business processes.

7. Appointment of a Data Protection Officer (DPO)

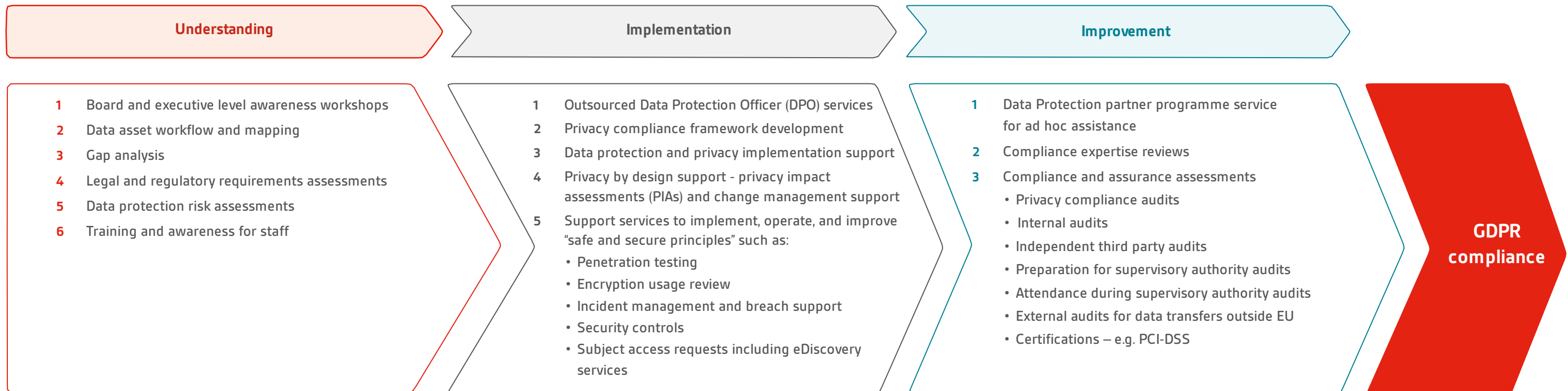
Organizations will now be required to appoint a DPO. The DPO must be independent and will report to the regulator and not the board of directors.



Achieving EU GDPR compliance

We have a range of services that can help you work towards GDPR compliance and continue to improve over time.

Did you know? BSI now have a standard (BS 10012) helping organizations demonstrate effective management of personal information, covering GDPR requirements. For more information visit [bsigroup.com](https://www.bsigroup.com)



← No matter where you are in meeting GDPR requirements, we can enable you to achieve compliance at each stage of the journey →



Data protection training courses

We provide a range of training courses in privacy and data protection. They focus on giving you the knowledge and skills to confidently build and manage data protection and privacy for your organization.

Certified Lead Implementer Professional (CLIP) for BS 10012:2017 Personal Information Management System including General Data Protection Regulations (GDPR) + ISO 27018

Five day course

Get Trained with our Certified Lead Implementer Professional Training Course to ensure your Personal Information Management Systems is as per BS 10012:2017. Also get your cloud services as per ISO 27018 & your organisation is GDPR compliant too.

By training with us you will gain an internationally recognized qualification that enables you to implement privacy management standards in your organization. You will also gain an in-depth knowledge and practice to plan, conduct, report and closing of Internal Personal Information Management System audit and continual improvement of the effectiveness of the Internal Audit Process. You will also take away sound knowledge of BS10012, ISO 27018 and global framework of GDPR.

What will you learn?

Upon completion of this training, delegates will be able to understand the key concepts and principles of privacy for protecting personal data and apply these concepts in practical business scenarios:

- Privacy concepts and PII categories, Privacy Principles, Privacy architecture based on ISO 29101, Phases of PII processing Lifecycle, Privacy Organization structure
- Requirements of BS 10012:2017 and GDPR to establish PIMS including Data inventory & data flow, Privacy Impact Assessments etc.
- Conduct a base line review of the organizations current position with regard to BS 10012:2017, ISO 27018, and GDPR.
- Integrate globally acceptable best practices with the present management system
- Complete the Certified Lead Implementer Professional BS10012:2017 and GDPR Certificate Exam

How will you benefit?

- An understanding of effective personal information management throughout an organization which protects the personally identifiable information (PII) within information and communication technology(ICT) systems.
- Understanding common privacy terminology and the common Privacy Principles
- Understand privacy safeguarding requirements
- Understanding and creating the Privacy architecture Framework throughout the PII processing Lifecycle
- Develop vital processes, policies and procedures that can be put into practice immediately including Privacy Impact Assessment, Risk Treatment, Data Inventory & Data Flow
- Create the framework for your own Personal Information Management System (PIMS)
- Gain knowledge to develop your PIMS framework and build awareness and support for privacy across your organization
- Gain the skills to plan, conduct, report and follow up an audit in accordance with ISO 19011
- Be confident that you have the capability to protect the personal information and meet stakeholder expectations
- Encourage continuous professional development across your organization

GDPR – enhancing data protection and privacy

The new EU General Data Protection Regulation (GDPR) will apply across all EU member states, with the official date for enforcement set for 25 May 2018. This reform has significant implications for business, not only for those based in the EU, but for all organizations operating within the EU market.

The new EU reform regulation aims to:

- **Reinforce** the rights of the individual – privacy by design and by default
- **Strengthen** the EU internal market through new, clear, and robust rules for the free movement of data
- **Ensure** consistent enforcement of these rules
- **Set** global data protection standards
- **Safeguard** a golden standard for data protection across all industries

Cybersecurity and Information Resilience

BSI 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



Our expertise is accredited by:



Find out more
Call: +91 11 2692 9000
Email: info.in@bsigroup.com
Visit: bsigroup.com