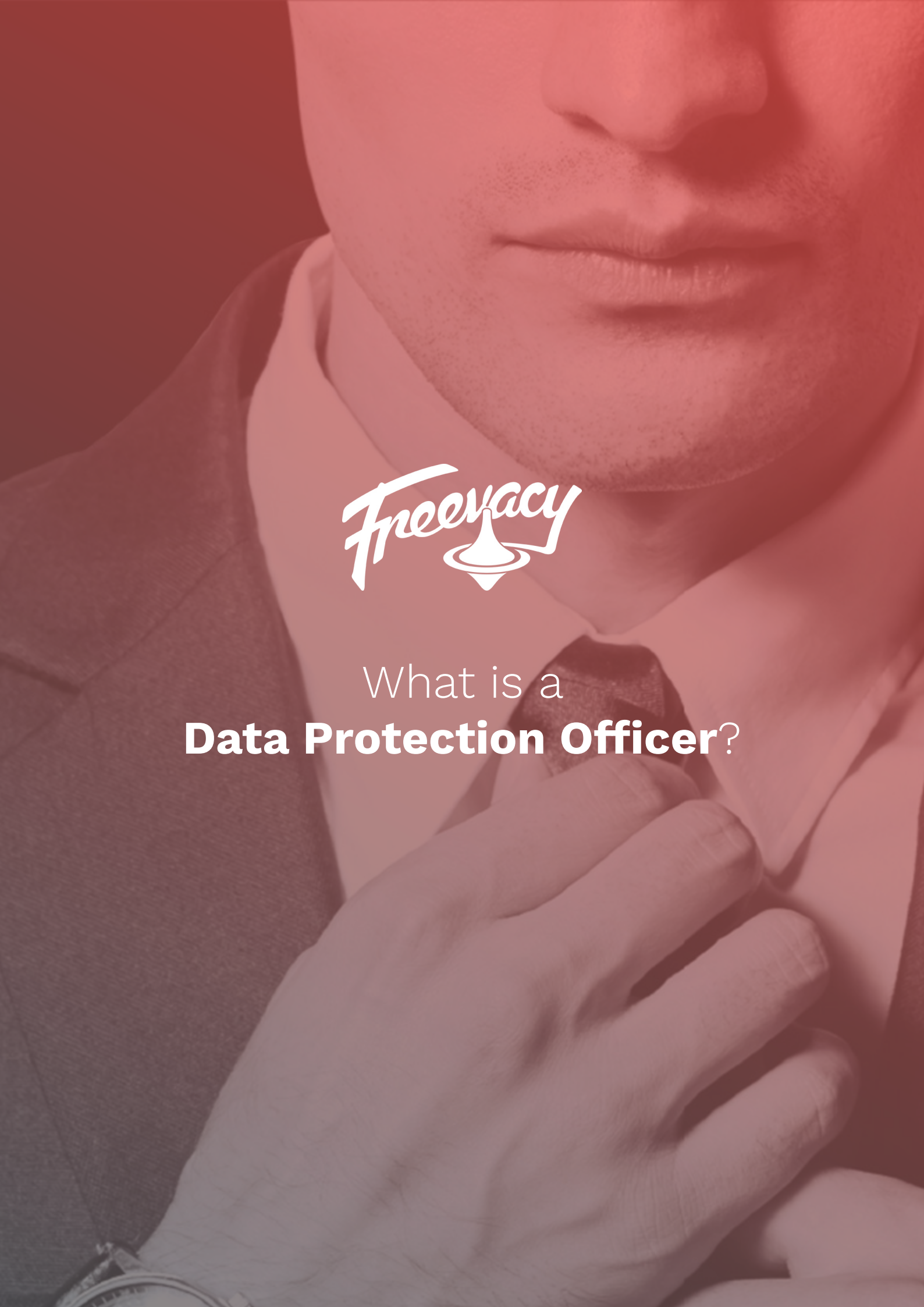


Freevacy

What is a **Data Protection Officer**?

INTRODUCTION

In the first in a series of linked articles about Data Protection Officers (DPOs) under the General Data Protection Regulation (GDPR), we take a detailed look at who exactly the Data Protection Officer is from the history of how the DPO evolved into a legally appointed position, essential information on fulfilling the role of a DPO, and a comparison with other data focussed senior executives within the organisation.

The GDPR represents the most significant overhaul in 25 years of privacy and data protection law. With its extraterritorial scope, the GDPR covers every organisation no matter whether they are a company, charity, or government body providing they have dealings with EU-based consumers.

Affected organisations are required to conduct a detailed review of their internal data protection policies and procedures to bring them in line with the GDPR. This includes supply-chain contracts, along with implementing robust mechanisms for data breach detection and reporting. An essential element of these preparations includes identifying if they are required to appoint a DPO.

> **The primary role of the data protection officer (DPO) is to ensure their organisation processes personal data of staff, customers, providers or any other individuals (referred to as data subjects) in compliance with the applicable data protection rules.**
>
> European Data Protection Supervisor

CONTENTS

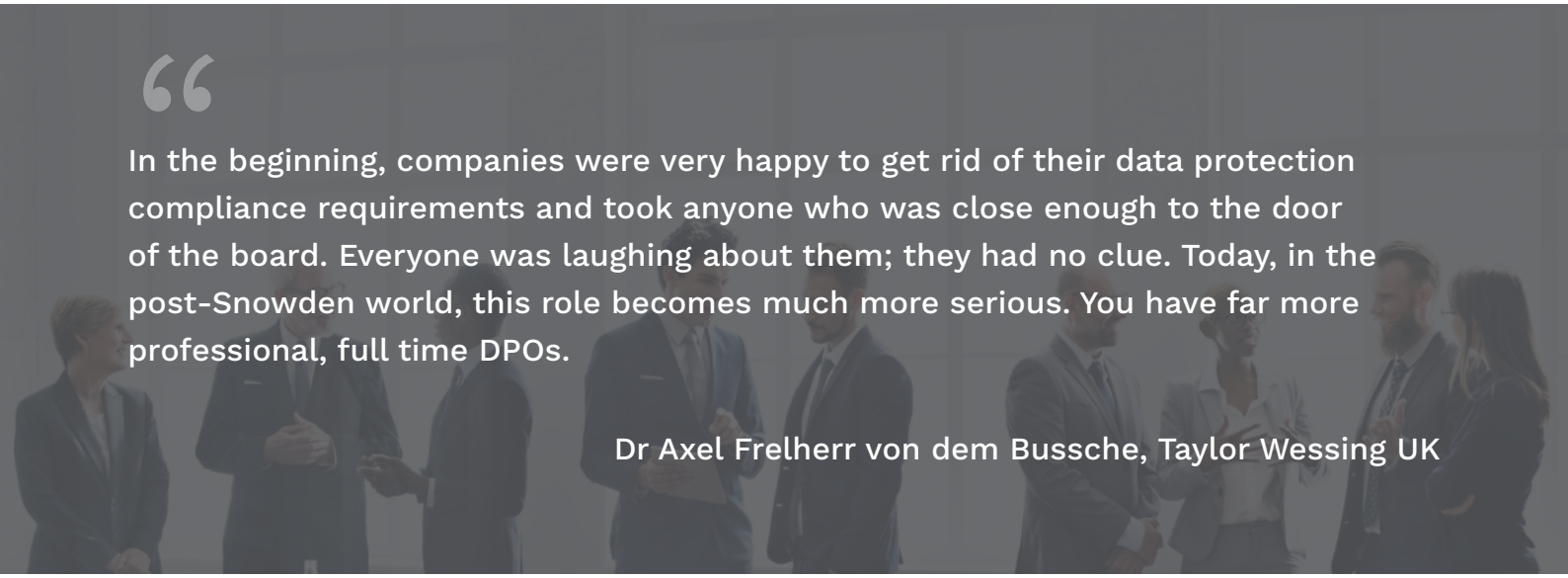
KEY FACTS ABOUT DATA PROTECTION OFFICERS

- A role defined within the legislation, the DPO is the appointed person responsible for monitoring compliance with the GDPR. Applies to Public (mandatory) and commercial organisations who handle data on EU citizens subject to criteria.
- The DPO must possess expert knowledge of data protection. They are required to advise on all aspects of data compliance across the organisation, including staff awareness and education initiatives.
- The GDPR does not define the qualifications of a DPO, leaving it to organisations themselves to select a person based on the specific requirements of the business. Organisations dealing with large volumes of highly sensitive data in an industry vulnerable to data breaches, i.e. airlines, banks, and government agencies, will likely require a higher calibre of DPO than a local widget-making factory.
- The DPO occupies a unique place in an organisation's structure. The GDPR sets out that a DPO should report directly to the highest management level of the organisation. It also states that management should not provide any instructions regarding the exercise of those tasks, or dismiss the DPO for exercising their role.
- The DPO is integral to an organisation's efforts to monitor and measure compliance, through Data Protection Impact Assessments (DPIAs), data audits, and to oversee the implementation of compliance tools and reporting mechanisms.
- The DPO must be funded and resourced appropriately. This includes having any or all the necessary team, premises, facilities and equipment required to deliver their obligations.
- The position of DPO is challenging, as it requires an ability to objectively examine the impact of data processing decisions on data subjects, whilst not allowing their judgment to be clouded by the objectives of the organisation.
- The position of DPO can be outsourced, and be full time or part-time, depending on the size of the organisation. Large companies, especially those that operate in multiple jurisdictions, may have to recruit a team; smaller organisations may outsource the role or fulfil on a part-time basis.
- A DPO has a responsibility to fully co-operate with the Information Commissioner's Office (ICO), the supervisory authority (SA) charged with overseeing the GDPR in the UK.
- Finally, DPOs help organisations to demonstrate their accountability. They communicate a message of openness, strengthening relationships and building trust between customers, service users, employees and the organisation.

HISTORY OF THE DATA PROTECTION OFFICER

The role of the DPO is almost 20 years old and was first defined under Section 8 of Regulation (EC) No 45/2001. Although now repealed and replaced1, the original regulation was passed to govern the processing of data by EU institutions and bodies, and the free movement of such data. Section 8 set out the rules around the appointment and tasks of the DPO, along with the requirements for notification and keeping a register of processing operations.

DPOs have been a fixture in German organisations since 2001 and are a mandatory appointment for those with more than nine people handling personal data. Their job, like DPOs under the GDPR, is not to look after the company's best interests, but to protect the interests of the owners of the data processed by the organisation. They are appointed by the Board but report under Germany's data protection laws, rather than an internal manager, and cannot be dismissed for carrying out their duties. German DPOs are not required to report the organisation to authorities if they do not implement the compliance methods outlined in reports to the Board; however, in a post-Snowden world, most companies and DPOs themselves are taking the role more seriously. In an IAPP article written by David Meyer, Dr Axel Freiherr von dem Bussche, a partner at Taylor Wessing UK, states:



> "In the beginning, companies were very happy to get rid of their data protection compliance requirements and took anyone who was close enough to the door of the board. Everyone was laughing about them; they had no clue. Today, in the post-Snowden world, this role becomes much more serious. You have far more professional, full time DPOs.
>
> Dr Axel Frelherr von dem Bussche, Taylor Wessing UK

France also had a DPO-like role as part of its national data protection law, called the correspondent à la protection des données[2].

And it's not just within the EU; in countries such as the Philippines, the role of DPO is also utilised to ensure organisational data protection. The Philippines Data Privacy Act of 2012 states, "a natural or juridical person or any other body in the government or private sector engaged in the processing of personal data of individuals living within and outside the Philippines" should appoint a DPO. Personal information controllers and personal information processors will be deemed a de-facto DPO under the Act. Other countries which have a requirement for a mandatory DPO in certain circumstances include Canada, Mexico, and Chile[3].

HOW THE GDPR SETS OUT THE ROLE OF THE DPO

Any examination of the role of DPO in 2019 must begin with the GDPR. To establish the reasoning behind the development of the role within the regulations, it is helpful to first look at Recital 97.

Recitals are vital components to understanding compliance obligations under the GDPR. The European Data Protection Board (see below) and other supervising bodies, including the EU Court of Justice, use the Recitals to check the Articles are being correctly interpreted in their application.

Recital 97 sets out the reasoning behind the existence of DPOs in the GDPR. It outlines that the DPO role exists to support the data controller monitor internal compliance with the GDPR. It also states that a DPO should have expert knowledge of data protection law and practices, which should assist the controller or processor to monitor internal compliance with the GDPR. In addition, the recital confirms that the level of expertise required of the DPO will be dependent on the processing activities undertaken by the controller and processor. Finally, it emphasises the importance of the DPO being free to perform their duties in an independent manner.

Articles 37, 38, and 39 provide the EU law applicable to DPOs.

Article 37 stipulates the rules around the designation of a DPO. They must be recruited or selected based on their professional qualities, particularly their knowledge of data protection law and their ability to deliver on the tasks set out in Article 39.

Article 38 sets out the position of the DPO and their role in the organisation. He or she should be given the tools they need to achieve their tasks and is immune from penalty or dismissal for performing their duties. They should also report to “the highest management level of the controller or the processor”.

Finally, Article 39 provides details about the DPOs tasks and duties:

- Inform and advise the Board, management, and employees of their obligations under the GDPR and other data protection laws (for example the California Consumer Privacy Act)
- Monitor compliance with the GDPR, other data protection laws, data protection policies and procedures, raise awareness, provide training, and conduct audits
- Advise on and monitor data protection impact assessments
- Cooperate with the Information Commissioner’s Office
- Be the initial contact for all data protection matters for queries, complaints, and requests for information by authorities

The Information Commissioner’s Office (ICO) points out that a key part of the DPOs role is one of risk assessment, ensuring the risks associated with the data processing being undertaken are considered, and are necessary in light of the nature, scope, context and purposes of the processing. The bigger the risk presented by a data processing task or project, the more attention it should receive from the DPO.

“

Isn’t having customers’ trust a cornerstone to good business?

Isn’t that intangible relationship with customers: loyalty, trust, repeat customers, something most companies want?

Accountability is at the centre of all this.

Elizabeth Denham, Information Commissioner

THE EUROPEAN DATA PROTECTION BOARD

The Article 29 Working Party was established under the law the preceded the GDPR, the EU Data Protection Directive (95/46/EC), as an independent and advisory Working Party on the Protection of Individuals with regard to the Processing of Personal Data. Its members were the EU's national supervisory authorities, the European Data Protection Supervisor (EDPS) and the European Commission.

The Working Party has since been transformed into the European Data Protection Board (EDPB) under the GDPR. The membership of the EDPB is similar except that it now has an independent Secretariat and legal powers.

The EDPB's primary role is to contribute to the consistent application of the GDPR throughout the EU. It advises the Commission, in particular on the level of protection offered by third countries or international organisations and promotes cooperation between national supervisory authorities.

Article 29 Working Party (WP29) Guidelines for Data Protection Officers
Even before the adoption of the GDPR, the then Article 29 Working Party recognised the importance of the DPO.

At a core issues plenary in June 2015, the WP29 argued that:

> The DPO is a cornerstone of accountability and a real tool of competitiveness for companies. Tasked with the implementation of accountability tools, they should be considered as the **compliance orchestrator** and the intermediary between all relevant stakeholders (e.g. supervisory authorities, data subjects, business partners).

Then, on 13th December 2016, the WP29 adopted a comprehensive set of Guidelines on Data Protection Officers (DPOs). These were updated on 5th April 2017.

The DPO guidelines aim to explain relevant sections of the GDPR where the correct interpretation is unclear. Although a complex document in itself, the guidelines provide useful information about the appointment and role of data protection officers, making it easier for organisations to meet their compliance obligations.

For instance, where Article 37(1) offers 3 specific cases for the designation of a DPO, the guidelines look at each aspect thoroughly to provide considerably more detailed advice. This includes a new point about accountability that states up-to-date DPO assessments should be maintained as a supervisory authority could request them at any time.

At its first constituent meeting on 25th May 2018, the EDPB confirmed that it had adopted the Article 29 Working Party DPO Guidelines.

THE ROLE PLAYED BY THE ICO REGARDING A DPO

GDPR compliance is overseen by the data protection authority of individual Member States. In the UK, this is the ICO. The ICO is an independent body, charged with upholding and protecting information rights in the public interest, promoting openness in public authorities and bodies, the private sector, and data privacy for individuals. As well as administering and advising on the GDPR, the ICO is responsible for upholding a range of privacy and information rights legislation, including the Data Protection Act 2018.

The GDPR provides limited scope for Member States to make provisions for how the regulations apply in their countries. This, among other elements of data protection law, such as processing data related to immigration, which is not covered by the GDPR, are provided for by the Data Protection Act 2018. Therefore, the two statutes must be read side by side, as opposed to the Data Protection Act 2018 being seen as a mere supplement to the GDPR.

The ICO provides a number of valuable resources about data protection officers. Not only does the ICO set out the role of the DPO and provide a helpful checklist, but it also provides full detail of accountability and governance requirements under the GDPR.

COMPARING THE ROLE OF THE DPO WITH OTHER DATA ROLES

It would be a mistake for an organisation to believe it was in compliance with the GDPRs requirements regarding a DPO because it already has a Chief Information Officer (CIO), or a Chief Information Security Officer (CISO). These roles are concerned with keeping the organisation's data safe and using it to meet strategic objectives. A DPO, on the other hand, has a duty to safeguard personal data held by the company, be it that of employees, suppliers, or consumers.

ROLE	COMPARISON WITH DPO
Chief Information Officer (CIO) – the most senior member of an organisation's IT department. It is a strategic business leadership position, charged with ensuring the IT department supports and meets overarching objectives and driving change and transformation where required.	The DPO may or may not sit on the Board. Regardless, their role is to look at the risks associated with the strategic objectives of the company in relation to personal data. They do not make decisions around growth and profitability, rather, they consider and advise on how GDPR compliance marries with such decisions and commercial ambitions.
Chief Information Security Officer (CISO) – a senior level executive whose role is to design and implement information security programmes. This includes policies and procedures to protect the organisation's communications, systems, and assets from internal breaches and external hackers.	DPOs monitor compliance of data protection policies and procedures and can conduct audits to ensure systems are in place protecting personal data from internal and external threats. Therefore, they will work closely with the CISO, advising them on the risks to personal data they have identified and how the security program can eliminate or mitigate these risks.
Chief Technology Officer (CTO) - oversees the current technology and creates relevant policy. They require the business knowledge necessary to align technology-related decisions with the organisation's objectives. It has been said that a CIO is an inward-facing role, whereas a CTO looks outward, for investment and partnerships which can be used to meet strategic goals.	A CTOs role involves evaluating risks and opportunities, and to this end, they and the DPOs objectives will be closely aligned. For instance, a CTO will be concerned with creating supplier contracts. These contracts will need to be analysed by the DPO to ensure that the supplier has the resources required to meet not only its own internal data protection responsibilities, but also to maintain GDPR compliance in all activities undertaken with the DPOs organisation.

COMPARING THE ROLE OF THE DPO WITH OTHER DATA ROLES CONT.

ROLE	COMPARISON WITH DPO
Chief Privacy Officer (CPO) – a senior level executive who is tasked with developing and implementing policies to protect data held by the organisation from unauthorised access. They also maintain a detailed knowledge of current privacy and data protection laws and understand how these apply to the organisation and the supply-chain.	In many respects, a CPO is an ideal choice to take on the role of DPO, given their required knowledge and experience. However, some commentators have noted that CPOs lack the independence and autonomy demanded by the GDPR with regards to the role of a DPO. This is especially true if they are responsible for procuring, implementing, and championing their employer's data processing systems.
Chief Marketing Officer (CMO) – responsible for the development, implementation and communication of the organisation's brand. The role is broader than a Marketing Director, who overseas the marketing department; i.e. a CMO is focused on strategy, and ensuring the brand is well-positioned for all future events, including possible M&As.	Although a CMO will have a deep understanding as to how data can be used within the business, they are unlikely to have the technical knowledge related to data protection and security that is required of a DPO. And as with the CPO, a CMOs role requires them to make decisions about how data is managed – this presents a conflict, given a DPO is responsible for governing data protection.

In practice, a DPOs role may come into direct conflict with those in IT or Marketing departments and senior managers or executives. For example, part of a DPOs role is to make sure only a minimum amount of data required to complete a transaction is collected and retained, and that the data subject can request it is amended or deleted on demand (subject to criteria).

Regardless of the strength and breadth of your existing team, your organisation needs to carefully examine whether it needs a DPO and undertakes a careful selection process to ensure the right person is recruited for the position.

THE GROWING IMPORTANCE OF THE DPO ROLE

As the world becomes increasingly digitally-centred, and as the line between privacy and the will of corporations to use personal data to facilitate profit and growth becomes more blurred, the role of a DPO in companies will become more pivotal.

It is worth remembering that a breach under the GDPR is a serious offence for which the maximum financial penalties can be severe.

Higher amount – up to €20 million (or sterling equivalent), or 4% global annual turnover of the preceding financial year, whichever is higher. These relate to more serious violations of the GDPR principles, to an individuals rights or transfers of data to third countries.

Standard amount – up to €10 million (or sterling equivalent), or 2% global annual turnover of the preceding financial year, whichever is higher. These involve a violation of the requirements placed on controllers and processors, which include the duties relating to the DPO.

In either case, the reputational damage created by misuse of data can be even more costly.

The number of employees entrusted with processing data, either in-house or governed by supplier contracts, continues to grow exponentially. Organisations need a central figure to not only manage compliance but to ensure everyone understands the rules and regulations around data protection and why they are important.

The DPO provides a link from the regulatory authority, to the board, through to the most junior member of staff processing personal data, and ultimately, the data owner. As an independent person, free from the constraints of internal politics and strategies, the DPO is not only a vehicle to ensure compliance but an insurance policy against the possibility of a costly, unintentional breach.

1. Regulation (EC) No 45/2001 has been repealed and updated by Regulation (EU) 2018/1725 The regulation covers “the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data,”
2. Recio, M. (2017). Practitioner's Corner · Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability. European Data Protection Law Review. 3. 114-118. 10.21552/edpl/2017/1/18.
3. Jackson, L (2013) The expanded role of the DPO, P. & D.P. 2013, 13(5), 9-11

SEE OUR AVAILABLE COURSES

BCS Foundation Certificate in **Data Protection**

The Foundation GDPR Certificate from the BCS is recommended for anyone involved in the collection, usage or protection of personal information.

FIND OUT MORE

IAPP Certified **Information Privacy Professional Europe**

The CIPP/E is the essential IAPP certification for privacy professionals covering Europe's framework of laws, regulations and policies, most significantly the GDPR.

FIND OUT MORE

BCS Practitioner Certificate in **Data Protection**

The GDPR Practitioner Certificate from the BCS is the leading industry qualification for UK focused DPOs and compliance professionals.

FIND OUT MORE

IAPP Certified **Information Privacy Manager**

The CIPM is a unique qualification in privacy programme management from the IAPP that teaches DPOs and senior compliance professionals how to turn policies into accountability.

FIND OUT MORE

BCS Practitioner Certificate in **Freedom of Information**

This BCS Practitioner Certificate is the recognised qualification for individuals with information access responsibilities under the FOIA or EIR.

FIND OUT MORE

IAPP Certified **CIPP/E & CIPM** Combination course

These two combined practitioner level certified courses from the IAPP are recommended for DPOs and other compliance professionals with privacy operations' responsibilities.

FIND OUT MORE

NEXT GUIDE IN THE SERIES

Do I need a Data Protection Officer? Appointing a DPO for business

In this the second of a series of linked articles about Data Protection Officers (DPOs) under the General Data Protection Regulation (GDPR), we make a detailed examination into the question surrounding whether to appoint a Data Protection Officer.

DOWNLOAD GUIDE

Freevacy is an independent GDPR training provider. We offer accredited BCS and IAPP training for DPOs, privacy professionals and anyone with data protection responsibilities. We also deliver bespoke courses that can be adapted to suit your particular learning requirements.

For more information, please call: 0370 04 27001
or email: **contact@freevacy.com**

www.freevacy.com