

Virtual Data Protection Officer (DPO)

What is a DPO?

The General Data Protection Regulation (GDPR) places significant emphasis on accountability and governance around the handling of data within organisations.

One of the requirements, depending on the activities of an organisation, is to appoint a Data Protection Officer (DPO).

DPOs will be responsible for informing and advising the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.

They are also charged with monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments, training staff and conducting internal audits.

DPOs are also the first point of contact for supervisory authorities and for individuals whose data is processed, including staff and customers...



...Under the GDPR, (Article 37), there are three main scenarios where the appointment of a DPO by a controller or processor (e.g. outsourced service providers) is mandatory.

A DPO must be appointed by most public authorities and by organisations carrying out large scale systematic monitoring of individuals or large scale processing of special categories of data in areas such as health, religion, race, sexual orientation and personal data relating to criminal convictions and offences.

Businesses should consider carefully whether they are required to designate a DPO. Guidance issued by EU's Article 29 Working Party on the role of a DPO makes it clear that all businesses should consider voluntarily appointing a DPO; and if a business chooses not to appoint a DPO the Guidelines recommend that the business maintains records of the reasons behind that decision to be able to demonstrate that all relevant factors have been properly considered.

Even if a business is not obliged under the GDPR to appoint a DPO, they may still need to bring an experienced privacy professional on board since the GDPR brings many new (or stricter) obligations to businesses which process personal data, such as:

- Privacy Impact Assessments (PIAs)
- Stronger rights for individuals
- Record keeping of processing operations
- Privacy by design and by default for each processing
- Breach notification to Data Protection Authorities

A DPO must have suitable professional qualities and expert knowledge of data protection law to fulfil the role. The biggest challenge for businesses will not be determining whether or not to appoint a DPO but finding DPO resource in what is already a competitive skills market.

It is also worth noting that failure to appoint a DPO where one is required under the GDPR could lead to fines as high as €10m or 2% of the company's worldwide turnover, whichever is higher.

WHAT IS GEMSERV'S VIRTUAL DPO SERVICE?

For many organisations, the requirement to appoint a DPO could pose a number of challenges.

The remit of a DPO is wide, covering independent supervision of a company's compliance with the GDPR, as well as advising and overseeing staff dealing with personal data.

DPOs will need to have a broad understanding of the company's technical and organisational structure, along with knowledge of IT infrastructure and technology. They also need an awareness of areas such as digital marketing strategy.

An individual identified to take on the role within an organisation may have significant knowledge of some of the areas for which the DPO is responsible, but is unlikely to have sufficient expertise across all.

Gemserv's Virtual DPO service acts as a trusted advisor to organisations and DPOs, providing additional support to ensure they meet the requirements, particularly in the early stages of the role.

The Virtual DPO service also ensures continuity at a time when there is a significant shortage of data protection professionals in the marketplace and high levels of churn.

Our indepth experience of working across many organisations and projects means we are well-placed to advise on 'best-fit' IT tools and solutions.

We can also work with inhouse teams to develop marketing approaches which avoid customer opt-in issues and therefore don't fall under the scope of GDPR.

Gemserv can work on one-off specific projects to support a DPO, bring together different elements and develop an overall strategy, or take responsibility for GDPR compliance across an organisation.



TYPICAL VIRTUAL DPO ACTIVITIES

As well as ongoing DPO support, our service can also assist organisations with one-off and interim projects. Gemserv will help scope out the key activities to ensure the type of engagement is best suited to an organisation's requirements.

Areas covered by our Virtual DPO service can include:

Strategy, Governance & Project Management Office (PMO)

- Establishing a clear mission, strategic objectives and metrics for data protection aligned with business strategy and structure to support overall business objectives. This includes establishing Risk & Opportunity Logs and Reporting & Governance frameworks.

Operational Requirements

- Developing a privacy policy and privacy & information notices to meet latest compliance requirements and undertaking privacy impact assessments.
- Ensuring data protection department processes and wider business systems support delivery of data protection objectives.
- Ensuring security and data management meet minimum standard requirements, with focused extensions for most critical data and processes.
- Ensuring communication materials and processes are effective and transparent for customers and stakeholders.
- Proactive management of Consent / Permissions.

Supplier and Contract Management

- Ensuring that suppliers are compliant and adequately managing risks and that contracts take account of data protection risks.

THE ADVANTAGES OF HAVING GEMSERV AS YOUR DPO

No additional costs for employee training	Organisations are required to appoint a DPO based on professional experience and provide their DPO with continuous training. Virtual DPOs from Gemserv have expert knowledge and have received advanced training without you paying for it.
Multi-Skilled	Our DPOs can utilise internal experts in information security, technologies, risk, compliance and projects to support organisations.
No conflict of interest	DPOs are required to 'act in an independent manner'. CEOs, IT, HR and Legal Advisors are not allowed to work as DPOs, which can make selecting a DPO a challenging
Efficiency	Our consultants' expert knowledge enables faster and easier implementation of required action in a practice-oriented way.
Flexibility	Organisations experiencing difficulty recruiting a qualified and experienced DPO can appoint a virtual DPO in the short to medium term.
Synergy effect	External DPOs can make use of their experience from other companies for your organisation's benefit.
Cost saving	<p>Organisations must provide adequate support to their DPO in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate.</p> <p>The package offer by an external DPO may well be more price-effective than then long-term costs of deploying your own staff resources.</p>



**If you would like to find out
more please contact us on:**

T: +44 (0)20 7090 1091

E: bd@gemserv.com

W: www.gemserv.com

 [@gemservinfosec](https://twitter.com/gemservinfosec)

