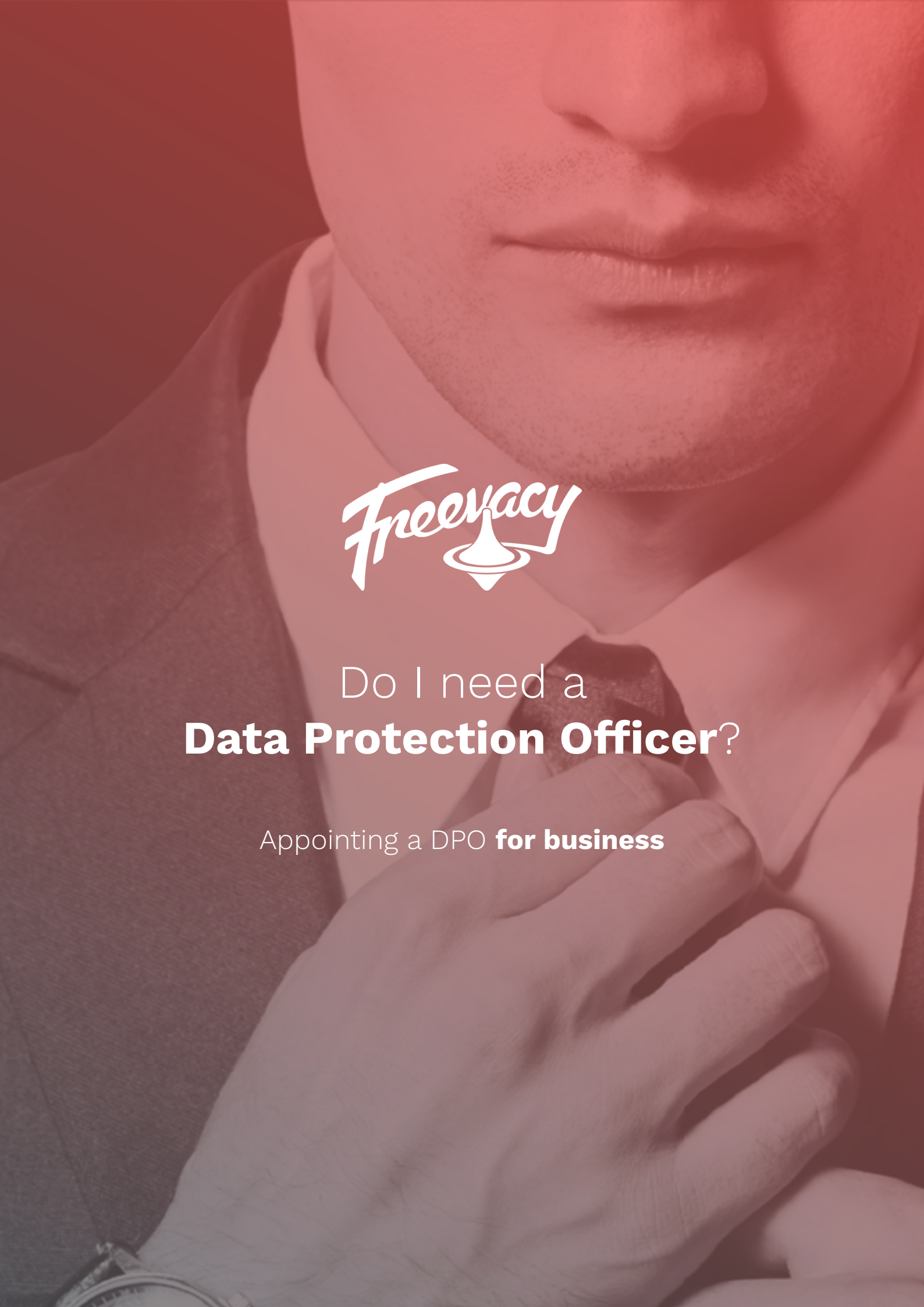

Freevacy

Do I need a **Data Protection Officer**?

Appointing a DPO **for business**

INTRODUCTION

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.

In this investigation, we look at the complicated criteria applying to businesses, along with the more straightforward situation relating to organisations delivering UK public services. To ensure our analysis is relevant for each audience, we have segmented our findings into two separate sections:

Appointing a DPO for Businesses – applies to commercial organisations operating in the UK (or from anywhere in the world), which process personal data about EU citizens.

DPOs and UK Public Services – applies to public authorities and bodies operating in the UK, which process personal data about EU citizens. Commercial organisations carrying out a public service under contract are also covered in this section.

APPOINTING A DPO **FOR BUSINESS** ›

APPOINTING A DPO **FOR UK PUBLIC SERVICE** ›

CONTENTS

APPOINTING A DPO FOR BUSINESS

For some businesses, the appointment of a Data Protection Officer (DPO) will be mandatory. The Article 29 Working Party (WP29) Guidelines for Data Protection Officers[1] highly encourages the appointment of a DPO to ensure an organisation meets its compliance obligations under the GDPR.

> Even when the GDPR does not specifically require the appointment of a DPO, organisations may sometimes find it useful to designate a DPO on a voluntary basis. The Article 29 Data Protection Working Party (WP29) encourages these voluntary efforts.

However, the cost and time required in recruiting such a specialist position must be taken into consideration. Therefore, it is imperative organisations understand not only whether they are legally required to appoint a DPO, but whether they should consider doing so voluntarily and the benefits of making such a decision.

THE BUSINESS CASE FOR A DPO

The outlook for the global economy in 2019 continues to be uncertain. In July, the International Monetary Fund (IMF) cut its global growth outlook once again. The global economic picture has worsened since April, amid ongoing trade tensions with China, the impact of sanctions against Iran on oil prices, and of course, Brexit is still in the balance. The risk of the UK leaving the EU in a disorderly exit could further slow growth, disrupt supply chains and weaken investment.

With the economic outlook so unpredictable, investing in a DPO may seem like a luxury rather than an opportunity to mitigate risk or drive growth. Despite this, even if your business is not required to appoint a DPO, serious consideration should be given to creating the position voluntarily.

Why?

First of all, data protection is an area which is continually evolving, so having a dedicated specialist leading the compliance programme means the business can position itself as a leader in the field. Other, more tangible advantages can be found in the direct impact that the DPO can have on decision making and revenue generation.

DPOS INPUT ON STRATEGIC DECISION MAKING

Companies in every sector of industry rely on quality information to conduct research and study in their pursuit of knowledge. A journey that begins with data collection typically involves the combination of strategy and technology in order to gain actionable insights, which can then be used to make informed business decisions.

The difference between whether management can uncover answers to critical business problems, or identify new trends and opportunities, comes down to what information is available at any given point in time, along with any analysis that is permissible thereafter.

Ultimately, organisations with a dedicated high-level individual monitoring risk and compliance will gain a significant competitive advantage over those without.

> **If companies are able to unlock the power of large-scale data, they will make 100 major decisions a year instead of 2-3. They will be able to predict the outcomes of these decisions with much greater accuracy and in real-time.**
>
> Krishna K. Gupta, Romulus Capital

It is difficult to imagine how such power and advantage could be unlocked, while at the same time managing risk and compliance, without a DPO being in place.

THE BUSINESS CASE FOR A DPO CONT.

DPOS EASE OBSTACLES IN THE SALES CYCLE

In its 2019 report, privacy is identified as a business differentiator that can seriously impact earnings. According to Cisco in its Data Privacy Benchmark Study sales delays due to customer concerns about data privacy continue to be an issue for most companies.

> **87% reported they have delays in selling to existing customer or prospects, up from 66% last year.**
>
> Cisco Data Privacy Benchmark Study 2019

The significant increase over last years statistic can be attributed to the heightened awareness of the importance of data privacy, following high profile data breaches such as the Cambridge Analytica and Facebook scandal, along with laws such as the GDPR becoming enforceable.

The average sales delay was 3.9 weeks (4.9 weeks in the UK) with 94% of delays lasting between 0 and 10 weeks. Some organisations reported delays of 25 to 50 weeks or more.

> **Privacy has become a board-level issue, and customers are making sure their business partners have adequate answers to their concerns before doing business together.**
>
> Cisco Data Privacy Benchmark Study 2019

The minimum impact of a sales delay will cause revenue to be put on hold for a period and can lead to missed targets. The subsequent repercussions, however, can have a more significant impact affecting employee remuneration, along with financial decisions and harm to investor relations.

Delayed sales can also turn into lost sales if customers seek alternative solutions from a competitor or cancel the project in its entirety.

A more in-depth investigation would no doubt uncover countless examples of the benefits a DPO can offer an organisation over and above ensuring GDPR compliance. Fundamentally, though, what further justification is needed to support the appointment of a DPO beyond intelligence, or revenue?

Other than your companies hard-earned reputation, of course.

WHERE TO BEGIN

Deciding on whether a DPO must or should be appointed requires an in-depth examination of:

- General Data Protection Regulation (GDPR),
- Data Protection Act 2018 (DPA18),
- EPDB adopted, Article 29 Working Party (WP29) Guidelines for Data Protection Officers
- Information Commissioner Office (ICO) advice and guidance

This paper provides a detailed analysis of both the GDPR and DPA18, the WP29 DPO Guidelines, along with expert commentators opinions and independent studies to help you decide whether to invest in a DPO. Regardless of your ultimate decision, GDPR compliance is still mandatory. This includes allocating adequate resources to ensure anyone processing personal data understands their duties and responsibilities.

KEY FACTS ABOUT WHETHER A BUSINESS NEEDS TO APPOINT A DPO

- In the final draft of the GDPR, considerations about appointing a DPO are based on the type, scale and frequency of the processing activities, not the number of employees.
- All commercial organisations need to consider whether a DPO is required. There are no exceptions. When carrying out an assessment, it is how and for what purpose data is being processed that matters, not the size of the organisation.
- Article 37 outlines the three situations where the mandatory appointment of a DPO is required. The criteria are complex and, in some circumstances, open to interpretation. Careful consideration is advised, and make sure to document your decision in writing.
- Private sector companies that have successfully tendered for contracts to deliver public services are advised to appoint a DPO.
- All forms of online tracking and profiling are listed as examples of regular and systematic monitoring. This includes data-driven marketing activities such as email retargeting, behavioural advertising, and big data operations. As part of the selection criteria, and when conducted at scale, these activities fall within the scope to appoint a DPO.
- Activities performed by an external processor (such as a marketing agency) that require a DPO, do not necessarily mean that the organisation is under the same obligation.
- Conduct regular assessments of your data processing operations to determine whether they meet the criteria to appoint a mandatory DPO. However, do not focus solely on being compliant with the GDPR, investigate the advantages of selecting a DPO voluntarily.

WHERE TO BEGIN CONT.

KEY FACTS ABOUT WHETHER A BUSINESS NEEDS TO APPOINT A DPO

- A DPO can enhance an organisation's reputation, not only with its customers, service users or audience but also with investors and other key stakeholders. As such, a DPO appointment demonstrates stability, a commitment to following compliance procedures, and the availability of resources to manage risks.
- Commercially astute DPOs can quickly identify the opportunities certain data processing activities present, then draft and execute a strategy of how to take advantage of such opportunities in a compliant way with appropriate risk-management in place.
- Where no DPO is appointed, resources still need to be allocated to oversee GDPR compliance. Once again, the decision not to appoint a DPO should be revisited regularly and documented in writing.

TOOLS TO HELP YOU MAKE YOUR DECISION

To help organisations determine if they should appoint a DPO, the ICO has developed a simple online DPO Assessment tool. It involves three questions and includes some examples and further reading to assist in making a decision. The tool takes around five minutes to complete.

At the end, it states that if you decide to appoint a DPO on a voluntary basis, they will need to be registered with ICO, and that even if your organisation is not required to appoint a DPO, someone in the business needs to be responsible for data protection.

Alternatively, the DPO Network Europe has created a DPO decision tree, which offers a more visual interface to help businesses assess whether they need to invest in a DPO.

WHAT TO DO IF YOU ARE STILL UNDECIDED ABOUT APPOINTING DPO

If the DPO Assessment or decision-tree fail to offer sufficient clarity on whether to appoint a DPO, you can also read the WP29 DPO Guidelines. Although complicated to read, the Guidelines add much-needed detail to support your assessment.

Alternatively, you can continue reading our analysis. In this next section of the paper, we unpick the uncertainties surrounding the more challenging aspects of Article 37(1), helping you to decide whether a DPO is required.

THE EVOLUTION OF THE DPO REQUIREMENT

To appoint or not to appoint a DPO was one of the most discussed and amended provisions in the drawing up and passing of the GDPR. The main objections came from Germany, which has required the mandatory appointment of a DPO since 2001. The European Union's largest economy was concerned the GDPR would undermine the government's current requirements which required almost all controllers to appoint a DPO.

Britain also had a great deal of comment regarding the appointment of DPOs. The Justice Committee suggested that the requirement for a mandatory data protection officer should be based on the sensitivity of the data being handled by the organisation rather than the number of employees, as the number of 250 was chosen merely for simplicity, this being what the EU defined as an SME.

The Federation of Small Businesses told the Committee that the requirement to appoint a DPO should not be mandatory for all SMEs as it is expensive to have one. They believed mandatory appointments should only be required in businesses which were **data-centric and monitor data on a daily basis**.

Ultimately, the Committee put forward a recommendation that whether or not an organisation should be required to have a DPO should be based on the type of business, and the sensitivity of the data being processed.

The Committee's recommendations were essentially taken up, resulting in Article 37(1), governing the designation of a DPO being finalised.

THE GDPR PROVISIONS REGARDING THE APPOINTMENT OF A DPO

Article 37(1) sets out three situations where it is mandatory to appoint a DPO:

1. The controller and the processor shall designate a data protection officer in any case where:
    1. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
    2. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
    3. the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.

ARTICLE 37(1) IN-DEPTH

In order to make an informed decision about whether to allocate the capital investment and resources necessary to make a DPO appointment, commercial organisations must first determine the meaning of a number of key provisions contained within Article 37(1).

This raises a number of questions:

- What are core activities?
- What is large scale processing?
- What counts as regular and systematic monitoring?
- What is special category data?
- Is it the controller or processor who is required to appoint a DPO?

Before we examine these questions, it is important to note that assessing whether to appoint a DPO is not a one-off exercise. The need for a DPO may alter over time. This can be due to natural business growth, entering a new market, or because of a change in data processing operations that warrant a DPO being installed.

Also, there is a popular misconception that an exemption exists for small businesses. This point was raised in a speech by Peter Brown of the Information Commissioner's Office at Infosec 2017.

> **I've heard plenty of people talking about there being a DPO exemption for SMEs – this is absolutely not the case.**
>
> Peter Brown, Senior Technology Officer of ICO

As noted above in the section discussing the evolution of the DPO requirement, early drafts of the regulations and negotiations put forward the idea that only businesses with more than 250 employees should require a DPO. This proposal was withdrawn from the final version of the GDPR.

What matters when it comes to deciding whether a DPO is required is not the size of the organisation, but how and for what purpose the entity processes data.

The ICO has created a webpage offering GDPR advice and guidance for smaller companies.

CORE ACTIVITIES

The ICO states that to qualify as a core activity the processing of personal data must constitute part of carrying out and achieving the businesses primary objectives.

The WP29 DPO Guidelines provide an example:

> A private security company carrying out surveillance of several private shopping centres and public spaces. The act of surveillance is a core activity of the company and to accurately monitor environments it needs to process personal data.

As such an organisation of this nature requires a mandatory DPO.

The processing of data for payroll, contacting clients, etc. are not regarded as a core activity because it does not relate to the carrying out of the **primary objectives** of the business. They are administrative tasks that all organisations must manage. However, like all matters related to personal data, GDPR principles must still be complied with when dealing with such material.

Grey areas in core activities
Like many components of the GDPR (and every other piece of legislation ever published), there are grey areas when it comes to defining core activities.

For example, there is a difference between someone who is self-employed having a list of their customers, and at the other end of the spectrum a large publishing organisation, which has an advanced customer relationship management (CRM) implementation.

- Whereas the former may add new contacts to their customer list through simple activities such as word-of-mouth referrals or networking events.
- The latter instead purchases third-party data lists to profile and build custom audiences in which to conduct highly targeted online behavioural advertising campaigns as part of a complex marketing strategy.

In this situation, the self-employed person would not need to appoint a DPO, while the publishing company may well require one, even though their core activity is publishing.

ARTICLE 37(1) IN-DEPTH CONT.

LARGE SCALE

Article 37 does not define **large-scale regular and systematic monitoring**; however, between the extremes of processing volumes of data, there exists another area open to interpretation. This fact was originally recognised by the WP29 DPO Guidelines but is most clearly outlined by the ICO which states:

When an organisation is deciding whether their data processing falls into the territory of **large-scale**, they should consider the:

- Number of individuals concerned
- Volume of data
- Variety of data
- Duration of the processing
- Geographical extent of the processing

The DPO Guidelines also provided examples of large-scale processing of data include:

- Processing of patient data in a hospital or large care facility
- Processing of travel data, i.e. an airline or public transport company
- Collecting statistics to be used by commercial organisations
- Processing of customer data by banks and insurance companies

National guidelines in other EU member states
Several EU member states have issued their own guidance on this topic.

In his post, On Large-Scale Data Processing And GDPR Compliance, Paul Breitbarth cites the example of the Dutch DPA releasing guidance on what constitutes large-scale processing for the healthcare sector, which defines large scale as 10,000+ patients.

In a LinkedIn post, the Data Protection Commissioner for Estonia, Viljar Peep did not feel European guidelines to appoint a DPO or conduct DPIAs were clear enough and decided to give his own definition for Estonia based on numbers of data subjects. The criteria vary depending on the category of data:

ARTICLE 37(1) IN-DEPTH CONT.

- 5,000 persons – Special categories and or criminal convictions/offences data
- 10,000 persons – High-risk data, which includes financial data, digital trust services such as e-signatures, communications data, real-time geolocation data, and profiling data with a legal consequence or a significant impact
- 50,000 persons – Any other data

In Hungary, the appointment of a DPO is mandatory in certain industries, for example, telecommunications providers and financial organisations. Croatia demands that a data security officer be appointed when a company has 20 or more employees.

The Czech Republic, Data Protection Authority, has similarly set a large-scale processing threshold of 10,000 data subjects before triggering a requirement to conduct a Data Protection Impact Assessment (DPIA). The Czech Republic advice additionally states that processing by more than 20 branches or employees is considered to be large scale.

Germany has also issued national advice relating to data processing operations subject to DPIAs, which defines what is meant by large scale. In contrast to other nations advice, the threshold Germany has set is five million people, or those covering at least 40% of the relevant population.

As can be seen, these national guidelines vary quite considerably. It must be noted that the population of Germany is greater than that of the Netherlands, Estonia, or the Czech Republic. This last example raises the question:

Should the size of a nation's population have a bearing on the large scale threshold?

Ultimately, in the absence of clearer guidance, the decision comes down to an organisation's own interpretation. To ensure compliance and to protect the organisation's interests should a data breach occur, the decision to appoint or not to appoint a DPO should be documented, along with evidence to support the ultimate choice.

ARTICLE 37(1) IN-DEPTH CONT.

REGULAR AND SYSTEMATIC MONITORING

The clearest explanation of regular and systemic monitoring comes from the ICO:

> **Regular and systematic** monitoring of data subjects includes all forms of tracking and profiling, both online and offline.
> An example of this is for the purposes of behavioural advertising.

While the GDPR offers no explanation for what regular and systematic monitoring of data subjects actually covers, the WP29 DPO Guidelines point out that a similarly worded concept of **monitoring of the behaviour of data subjects** is mentioned in recital 24.

Here the definition is clear (albeit somewhat wordy) and includes all forms of online tracking or profiling.

Recital 24 states:

> In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

While monitoring of data subjects is a common practice online, the DPO Guidelines reminds data controllers that:

> The notion of monitoring is not restricted to the online environment and online tracking should only be considered as one example of monitoring the behaviour of data subjects.

The DPO Guidelines also provide a granular definition of both **regular** and **systematic**.

Regular is interpreted as meaning one or more of the following:

- Ongoing or occurring at particular intervals for a particular period
- Recurring or repeated at fixed times
- Constantly or periodically taking place

ARTICLE 37(1) IN-DEPTH CONT.

And systematic as meaning one or more of the following:

- Occurring according to a system
- Pre-arranged, organised or methodical
- Taking place as part of a general plan for data collection
- Carried out as part of a strategy

In addition to clarifying what the terms regular and systemic mean, the DPO guidelines have also provided a set of practical examples. The list is not exhaustive but is comprehensive enough for comparison against other processing activities.

Example activities that may constitute regular and systematic monitoring:

- Operating or providing a telecommunications network or services
- Email retargeting and data-driven marketing activities
- Profiling and scoring for purposes of risk assessment (e.g. for the purposes of credit scoring, the
- establishment of insurance premiums, fraud prevention, detection of money-laundering)
- Location tracking, for example, through mobile apps; loyalty programs
- Behavioural advertising
- Monitoring of wellness, fitness and health data via wearable devices
- Closed-circuit television (CCTV)
- Connected devices, e.g. smart meters, smart cars, home automation, etc.

ARTICLE 37(1) IN-DEPTH CONT.

SPECIAL CATEGORY DATA

A DPO is required where processing takes place on a large scale and consists of special categories of data or personal data relating to criminal convictions.

Special categories of personal data
Special category data is similar to the concept of sensitive personal data, referred to in the Data Protection Act 1998. Under the GDPR, special categories of personal data are governed by the principles defined in Article 9.

Article 9(1) states:

Processing of special categories of personal data revealing:

- Racial or ethnic origin
- Political opinions
- Religious and philosophical beliefs
- Trade union memberships or other associations

Or the processing of:

- Genetic data or biometric data used for identification
- Health data
- Data concerning a person's sex life or their sexual orientation

The processing of special categories of personal data is prohibited unless one of the specific grounds set out in the GDPR applies.

These include:

- The data subject providing their explicit consent
- Processing is necessary for carrying out obligations or exercising rights under employment, social security or social protection laws, or under a collective agreement
- The data is required for disclosure purposes in legal claims

ARTICLE 37(1) IN-DEPTH CONT.

When evaluating if a business is obliged to appoint a DPO, close attention should be given to whether special categories of personal data are being processed, as illustrated above.

Broadly adopted marketing practices such as behavioural and location-based advertising or any other methods used to track individuals online, such as scraping data from social media platforms, when conducted on a large scale will require the appointment of a DPO.

Other industry sectors or businesses whose data processing activities will likely be captured by Article 9(1) include:

- Insurance providers
- Private sexual health clinics
- Private medical clinics
- Private education
- Pharmaceutical and medical research organisations
- And certain NGOs who work in areas concerning ethnicity, religion, and race issues

Personal data relating to criminal convictions and offences

Article 10 relates to specific safeguards for data relating to criminal convictions:

> Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

ARTICLE 37(1) IN-DEPTH CONT.

PROCESSING ACTIVITIES UNDERTAKEN BY AN EXTERNAL BODY (PROCESSOR)

If the personal data processing operations fit the criteria to appoint a DPO, this will apply to whether the processing is conducted by a controller or processor.

However, according to the WP29 DPO Guidelines, if a processing activity requires the processor to appoint a DPO, this does not automatically require the controller to take similar steps. The same is also true vice versa.

An example in the DPO Guidelines is as follows:

> A medium-size tile manufacturing company subcontracts its occupational health services to an external processor, which has a large number of similar clients. The processor shall designate a DPO under Article 37(1)(c) provided that the processing is on a large scale. However, the manufacturer is not necessarily under an obligation to designate a DPO.

The DPO elected by a processor also supervises activities carried out by the processor organisation when acting as a data controller in its own right (e.g. HR, IT, logistics).

VOLUNTARY APPOINTMENT OF A DPO

Any business may decide to appoint a DPO, even where there is no legal obligation to do so.

In this situation, the voluntarily appointed DPO will be expected to carry out their responsibilities under articles 37 to 39 as if they are a mandatory appointment.

Regardless of whether the GDPR obliges you to appoint a DPO or not, you must ensure that your organisation has sufficient resources on hand, who possess the necessary level of knowledge in data protection law to carry out the obligations required under the GDPR.

For businesses who are not required to make a mandatory appointment, remember the two key points at the top of this article outlining the advantages of investing in a DPO:

- A DPO can enhance an organisation's reputation, not only with its customers, service users or audience but also with investors and other key stakeholders. As such, a DPO appointment demonstrates stability, a commitment to following compliance procedures, and the availability of resources to manage risks.
- Commercially astute DPOs can quickly identify the opportunities certain data processing activities present, then draft and execute a strategy of how to take advantage of such opportunities in a compliant way with appropriate risk-management in place.

Finally, if you decide that you don't need to appoint a DPO, it is best practice to record this decision to demonstrate compliance with the accountability principle. And, remember to re-visit this conclusion on a periodic basis, or as and when your processing operations change.

NOT APPOINTING A DPO?

Data protection is a senior executive level priority for every business. Regardless of whether or not a company is required to appoint a DPO, it is still a legal obligation to comply with the GDPR.

Failure to do so could leave an organisation open to liability if a breach occurs.

Morrisons Data Breach
Although no cases have been brought under the Data Protection Act 2018 as yet, in the case of Various Claimants v WM Morrison Supermarkets Plc [2018] EWCA Civ 2339, brought under the 1998 Act, the Court of Appeal held the employer was vicariously liable for the employee's acts away from the workplace where those acts formed a sequence of planned events leading to the commission of the wrongdoing. This was the case even though the malicious action was designed to injure the employer as opposed to the data subjects.

This judgment means that where an employer is the data controller, they are highly exposed to potential claims from the victims of a data breach caused by a rogue employee.

The decision of *Various Claimants v WM Morrison Supermarkets Plc* is to be appealed to the Supreme Court. This is the law at the time of writing (April 2019).

When deciding not to appoint a DPO, companies are recommended to take the following actions:

Keep a detailed record of events
Where a business determines that it is not required to make a mandatory DPO appointment and chooses not to do so voluntarily, the executive management team are advised to create a detailed account of the decision-making process.

In the event that the supervisory authority (the ICO) has cause to ask why there is no DPO in place, the company will be able to outline its reasoning. Furthermore, if the business made an error and should have appointed a DPO, the ICO is more inclined to take into account the conclusions arrived at by the companies executives, and offer advice in place of a more harsh alternative.

Make regular assessments
Given that the nature of business is one of change and growth, the decision not to appoint a DPO should be reviewed regularly, especially if there is a change in data processing operations.

It is easy to imagine an organisation unwittingly falling through the gaps of GDPR compliance, simply because following an initial review (perhaps before the 25th May 2018) changes to the personal data processing practices of the company are ignored, with management taking for granted that compliance is still being achieved.

NOT APPOINTING A DPO? CONT.

Appoint a data protection lead

The amount of resource required to oversee GDPR compliance will vary from business to business, depending on the size and complexity of its data processing operation. Just as every company must assess whether to appoint a DPO, so must it determine how the data protection programme will be administered where the services of a DPO are deemed unnecessary.

Without having to follow the strict conditions to appoint a DPO as defined under Article 38, companies have more flexibility regarding who can lead the GDPR compliance process.

It is worth noting, however, that while there is no alternative to making such an appointment, there is no requirement for this position to be internally filled.

The WP29 DPO Guidelines highlights this:

> Nothing prevents an organisation, which is not legally required to designate a DPO and does not wish to designate a DPO on a voluntary basis to nevertheless employ staff or outside consultants with tasks relating to the protection of personal data.

In these situations, there must be no confusion about their position or title and the role they fulfil. Under no circumstances must they be designated the title Data Protection Officer.

For more information about the day to day aspects of GDPR compliance, we take a detailed look into what a business is required to do when not appointing a DPO in the fifth article of the series.

MAKING THE RIGHT DECISION

Most positions in organisations fall into one of two camps.

They are either:

- **A business cost**
- **A revenue generator**

A DPO is one of the few roles which falls into both camps, as long as the correct appointment is made. Not only does a DPO require an in-depth knowledge of data protection laws, both throughout Europe and internationally, and a background in compliance, they also need to understand the practicalities of running a commercial entity.

When appointing a DPO, the best candidate will be one that fits your organisation – taking into account its size and market sector, plus its values and commercial ambitions. Decisions will need to be made regarding whether a full-time DPO is the best way to ensure GDPR compliance, or whether other options, such as making the role part-time or a job-share or appointing an external company is the best way forward.

Like most matters involving the GDPR, on a surface level, the appointment of a DPO seems straight-forward. But dig a little deeper, and it becomes clear that multiple factors need to be considered, and even then, the answer may not be clear. External advice can be invaluable to assist with such a decision

1. The Article 29 Working Party (WP29) was transformed into the “European Data Protection Board” (“EDPB”) under the GDPR

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

The role of the Data Protection Officer

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.

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