Mind the GDPR (Pt 2)

In the second of a series of articles, Rollits LLP consider the role of data protection officers & the issues surrounding obtaining valid consent

IN BRIEF

- What the appointment of a data protection officer means in practice.
- When is it appropriate to rely on consent as a lawful basis for processing personal data?

In the first part in this series on the General Data Protection Regulation (GDPR), we considered why current data protection legislation needed updating and provided an overview of the key provisions under the GDPR (see 'Mind the GDPR', *NLJ*, 22 September 2017, p 8). Our focus now turns to two key action points organisations will need to consider early on in their preparations for the GDPR: (1) the appointment of a Data Protection Officer (DPO) and what that means in practice; and (2) when it is appropriate to rely on consent as a lawful basis for processing personal data.

Appointment of a DPO

Under the GDPR, both controllers and processors are under an obligation to appoint a DPO where:

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

While it is quite clear that public authorities (ie organisations that are subject to the Freedom of Information Act 2000) are required to appoint a DPO, the position for many private organisations is unclear due to the rather ambiguous wording adopted in the GDPR.

According to the *Guidelines on Data Protection Officers* issued by the Art 29 Data Protection Working Party (the Guidelines), 'core activities' means primary activities 'necessary to achieve the controller's or processor's goals'. For example, processing employee personal data will (one would assume) be ancillary to achieving an organisation's goals and so if an organisation only processes employee personal data, it is unlikely that it will be required to appoint a DPO. However, organisations will often undertake multiple activities and the assessment as to which of those activities are primary and which are secondary might prove to be challenging in practice.

'Regular and systematic monitoring' is another phrase which requires further clarification. Recital 24 of the GDPR indicates that this term includes tracking and profiling data subjects on the internet, including for the purposes of behavioural advertising. The Guidelines go further and state that monitoring is not restricted to the online environment.

Processing of personal data must be carried out on a 'large scale' before the requirement to appoint a DPO is triggered. The GDPR does not define 'large scale', but some clarification is provided in Recital 91 of the GDPR which states that it includes 'large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects' (although Recital 91 relates to Data Protection Impact Assessments rather than DPOs and so its applicability is debatable).

The Guidance states that in assessing whether or not processing is large scale or not, organisations should consider the number of data subjects concerned, the volume of data being processed, the duration, or permanence, of the data processing activity and the geographical extent of the processing activity. Notwithstanding the above, until more definitive guidance is available organisations will invariably take different approaches as to what should be considered 'large scale'.

Having attempted to apply the GDPR and the Guidelines to their processing activities, organisations may be forgiven for being uncertain as to whether or not the appointment of a DPO is mandatory for them. Even the Guidelines refer to there being a 'large grey zone' between the examples provided in the Recitals to the GDPR. Organisations which sit in the grey zone may wish to appoint a DPO on a voluntary basis which (whilst good practice from a data protection perspective) does come with a health warning that the requirements under the GDPR as to designation, position and tasks of the DPO apply as if the designation had been mandatory and this may cause issues (as detailed below).

Organisations that decide not to appoint a DPO should document the internal analysis carried out to determine whether or not they are required to appoint a DPO in order to demonstrate that the relevant factors have been taken into account should it ever be called into question. Irrespective of whether or not an organisation should appoint a DPO pursuant to the GDPR, every organisation should ensure that it allocates appropriate staff and resources towards ensuring compliance with the GDPR.

Role of the DPO

Anyone who has been appointed to be their organisation's DPO (whether or not on a voluntary basis) can take comfort in the knowledge that they will not be held personally responsible if their organisation is not compliant with the GDPR—such responsibility lies with the controller or processor.

The DPO's primary role is to enable compliance with the GDPR. This is achieved through fostering a data protection culture within the organisation by raising awareness, training staff and carrying out data protection audits. DPOs are also required to monitor compliance with the GDPR by collecting and analysing information, checking compliance with data processing activities and informing, advising and issuing recommendations to their organisation.

In order to fulfil the above tasks, DPOs are required to have 'expert knowledge on

data protection law and practices' pursuant to Art 37(5) of the GDPR. The GDPR does not stipulate what is meant by 'expert knowledge' and there is no baseline as to the level of qualifications required by the DPO to demonstrate sufficient expertise (although, clearly some training is required).

When selecting an appropriate person to fulfil the role of the DPO, organisations can either appoint an appropriate staff member or, where that is not suitable, the tasks can be outsourced to a third party. If a staff member is to be appointed to fulfil the role then such staff member must be able to perform their task in an independent manner. The DPO cannot be instructed how to deal with a matter (eg, how to investigate a complaint or whether to consult the ICO) or to take a certain view of an issue related to data protection law.

The Guidance states that the 'DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data' and that 'as a rule of thumb' this is likely to preclude people in senior management positions such as chief executive, head of marketing department and head of human resources from being the DPO. Therefore, if an organisation does wish to tag the role of DPO on to someone in a senior management position, careful consideration has to be made as to whether there are any potential conflicts and (if there are) how those conflicts can be managed.

If the role of DPO is to be fulfilled by a third party then, whilst there are unlikely to be any conflict issues, other problems may arise. For example, the DPO should be involved in all discussions relating to the protection of personal data and their presence is recommended where decisions with data protection implications are taken by the organisation. Therefore, ensuring that the DPO has sufficient availability to meet the organisation's requirements will be a key factor when outsourcing the role of DPO to a third party.

Consent

Under the Data Protection Act 1998 (DPA 1998) personal data must be processed fairly and lawfully. In order to demonstrate compliance with this principle, an organisation has to issue a fair processing notice and satisfy one of the fair processing conditions set out in the DPA (for example, that the data subject has given consent to that processing, or that processing is necessary to perform a contract with the data subject or to comply with a legal obligation of the data controller). This will remain the case under the GDPR. Consent is often used by data controllers as the primary mechanism for demonstrating compliance with the fair and lawful processing principle. However, consent is not always the best condition to rely on. Consent may be withdrawn by the data subject, or the reasons for which consent was originally sought may change. Furthermore, the data subject may not have any real choice over whether they give consent or may feel compelled to give consent (for example if an employer requests consent from an employee and the employee does not want to appear difficult).

The consent requirements under the GDPR are more onerous than under the DPA and this means that organisations will need to consider (where consent is used as the lawful basis for processing personal data) whether consent is appropriate or whether an alternative lawful basis should be relied on for processing that personal data.

The GDPR defines consent as 'any freely given, specific, informed and unambiguous indication of the data subjects wishes by which he, or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. This means that pre-ticked boxes, silence from the data subject or opt-out boxes will no longer suffice.

Consent is only appropriate if it provides real choice and control. The Information Commissioner's Office's draft 'GDPR Consent Guidance' states that public authorities, employers and organisations in a position of power should avoid relying solely on consent as there is an imbalance in the relationship and so consent may not be considered freely given.

Consent should be granular and must be separate from other terms and conditions. Consent must also be verifiable—this means that organisation relying on consent will need to maintain records demonstrating specifically what a data subject has consented to, what they were told and when and how they consented. If an organisation determines that consent is the appropriate legal basis for processing personal data it should review the consent mechanisms it has in place to establish whether they comply with the GDPR requirements. If the consent the organisation has obtained does not meet the stricter GDPR requirements then it will not be valid consent once the GDPR takes effect and steps should be taken now to obtain consent which does meet those requirements.

Summary

Two stepping stones which should be trodden early on in an organisation's path towards GDPR compliance are assessing whether a DPO is required and reviewing where consent is used as the lawful basis for processing personal data. Failure to tackle these initial steps could have an adverse knock-on effect when dealing with other elements of GDPR compliance and could leave the organisation in deep water. **NLJ**

David White, senior solicitor & **Tom Morrison,** partner, Rollits LLP (www.rollits.com).

Next time: obligations imposed on data processors under the GDPR & data processing agreements.