

# AXIA COMPLIANCE

## DPO as a service (Virtual DPO)

### What is a data protection officer?

A Data Protection Officer (DPO) is an experienced data protection consultant who helps your business meet and maintain data protection regulations, as well as give advice and guidance on all data privacy matters. A DPO plays a crucial role in protecting personal data within your organisation, helping maintain GDPR compliance.

### Is a DPO mandatory?

For many businesses, a full-time individual in this role is not required and also expensive so outsourcing to a data protection professional can alleviate workload on employees and provide an objective perspective on compliance.

### Do we need a data protection officer?

The GDPR stipulates that an organisation **must** appoint a statutory Data Protection Officer (DPO) if any of the following apply:

1. The organisation is a public authority or body;
2. As part of its core activities the organisation monitors individuals regularly and in a systematic way on a large scale. For example, tracking and monitoring individual's behaviour, such as on the internet or on CCTV; or
3. As part of its core activities the organisation processes large volumes of special category data (i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data about a person's sex life or sexual orientation) or criminal conviction or offence data.

However, if an organisation does not meet the triggers for a statutory DPO, they may still decide to appoint a voluntary DPO.

Appointing a DPO voluntarily is also advised as this highlights data protection compliance and provides a point of contact for data subjects and regulators. It is worth noting that if an organisation decides to voluntarily appoint a DPO, the statutory requirements set out in the GDPR will apply to the voluntary DPO in the same way as if a mandatory DPO appointment was required.

This includes the requirement for the DPO to act independently, to fulfil the duties set out in the GDPR and to be provided with adequate resources to fulfil those duties.

# AXIA COMPLIANCE

## **What if we decide not to appoint a data protection officer?**

Provided that you are not required to appoint a DPO, because you aren't caught by any of the criteria set out in the GDPR, there is no problem with you deciding not to appoint one. However, it is important that you are confident in your assessment as if a DPO is not appointed, when one is required, the organisation will be in breach of the GDPR, and at risk of an administrative fine of up to 2% of annual global turnover or about £8.5 million, whichever is greater and/or enforcement action.

## **What are the benefits of outsourcing the role?**

Whilst the DPO can form part of an internal role it is important that the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests. Many internal DPOs that we speak to say that this can often be a challenge, and they can feel conflicted between the statutory duties that they have as a DPO and the other elements of their role which can drive them towards a decision that is more in line with the commercial objectives that they know the business is trying to achieve. This is one of the main benefits of outsourcing the role, as it enables the organisation to maintain the independent status of a DPO, and to remove any questions around whether a DPO has been subject to a conflict of interests when making decisions in relation to the processing of personal data by the organisation.

Another major benefit of outsourcing the role is that you can be confident that the outsourced DPO has a full understanding of the statutory obligations that must be complied with when undertaking the role and has adequate resources to fulfil those duties. Again, this can often be a challenge to those individuals that perform the role of the DPO internally alongside other responsibilities, as they can find that they don't have the bandwidth to fulfil the DPO responsibilities to the level that they would like and can therefore find themselves unable to properly assess the data protection risks that an organisation is carrying or to become a blocker in the process.

And finally, outsourcing the role can provide organisations with the opportunity to benchmark what they do against other organisations in a similar sector or of a similar size, as the outsourced DPO will often have experience of working with other organisations and with the ICO. They will therefore be able to bring that perspective to the table and provide you with the confidence that you are handling a matter, for example a data breach, in the way that the ICO expect.

## **How can AXIA Compliance help?**

An AXIA DPO consultant can help with all data protection related matters, including monitoring internal compliance, informing on data protection obligations, and acting as a contact point for the supervisory authority and data subjects.

# AXIA COMPLIANCE

The responsibilities of a DPO include:

- o ICO registration
- o Data breach support and response (including liaison with the ICO)
- o Breach response
- o Data subject access request support (SAR)
- o Policy and procedure support and advice
- o Both UK and EU representation
- o Data mapping support and advice
- o Data Protection Impact Assessments (DPIAs)
- o Assisting with customer questionnaires and due diligence
- o General GDPR support
- o Arranging GDPR staff training

## Scalable pricing, tailored to your business

Every business is unique, so we offer tailored pricing to suit your business and regulatory needs. We recommend talking to our expert DPO team who ensure you get the best value.

## What is included in the AXIA DPO Service?

Our Virtual DPO Service includes all the services below:

DPO SERVICE		DESCRIPTION	
Support type		Named individual DPO	
Hours		8 hours monthly	
GAP ANALYSIS			
Comprehensive Gap Analysis		A detailed assessment and report with actionable insights	
Remediation & Improvement Plan		A strategic plan to address identified gaps and support enhanced compliance	
Implementation Plan		Executing the recommended plans to support compliance and improve data protection practices	
DATA PROTECTION GOVERNANCE			
Registration requirements		Registration requirements of DPO with the supervisory authority	
Registration as a controller or processor with the supervisory authority		Assist with your registration as a controller or processor with the supervisory authority	

# AXIA COMPLIANCE

## Establishing Data Protection Governance Structures

Developing and supporting the formation of a robust data protection framework, including the development of a privacy office and defined roles and responsibilities, such as privacy champions

### Data protection and privacy operations

Records of Processing Activities (ROPA)



Conducting Legitimate Interest Assessments (LIA)



Performing Data Protection Impact Assessments (DPIA)



Supporting privacy by default and design



Supporting Data Subject Rights (DSR) requests



Cross-border transactions



Incident and breach reporting



### Policies and procedures

#### Core policies

**Review of existing policies and/or updating/writing of new policies, including**



Website Privacy Notice



Employee Privacy Notice



Data Protection Policy






Data Processing Agreement



Data Retention Policy



# AXIA COMPLIANCE

Data Subject Rights Policy,	
Incident/Breach Policy	
Training Policy and logs	
<b>Additional policies</b>	
<b>Review of existing policies and/or review of outstanding/missing policies, including</b>	
Acceptable Usage Policy	
BYOD	
Access Control Policy	
Social Media Policy	
Business Continuity Plan	
Whistleblowing Policy	
Other bespoke policies / procedures and additional logs on request	Time and materials
DPO meetings with Board or Committee (max 1 hour 30 minutes)	Up to three meeting per year
Interim progress report (at 6 months)	
Full progress report (at 12 months)	
<b>Training and awareness</b>	
Overview of data protection laws for Senior Management	
Pre-recorded GDPR training materials for employees.	

# AXIA COMPLIANCE

<b>Vendor management and due diligence contractual agreements:</b>	Time and materials
DPAs, IGTA's, SCC's, TIA's. Strategic support and advice on legal documents included.	
<b>Legal assistance with vendor management:</b>	Time and materials
Due diligence, negotiations, preparing contracts, reviewing contracts	
Audits (e.g. preparing for ICO visit, regulatory reviews or review of a function)	Time and materials