The role of the DPO—what you need to know

Anita Bapat and James Henderson consider the GDPR's requirements on appointing a Data Protection Officer, and the factors to be taken into account in allocating responsibilities

The forthcoming EU General Data Protection Regulation ('GDPR') enters into force in May 2018 and requires, for the first time in the EU, some organisations to appoint a Data Protection Officer ('DPO'). With regard to DPO appointment currently, there is inconsistency across the EU. Some countries, such as Germany and Spain, mandate the appointment of a DPO in certain circumstances. Other countries permit organisations to voluntarily appoint DPOs, and in doing so reduce a company's obligations in other areas of data protection law (for example, by providing an exemption to notifying the company's processing activities to the data protection authority).

The mandatory obligation to appoint a DPO forms a key part of the strengthened accountability obligations found in the GDPR, alongside new obligations on organisations to carry out data protection impact assessments, implement the principles of privacy by design and by default, and to maintain internal records of their data processing activities.

Mandatory appointment

Data controllers and data processors must appoint a DPO if they carry out processing involving the 'regular and systematic monitoring of data subjects on a large scale' or if they process sensitive personal data or data relating to criminal convictions and offences 'on a large scale'. Public authorities will also need to appoint a DPO. There is significant interpretative uncertainty regarding the terms 'systematic', 'regular', and 'large scale', and the terms are not further defined in the GDPR.

It is assumed that organisations will need to determine whether their processing activities meet those criteria themselves, although this is not entirely clear and leaves open the possibility of an EU data protection supervisory authority ('SA') making such a determination. In either case, guidance is required to clarify which activities meet those criteria, and to set threshold tests with regard to each. We would argue, for instance, that ad hoc monitoring of account holders who are flagged as potential victims of fraud should not fall within the criteria, but an organisation whose core activities consist in monitoring individuals to prevent fraud should be caught. Clarity from European privacy regulators in this regard would be welcome.

The GDPR also contains a provision allowing the EU or Member States to designate additional categories of controllers or processors that will also need to appoint DPOs. The number of organisations that must appoint DPOs is therefore likely to be wider than the categories above, once additional organisations are designated. This could potentially lead to difficulties for organisations where there are disparate national and EU laws requiring the DPO appointment, particularly where DPO's role is defined differently under national law. In such cases, organisations will need to decide whether to appoint multiple individuals to act in the different DPO roles, or whether to appoint a single DPO to fulfil all of the requirements. This may also lead to confusion amongst individuals seeking to exercise their data protection rights, or simply to contact the organisation, particularly where there are multiple people listed as the organisation's DPO.

Selecting a DPO

When appointing a DPO, organisations must make their selection on the basis of their 'professional qualities', on their 'expert knowledge of data protection law' and ability to perform the role of DPO (the details of which are discussed further below). There is no requirement for a specific qualification and so it is not clear what level of knowledge of data protection law a DPO will require. We would expect common standards to be developed in due course, possibly including EU-wide certification programs for individuals to demonstrate they have the appropriate knowledge of data protection law to perform the role of DPO.

Organisations are not limited to members of staff when considering candidates for the DPO role, but may choose to appoint an outside contractor to perform the role on the basis of a service contract. Where an external DPO is selected, it will be important for

organisations to ensure that the DPO is able to form productive relationships with internal stakeholders and colleagues in order to perform the DPO role adequately.

On the other hand, an external DPO perhaps has an additional façade of independence which an internal DPO may not be able to demonstrate, particularly if the chosen individual already has close working relationships with the stakeholders whose actions they will be required to monitor.

Where an employee is chosen as the DPO, there is nothing to prevent that individual from also performing other roles at the organisation, provided such roles do not affect his or her ability to adequately perform the role of DPO. The appointment of an internal DPO may also raise confidentiality and conflict of interest issues, and it will be important for organisations to develop policies and procedures to manage any such issues. Finally, it is important to note that groups of organisations may appoint a single DPO for the whole group, provided that the DPO is accessible from each of the company's EU establishments.

Voluntary appointment

The GDPR is silent as to whether organisations may voluntarily elect to appoint a DPO if they are not required by law to do so. Many organisations currently appoint DPOs voluntarily, and we expect this practice to continue. In particular, data processors may find it easier to demonstrate their commitment to compliance with the GDPR by voluntarily appointing a DPO. This appointment provides both an indicator to an organisation's customers, and regulators, that the organisation takes its data protection obligations seriously, and is committed to building an effective and accountable privacy programme.

"As the GDPR states that DPOs 'shall have at least the following tasks', it seems open for Member States or other EU regulatory bodies to prescribe additional tasks for DPOs. Such additional rules could potentially lead to confusion for DPOs if they are subject to inconsistent obligations across the EU."

It is not currently clear whether a voluntarily appointed DPO would be subject to all of the requirements of the GDPR and would be treated as a mandatorily appointed DPO. We would argue that this should *not* be the case, as the organisation (and the risks associated with its processing activities) does not meet the risk threshold set out in the GDPR for the appointment of a DPO. In such cases, the organisation would be free to determine the role and duties of its appointed DPO as it sees fit.

It should also be noted that once a DPO has been selected, there is no requirement to register his or her appointment with EU SAs. However, the appointing organisation is required to publish the contact details of the DPO, including in its privacy information notices, and to communicate the DPO's name and contact details to its SA.

Position of the DPO

The GDPR contains a number of rules relating to the role of the DPO aimed primarily at ensuring the independence of DPOs, and in ensuring they have adequate resources to allow them to effectively perform the role.

Firstly, the GDPR requires the organisation to ensure the DPO is involved, 'properly and in a timely manner' in all data protection related issues. In addition, the organisation must provide resources to the DPO to enable him or her to carry out the DPO's assigned tasks, and to maintain his or her expert knowledge of data protection law. The DPO will need to be involved in all data protection-related issues affecting the business. The level of responsibility, and accordingly the level of resources needed to adequately perform the role, will therefore vary significantly by organisation.

A large organisation with multiple EU operations, that focusses on processing personal data collected from multiple sources, will require a more well-resourced DPO than a smaller domestic based company with only minimal exposure to personal data. The GDPR is not prescriptive as to the resources to be made available to the DPO, and again what is appropriate will depend largely on the organisation in question. Resources are likely to include, amongst other things, a budget for the DPO and (potentially) his office, training materials and legal resources, access to outside legal counsel, IT and other technical resources, allowances to visit conferences and other learning opportunities.

Perhaps the most important aspect of the DPO's role is that the DPO must be independent of the management of the organisation, and that the DPO must not 'receive any instructions regarding the exercise of those tasks'. The DPO must also report directly to the 'highest management level' of the organisation. It is not clear whether this means directly to the Chief Executive Officer, or to some other part of the management of the company. In practice, this is likely to mean that the DPO will need to report into the board of the organisation, most likely via the organisation's Chief Compliance Officer or Chief Legal Officer, depending on the management structure of the organisation.

For organisations whose main business is the processing of personal data, it may be that the DPO has a direct position on the board. In any

(Continued on page 16)

(Continued from page 15)

event, reporting lines should be 'true' reporting lines, that enable the DPO to report to individuals who have the power to make binding decisions and real changes to the organisation's privacy practices, particularly after a specific incident of non-compliance.

The DPO role

The GDPR sets out in detail the minimum responsibilities of the DPO role. These include, informing and advising the organisation and its employees of the obligations of the GDPR and other data protection law; monitoring compliance of the organisation, both its practices and policies, with the GDPR and other data protection laws; raising awareness of staff of data protection law; providing relevant training to staff; carrying out data protection-related audits; providing advice to the organisation, where requested, in relation to the carrying out of data protection impact assessments ('DPIAs') and the organisation's wider obligations with regard to DPIAs; and acting as a contact point for the organisation's SA.

In addition to those tasks, the DPO will also need to act as a contact point for individuals. Individuals may elect to contact the DPO on all issues relating to the processing of their personal data, and may also exercise their rights under the GDPR (for example, to obtain subject access or object to processing) by contacting the DPO. The DPO will therefore have a clear 'internal' and 'external' aspect to their role, and it will be important to ensure that these do not interfere with one another.

The appointed DPO must at all times have regard to 'the risk associated with the processing operations, taking into account the nature, scope, context and purposes of processing.' This is an overarching obligation which means that the role of the DPO will vary in proportion to the risks to the rights of individuals affected by the organisation's processing of personal data.

It will be important for organisations to properly delineate the role of the DPO, in accordance with not only the GDPR, but also with the organisations internal management structures, practices and culture. For example, some organisations may not wish for their DPOs to be in direct communication with the organisation's SA, but would rather such communication is handled by the in-house legal or compliance team. In some circumstances, there may be strong reasons for doing so, such as maintaining legal privilege of those communications. In addition, in some cases where the DPO is also an in-house legal data protection counsel, the DPO may in fact be precluded from communicating with the SA due to relevant legal privilege rules.

Finally, given that DPOs must be independent of the management of the organisation, in some cases it may be appropriate for management of the organisation to communicate directly with the SA, rather than the DPO. This applies particularly where there is disagreement between the DPO and management as to the appropriate course of action.

As the GDPR states that DPOs 'shall have *at least* the following tasks', it seems open for Member States or other EU regulatory bodies to prescribe additional tasks for DPOs. Such additional rules could potentially lead to confusion for DPOs if they are subject to inconsistent obligations across the EU, perhaps hampering the ability for organisations to appoint a pan-EU DPO responsible for the role across an organisation's EU offices.

Conclusion

The role of the DPO has become increasingly important over the last several years for data protection compliance and risk management, and with the introduction of the DPO obligation under the GDPR, this trend is set to continue.

While the GDPR contains detailed provisions as to the selection, position and tasks of DPOs, there are still significant and challenging practical questions regarding how the role will work on a day-to-day basis. The Article 29 Working Party (an advisory group of EU data protection regulators formed under the current Directive) is currently preparing guidance on the role of the DPO under the GDPR, and it is hoped that this will provided some clarity to organisations that will need to appoint a DPO. Although the GDPR will enter into force in 2018, there are a number of steps that organisations can take now to begin their preparations, including:

- reviewing the DPO appointment requirements and criteria, and evaluating whether there are potential internal candidates for the role, or whether outside assistance will be required;
- ensuring that a suitable individual is adequately trained to meet their DPO obligations;
- considering potential budgetary and resource planning for the future DPO;
- liaising with existing DPOs regarding changes to the role in future; and
- monitoring on-going guidance and publications from EU privacy regulators and bodies regarding the role of the DPO.

Anita Bapat and James Henderson
Hunton & Williams
abapat@hunton.com
jhenderson@hunton.com