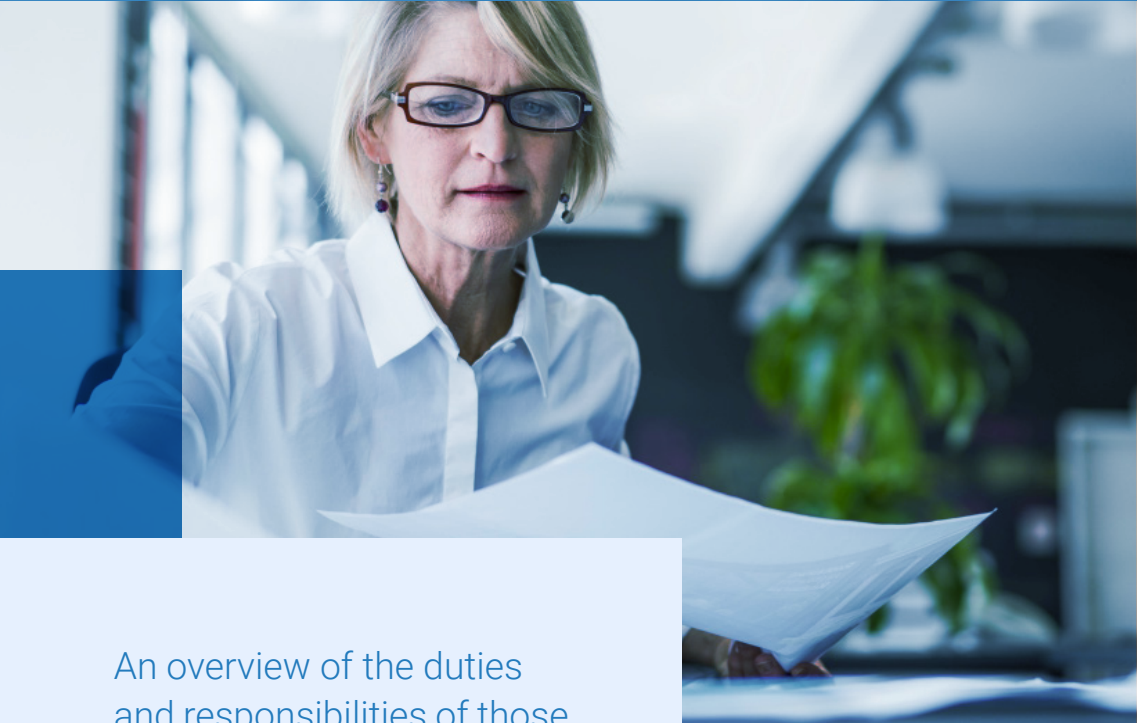




10 MINUTE GUIDE

# The Data Protection Officer



An overview of the duties and responsibilities of those who ensure compliance with data protection law.

Privacy Made Practical<sup>®</sup>

# What is a Data Protection Officer?

A Data Protection Officer (DPO) works within your organisation to ensure your compliance with data protection law – the GDPR, the UK Data Protection Act 2018, and any other laws that may apply, like the Privacy and Electronic Communications Regulation 2003 (PECR).

The DPO has the following minimum duties:

- Monitor compliance
- Provide advice on data processing and data protection
- Act as your contact point with the regulator
- Carry out risk assessment and risk management with regards to data processing

The DPO needs to be involved with all issues of processing personal data. They must be kept informed of your organisation's processing, and should be consulted whenever decisions are taken about processing.

The DPO doesn't make decisions – that's your responsibility – and they're not involved in implementation. Their job is to provide advice and guidance, and to hold you to account. As a result, they have to be demonstrably independent. The law says that:

- A DPO must receive no instruction from their organisation on how to carry out their duties
- The DPO must report directly to the top level of management
- You may not dismiss or discipline a DPO for carrying out their duties

The DPO doesn't have to be responsible for maintaining your records – Data Protection Impact Assessments, Data Catalogues, Records of Data Processing, Risk Registers and so forth – but this is often an additional task they perform.





## Who needs a DPO?

Your organisation **must** have a DPO if any of the following apply:

- You are a public body – a part of government, a non-departmental public body or a government-funded public service.
- You carry out large scale processing of sensitive information or criminal record data. Sensitive information is formally known as “Special Category Data” as defined in Article 9 of the GDPR, and includes health information, sexuality and sexual behaviour, religious and philosophical beliefs, political beliefs and allegiance and trades union membership.
- Your core activity involves regular and systematic and large scale monitoring of data subjects.

*Note that this section is specific to the UK. Each country in Europe has some latitude to change the requirements for having a DPO, so if you operate outside the UK you need to check your local version of the law.*

Unhelpfully the GDPR itself contains no definitions of “large scale”, “regular”, “systematic” or “monitoring”. However, the Article 29 Working Party – which is the rather clunky name for the collective of European data protection regulators – has published extensive guidance in this area, which is in the references at the end of this paper.

The very short version is that if you’re in the business of processing data – like a marketing agency, or a private security firm, or an insurer – you must have a DPO.

If you process special category data or have a lot of data about people (including for instance detailed financial information) and you’re a multi-person organisation, not a single individual – like a school, a GP practice or an accountancy firm – then you need a DPO.

The Working Party also suggests that it’s good practice to appoint a DPO if you are a private organisation which carries out a public function – they see this as an extension of the requirement for all public bodies to have a DPO.

## Who can be your DPO?

Your DPO doesn't have to be full time or an employee. You can use a contractor, or a service; you can also share a DPO with other organisations.

What's most important is that you demonstrate that the DPO has no conflict of interest and is independent. This means that the DPO cannot be involved in decision-making about what data you process, how you process it and why. They can only give advice.

As a result, you can't combine the DPO role with a senior management position (CEO, CFO, Partner, Head of IT etc) or with any role that's involved in implementing your data processing – so usually that rules out other people in your IT and marketing departments as a minimum.

There are also specific rules about the competence of the DPO. In the legislation, these are expressed in quite vague terms, but it's clear that the regulation expects local regulators both to enforce these rules and to develop more specific guidance. In short, they have to have:

- An appropriate level of expertise – either from experience or by qualification;
- The right professional qualities – meaning knowledge both of regulation and of your sector and your organisation in particular;
- The ability to fulfil their tasks – this relates both to personal qualities such as integrity and professional ethics and to their authority and position within your organisation.

Your organisation has to support the DPO with the necessary resources to perform their role: Key points here include:

- Support from senior management
- Sufficient time to fulfil their duties
- Adequate budget, infrastructure and staff
- Continuous training





## Why use a service instead of hiring someone?

As you will have seen from the rest of this paper, appointing an internal DPO is a hard circle to square for many organisations. Covering the requirements for independence, expertise, ongoing support and training and adequate resources while not combining the role with any senior decision-making means an expensive recruit who will be hard to motivate and retain.

Using the Securys DPO service gets you a properly independent view, with substantially greater resources behind it than you are likely to want to fund on your own. Our commitment to quality, including the maintenance of a wide range of formal data protection and information security qualifications lets you show your customers that you take their privacy seriously.

We also take on the continuous training obligation and ensure that you receive continuity of service. The DPO service is combined with our Helpline, so you can turn to us for a broad range of data protection and cyber security advice as part of the package, and we can provide ready-made templates for all of your record keeping and documentation and help you complete and maintain them.

## Further reading and references

[Securys DPO-as-a-service](#)

[Full text of the GDPR \(see Articles 9, 10, 37 and 38\)](#)

[ICO guidance on the DPO role](#)

[Article 29 Working Party guidance on the DPO](#)

[Article 339 of the Treaty of Lisbon \(referenced under duty of confidentiality in the A29WP guidance\)](#)

# About Securys

Securys is a specialist data privacy consultancy with a difference.



Download the eBooks here:

[Privacy Made Positive from Securys](#)

We're not a law firm, but we employ lawyers. We're not a cybersecurity business but our staff qualifications include CISSP and CISA. We're not selling a one-size-fits-all tech product, but we've built proprietary tools and techniques that work with the class-leading GRC products to simplify and streamline the hardest tasks in assuring privacy. We're corporate members of the IAPP, and all our staff are required to obtain one of more IAPP certifications. We're ISO 27001 and ISO 27701 certified and have a comprehensive set of policies and frameworks to help our clients achieve and maintain certification. Our relentless focus is on practical operational delivery of effective data privacy for all your stakeholders.

We're not just a consultancy. We're your privacy engine room. We can stand in your boardroom and do strategy with the best of them, and work with your compliance teams to solve knotty problems. We can audit your compliance and deliver drillable risk dashboards across the organisation. But above all, we can get involved at ground level and help your frontline teams get the job done. That's Privacy Made Practical™.

