BRODIES LLP

GDPR - THE ROLE OF THE **DATA PROTECTION OFFICER**

One of the changes introduced under the General Data Protection Regulation (GDPR) is the requirement for certain organisations to appoint a Data Protection Officer (DPO). This guide explains what a DPO is, who needs to appoint one and what the DPO will do.

What is a Data Protection Officer?

A DPO is someone, either an employee or a professional hired externally, who has responsibility for ensuring that their organisation is compliant with GDPR.

The DPO should:

- Provide advice and guidance to the organisation and its employees on the requirements of the GDPR
- Monitor the organisation's compliance
- Be consulted and provide advice during Data Protection Impact Assessments
- Be the point of contact for data subjects and for cooperating and consulting with national supervisory authorities, such as the Information Commissioner's Office

DPOs should also take responsibility for carrying out data audits and oversee the implementation of compliance tools. The DPO must be able to act independently, be adequately resourced and be able to report directly to senior management to raise concerns.

What organisations must appoint a DPO?

There are three specific criteria around the requirement to appoint a DPO:

- Where the processing is carried out by a public authority or body;
- Where the "core activities" of the controller or processor consist of processing operations which require regular and systematic monitoring" of data subjects on a "large scale"; or
- Where the "core activities" of the controller or processor consist of processing on a "large scale" of "special categories of personal data" or data relating to criminal convictions and offences.

The requirements apply to both controllers and processors.

The Article 29 Working Party (WP29) suggests that "core activities" should include activities where the processing of data forms an inextricable part of the controller or processor's activities. For example, a hospital's core activity is the provision of health care, which requires processing of special category personal data such as health records. The hospital must therefore appoint a DPO. Conversely, processing such data for payroll and employment purposes would be ancillary to an organisation's core activities.

When considering whether processing is "large scale", the WP29 recommends that organisations consider duration and scope (in terms of volume of personal data and data subjects). Monitoring includes more than just online monitoring. It includes data-driven marketing, credit scoring, location tracking, CCTV, and using data from connected devices such as wearables, smart meters and home automation.

While a controller may not be required to appoint a DPO, the processor they engage might be. A controller may hire a processor for certain analytical purposes; which may be small-scale and ancillary to the controller's business, whereas the processor may be performing such analysis on a large scale as a core activity.

My organisation does not meet those criteria. Should I still appoint a DPO?

The WP29 recommends documenting the internal analysis which concludes why it is not necessary to appoint a DPO. An organisation can voluntarily decide to appoint a DPO. If they do so, then the relevant provisions in the GDPR governing the role of a DPO will apply.

Where an organisation does not wish to be bound by the rules relating to DPOs, organisations should still consider appointing members of staff or outside consultants to work specifically in data-protection related roles. However, organisations should make it expressly clear that these people are not DPOs and do not have the same powers and responsibilities.

Who can I appoint as my DPO?

The person appointed as a DPO must have "expert knowledge" of data protection law and practices. However, neither the GDPR nor the WP29 sets out any formal test for determining that knowledge. The DPO should also be familiar with the sector within which the organisation operates.

The DPO must not be subject to any conflict of interest. The WP29 considers that combining the role of a DPO with senior management positions may give rise to a conflict of interest. This means that it is unlikely that the DPO can be a chief executive, or senior executive or manager in the Finance, HR, Marketing or IT departments.

Can I outsource my DPO to a third party?

Yes. DPOs can be shared with another organisation (for example within a corporate group or amongst similar public bodies) or outsourced to a service provider.

However, the WP29 emphasises that this can only happen where it is done in a way that does not create a conflict of interest or impact upon the ability of the individual to perform his or her duties as a DPO. In particular, the DPO will need to have sufficient knowledge of the organisation, resources and involvement in discussions and decisions relating to the organisation's handling of personal data.

When should the DPO be appointed?

The DPO should be appointed as soon as possible after the organisation determines that one is required. The DPO will play an important role in their organisation's journey to GDPR compliance.

More information

You can follow the latest developments on the GDPR, including the latest guidance from regulators, on our GDPR microsite: **brodies.com/GDPR** or our blog: **http://techblog.brodies.com**

Key contacts

To discuss how the GDPR will impact on your organisation, or how Brodies can assist you with your preparations, please get in touch with a member of Brodies' data protection and information law team.

Grant Campbell
PARTNER
+44 (0)131 656 0115
grant.campbell@brodies.com

Martin Sloan
PARTNER
+44 (0)131 656 0132
martin.sloan@brodies.com

Christine O'Neill
PARTNER
+44 (0)131 656 0286
christine.oneill@brodies.com

Charles Livingstone
PARTNER
+44 (0)131 656 0273
charles.livingstone@brodies.com