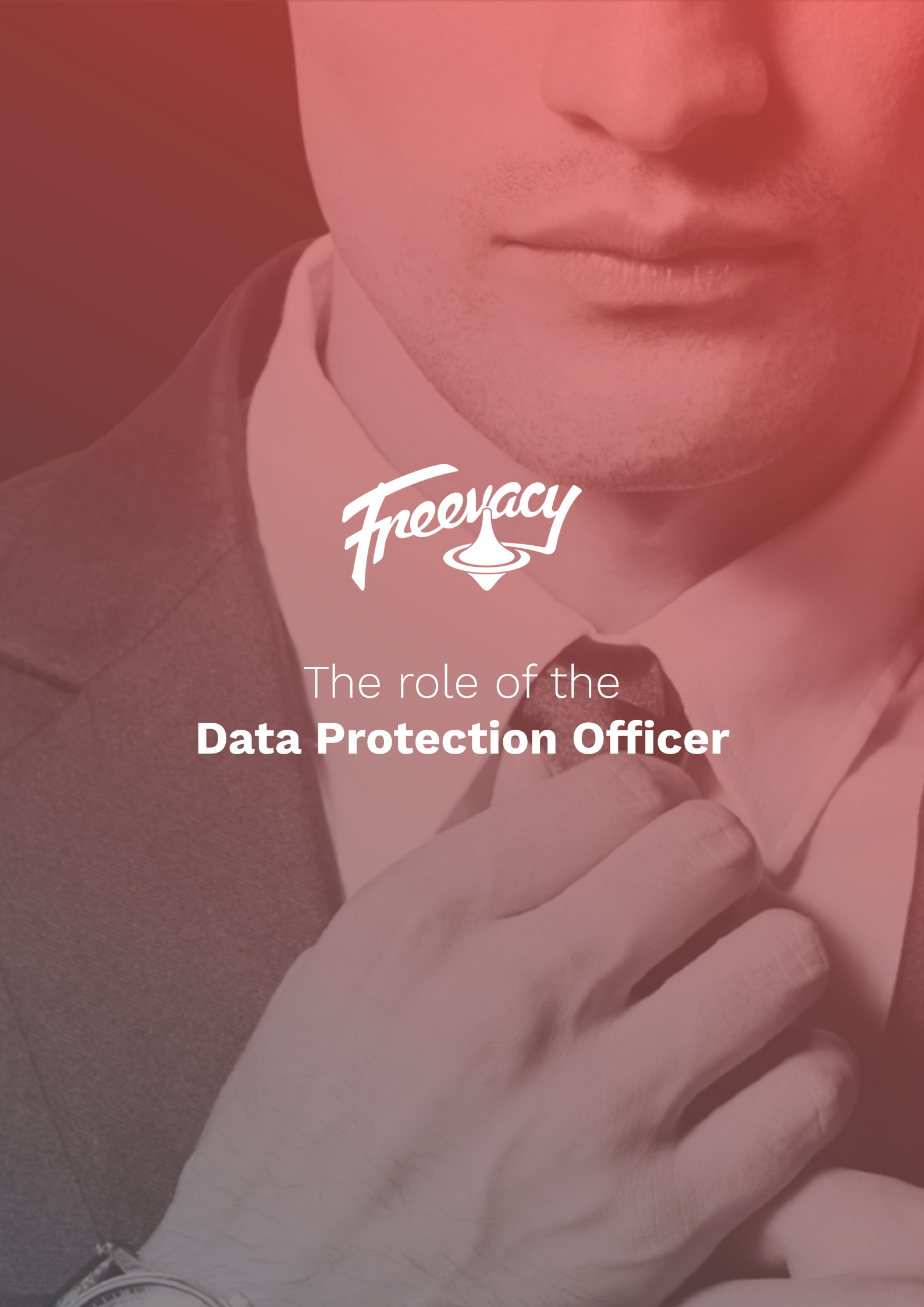

Freevacy

The role of the **Data Protection Officer**

INTRODUCTION

In this, the third of a series of linked articles about Data Protection Officers (DPOs) under the General Data Protection Regulation (GDPR), we discuss the role of the DPO. Whether a DPO is a required or voluntary appointment, your organisation is making a significant investment in creating and maintaining the position. It is therefore imperative that the role of the DPO is understood in its entirety, to ensure it becomes a revenue-generating position, as opposed to a cost.

As mentioned in the opening statement, when researching or planning the role of the DPO, there are two areas of the GDPR, which need to be considered. The position of the DPO, which is covered under Article 38, and the tasks of the DPO, which are listed in Article 39.

It is, however, not enough just to understand the duties that the DPO must fulfil. You also must take into consideration how the DPO must go about fulfilling those duties. This brings into question matters such as the level of autonomy that the DPO should be given and who they report to.

CONTENTS

KEY FACTS ABOUT THE ROLE OF A DPO

- The success of a DPO will be measured on their ability to implement and maintain a GDPR compliant data processing operation. It is important to note, however, that the DPO can only achieve this objective where they receive the full backing of the organisation.
- In establishing the role, identify the funding, the resources and where to deploy the DPO within the organisational hierarchy. The DPO must be in a position to perform their tasks without oversight or instruction and be able to report their findings to the board.
- The DPO will be required to perform all the tasks defined under Article 39, no matter whether the position is full-time or not. The same applies where the role is filled internally or outsourced to a specialist external consultant.
- Where the DPO is assigned additional duties to those listed under Article 39, take care not to create a conflict of interest.
- The DPO is expected to advise on any matters that relate to privacy and compliance with the GDPR. Always ensure the DPO is informed and consulted about all aspects of data protection at the earliest stage possible, particularly at the outset of a project. The DPO is also required to lead employee awareness and training activities.
- The main task that the DPO is responsible for involves monitoring compliance with the GDPR, related privacy regulations, and national data protection laws. This includes conducting data audits, risk assessments, and where necessary, offering advice about where to carry out data protection impact assessments, and evaluating their results.
- The DPO is also the point of contact for individuals (customers and employees) to request information about the processing of their personal data, and for the supervisory authorities (in the UK this is the ICO).
- Finally, the DPO cannot be penalised or dismissed for performing their tasks. They can be removed if they are guilty of other types of misconduct such as harassment or fraud.

ARTICLE WP29 COMMENTS ON THE ROLE OF THE DPO

The Article 29 Working Party (WP29) Guidelines for Data Protection Officers[1] highlights how the GDPR sees the role of the DPO as a **key player** in the new data governance system.

The Guidelines take this further, clarifying where DPOs should focus their attention:

> The DPOs primary concern should be enabling compliance with the GDPR.

It goes on to say:

> The DPO plays a key role in fostering a data protection culture within the organisation and helps to implement essential elements of the GDPR, such as:
>
> - The principles of data processing
> - Data subjects' rights
> - Data protection by design and by default
> - Records of processing activities
> - Security of processing
> - Notification and communication of data breaches

However, when it comes to performing their duties, the Guidelines are clear:

> Ability to fulfil the tasks incumbent on the DPO should be interpreted as both referring to their personal qualities and knowledge, but also to their position within the organisation.

Future updates

The WP29 DPO Guidelines provide a reference to best practice and are designed to assist controllers and processes comply with the law and assist DPOs in their role.

They also make clear that they will be updated as the GDPR and role of the DPO becomes embedded into the data protection landscape.

POSITION OF THE DPO

Article 38 of the GDPR provides for the position of the DPO.

It states that the DPO should be:

- Involved in a timely manner in all issues related to the protection of personal data
- Provided with the resources required to perform their tasks under Article 39 of the GDPR and maintain their expert knowledge
- Independent and free from instruction on how to do their job, or to dismissed or penalised for performing their tasks
- Able to report to the highest level of management
- The contact person for all matters regarding personal data for external and internal stakeholders
- Bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law
- Able to perform other tasks and duties as long as there is no conflict of interest

REPORTING LINES

As already mentioned, Article 38(3) of the GDPR requires that the DPO carries out his or her duties independently and reporting directly to the **highest management level.**

However, when you consider that Article 5(2) declares responsibility for GDPR compliance resides solely with the controller, then it would surely be counter-productive not to provide the DPO with the access they require to report their findings.

What does the highest management level actually mean?
At this point in time, no further clarification is available in either the regulation or within the WP29 DPO Guidelines about the type of reporting line that is required.

This leaves considerable room for interpretation.

In an article written for the International Association of Privacy Professionals (IAPP), Carolin Stenz and Sarah Taïeb discuss this very point:

POSITION OF THE DPO CONT.

> In corporate language, executive management is a global term that includes the senior management level, but also lower management levels.
>
> The highest management level, on the contrary, may designate the board of directors as well as the highest executive, or senior management, meaning the positions of chairman, managing directors, executive directors, executive VP and the so-called C-level management (chief executive officer, chief financial officer, chief operating officer, chief information officer), the so-called executive board, with day-to-day responsibilities and specific executive powers.
>
> Carolin Stenz & Sarah Taïeb (Global DPO), Ipsen Group

The authors refer to Paul Lambert's analysis in his book The Data Protection Officer, where he views that reporting to the highest management level corresponds to requiring senior management involvement, therefore reporting should be at Board level. He argues that this would give the DPO the independence they need and ensure their role is not hampered by inferior management functions that have not come directly from the Board itself.

Organisations will need to implement a governance structure incorporating a DPO in a way which reflects the nature of their business. What is critical, in terms of compliance, is that the DPOs reporting lines are clear and well documented.

POSITION OF THE DPO CONT.

INVOLVING THE DPO IN ALL DATA PROTECTION MATTERS

The WP29 DPO Guidelines state that the DPO and their team must be involved at the earliest stage possible in all aspects of data protection.

> It is important that the DPO be seen as a discussion partner within the organisation and that he or she be part of the relevant working groups dealing with data processing activities within the organisation.

Therefore, a part of the governance policy of an organisation must relate to informing and consulting with the DPO at the outset of a project. In addition, time must be provided for a proper risk assessment to take place and for the DPO and their team to implement any steps necessary to mitigate any risks identified.

To ensure the DPO has knowledge and oversight of all data protection matters, the organisation employing them should:

- Invite the DPO to participate regularly in meetings of senior and middle management.
- Ensure the DPO is present when decisions with data protection implications are taken. All relevant info should be passed on to the DPO in a timely manner to allow them time to construct adequate advice.
- Give the opinion of the DPO due weight. In case of disagreement, the WP29 recommends, as good practice, to document the reasons for not following the DPOs advice.
- Ensure the DPO is promptly consulted once a data breach or another incident has occurred.

Depending on the type of organisation, the best practice may involve the data controller and/or processor drafting policies and procedures which set out how the DPO fits into the organisation and when they should be consulted.

RESOURCING THE DPO

When it comes to resourcing, Article 38(2) defines this as:

> The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

The WP29 DPO Guidelines are more thorough in their advice. It infers that the necessary resources should include:

- Active support from the board of directors
- Time to complete the duties and requirements of the role
- Adequate financial backing with access to facilities, systems, equipment and personnel
- Access to other departments such as IT, HR, legal and security,
- Where necessary establishing a team of staff to support the DPO
- Make sure all employees are aware of the existence of the DPO role and function
- Support the DPOs requirement for continuous professional development

In regards to supporting the DPO, he or she, along with any supporting personnel, must be given every opportunity to stay up to date and be encouraged to continue their professional development. In an article for the IAPP, Thomas Shaw emphasises the skills your DPO should have. In particular:

> **DPOs must have significant experience in privacy and security risk assessment and best practice mitigation, including significant hands-on experience in privacy assessments, privacy certifications/seals, and information security standards certifications.**
>
> **Thomas Shaw, CIPP/E, CIPP/US**

Practitioners fulfiling the role of the DPO can look towards professional workplace qualifications from the IAPP and BCS to develop their skills.

RESOURCING THE DPO CONT.

THE INDEPENDENCE OF THE DPO

Article 38(3) states clearly that:

> The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those (Article 39) tasks.

The WP29 DPO Guidelines describe this as a basic guarantee to:

> Help ensure that DPOs can perform their tasks with a sufficient degree of autonomy within their organisation.

The Guidelines also highlight part of Recital 97, which clarifies how the freedom to perform their duties unimpeded applies regardless of how the DPO is appointed.

Recital 97 describes this as:

> Data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

In reality, this means that the DPO must not be given instructions on any areas they can or cannot get involved, providing they are fulfilling their obligations under Article 39.

This includes receiving instructions about:

- The desired outcome or result
- How to investigate a complaint
- Whether to consult the supervisory authority
- How to interpret data protection law

However, while the DPO cannot be given direction over matters relating to their role, the WP29 DPO Guidelines point out the limit of their powers:

> The autonomy of DPOs does not, however, mean that they have decision-making powers extending beyond their tasks pursuant to Article 39.

Be prepared for disruption

Katalina Bateman states in her article, GDPR Series: the role of the DPO – overcoming the GDPR hurdle2, published in the Privacy & Data Protection Journal, that the independence of the DPO must run parallel to "maintaining a constructive relationship with colleagues generating profit for the business and this could prove challenging for both sides".

The author provides the example of circumstances where the DPO has to call a halt to the processing of personal data whilst a risk assessment takes place, thus delaying the completion of a particular project.

RESOURCING THE DPO CONT.

DISMISSAL OR PENALTY FOR PERFORMING TASKS

Article 38(3) states that DPOs:

> Shall not be dismissed or penalised by the controller or the processor for performing their tasks.

This requirement helps ensure DPOs have the autonomy to act independently and without fear of retaliation or adverse consequences for performing their data protection tasks.

Penalties or the threat of a penalty may take a variety of forms and may be direct or indirect. The WP29 DPO Guidelines provides examples of penalties such as the:

- absence or delay of promotion;
- prevention from career advancement;
- denial from benefits that other employees receive.

However, a DPO can be dismissed for reasons other than performing their tasks as a DPO if they breach basic elements of employment such as having participated in sexual harassment or workplace bullying or commit other forms of gross misconduct.

With this in mind, the Guidelines note how:

> The more stable a DPOs contract is, and the more guarantees exist against unfair dismissal, the more likely they will be able to act in an independent manner. Therefore, the WP29 would welcome efforts by organisations to this effect.

COMMUNICATING CONFIDENTIALLY WITH DATA SUBJECTS

The DPO must be able to efficiently communicate with data subjects.

This means that:

- Communication should be in the same language used by the supervisory authorities and the data subjects concerned
- The DPO is available to data subjects by being located on the same premises as employees, via telephone, or other secure means of communication

Article 37(7) also states:

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

The objective of these requirements is to ensure that data subjects (both inside and outside of the organisation) can easily and directly contact the DPO without having to contact another part of the organisation. Confidentiality is equally important: for example, employees may be reluctant to complain to the DPO if the confidentiality of their communications is not guaranteed.

With this in mind, it is important to note Article 38(5):

> The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

TASKS OF THE DPO

The tasks of the DPO are set out under Article 39 of the GDPR.

1. The data protection officer shall have at least the following tasks:
    1. To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
    2. To monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
    3. To provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
    4. To cooperate with the supervisory authority;
    5. To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.
2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

The words **at least** are important here.

The GDPR recognises that every organisation is different; therefore, these tasks should be seen as a minimum regarding the scope of the DPOs role.

The ICO provides further information about the tasks expected of the DPO on its dedicated page for data protection officers.

TASKS OF THE DPO CONT.

Data Protection Impact Assessments

Risk management is a key part of a DPOs tasks. Therefore, the DPO needs to have access to and control over data maps, processing policies and procedure, and to be informed immediately about potential new projects and revenue streams which could involve the processing of personal data.

The WP29 DPO Guidelines state that as far as the data protection impact assessment (DPIA) is concerned, the controller or the processor should seek the advice of the DPO, on the following issues, amongst others:

- Whether or not to carry out a DPIA
- What methodology to follow when carrying out a DPIA
- Whether to carry out the DPIA in-house or whether to outsource it
- What safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects
- Whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with data protection requirements

The ICO provides an excellent resource for data protection impact assessments on its website.

Record Keeping

It is vital to note that as far as record keeping responsibilities go, it is for the controller or processor to ensure adequate records of processing operations are created and kept.

However, this task can be passed onto the DPO as long as overall responsibility remains with the controller or processor. These records are also essential resources for the DPO to perform their tasks of monitoring compliance, informing, and advising the controller or the processor.

SUMMARY

As will be discussed in Appointing a DPO, to perform the tasks required, a DPO needs to be possessed with a combination of hard and soft skills.

- **Hard skills** - knowledge of data protection, cybersecurity, and compliance
- **Soft skills** - communication with multiple stakeholders simultaneously, managing conflicting objectives such as GDPR compliance versus company targets.

Being able to balance these skills and objectives is why the positioning within the organisation of the DPO is critical, to ensure they have the independence, resources, and confidence to perform their job effectively.

1. The Article 29 Working Party (WP29) was transformed into the “European Data Protection Board” (“EDPB”) under the GDPR
2. Bateman, Katalina "GDPR series: The role of the DPO - overcoming a GDPR hurdle" PDP Journals, Volume 17, Issue 5, 2017

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

Appointing a Data Protection Officer

In this, the forth of a series of linked articles about Data Protection Officers (DPOs) under the General Data Protection Regulation (GDPR), we examine some important aspects related to the appointment of a DPO.

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