TAYLOR WALTON SOLICITORS

Practice Note on
GDPR: Does your organisation need to appoint a Data Protection Officer?

The GDPR marks a change in approach to data protection regulation in the EU that places greater emphasis on self-regulation and internal accountability.

One aspect of the new approach is that for certain organisations it will be mandatory to designate a Data Protection Officer (DPO). The GDPR sets out a number of requirements regarding the role the DPO must fulfil and the tasks they must undertake.

Under the Data Protection Act 1998, although the Information Commissioner recommended that responsibility for compliance with data protection laws was assigned to a senior manager within an organisation, this was not a mandatory requirement. It is therefore important for businesses to understand the new requirements in relation to the role of DPO.

What is the role of the DPO?

Article 39 of the GDPR requires the DPO to carry out the following tasks:

- To inform and advise the organisation about its obligations to comply with the GDPR and other data protection laws;
- To monitor compliance with the GDPR and other data protection laws and internal data protection policies. This includes managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- To advise on, and to monitor, data protection impact assessments;
- To cooperate with the supervisory authority (the ICO in the UK); and
- To be the first point of contact for supervisory authorities and for individuals whose data is processed.

The DPO should take a risk based approach to their activities, in other words, focus should be placed on the riskier activities of the organisation.

The GDPR says that further tasks and duties can be assigned to the DPO, so long as they don't result in a conflict of interests with the DPO's primary tasks. ***ICO Example***: A company's head of marketing plans an advertising campaign, including which of the company's customers to target, what method of communication and the personal details to use. This person cannot also be the company's DPO, as the decision-making is likely to lead to a conflict of interests between the campaign's aims and the company's data protection obligations.

When is it mandatory to appoint at DPO?

Whilst many organisations will make certain persons responsible for matters relating to data protection, the appointment of a DPO is mandatory under the GDPR for the following organisations:

- Public authorities or bodies;
- Organisations whose core activities involve regular, systematic and large-scale monitoring of data subjects. ICO example: A large retail website uses algorithms to monitor the searches and purchases of its users and, based on this information, it offers recommendations to them. As this takes place continuously and according to predefined criteria, it can be considered as regular and systematic monitoring of data subjects on a large scale; and
- Organisations whose core activities consist of the large-scale processing of special categories of data or data relating to criminal convictions and offences. ***ICO example***: A health insurance company processes a wide range of personal data about a large number of individuals, including medical conditions and other health information. This can be considered as processing special category data on a large scale.

An organisation must appoint a single DPO to carry out the tasks required in Article 39, but this doesn't prevent it appointing other data protection specialists as part of a team to help support the DPO. The DPO must be knowledgeable about data protection issues.

The Data Protection Act 2018 (which amongst other things incorporates the GDPR into UK law) also sets out further requirements for the mandatory appointment of a DPO in the field of law enforcement. In practice, there are only likely to be limited cases where an organisation that is not required to appoint a DPO under GDPR is required to appoint one under the DPA 2018 on the basis that most organisations which deal with law enforcement will also be public bodies.

What are core activities?

Guidance provided by the European Data Protection Board (EDPB), suggests that an organisation's core activities are those key operations necessary for achieving the organisation's objectives but warns against excluding from this definition any activities where the processing of data form an inextricable part of an organisation's activities. The Guidance gives the example of a hospital, whose core business is providing healthcare. As a hospital needs to process patient health data to provide healthcare services safely and effectively the processing should be considered one of the hospital's core activities.

Is the processing large scale?

The GDPR does not indicate what qualifies as "large scale". The EDPB Guidance states that when reaching a decision as to what qualifies as large scale, the following factors should be considered:

- The number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
- The volume of data and/or the range of different data items being processed;
- The duration, or permanence, of the data processing activity; and
- The geographical extent of the processing activity.

Should we appoint a DPO on a voluntary basis?

You can appoint a DPO if you wish, even if you aren't required to. If you decide to voluntarily appoint a DPO you should be aware that the same requirements of the position and tasks apply had the appointment been mandatory.

It is important to note that all organisations that process personal data must comply with the GDPR, regardless of whether they have appointed a DPO. The fines available to supervisory authorities under the GDPR are likely to prompt many organisations that are under no obligation to appoint a DPO to designate data protection responsibilities to a particular person to assist with demonstrating compliance. To avoid being made subject to the DPO provisions of the GDPR, organisations must ensure that there is no confusion over whether the role can be regarded as a DPO.

The following measures may assist with this:

- Do not assign the title "data protection officer" to an appointment if the individual is not in fact a DPO for GDPR purposes. A better title may be "data compliance manager". If an individual was called a data protection officer for the purposes of the old legislation, consider a change in title;
- Assign data protection-related tasks to those in related fields, such as ethics or compliance; and
- Consider whether the responsibilities normally assigned to the DPO could be shared among a number of individuals in the organisation.

Supporting the DPO

Where a DPO is appointed, the organisation must ensure that:

- The DPO is involved, closely and in a timely manner, in all data protection matters;
- The DPO reports to the highest management level. This doesn't mean the DPO has to be line managed at this level but they must have direct access to give advice to senior managers who are making decisions about personal data processing;
- The DPO operates independently and is not dismissed or penalised for performing their tasks;
- Adequate resources (sufficient time, financial, infrastructure, and, where appropriate, staff) are provided to enable the DPO to meet their GDPR obligations and to maintain their expert level of knowledge;
- The DPO is given appropriate access to personal data and processing activities;
- It seeks the advice of your DPO when carrying out a DPIA; and
- The details of the DPO are recorded as part of the records of processing activities.

Are DPO's liable under the GDPR?

The GDPR does not provide for any specific liability for the DPO for non-compliance. Under GDPR the data controller or processor remains responsible for compliance with data protection laws. Satisfactory arrangements in relation to the appointment, support and autonomy of the DPO will assist with demonstrating compliance with the GDPR generally.

Taylor Walton LLP

Updated October 2018

This note is a general guide only and should not be relied on as a substitute for specific legal advice.