



Global Data Privacy Experts

The Data Protection Officer

10 MINUTE GUIDE

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



Privacy Made Practical®



Visit www.securys.com.jm to discover more.

What is a Data Protection Officer?

A Data Protection Officer (DPO) works within your organisation to ensure your compliance with relevant data protection legislation and any other laws and regulations that may apply.

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;
- Assisting individuals in the exercise of their rights.

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

The DPO doesn't make business decisions – that is your responsibility – and they are not involved in implementation. Their job is to provide advice and guidance, and to hold your organisation 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;
- In most countries, you may not dismiss or discipline a DPO for carrying out their duties.

The DPO does not 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 an additional task they may perform.

We'll ensure you're compliant and help you process data efficiently and ethically.

Visit www.securys.com.jm
to discover more.

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 personal data or criminal record data. Sensitive personal data varies by country, and usually includes health, religious, or political data, but in certain countries can include financial or criminal data;
- Your core activity involves regular large-scale monitoring of data subjects.

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 very likely need to 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 not a single individual – like a school, a GP practice or an accountancy firm – then you very likely need 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 outsource your needs; you can also share a DPO with other organizations.

You cannot 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:

- Expertise – either from experience or by qualification.
- The right professional qualities – meaning knowledge both of regulation and of your sector and your organization 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 organization.

We'll ensure you're compliant and help you
process data efficiently and ethically

Visit www.securys.com.jm
to discover more.

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?

Appointing an internal DPO can be a hard circle to square for many organizations. 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 outsourced DPO as a service gets you an independent view with substantially greater resources than you are likely to be able to fund on your own. Our commitment to quality, while maintaining a wide range of formal data protection and information security qualifications, highlights to your customers that you take their data privacy seriously.

We also make sure that your organization is trained as required, while avoiding individual points of failure associated with having a small data privacy function. Our outsourced DPO as a service is combined with our Helpline and Assisted Compliance offering meaning you can turn to us for a broad range of data protection and information security advice as part of your package. As part of our support, we can provide ready-made templates for all of your record keeping and documentation and help you complete and maintain them.

We'll ensure you're compliant and help you process data efficiently and ethically.



About 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.



Download the eBooks here:

Privacy Made Positive from Securys

We're not just a consultancy. We're your privacy engine room. We can stand in your boardroom and do strategy with your top team, 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®.

