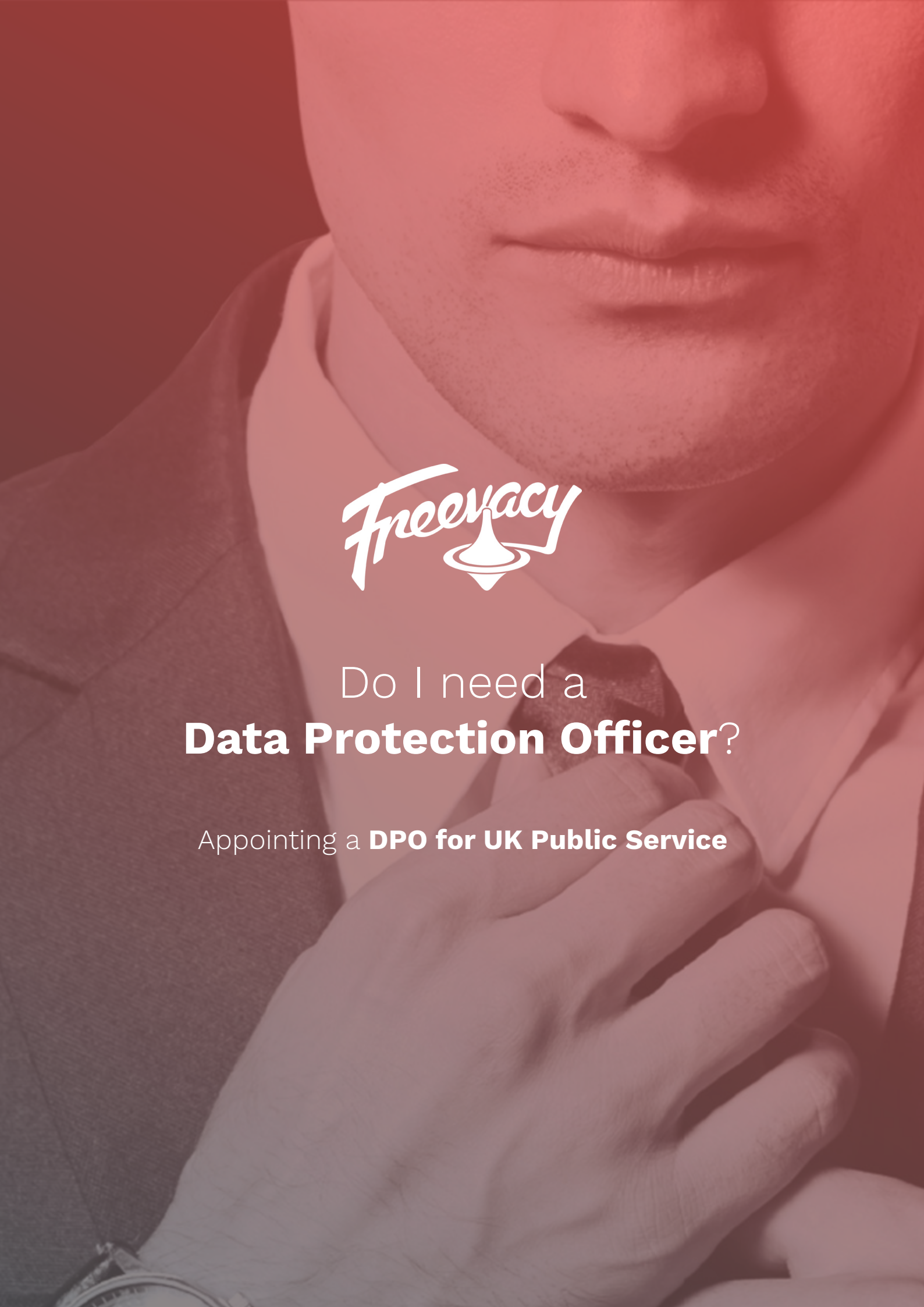

Freevacy

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

Appointing a **DPO for UK Public Service**

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 UK PUBLIC SERVICE

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.

APPOINTING A DPO FOR UK PUBLIC SERVICE CONT.

KEY FACTS ABOUT WHETHER AN ORGANISATION NEEDS TO APPOINT A DPO

- The issue of whether or not an organisation needs to appoint a DPO was a much-amended provision in the GDPR.
- Article 37 governs the three situations where the mandatory appointment of a DPO is required: (a) public authorities or bodies, (b) core activities involving large-scale processing, (c) core activities concerned with processing of special categories of data, pursuant to Article 9 or relating to criminal convictions as per Article 10.
- Private sector companies that have successfully tendered for contracts to deliver public services are advised to appoint a DPO.
- WP29 DPO Guidelines state that simply because a (data) processor is required to appoint a DPO, it does not mean a (data) controller is under the same obligation and vice versa.

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.

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.

The Commission 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.

The decision to appoint a DPO is (with limited exceptions) a foregone conclusion as far as public authorities and bodies are concerned.

This still leaves three questions relating to Article 37(1)(a) that require clarification:

- What is a public authority or body?
- What exceptions apply to public organisations concerning mandatory DPO appointments?
- What constitutes a private organisation delivering public services?

ARTICLE 37(1) IN-DEPTH

To add extra detail to Article 37(1) the following section examines the conditions applying to public authorities and bodies, including commercial organisations delivering public services.

Article 37(1) explicitly states that public authorities and public bodies, along with commercial organisations who have contracts to carry out public functions (for example the running of an immigration detention facility) which process personal data, must appoint a DPO. although, Courts acting in their judicial capacity are excluded.

WHAT CONSTITUTES A PUBLIC BODY OR AUTHORITY UNDER THE GDPR?

The first step in establishing whether a DPO is required is to investigate whether or not the organisation in question is a public authority or body for the purposes of the GDPR.

The GDPR does not provide a definition for a **public body** and therefore, reference must be made to national law. In the UK this is defined under The Data Protection Act 2018 (DPA18), in section 7 and section 21, which states:

1. In England and Wales: a public authority as defined by the Freedom of Information Act 2000 (FOIA), in section 3(2), in schedule 1, and in sections 5(1)(a)

2. In Scotland: a Scottish public authority as defined by the Freedom of Information (Scotland) Act 2002 in schedule 1

3. An authority or body specified or described by the Secretary of State in regulations, so long as they are performing a task carried out in the public interest or in the exercise of official authority vested in it

Note (3) applies to the entire UK.

ARTICLE 37(1) IN-DEPTH CONT.

EXCEPTIONS TO THE PUBLIC BODY OR AUTHORITY REQUIREMENT

Exceptions to the mandatory requirement to appoint a DPO are set out in the Data Protection Act 2018, section 7(3) and (4).

Section 7(3) refers to small local authorities:

> The references in subsection (1)(a) and (b) to public authorities and Scottish public authorities as defined by the Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002 do not include any of the following that fall within those definitions:
>
> 1. A parish council in England
> 2. A community council in Wales
> 3. A community council in Scotland
> 4. A parish meeting constituted under section 13 of the Local Government Act 1972
> 5. A community meeting constituted under section 27 of that Act
> 6. Charter trustees constituted:
> 7. 1. (i) Under section 246 of that Act
>   2. (ii) Under Part 1 of the Local Government and Public Involvement in Health Act 2007
>   3. (iii) By the Charter Trustees Regulations 1996

Under section 7(4), the Secretary of State can in certain circumstances deem a person or organisation not a public body for the purposes of GDPR.

> The Secretary of State may by regulations provide that a person specified or described in the regulations that is a public authority described in subsection (1)(a) or (b) is not a public authority or public body for the purposes of the GDPR.

It is crucial to note that regardless of the exceptions contained in section 7(3) and (4) if the organisation is processing data, it must still comply with all GDPR requirements.

Furthermore, if the processing of personal data is substantial, and/or contains special category data, it may be prudent to appoint a DPO, even if only on a part-time basis.

The ICO has created a GDPR FAQ page for small local authorities.

PRIVATE SECTOR COMPANIES CARRYING OUT PUBLIC FUNCTIONS

There are few areas of the public sector in which private companies are not contracted to carry out services.

For example:

- G4S, Serco, and Sodexo operate privately-run prisons.
- G4S also operates some immigration detention centres and housing accommodation for asylum seekers.
- Health and care services is another area where private companies such as Allied Healthcare provide contracted services on a large scale.

In fact, when you count outsourced IT functions and other back-office services, there are few public functions which are not supported in whole or in part by private organisations.

Where a private company has successfully tendered for a public service contract and is delivering the agreed functions for a public authority or body, the WP29 DPO Guidelines recommend that a DPO is appointed.

It states:

> Even though there is no obligation in such cases, the WP29 recommends, as a good practice, that private organisations carrying out public tasks or exercising public authority designate a DPO. Such a DPOs activity covers all processing operations carried out, including those that are not related to the performance of a public task or exercise of official duty (e.g. the management of an employee database).

WHAT IF YOU ALREADY HAVE A DPO

Some public authorities and bodies appointed a DPO prior to the GDPR coming into force in May 2018. To ensure compliance, these bodies were required to examine the existing role and tasks of the DPO and ensure it matched the requirements laid down by the GDPR.

One of the key factors of an existing DPOs role to examine is whether or not they are independent in a way that satisfies GDPR requirements. In addition, any conflicts of interests need to have been identified and remedied.

SUMMARY

If it is established that an organisation is a public body under section 7 of the Data Protection Act 2018 and is not covered by one of the exceptions set out in section 7(3) and (4), then it is mandatory to appoint a DPO. If a DPO already exists, the role must be examined to ensure it is fully compliant with the GDPR provisions.

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