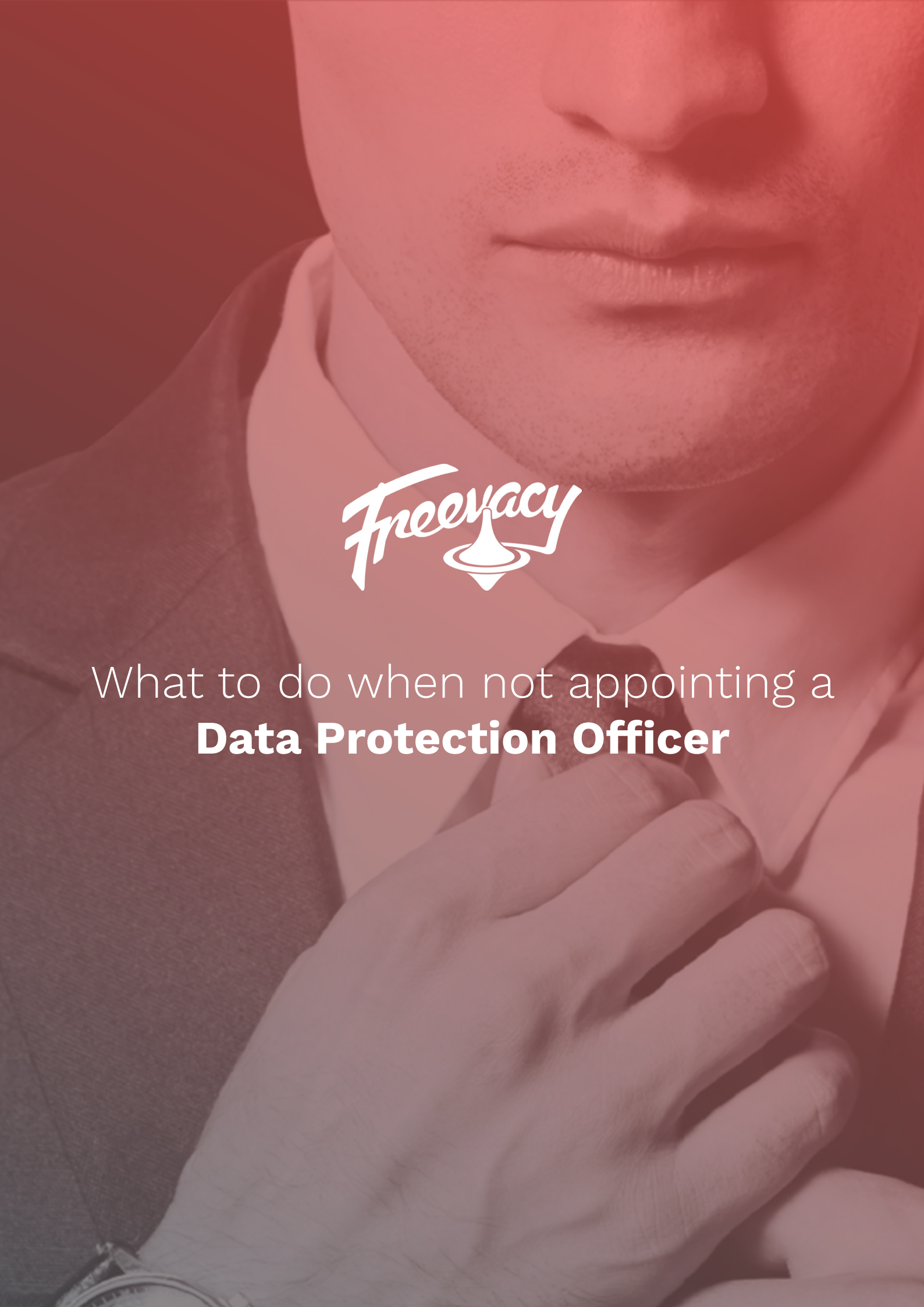


Freevacy

# What to do when not appointing a **Data Protection Officer**

# INTRODUCTION

In this, the fifth of a series of linked articles about Data Protection Officers (DPOs) under the General Data Protection Regulation (GDPR), we discuss how an organisation can implement and maintain a privacy compliance programme when it is not required to appoint a DPO and chooses not to do so voluntarily.

It is important to note, however, that irrespective of whether a DPO is appointed, the maximum financial penalties for breaching the GDPR are the same across the board:

**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.

Complying with the GDPR and the Data Protection Act 2018 (DPA18) is no small measure. In reality, the DPO operates as the central hub from which to disseminate data protection related strategy, communication, or training throughout the organisation. And because the DPO is independent and protected from sanctions for performing their duties, the organisation can be confident that data protection compliance is achieved. This is providing they appoint the right person, of course, and that they act upon any recommendations, advice and guidance being offered.

For companies, charities, and exempt public bodies who do not have a DPO in place, GDPR compliance must be carefully planned and executed. This article lays out how to meet your data protection responsibilities without a DPO and the pitfalls to avoid when putting systems in place.

# CONTENTS

# KEY FACTS FOR MEETING GDPR COMPLIANCE WITHOUT A DPO

- In situations where there is no mandatory requirement to appoint a DPO, choosing not to appoint a DPO voluntarily is nevertheless acceptable, despite the DPO Guidelines recommendations to the contrary. Maintain an accurate record of the decision-making process identifying how a DPO is not required, and revisit the issue regularly to ensure that your circumstances do not change.

- Remember, it is always the organisation that is accountable for GDPR compliance. Even without a DPO, companies, charities, and exempt public bodies are still obliged to satisfy all the GDPR requirements, along with any related regulations and national privacy laws. Not doing so will risk severe sanctions.

- Assign somebody with the responsibility to implement and maintain a data protection programme. A key part of their role will involve record keeping and ensuring policies and procedures are regularly updated and followed.

- To achieve compliance, follow each of the GDPR Principles and ensure that lawful conditions to process personal data are always met. Uphold the remaining rights of the data subjects involving overseas transfers and ensure all processing of personal data complies with the requirements of privacy by design and default. Make sure to implement all physical or technological security measures required within the GDPR.

- Take note. when reporting a data breach under the GDPR, the 72 hours clock starts ticking the moment you become aware of the breach.

- If you take your GDPR responsibilities seriously and implement reasonable measures to protect personal data, then the ICO will recognise your efforts. Treat cybersecurity as a boardroom issue, demonstrate transparency and accountability for your customer data and should the worst happen the ICO will not usually have an issue.

- Meeting GDPR compliance obligations not only results in customer confidence, it also assures investors and lenders that your organisation is professional and well-organised.

# ADVICE AND GUIDANCE ABOUT APPOINTING A DPO (OR NOT)

## ARTICLE 29 WORKING PARTY

The Article 29 Working Party (WP29) Guidelines for Data Protection Officers[1] highly encourages the appointment of a DPO1 to ensure an organisation meets its compliance obligations under the GDPR.

Even if a DPOs appointment is not required under Article 37, the WP29 DPO Guidelines states that organisations may sometimes find it useful to designate a DPO voluntarily.

> The DPO is a cornerstone of accountability and that appointing a DPO can facilitate compliance and furthermore, become a competitive advantage for businesses.
>
> In addition to facilitating compliance through the implementation of accountability tools (such as facilitating data protection impact assessments and carrying out or facilitating audits), DPOs act as intermediaries between relevant stakeholders (e.g. supervisory authorities, data subjects, and business units within an organisation).

## INFORMATION COMMISSIONERS' OFFICE (ICO)

The ICO clearly states on its page for data protection officers that even where no DPO is in place, organisations must still ensure their employees are given all the necessary training and support they require in order to comply with the GDPR.

> Regardless of whether the GDPR obliges you to appoint a DPO, you must ensure your organisation has sufficient staff and resources to discharge your obligations under the GDPR. However, a DPO can help you operate within the law by advising and helping to monitor compliance. In this way, a DPO can play a key role in your organisation's data protection governance structure and to help improve accountability.

As discussed earlier in this series, it is recommended that if you decide not to appoint a DPO, you record the decision and your reasons for it in writing. If something goes wrong, being able to show that you considered the risks can help to reduce the likelihood you will receive any enforcement action from the data protection authority.

# ACCOUNTABILITY AND THE SCOPE OF THE GDPR

It is not the DPO who is responsible for GDPR compliance. The regulation states how it is the organisation that is responsible for adhering to data protection law, along with being able to demonstrate how this compliance is being achieved (accountability).

Article 24(1) defines the responsibilities of the controller:

> Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.

Accountability is a core principle of the GDPR. It requires organisations to put controls in place to measure compliance and thus demonstrate accountability.

The ICO has a page dedicated to accountability and governance, describing its benefits as:

> Taking responsibility for what you do with personal data, and demonstrating the steps you have taken to protect people's rights not only results in better legal compliance, it also offers you a competitive edge.
>
> Accountability is a real opportunity for you to show, and prove, how you respect people's privacy. This can help you to develop and sustain people's trust.

Where a DPO is not appointed, the organisation still needs to show how it complies with the GDPR where it processes personal data.

It is important to note that this does not only apply to organisations based in the EU. Any overseas-based business processing EU citizen's data also needs to maintain compliance. An article written by Privacy International offers an excellent summary of how the GDPR is extraterritorial in its scope, and what that means:

> **Companies based both within the EU and those who target people in the EU are included within GDPRs scope, and thus subject to its obligations, and if they fail to comply its sanctions.**
>
> Why and how GDPR applies to companies globally, Privacy International

“

A DPO alone does not protect the company from breaches nor from penalties.

Instead, it is whether a company has operationalised data protection and is able to demonstrate accountability.

Luis Alberto Montezuma & Qian Li Loke, IAPP

# THE TASKS AND POSITION OF THE DPO

The tasks and postion of the DPO were discussed earlier in the series in the article about the role of the data protection officer. Therefore, they will only be covered briefly here.

Article 39 of the GDPR states:

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.

Article 38(3) states that the position of a DPO should:

1. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks.
2. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks.
3. The data protection officer shall directly report to the highest management level of the controller or the processor.

As such, DPOs must be provided with the resources required to carry out those tasks and be given independence to make decisions related to how best to comply with their tasks.

# APPROACHING GDPR COMPLIANCE WITHOUT A DPO

If a DPO is not appointed, it will be up to the organisation to establish how to achieve GDPR compliance and what measures are required to demonstrate accountability.

Many businesses, charities, and local public bodies who took the decision not to appoint a DPO invested heavily in preparing for the GDPR, before the 25th May 2018.

Those who haven't should begin with the following set of actions:

- Conduct a data audit to identify what personal data is being processed
- Determine the legal basis for which this personal data is being collected
- Update any data protection policies and procedures
- Re-write privacy notices using clear and easy to understand language
- Examine and update supplier contracts to incorporate GDPR clauses
- Keep a record of all matters relating to data protection
- Make regular reviews of the decision not to appoint a DPO
- Provide regular data protection training to employees

## COMPANIES ARE STILL AT RISK

As survey after survey show, many organisations have not made the necessary changes to fully comply with the GDPR, leaving them open to fines and reputational damage.

In particular, the results from a joint survey conducted across 18 countries by the Global Privacy Enforcement Network (GPEN) highlights how organisations should be doing more to achieve privacy accountability.

Established in 2010, GPEN is made up of data protection regulators from around the globe and is currently co-chaired by the UK's ICO and the Office of the Privacy Commissioner in New Zealand. It found that many of the surveyed organisations were not equipped to deal with complaints from data subjects or how to handle data security incidents. Head of Intelligence for the ICO Andy Stevens, said:

“

The findings suggest that whilst organisations contacted by the ICO and our international partners have a good understanding of the basic concept of accountability, in practice there is significant room for improvement.

It is important that organisations have appropriate technical and organisational measures in place. This includes having clear data protection policies, taking a "data protection by design & default" approach and continuing to review and monitor performance and adherence to data protection rules and regulations.

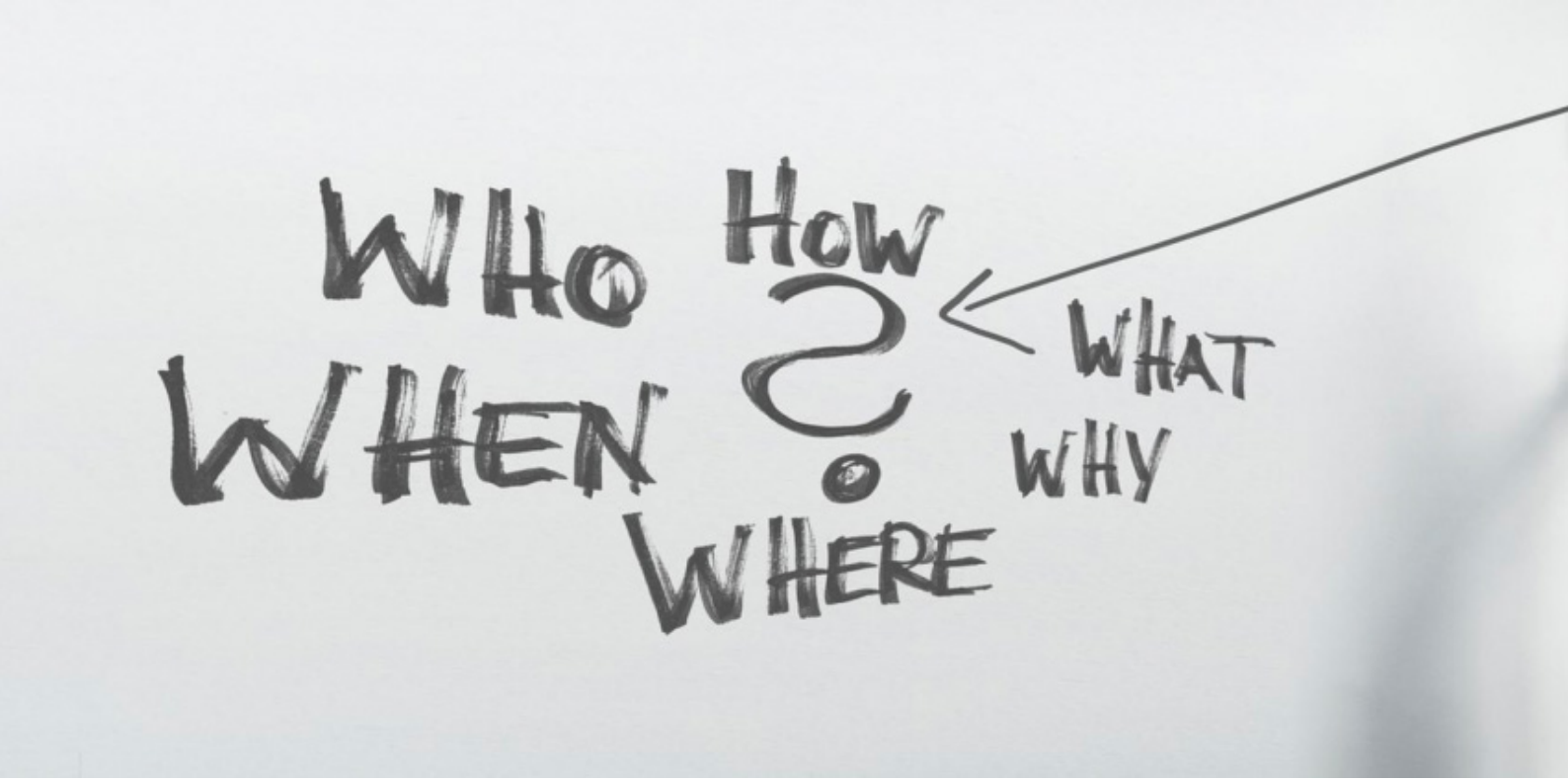
dam Stevens, Head of Intelligence, ICO

# HOW TO MEET KEY AREAS OF GDPR COMPLIANCE WITHOUT A DPO

In this section, we examine three fundamental areas of the GDPR in which the DPO would be involved. One has a direct impact on daily operations, but all are integral to creating long-term strategies, policies, and procedures.  Getting these tasks right will have a significant impact on whether an organisation can achieve GDPR compliance without a DPO.

The three areas are:

- Subject Access Requests (SARs)
- Data Protection Impact Assessments (DPIAs)
- Data Breaches



# SUBJECT ACCESS REQUESTS (SAR)

In a recent blog article, Suzanne Gordon, Director of Data Protection Complaints and Compliance at the ICO, explains in plain language this fundamental right we all have under data protection law.

> **Anyone in the UK has the legal right to find out what information is held about them by organisations and ask for a copy free of charge within one calendar month. This is known as a subject access request (SAR).**
>
> Suzanne Gordon, Information Commissioners' Office

## HOW THE GDPR DEFINES SARS

Article 15 of the GDPR outlines the right of access by data subjects.

Specifically, it says:

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information.

# SUBJECT ACCESS REQUESTS (SAR) CONT.

In addition, the data subject is entitled to any **supplementary Information** that relates to the personal data that you hold on them.

These include:

1. The purposes of the processing
2. The categories of personal data concerned
3. The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations
4. Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
5. The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
6. The right to lodge a complaint with a supervisory authority
7. Where the personal data are not collected from the data subject, any available information as to their source
8. The existence of automated decision-making, including profiling

If data is being sent to a third country (i.e. a State outside the European Union), then the data subject can also ask to see what protections have been put in place to arrange a secure transfer.

## HOW TO HANDLE SARS

It is important to note that a SAR does not have to be submitted formally or specifically labelled as such. Therefore, it is necessary to ensure that everyone in your organisation is trained on how to interpret when a SAR is delivered, be it verbally or electronically.

To ensure each SAR is handled correctly, clear and concise policies should be in place, so every instance is handled consistently.

Your policy should include steps to:

# SUBJECT ACCESS REQUESTS (SAR) CONT.

- Log and date all SAR requests
- Verify the identity of the requester to ensure they are genuine
- Acknowledge receipt of the SAR
- Obtain any additional information required to complete the request
- Identify the requested personal data and supplementary information
- Ensure staff understand SAR completion timescales (1-month in most cases)
- Use consistent and plain language to answer the request
- Handle third-party data within requested personal information
- Ensure staff know how to handle requests from third-parties
- Identify when a SAR should be refused

If your IT systems allow it, you may find it more efficient to set up a **self-service** portal which enables users to access information regarding the personal data your organisation holds for themselves.

Things can get tricky where a business, charity, or small local authority outsources its personal data processing functions to an external body (Processor). In these cases, it is imperative to ensure that every supplier contract (Processor Contract) includes provisions for GDPR compliance. The ICO makes it explicitly clear that the controller is responsible for complying with SARs and therefore, your processing contracts must ensure you can meet your obligations within the time-frame.

Finally, it is best practice to record compliance with each stage of the SAR policy for every request. That way, if a complaint is made, you have evidence to show you took all appropriate steps required.

# DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Article 35, defines the data protection impact assessments (DPIAs), which is a critical new compliance obligation under the GDPR.

Their purpose is to help identify and minimise any risks in your data processing activities that, if left unchecked, have the potential to cause harm. DPIAs are mandatory in certain situations and play a central part in demonstrating accountability.

As a tool, the DPIA forms part of the data protection by design approach which is used proactively in the early development stages of a product, service or process, as well as throughout its lifecycle.

## HOW TO HANDLE DPIAS WITHOUT A DPO

A key task of a DPO is to manage and communicate DPIAs.

Because a DPO is independent and reports to the highest level of management, they are perfectly placed to advise and oversee the undertaking of a DPIA as they can operate at a strategic level within the organisation. And crucially, a DPO cannot be dismissed for performing their duties in terms of providing advice and guidance. For example, the DPO may give an opinion regarding an identifiable risk concerning the processing of personal data which is subsequently ignored, despite the fact the advice has been received at the highest level. In such a case, if the DPO informs the ICO regarding a serious risk or breach, they cannot be dismissed for taking such an action.

Organisations which choose not to appoint a DPO must find a way to:

- Ensure a DPIA is conducted when necessary, and
- Provide GDPR guidance to any project leader conducting a DPIA and when to hold one, even if such decisions require the organisation to invest capital to protect personal data or shelve the project altogether if the risk is deemed too great.

Often this is achieved by outsourcing the task to a specialist in GDPR compliance. In such cases, it is essential that the person carrying out the DPIA is provided with all the necessary information regarding the project and has someone in the organisation they can liaise with to clarify any questions.

## WHEN IS A DPIA REQUIRED?

Article 35(1) requires that data protection impact assessments (DPIAs) are needed if a particular data processing activity is:

> Likely to result in a high risk to the rights and freedoms of natural persons.

# DATA PROTECTION IMPACT ASSESSMENT (DPIA) CONT.

High-risk activities are deemed to include:

- Systematic and extensive profiling
- Processing special categories of data (see Article 9 & 10)
- Systematic monitoring of publicly accessible areas on a large scale

The WP29 has published guidelines on Data Protection Impact Assessment outlining nine areas (summarised here by the ICO), which constitute high-risk:

- Evaluation or scoring
- Automated decision-making with legal or similar significant effect
- Systematic monitoring
- Sensitive data or data of a highly personal nature
- Data processed on a large scale
- Matching or combining datasets
- Data concerning vulnerable data subjects
- Innovative use or applying new technological or organisational solutions
- Preventing data subjects from exercising a right or using a service or contract

It is worth noting, that in accordance with Article 35(4) the supervisory authorities for each EU Member State are obliged to submit draft DPIA lists to the EDPB classifying their high-risk data processing activities which will require a DPIA.

Ultimately, however, as the ICO explains on its dedicated DPIA page:

> It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

# DATA PROTECTION IMPACT ASSESSMENT (DPIA) CONT.

In her article, A practical guide to conducting data protection impact assessments[2], published in the Privacy and Data Protection Journal, Sandy Tsakiridi states:

> **A DPIA should be carried out sufficiently early and in any event, prior to the actual processing, which is in line with the privacy by design and by default requirement of the GDPR. From an operational point of view, considering DPIAs at the outset of a new project (as opposed to enacting changes further down the line) will require less time and resources. Therefore, DPIAs should not be an afterthought, but rather addressed at the planning stage.**
>
> Sandy Tsakiridi, Fieldfisher

It is unlikely that businesses, charities and local authorities operating without a DPO will have a defined DPIA process. Furthermore, DPIAs may only be necessary on an ad hoc basis. The issue for organisations like these is that conducting a DPIA could end up being a time-consuming and costly exercise.

As the GDPR does not provide specific criteria about the form or structure of a DPIA, it means organisations can develop a suitable process that reflects the nature, size and complexity of their processing operations. It should be more cost effective too.

## WHAT TO INCLUDE IN A DPIA

The ICO states that a DPIA should contain the following elements:

- A description of the nature, scope, context, and purposes of the processing
- An assessment of the necessity, proportionality, and compliance measures
- Identification and assessment of the risks to individuals
- Identification of any additional measures to mitigate those risks

# DATA PROTECTION IMPACT ASSESSMENT (DPIA) CONT.

For further advice, the ICO provides a detailed online DPIA resource.

According to the ICO, a good DPIA will provide proof that:

- you have considered the risks related to your intended processing
- you have met your broader data protection obligations

Lastly, the WP29 guidelines state that all major elements of the DIPA should be recorded, and controllers should consider publishing a summary or conclusion of their DPIA so it can be referenced by data subjects.

# DATA BREACHES

Hardly a day goes by without news breaking of a serious data breach resulting in the loss of information belonging to millions of people. These incidents happen so frequently now that the likelihood your personal data is on sale on the dark-web is almost inevitable.

Not all data loss is down to international corporations or tech companies, however. The reality is, data breaches affect every organisation, regardless of size, sector, or location. Whether its the result of a sophisticated cyber-attack, a rogue employee acting out, or a simple human error, the number of incidents leading to the loss of personal data are becoming increasingly more common.

To give an indication of the scale of the problem, the European Commission released an infographic outlining the GDPR in numbers on the first anniversary of the regulation becoming applicable. The data was compiled by the EDPB using statistics recorded from all 28 EU Member States. In total, 144,376 queries and complaints were recorded, along with 89,271 personal data breach notifications. In the UK, the ICO also released an update: GDPR one year on, in which it reports over 40,000 data protection complaints and 14,072 personal data breaches, up from 3,300 the year earlier.

## WHAT HAPPENS AFTER A DATA BREACH IS REPORTED TO THE ICO

The ICO is clear how it will not hesitate to act where any organisation is either willfully or negligently in breach of data protection law.

The ICO objectives for taking regulatory action following a data breach include:

- We will respond swiftly and effectively to breaches, focusing on those involving highly sensitive information, adversely affecting large groups of individuals or those impacting vulnerable individuals.
- We will be effective, proportionate, dissuasive and consistent in our application of sanctions, targeting our most significant powers on organisations and individuals suspected of repeated or willful misconduct or serious failures to take proper steps to protect personal data.

Of the 14,072 personal data breaches reported to the ICO, 12,000 were closed within the year. Of these, the first 82% required no further action. The next 17.5% of organisations were advised to take some action. In fact, only 0.5% of cases resulted in either an improvement plan or a monetary penalty.

On the one hand, these figures confirm there is a tendency to over-report. However, they also highlight how the ICO will take a more favourable approach with any organisation that has implemented a privacy compliance programme.

# DATA BREACHES CONT.

> **Treat personal data with respect, follow data protection law, and notify the authorities if something goes wrong. Statistics show the ICO is far more lenient to businesses who adhere to the GDPR than those who do not.**
>
> Joyce Allen, CIPP/E, BCS Practitioner in DPA18 & FOIA | Freevacy

## THE GDPRS PROVISIONS FOR REPORTING A PERSONAL DATA BREACH

Recital 87 sets out the reasoning behind the requirement to notify the supervisory authority and the data subject of a personal data breach under the GDPR.

It states:

1. It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject.

2. The fact that the notification was made without undue delay should be established taking into account, in particular, the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject.

3. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

Furthermore, Article 33(1) goes on to state:

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

# DATA BREACHES CONT.

## WP29 GUIDELINES ON PERSONAL DATA BREACH NOTIFICATION

In February 2018, the WP29 published updated guidelines on data breach notification. One of the many aspects the information clarifies is when an organisation is deemed to have knowledge that a data breach has occurred.

It states:

> WP29 considers that a controller should be regarded as having become **aware** when they have a reasonable degree of certainty that personal data has been compromised.

The guidelines go on to say:

> The controller is required to implement all appropriate technical protection and organisational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects.

In the absence of a DPO monitoring risks, it will fall on the IT department to ensure the organisation has suitable policies and up-to-date tools required to spot a data breach.

Also, the WP29 makes clear:

> The emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required.

## WHERE A PROCESSOR IS INVOLVED

A processor has a duty to inform a controller immediately after a data breach is known to have occurred. Therefore, if you are contracting out any data processing functions to an external body, due diligence must be completed on the processor's own ability to comply with Article 33 principles (as well as the GDPR overall).

The ICO confirms this on its page dedicated to personal data breaches, stating:

> If you use a processor, the requirements on breach reporting should be detailed in the contract between you and your processor, as required under Article 28.

To assist organisations further, the ICO has published guidance on contracts and liabilities between controllers and processors.

# DATA BREACHES CONT.

## HOW TO RESPOND TO A PERSONAL DATA BREACH

First of all, it is important to understand what constitutes a personal data breach.

The definition of a data breach is broader than simply losing an individual's personal information. In reality, it covers any security incident that leads to the unauthorised disclosure or access to personal data.

For example:

- Unauthorised access by an external individual, organisation or body
- Deliberate or accidental access by an unauthorised employee
- Sending personal data to an incorrect recipient
- Loss or theft of unencrypted computing devices that contain personal data
- Altering personal data without permission
- Loss of availability of personal data

## REPORTING A PERSONAL DATA BREACH

In the UK, the ICO is the supervisory authority to report a personal data breach. Before getting in contact, prepare a detailed and accurate assessment of the breach.

The information you prepare should help to:

- Explain what has happened
- Outline when and how you discovered the breach
- Confirm who has been affected
- Identify what harm has potentially been caused
- Propose what you are doing to mitigate the impact

The GDPR recognises how not all the information will be available immediately after having become aware of a breach. It advises that the details may be provided in phases providing there is no undue delay. However, it is important that every action taken is recorded in writing so the ICO can check for compliance.

# DATA BREACHES CONT.

## NOT SURE WHETHER TO REPORT A BREACH?

The ICO has produced an online data breach self-assessment tool to help determine if notification is necessary.

## NOTIFY THE DATA SUBJECT

In addition to reporting a breach to the ICO, any affected data subjects may also need to be informed.

Article 34 covers the communication of a personal data breach to the data subject.

It states:

> When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

Let affected users know using language that is easy to understand:

- What has happened
- A point of contact they can deal with
- The potential implications of the breach
- What is being done to minimise the impact

However, data subjects do not require to be personally informed providing:

- The data was encrypted (or similar appropriate measures)
- Subsequent actions have minimised the high-risk to data subjects
- Public communication to the data subjects is provided instead

# FINAL THOUGHTS

For the many mid-sized companies to large corporates who have chosen not to appoint a DPO, their compliance teams, legal representatives, and IT departments will need to work together in order to accomplish the tasks laid out in Article 39.

It is a different situation for smaller businesses, charities and exempt public authorities or bodies, where the luxury of being able to draw on talent from various teams may not be available, and the cost of outsourcing such expertise will likely be prohibitive.

It is clear how the advantages of compliance extend far beyond simply being able to avoid a large fine and a damaged reputation. By having the right policies and procedures in place, keeping accurate records, and ensuring staff are given the training and support they need, data protection can become a streamlined and organised process. Not only does this provide reassurance to customers, but investors and lenders are also more confident in working with organisations who have a clear and robust compliance system in place. Therefore, ensuring that the role of a DPO is carried out regardless of an official appointment is a sound investment.

Lastly, if you choose not to appoint a DPO, then you must not under any circumstances call the individual overseeing privacy compliance a Data Protection Officer. Anyone with this title is required to fully comply with the statutory requirements of that role, including notifying the ICO. Call this person a data protection manager, or assistant, or advisor - basically anything other than an officer.

1. The Article 29 Working Party (WP29) was transformed into the “European Data Protection Board” (“EDPB”) under the GDPR
2. Tsakiridi, S (2018) A practical guide to conducting data protection impact assessments, P. & D.P. 2018, 18(7), 13-15

# 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

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