The Role of the Data Protection Officer – Is Your Organisation DPO Ready?

Stephen Scott

Senior Manager, Information Governance

UK Superbrands 2017

INVESTORS IN PEOPLE

By Royal Charter

Through the passion and expertise of our people, BSI embeds excellence in organizations across the globe to improve business performance and resilience.

Cybersecurity and Information Resilience – what we do

We 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.

bsi.

What do we do?

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

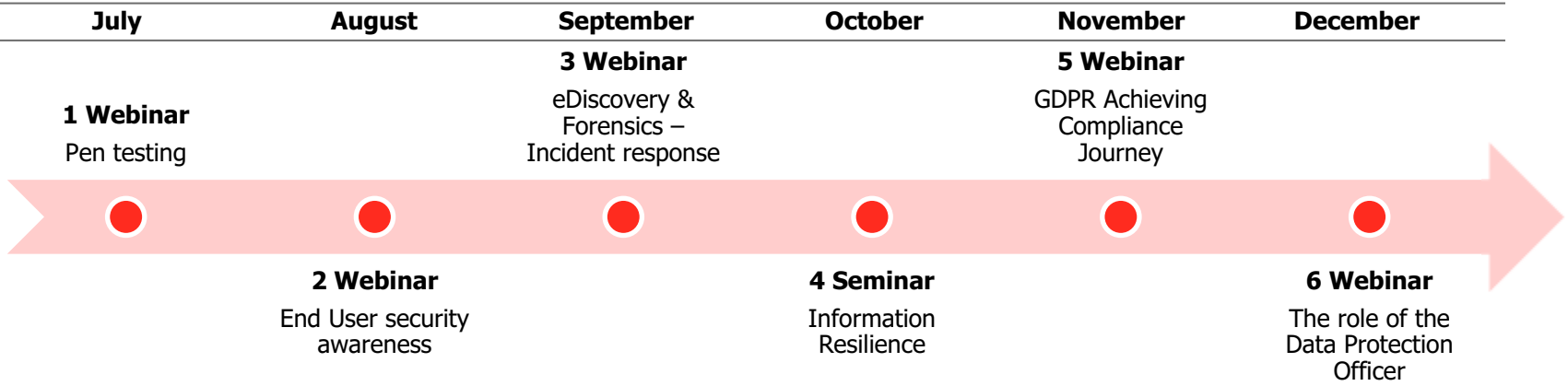
GDPR services, information lifecycle management and eDiscovery and forensics

Compliance and testing

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

bsi.

Path to GDPR – Cybersecurity and Information Resilience Services

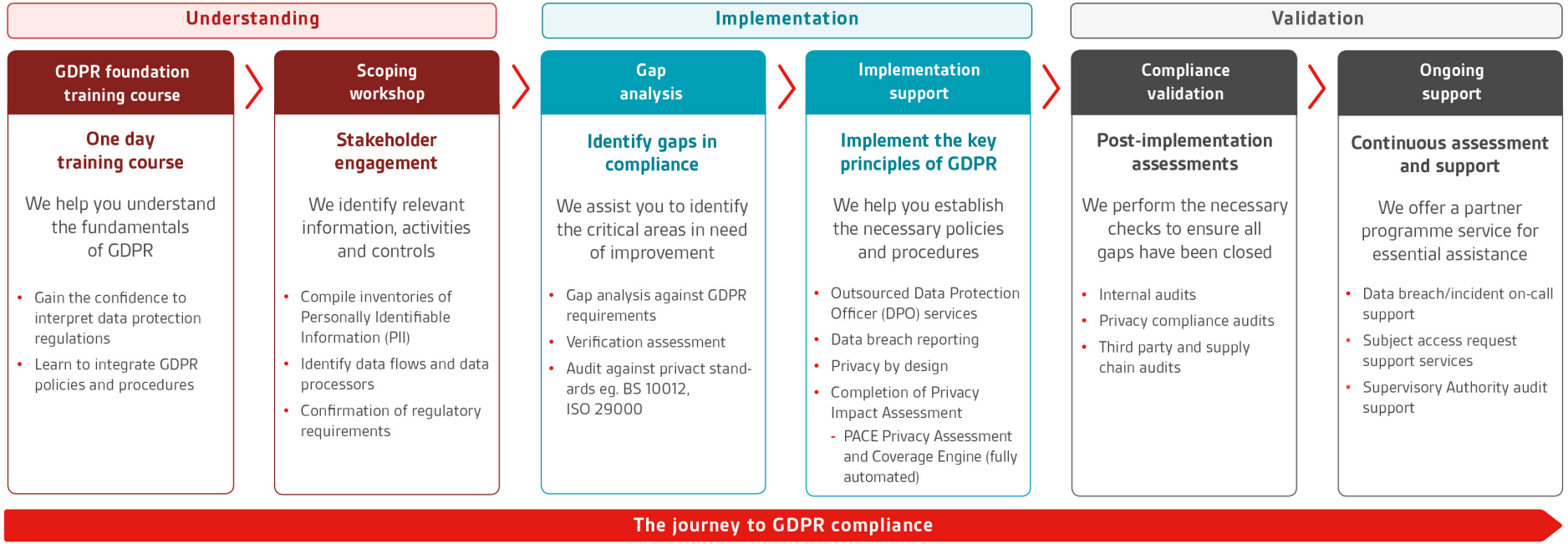


Webinar Series:

1. **Penetration Testing (Jul17) –** ensuring an organization's customer and prospect data is secure
2. **End User Security Awareness (Aug17)** – Untrained employees - the weakest link in your cybersecurity defence
3. **Incident Response (Sept17) –** You have 72 hours to respond after a breach... was personal data compromised?
4. **Information Resilience Series Event (Oct17)** – Manchester 17th October 2017
5. **GDPR Achieving Compliance Journey (Nov17)** – a step-by-step methodology for achieving compliance
6. **GDPR – the role of the Data Protection Officer (Dec17)** – Is your organization's DPO ready?

bsi.

BSI GDPR Compliance Professional Services



General Data Protection Regulation in 1 Minute

- Aims to **protect** the personal data of EU citizens
- Puts individuals back in **control** of their personal data
- Applies to all EU member states, any organization who operates within the EU market, or who holds information on EU data subjects
- Requirement to **report** a data breach to the data protection commissioner, within 72 hours of becoming aware of any breach
- **Fines** of up to €20 million or up to 4% of annual worldwide turnover for non-compliance
- Comes into force on the **25th May 2018**
- Data Protection Officer (DPO) appointment
- No opt out for UK with **Brexit**

Webinar Objectives

- Gain an understanding of what a DPO is;
- Understand what the GDPR stipulates about the role;
- Help you identify whether you need a DPO or not; and
- Have enough information to bring back to your organisations to further the conversation.

What is a Data Protection Officer (DPO)?

What is a DPO?

Under the GDPR

- A data protection officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR). Data protection officers are **responsible for overseeing** data protection strategy and implementation to ensure compliance with GDPR requirements

Qualifications

- The GDPR does not include a specific list of DPO credentials, but Article 37 does require a data protection officer to have "**expert knowledge of data protection law and practices**." The Regulation also specifies the DPO's expertise should align with the organization's data processing operations and the level of data protection required for the personal data processed by data controllers and data processors.

Lines of Defence – Where does the DPO Fit In?

Tasks & Required Expertise of the DPO?

Tasks of the DPO (Article 39)

Compliance

- **Inform and advise** organisation and employees of obligations under GDPR
- The DPO is **the voice** of data protection compliance within an organization
- **Monitor** GDPR compliance for their organisation
- **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
- **Training** staff involved in safe data processing and data handling
- Maintaining **comprehensive records** of all data processing activities conducted by the company

Tasks of the DPO (Article 39)

Data Protection Impact Assessments (DPIAs)

- Monitoring performance

- **Providing advice** on the impact of data protection efforts **upon request [Article 35]**

Tasks of the DPO (Article 39)

Liaison with Supervisory Authorities

- Act as the contact point for the supervisory authority on issues relating to processing, and to consult, where appropriate, with regard to any other relevant matter.
- Cooperation with supervisory authority upon request (audit, complaint, information on processing activities
- Data Breach reporting (discussed in more detail later)

Personal Responsibility of the DPO? (Article 24)

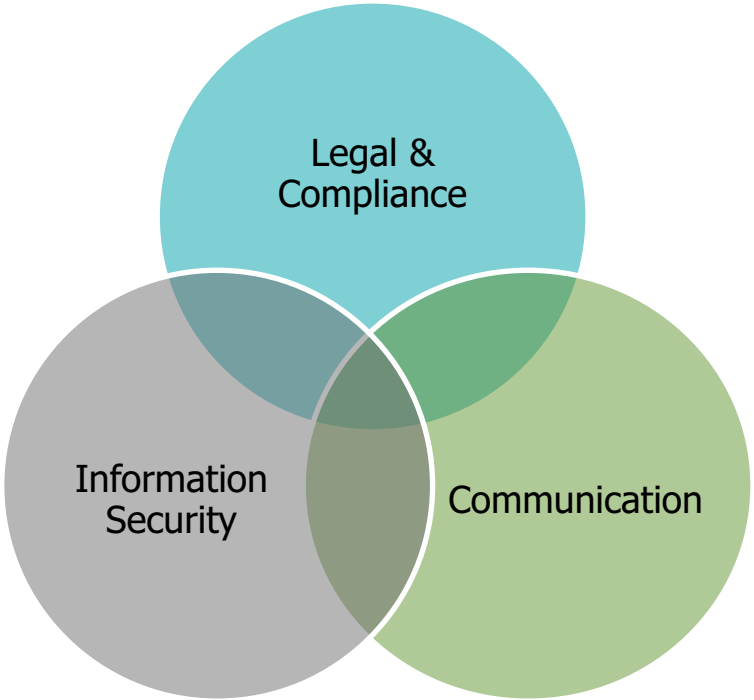
Article 24 - "Responsibility of the controller"

- As stated in Article 24, responsibility for compliance lies with the Senior Management within a controller or the processor

- The DPO **is not** personally responsible for non-compliance with the Regulation

Expertise and Skills of a DPO (Article 37)

Overlap of Disciplines



Expertise and Skills of a DPO (Article 37)

- Expertise in national and European data protection laws and practices;
  - An in-depth understanding of the GDPR;
- Sufficient understanding of the processing operations carried out by the controller
- Expertise in Privacy and Information Governance structures
  - Policies, procedures
  - Reporting
  - Frameworks

Expertise and Skills of a DPO (Article 37)

- In-depth understanding of information security and data protection needs of the controller
- Information Security Auditing
- Understanding of data breach response and Digital forensics skills, which are key to effective incident management
- Understanding of security controls
- Knowledge of available technical solutions like e.g. Data Leakage Prevention systems, which may help in protecting personal data

Expertise and Skills of a DPO (Article 37)

- Sufficient understanding of the processing operations carried out by the controller
- Training and communication throughout the organisation
  - Upward
  - Downward
- Personal availability – either physically or electronically

Key Role of the DPO – Data Breach Reporting

DPO – Data Breach Reporting

"**Data Breach incident**" means any real or suspected event that may involve the loss or disclosure of personal or sensitive personal data.

Examples include:

- Unauthorized access to data, especially confidential data like a person's name and address
- Loss of a device which includes personal information
- Security breach incident where personal data may have been accessed
- Verbal disclosure to an unauthorised party
- Email with personal information being sent to the wrong destination
- etc.

DPO – Data Breach Reporting

- Data controllers must notify most data breaches to the **Data Protection Authority** (DPA)
- "Where feasible" **no later than 72 hours** after the breach
- A **reasoned** justification must be provided if this timeframe is not met

DPO – Data Breach Reporting

Exemptions:

- Notification does not need to be made to the DPA if the breach is **unlikely to result in a risk** to the rights and freedoms of individuals
- The threshold for notification to data subjects is that there is likely to be a "high risk" to their rights and freedoms
- So for example, if encryption has been applied, no risk presents itself

DPO – Data Breach Reporting

What does a notification look like?

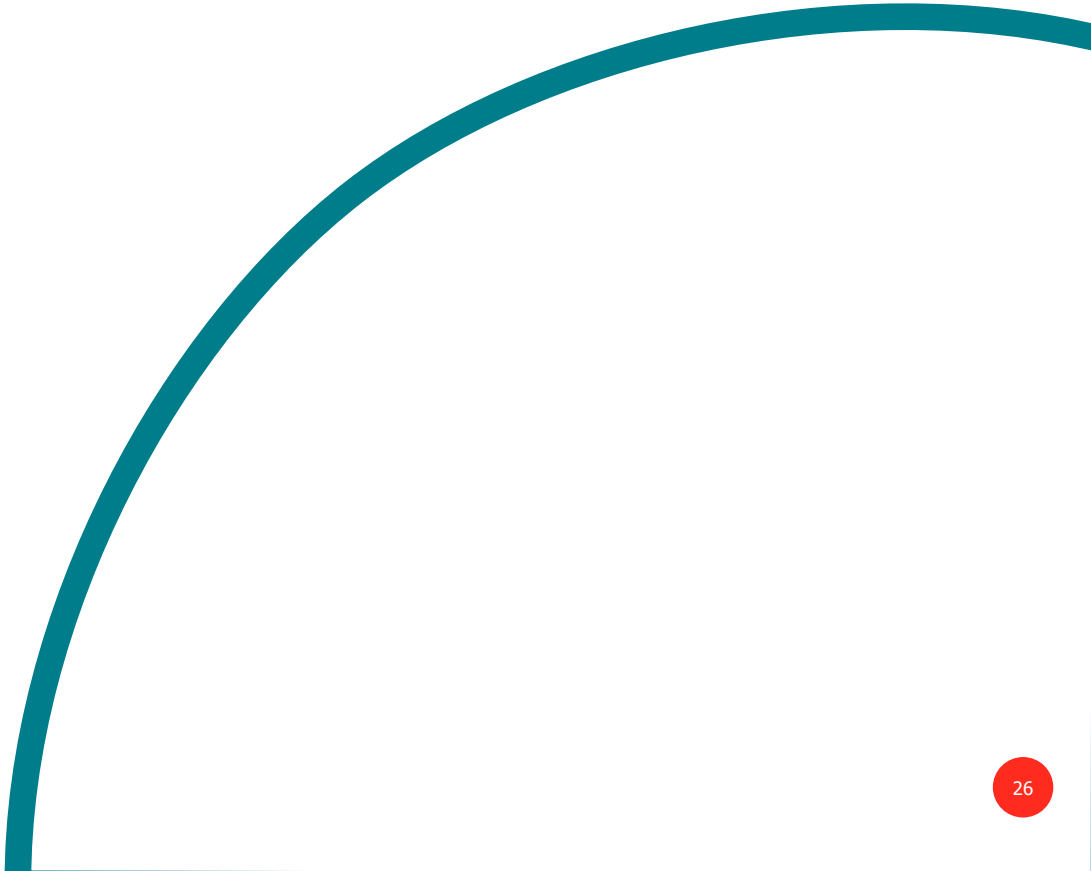
- Notification must include:
  - Categories and approximate numbers of individuals and records concerned
  - The name of the organisation's Data Protection Officer
  - Consequences of the breach
  - Measures to mitigate the harm

DPO – Data Breach Reporting

- But how do we classify the incident?

- How can we evaluate the incident and identify the people and data involved quickly?

Who needs a DPO?



Do You Need a DPO?

- A DPO must be designated where::
  - The processing is carried out by a **public authority or body**, except for courts acting in their judicial capacity;
  - The organisations **core activities** involve "regular and systematic monitoring of data subjects on a large scale
  - The organisations **core activities** of the controller or the processor consist of processing on a large scale of special categories of data, and personal data relating to criminal convictions and offences

- **What's "LARGE SCALE"??**
- **What's Regular and Systematic Monitoring??**

- Also think about single DPO for a group (Article 37)
  - A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

Do You Need a DPO?

Alternative Option

- Where the organisation decides that they don't need a DPO, it may be advisable to have a person who "is responsible for Data Protection".

Cant be dismissed:

- He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks.

- The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

Who Can Be A DPO?

Conflict of Interests… (Article 38)

- The DPO may not hold a position within the organisation that allows them to determine the purposes and means of processing of personal information
- The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks referred to in Article 39

- Conflicting positions may include:
  - Senior Management
  - Heads of department heavily involved in the processing of personal data (IT, Operations, HR, etc.)

DPO Options

What are the options?

- Employ a new staff member with appropriate level of experience and qualifications
  - Fixed term contractor
  - Full time staff member
- Transition an existing staff member from their current role
- Utilise the services of a third party service provider

Governance Options for Medium to Large Companies

- Level 1 – Front Line Staff / Line Management
- Level 2 – Record / Local Data Officers
- Level 3 – DPO or Allocated Responsible Person

Quarterly meetings with Record / Local Data Officers should take place to drive continual compliance.

The Bad News

No one element will solve your problems

For compliance, you will need…

- Privacy Governance
- Defensible Position
- Structure Methodical Approach
- Specialist software
- Broad range of Experience
- Legal advice

The Good News

BSI Cybersecurity and Information Resilience consultants provide:

- GDPR Project Management ✓
- Specialist Consultancy Advice ✓
- Implementation Support ✓
- Specialist Software ✓
- DPIA and Policy Development ✓
- Experience with Supervisory Authorities ✓

BSI Services – Outsourced DPO

DPO-as-a-Service

- Data protection implementation support
- Data Protection Officer (DPO) services (onsite and/or virtual)

  BSI's outsourced **Data Protection Officer 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.
- Data protection / privacy impact assessments
- Data protection training
- Data protection audit support (internal and/or external)

BSI – Where we've worked

BSI can tailor solutions to businesses of all sizes and capabilities:

- Utilities
- Credit Unions
- Pensions
- Legal
- Technology
- Government
- Retail
- Transport

How to Select a DPO Training Programme

The Data Protection Commissioner recommends that the following non-exhaustive list of factors be taken into consideration when selecting the appropriate DPO training programme:

- the content and means of the training and assessment;
- whether training leading to certification is required;
- the standing of the accrediting body; and
- whether the training and certification is recognised internationally.

Source: https://www.dataprotection.ie/docs/14-8-2017-Guidance-on-qualifications-for-DPOs-(GDPR)/1643.htm

BSI GDPR Training Services

GDPR Training Courses

1. GDPR Foundations
2. Certified Information Privacy Professional EU (CIPP/E)
3. Certified Information Privacy Manager (CIPM)
4. Certified Information Privacy Technologist (CIPT)

1. Training – GDPR Foundation Course

- Our one-day foundation training course to the General Data Protection Regulation (GDPR) will help you understand how it could apply to your organization and the potential benefits.
- By attending this course you will be better prepared to carry out a discussion around the new regulation, conform to the parameters, as well as understand the background, updated concepts, principles, terms and definitions used in the new GDPR.

2. Training – CIPP/E

- Get global recognition as a data protection professional with our Certified Information Privacy Professional Europe (CIPP/E) course.
- This 2 day training course encompasses pan-European and national data protection laws, key data protection terminology and practical concepts concerning the protection of personal data and trans-border data flows.

3. Training – CIPM

- The Certified Information Privacy Manager (CIPM) is the world's first and only certification in privacy programme management.
- When you earn a CIPM, it shows that you know how to make a privacy programme work for your organization. In other words, you're the go-to person for day-to-day operations when it comes to data protection.

4. Training – CIPT

- The Certified Information Privacy Technologist (CIPT) is the first and only certification of its kind worldwide.
- It was launched by the International Association of Privacy Professionals (IAPP) in 2014 to meet the growing need that only tech pros can fill - securing data privacy at all stages of IT product and service lifecycles.

Questions?

Stephen Scott
Senior Manager| BSI Cybersecurity & Information Resilience
E: cyber.ie@bsigroup.com
T: +353 1 210 1711

UK Superbrands 2017

INVESTORS IN PEOPLE

By Royal Charter

Get in touch

UK

Phone: 00 44 345 222 1711

Email: cyber@bsigroup.com

Global

Phone: 00 353 1 210 1711

Email: cyber.ie@bsigroup.com