



Below is an example of how our Pseudo Data Protection officer Scheme works in practice.

Who must appoint a DPO?

Under the GDPR, both controllers and processors must appoint a DPO in certain specified circumstances. Article 35 makes it clear that the obligation to appoint a DPO applies: -

- To all public authorities processing personal data (except for courts acting in their judicial authority); or
- Where the “core activities” of an entity involves “regular and systematic monitoring of data subjects on a large scale“; or
- Where the “core activities” of an entity involves “large scale” processing of “special categories of data” (such as data concerning health, racial or ethnic origin, political opinions, religious or philosophical beliefs.).

As yet the term ‘large scale’ has not been defined. Also note the processing must be ‘core’ to the business.

The duties of a DPO?

- Informing and advising the controller or processor and its employees of their obligations to comply with the GDPR and other Union or Member State data protection laws.
- Monitoring compliance with the GDPR and other Union or Member State data protection laws, including managing internal data protection activities, training data processing staff, and conducting internal audits.
- Advising with regard to data protection impact assessments.
- Serving as the contact point for, and cooperating with, the relevant DPA on issues relating to the processing of personal data.
- Being available for inquiries from data subjects on issues relating to data protection practices, withdrawal of consent, the “right to be forgotten”, and related rights.

Rights of a DPO

- Companies must provide DPOs with the necessary company resources to fulfil their job functions and for their own ongoing training.
- DPOs must also have access to the company’s data processing personnel and operations, significant independence in the performance of their roles, and a direct reporting line “to the highest management level” of the company.
- DPO’s are shielded from dismissal or penalty for performing their tasks from within its employee base.

Must a DPO be qualified?

The GDPR does not identify the precise credentials DPOs must carry, but does require that they have “**expert knowledge of data protection law and practices.**”

A DPO may be either an employee of the organisation or an external third party providing DPO services.

Outsource your DPO Responsibilities to the Experts

EXAMPLE Assuming a client has a single site office, employs a medium number of staff, say 50 employees, some of which work from home, and they have the usual organisation structure; HR, Finance, Marketing, Fundraising, Sales, Retail etc, we could take on the responsibility of named DPO for them. A member of staff would still need to be employed by the organisation to perform the day to day role, and implement our instructions, however, the Griffin House Consultancy will be the named DPO and external oversight.

Process

1. Perform initial audit
2. Issue audit report & recommendations (This may require remedial action)
3. Appoint & Name GHC as DPO
4. Decide on correct remote support plan depending on requirements
5. GHC to conduct onsite or remote regular reviews

Fees will depend on individual circumstances. Contracts are issued for a minimum two year period, a formal quote will be issued and all fees are plus expenses & VAT

Why outsource?

- Specialist Expertise as and when you need it
- No employment contracts/pensions etc
- Minimal training of staff internally
- External oversight of processes
- Due diligence defence in case of breach
- Reliability and Consistency
- Knowledgeable, Experienced Privacy Experts, Consultants & Trainers
- Proactive guidance to identify problems before they become an issue
- Protection of brand and reputation

Griffin House Consultancy, Griffin House, Wickenby, LINCOLN, LN3 5AB, UK

| T. +44 (0) 1673 885533 | E. enquiries@griffinhouseconsultancy.co.uk | W. www.griffinhouseconsultancy.co.uk |