EU General Data Protection Regulation (GDPR)

DPO as a Service

A whitepaper

bsi.

...making excellence a habit™

Introduction

"Information resilience empowers organizations to safeguard its information – physical, digital and intellectual property – throughout its lifecycle from source to destruction. This requires the adoption of security-minded practices enabling stakeholders to gather, store, access and use information securely and effectively."

Michael Bailey, EMEA Director of Professional Services, BSI Cybersecurity and Information Resilience

To achieve a state of information resilience, organizations must address four interconnecting sub-domains:

1. Cybersecurity 2. Information management and privacy

3. Security awareness and training 4. Compliance to requirements

This whitepaper discusses the challenges faced by organizations in complying with their obligations under the General Data Protection Regulation (GDPR) and explores possible solutions such as appointing an outsourced Data Protection Officer (DPO) or Privacy Officer.

This paper focuses on the typical activities that should be undertaken by a DPO to meet GDPR compliance and also includes recommendations and best practices. Information is provided on some of the common pitfalls and problems that organizations face with appointing someone into a new regulated role.

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

GDPR – The appointment of a Data Protection Officer (DPO)

The GDPR came into full force on 25 May 2018 and one of its noteworthy requirements is the mandatory appointment of a Data Protection Officer where your organization meets any of the following criteria (under Article 37):

- you are a public authority or body processing and controlling personal data
- you are a data controller or processor whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale
- your core activities (as a controller or processor) consist of processing on a large scale of special categories of data

Determining whether or not you need to appoint a DPO depends on the scope and scale of your data processing. However, even if your organization is not obligated to do so, appointing a DPO or a Privacy Officer demonstrates management's commitment to enshrine Data Protection compliance as a central tenet of your organization's values.

Appointing a DPO is a positive commitment to upholding the privacy rights of data subjects such as your employees, customers and others. You must ensure that your organization has sufficient staff and resources to discharge your obligations under the GDPR.

Any failure in meeting the obligations could result in potentially significant supervisory authority fines, but as important is the potential for reputational damage to the business and to the trust relationship with customers.

DPOs are not personally responsible in cases of non-compliance with the GDPR. The Regulation makes it clear that the burden of data protection compliance falls squarely at the door of senior management. Data protection compliance is a responsibility of the controller or the processor.

Meeting GDPR compliance obligations truly challenges organizations to find cost-effective, practical and pragmatic responses that help reduce the compliance burden while ensuring expert advice and support is available. The DPO is a keystone for accountability and appointing a DPO (even when not expressly mandated) facilitates compliance and enables a competitive advantage.

Compliance challenges

A robust privacy programme is required to address numerous operational privacy and data protection issues if an organization is to be in compliance with its obligations under the GDPR.

The aim of the GDPR (and what supervisory authorities have indicated they expect to see) is for organizations to implement a formal data protection or privacy programme that addresses issues on the basis of risk.

The challenge presented to organizations with having a privacy programme that adequately addresses GDPR's compliance demands can be understood fully when you review Articles 37 to 39 of the Regulation:

- **Article 37**[1] requires the DPO to have "expert knowledge of data protection law and practices", to ensure they are able to fulfil their tasks as detailed in Article 39
- **Article 38**[2] gives clear advice in terms of the independence of the DPO in performing their duties and the obligations of senior management to provide adequate resources to support them
- **Article 39**[3] expressly outlines the tasks that the DPO is expected to undertake and deliver, adopting an appropriate risk-based approach

1 Article 37, GDPR https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
2 Article 38, GDPR https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
3 Article 39, GDPR https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Who is the DPO?

A DPO is effectively senior management's independent and trusted data protection adviser. The DPO should be involved, properly and in a timely manner, in all issues which relate to the protection of personal data; therefore, they are a critical cog in the data protection compliance programme.

A DPO must not only have expert knowledge of data protection laws and operational practices but in order to sufficiently discharge their duties as envisaged by the regulation, the DPO must be a true privacy advocate.

The role of the DPO demands a combination or multiple and differing skillsets, which traditionally organization are unlikely to find in an existing single internal resource and may find difficult locate in any single person.

The skills required by a successful DPO include:

- risk management
- audit
- compliance
- expert knowledge and interest in privacy legislation
- understanding of normal business processes (e.g. change management, procurement, project management, vendor and contract management; business development, recruitment, marketing, etc.)
- information security and IT operations.

Sufficient resources must be made available to the DPO for them to carry out their statutory duties as mandated by the GDPR. Establishing a supporting team of professionals or utilizing an outsourced or co-sourced resourcing model is an efficient way to ensure these resources are accessible when require.

Where does the DPO sit in the organization?

Article 38 of the GDPR outlines that the DPO is an independent function that reports directly to the highest level of management.

Accordingly, and in order to be able to deliver upon the mandate of being management's independent data protection adviser, the DPO must be free of any actual or perceived conflicts of interest. While the GDPR expressly permits the DPO to hold other positions within an organization, these activities must not create or appear to create any conflict with the independence of the DPO.

Internal appointments of the CISO, ISO, IT manager, ITSO, Head of Audit, Head of Compliance, etc. could create actual or perceived conflicts with the duties of the DPO.

The European Data Protection Supervisor's guidelines[4] for ensuring an independent DPO are a useful reference point when considering where the role sits, its authority and reporting line:

To avoid conflict, it is recommended that:

- a DPO should not also be a controller of processing activities (for example if they are Head of Human Resources)
- the DPO should not be an employee on a short or fixed term contract
- the DPO should directly report to the organization's highest management level, and not a direct supervisor
- a DPO should have responsibility for managing their own budget to ensure independence

4 https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

Tasks and activities of the DPO

The regulation clearly establishes the remit of the DPO's role within the controller or processor, including:[5]

- to inform and advise the business and employees of their data protection obligations
- to monitor compliance with the GDPR, other Union or Member State legislation and with the organization's policies, including
  - the assignment of responsibilities
  - awareness-raising
  - training of staff
  - related audits
- to advise, where requested, regarding Data Protection Impact Assessments (DPIAs) and monitor their performance
- to cooperate and consult (where required) with the supervisory authority
- to adopt a risk-based approach taking into account the nature, scope, context and purposes of processing

This broad remit includes both reactive and proactive approaches to compliance, for example:

- advising on the applicability of data subject rights in response to data subject requests
- advising on requirements for DPIAs
- monitoring compliance through regular compliance reviews, security audits, third party reviews
- proactively training staff and management
- responding to and advising management in data breaches or
- liaising with and responding to supervisory authority requests

5 Article 39, GDPR https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Appointing the DPO

Many organizations struggle to justify the expense of employing a designated person with responsibility for data privacy on a full-time basis. Indeed, allocating the DPO role to an internal employee can be short-sighted and ineffective as it may:

- over burden an already busy employee who has not the necessary time needed to attend to the demands of privacy in addition to the demands of their "day" job
- be allocated to someone who doesn't have the necessary data protection expertise and experience
- not sufficiently address the independence requirements of the role resulting in a conflict of interest

GDPR recognizes that many organizations will be challenged in appointing an internal DPO, especially with regard to sufficiently meeting the expertise and independence requirements of the role. Therefore, the Regulation expressly provides that controllers and processors can outsource the appointment on the basis of a service contract[6].

Procuring external support (such as fully outsourced DPO, co-sourced DPO or additional support on demand) is an effective and practical solution for many organizations that helps:

- **Meet** the independence requirements for the DPO role without compromise
- **Reduce** the overhead costs associated with employing an internal DPO
- **Eliminate** the key person dependency risks associated with an internal DPO
- **Quickly access** specialized, skilled and experienced advisory in the event of a personal data breach

Procuring outsourced support brings the benefits of flexibility, scalability and access on demand to multi-disciplinary expertise.

Readily available access to independent, professionally qualified and expert professionals enables management to concentrate on their core business activities.

Example of tasks performed by an outsourced DPO

The external or outsourced DPO will perform a similar role to an internally appointed DPO and this will be governed through the use of a service contract with a clearly defined scope of DPO services.

Management will typically agree the support needed and, following a risk assessment to ensure that a risk-based approach to activities is maintained, the external DPO's services can include the following (this list is indicative and non-exhaustive):

- oversee the development and maintenance of a centralized data register for all data held and processed by an organization (Article 30 obligation)
- having a complete overview, the DPO will challenge data owners under the principles of "lawfulness, accuracy, minimization, purpose, security and limitation"
- advise management, when requested, on the necessity of performing a DPIA or LIA (Legitimate Interest Assessment)
- advise on mitigating measures that can be implemented to protect personal data: for example, anonymization
- advise on transfer mechanisms needed to be in place for any data being transferred outside the EEA in compliance with the GDPR
- review and advise on policies, processes and procedures related to the processing of personal data
- assist in the development and advise of the execution of subject access request procedures
- act as a single point of contact for data subjects, employees and management for data protection matters
- provide or oversee data protection awareness and training
- assist and advise the organization in responding to a data breach
- act as the liaison for the supervisory authority
- provide regular updates, reporting directly to senior management

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.

6 Article 37, GDPR https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Conclusion

The GDPR represents a significant challenge for organizations to operationalize data protection compliance. Further global developments in privacy mean that the demand for compliance will only intensify. Ever increasing consumer expectations and awareness of regulations, along with regulatory enforcement will drive organizations to ensure they have sufficient resources and expertise to cope.

Controllers and processors must fulfil clear legal obligations. Failure to do so could result in significant damage including:

- supervisory authority fines
- long-term reputational damage
- increased civil action from affected customers or citizens

The appointment of a DPO is not a mandatory requirement for all organizations. However, appointing a specialist external firm to provide DPO or Privacy Officer services allows an organization to concentrate on its core business, ensuring that expert advice is available when needed. The DPO is a keystone of data protection accountability. Appointing a DPO (even when not expressly mandated) can help compliance and enable a competitive advantage.

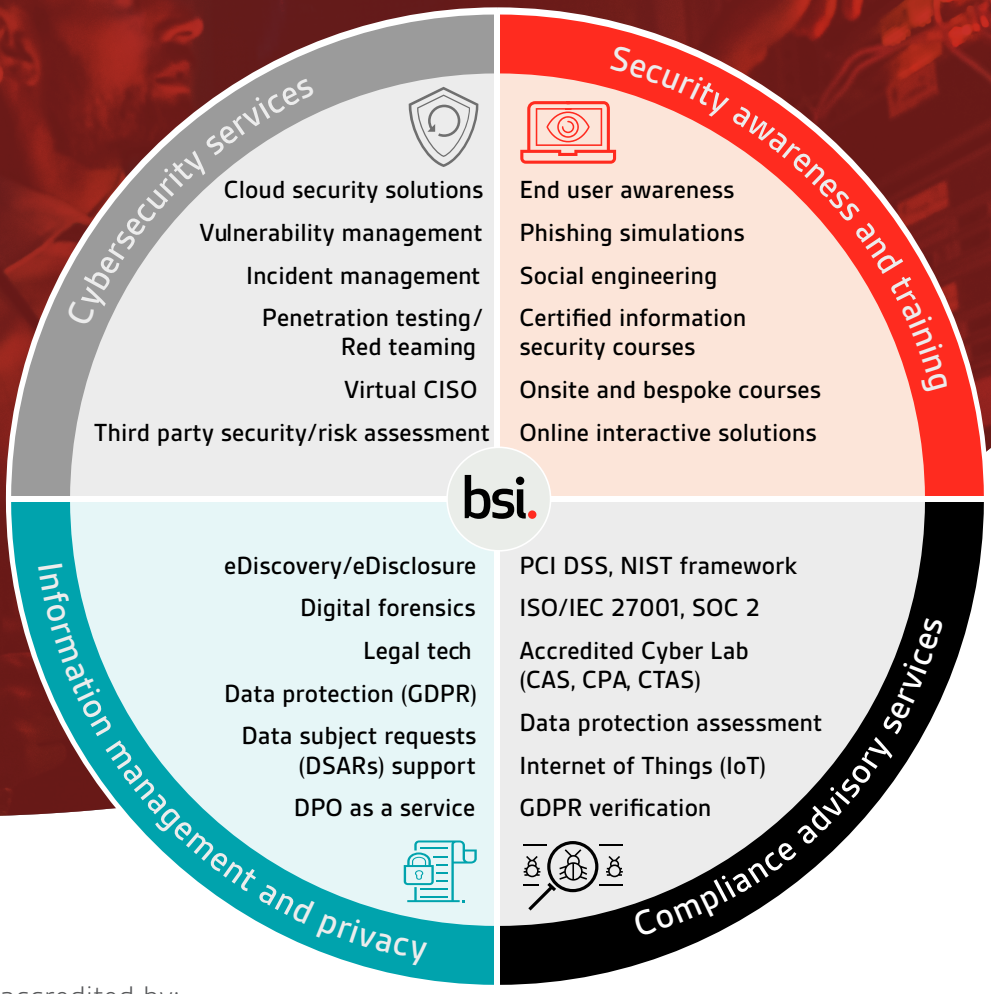
BSI aims to provide clients with the assurance that their GDPR obligations are being actively addressed in a pro-active, risk-based manner.

Our qualified, experienced and expert data protection consultants can support your organization in meeting its Data Protection Officer needs. BSI can help you transform the regulatory constraints of GDPR from mere compliance into a differentiating competitive advantage.

BSI Cybersecurity and Information Resilience

Protecting your information, people and reputation

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:



Our expertise is accredited by:

CREST

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR™

CYBER ESSENTIALS

CREST STAR

CHECK IT Health Check Service

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

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

Copyright © 2018 The British Standards Institution. All Rights Reserved.