bsi.

...making excellence a habit.™

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

Understanding

1. Board and executive level awareness workshops
2. Data asset workflow and mapping
3. Gap analysis
4. Legal and regulatory requirements assessments
5. Data protection risk assessments
6. Training and awareness for staff

Implementation

1. Outsourced Data Protection Officer (DPO) services
2. Privacy compliance framework development
3. Data protection and privacy implementation support
4. Privacy by design support - privacy impact assessments (PIAs) and change management support
5. Support services to implement, operate, and improve "safe and secure principles" such as:
   - Penetration testing
   - Encryption usage review
   - Incident management and breach support
   - Security controls
   - Subject access requests including eDiscovery services

Improvement

1. Data Protection partner programme service for ad hoc assistance
2. Compliance expertise reviews
3. Compliance and assurance assessments
   - Privacy compliance audits
   - Internal audits
   - Independent third party audits
   - Preparation for supervisory authority audits
   - Attendance during supervisory authority audits
   - External audits for data transfers outside EU
   - Certifications – e.g. PCI-DSS

GDPR compliance

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

Call: **+852 3149 3300** Email: **hk@bsigroup.com** Visit: **bsigroup.com/en-HK**

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

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 EU General Data Protection Regulation (GDPR) foundation

One day course

In this one day course, our expert tutor will explain the requirements of the General Data Protection Regulation (GDPR), to help you understand how it could apply to your organization and the benefits of adopting it.

This is a foundation, non-technical course for both technical and general management interested in learning about GDPR and achieving compliance with the regulation.

How does the EU GDPR foundation course help:

You will gain knowledge on how to adhere to the new regulation and kick-start compliance with a variety of activities, such as a personal data scoping exercise and gap analysis, a privacy impact and risk assessment, or a full data protection audit.

Certified Information Privacy Professional/Europe (CIPP/E)

Two day course

The CIPP/E covers the fundamental pan-European and national data protection laws. It is the most recognized credential of its kind in the data protection and privacy field.

The course examines industry best practices in privacy compliance concepts of data protection and trans-border data flows. The CIPP/E covers critical topics like the EU-U.S. Privacy Shield and the GDPR.

How does CIPP/E help with GDPR requirements:

Achieving the CIPP/E demonstrates you have the comprehensive GDPR knowledge and understanding to ensure compliance and data protection success.

Certified Information Privacy Manager (CIPM)

Two day course

The CIPM certification is the "how-to" in day-to-day privacy operations. A CIPM will help you to structure an organizations' privacy team effectively. It equips you with the ability to develop, implement, and measure a privacy program framework while utilizing the privacy operational lifecycle: access, protect, sustain, and respond.

How does CIPM help with GDPR requirements:

A CIPP/E combined with a CIPM means that you are uniquely equipped to fulfill the requirements of a Data Protection Officer.

Certified Information Privacy Technologist (CIPT)

Two day course

CIPT certifies delegates in the knowledge of privacy and data protection related issues, in the context of design and implementation of information and communication technologies. It looks at the privacy considerations for IT systems and applications. It examines industry standard guidelines for the collection, use, retention, and destruction of data.

CIPT provides a solid foundational level in data protection and privacy laws, concepts and regulations, while giving delegates the knowledge to create their information privacy infrastructure.

How does CIPT help with GDPR requirements:

CIPT will enable you to build your organization's privacy and data protection infrastructure, ensuring 'privacy by design', a key GDPR value.

Call: **+852 3149 3300** Email: **hk@bsigroup.com** Visit: **bsigroup.com/en-HK**

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

Find out more

Call: +852 3149 3300

Email: hk@bsigroup.com

Visit: bsigroup.com/en-HK

bsi.