MOORE STEPHENS

Update

Governance, risk & assurance

PRECISE. PROVEN. PERFORMANCE.

Leading your privacy response

The role of a Data Protection Officer (DPO) or data controller has never been in the public eye so much lately. Following the enforcement of the EU General Data Protection Regulation (GDPR) on 25 May 2018, some organisations are now required to have a DPO to achieve GDPR compliance. As a result of this specific GDPR requirement it is predicted that 28,000 additional DPO's will be required by organisations.

What is a DPO?

A DPO is a significant position within an organisation that is responsible for overseeing data protection strategy and implementation ensuring compliance with GDPR not just at 25 May 2018 but also as a forward looking compliance project plan.

Does your organisation need a DPO?

A DPO is a mandatory requirement for some organisations under GDPR. Your organisation is required to have a DPO if you process or store large amounts of personal data, whether for employees, individuals external to the organisation, or both.

DPOs must be appointed for all public authorities, and where the core activities of the controller or processor involve regular and systematic monitoring of data subjects on a large scale, or where the entity conducts large scale processing of special categories of personal data.

What are the responsibilities of a DPO?

DPOs are responsible for educating the organisation and its employees on important compliance requirements, training staff involved in data processing, and conducting regular security audits. DPOs also serve as the point of contact between the organisation and any supervisory authorities that oversee activities related to data.

The responsibilities of a DPO include, but are not limited to the following:

- inform and advise your organisation and staff who process personal data of their obligations as per the GDPR and other local data protection provisions;
- monitor compliance with GDPR, with other local data protection provisions and with the data protection policies of your organisation, including the assignment of responsibilities, awareness-raising and training of your staff involved in data processing;
- conducting audits to ensure compliance addressing any issues proactively;
- monitoring performance and providing advice on the impact of data protection efforts;
- cooperate with the supervisory authority; and act as the organisations contact point on issues related to the processing of personal data;
- respond to data subjects whose data is processed on all issues related to the processing of their data and the exercise of their rights under GDPR;
- maintaining the comprehensive records of all data processing activities conducted by the organisation, including the purpose of all processing activities, which must be made public on request.

What if your organisation falls outside the scope of having a DPO?

If your organisation falls outside of the scope to have a mandatory DPO, there is still a requirement under GDPR for you to fulfil the role of a data controller.

A less significant role within an organisation a data controller is best defined as an individual designated with the role of ensuring compliance with any regulatory requirements and is

known to be the point of contact across the organisation who will be expected to handle any events that materialise in respect of data protection. Despite this a data controller is still expected to fulfil the majority of the responsibilities of a DPO.

DPO/data controller outsourcing

We have developed a team of experts that can work with your organisation to ensure that it meets the DPO or data controller requirements of GDPR. It has been designed taking into account the range of size of organisation this applies to and the amount of time that would be required on a monthly basis. An outsourced approach is cost effective and flexible, with assurance of compliance.

There are four different tiers for your organisation to consider and the following matrix outlines the types of service your organisation will receive within each tiered offering:

Service tier	Budget Essential	Essential	Essential Plus	Premium
Privacy risk assessment	• Annual risk assessment	• Annual risk assessment	• Annual risk assessment • Up to 3 ad-hoc/project risk assessments	• Annual risk assessment • Up to 12 ad-hoc/ projects or systems
Compliance monitoring plan	• Plan based on privacy risk assessment • Monitoring up to 1 day per quarter	• Plan based on privacy risk assessment • Monitoring up to 2 days per quarter	• Plan based on privacy risk assessment • Monitoring up to 5 days per quarter	• Plan based on privacy risk assessment • Monitoring up to 12 days per quarter
Quarterly board meetings	• Report submitted quarterly to board/ senior management on compliance, incidents and outstanding issues	• Report submitted quarterly to board/ senior management on compliance, incidents and outstanding issues	• Attendance and report to board quarterly on compliance, incidents and outstanding issues	• Attendance and report to board/senior management as needed (up to 16 meetings per year) on compliance, incidents and outstanding issues
Point of contact for the organisation internally	• Helpdesk queries managed and responded to	• Helpdesk/queries managed and responded to	• Helpdesk/queries managed and responded to • 2 days legal opinion per annum	• Helpdesk/queries managed and responded to • Onsite support and response at least weekly • 5 days legal opinion per annum
Training		• Single session annually for staff	• Twice yearly sessions for staff • Board briefing and training annually	• Quarterly sessions for staff • Board briefing and training annually
Oversee breaches		• Maintenance of register	• Maintenance of register • Investigation of one breach/incident (up to 3 days of time) where needed	• Maintenance of register • Investigation of up to 12 incidents per year

For further information please contact:

Christopher Beveridge – Head of Privacy
christopher.beveridge@moorestephens.com

Robert Noye-Allen – Partner
robert.noye-allen@moorestephens.com