Data Protection Officers – a world of uncertainty

September 2017

The General Data Protection Regulation (GDPR) provides that a data protection officer (DPO) must be designated in certain circumstances. While some guidance has been issued in this respect, important questions as to whether a DPO must be appointed and, if so, whom to appoint, remain unanswered.

This briefing was first published in Privacy Laws & Business UK Report, Issue 93.

Questions still to be answered

The GDPR will apply from 25 May 2018. Amongst the new requirements is an obligation to appoint a data protection officer (DPO) in certain circumstances.

We are therefore often asked by businesses whether they should appoint a DPO, how to satisfy the DPO's required level of data protection knowledge, and, specifically, whether a General Counsel (GC) can be the DPO. These questions arise because the current lack of case-law, together with the limited guidance available, gives rise to uncertainty. This is unfortunate, not least since failing to appoint a DPO when required to do so risks fines of up to €10m or 2% of annual worldwide turnover, whichever is higher.

The role of a DPO

The primary duty of a DPO is to ensure compliance with the GDPR. This does not only entail advising on the legality of specific initiatives upon request, but extends beyond that. The GDPR provides that proactive steps must be taken to ensure that the DPO is:

"involved, properly and in a timely manner, in all issues which relate to the protection of personal data."

In addition to such an advisory role, a DPO has a supervisory role and, as such, must be in a position to monitor that the organisation complies with data protection laws and its internal policies.

A DPO also has an important task in relation to infusing the organisation with awareness of the GDPR requirements by providing training, polices and the like. Indeed, such awareness is a precondition for establishing the processes and procedures needed to ensure compliance.

Finally, the DPO must cooperate with, and serve as a point of contact for, the supervisory authorities and the data subjects, i.e. the individuals whose data is being processed. This does not entail an obligation to disclose confidential information. To the contrary, the GDPR explicitly provides that DPOs are bound by confidentiality concerning the performance of their tasks.

To ensure that the DPO's tasks can be carried out effectively, organisations are required to support their DPOs by providing adequate resources whether in the form of time, financial resources, training or support from other departments and senior management.

Importantly, the DPO must be able to carry out their role in a completely independent manner

and must not be dismissed or penalised for performing their duties when, for example, a course of recommended action is not to management's liking.

Management is not obliged to follow a DPO's advice, but it must be taken into consideration and, if departed from, it is recommended by the Article 29 Working Party (A29WP) to document the reason for doing so. This is in line with the GDPR's overarching accountability requirements.

In what circumstances is a DPO required?

Under Article 37, a private sector organisation (as opposed to a public authority or body) must appoint a DPO if:

> *"the **core activities** of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require **regular and systematic** monitoring of data subjects on a **large scale**; or … processing on a **large scale** of special categories of data …. and personal data relating to criminal convictions and offences….."*
> *(emphasis added)*

The exact meaning of these criteria is not spelled out in the GDPR. However, the A29WP has published guidance which provides a useful starting point.

As we explain below, the analysis of whether an organisation's processing is "large scale" or "regular and systematic" is more straightforward than that for whether it is part of an organisation's "core activities".

Large scale

The recitals to the GDPR indicate that large scale processing should be understood as processing of a considerable amount of personal data at a regional, national or supranational level and which could affect a large number of individuals. By comparison, processing carried out by an individual lawyer or health care professional in respect of clients/patients is stated as not being carried out on a large scale. As recognised by the A29WP, many real life processing operations fall between these extremes. Whilst these recitals are in the context of data protection impact assessments rather than DPOs, as acknowledged by the A29WP, this is likely to be a starting point for the DPO analysis too.

The A29WP recommends taking into consideration factors such as the number of individuals affected, the volume of data, the geographical extent and duration of the processing activity. The A29WP also provides a number of examples it considers as being large scale processing, including processing of personal data for behavioural advertising by a search engine and processing of customer data in the regular course of business by an insurance company or a bank.

While there will be exceptions, most large organisations engaged in monitoring or processing of special categories of data (previously generally known as sensitive personal data) or criminal records on a regular basis in respect of their customers will, in practice, arguably do so on a large scale within the meaning of the GDPR.

Regular and systematic

Once it has been established that an organisation carries out monitoring activities such as location tracking, behavioural advertising, risk profiling, surveillance or tracking employee working hours, it should be straightforward to establish whether it is "regular and systematic". As supported by the A29WP guidance, that criteria will in practice most often be fulfilled – one of the few exceptions being where the duration of the monitoring activity is very limited because it is carried out as part of a pilot project or in relation to a particular event.

Core activity

According to the GDPR recitals:

"the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities."

In light of that, the A29WP considers "core activities" to be those key operations necessary to achieve the organisation's goals as well as those operations which form an inextricable part of its core activities.

Clearly an organisation offering a product or service which consists of processing personal data has such processing as its core activity – for instance an organisation offering profiling services in relation to credit scoring. Also, whilst a hospital's core activity is strictly speaking the provision of healthcare, it will, as stated by the A29WP, be obliged to appoint a DPO because the processing of patient medical records is inextricably linked to its core activity.

On the other hand, the reference to "ancillary activities" makes it equally clear that the mere fact that an organisation processes personal data on a regular basis does not necessarily mean that such processing should be considered a core activity. The A29WP is clear that organisations which only process the types of personal data set out in Article 37 in relation to HR, IT and other traditional support functions would not, therefore, be obliged to appoint a DPO. That applies regardless of whether the support function in question is, as will often be the case, essential to the core activity.

This of course begs the question: what is the criteria for determining whether an activity should be characterised as a support activity or an activity inextricably linked to the core activity?

The A29WP does not attempt to specify the relevant criteria in any detail and does not give examples in respect of those scenarios where the assessment will be less obvious. This creates significant uncertainty.

We therefore discuss opposite some suggested criteria that we consider to be helpful in this assessment.

Suggested criteria for determining if processing is 'inextricably linked'

Is the core activity conditional on such processing?

If the core activity is conditional upon the processing this suggests that the processing is inextricably linked. This may be because of legal requirements or could also be due to contractual obligations or customer demand.

To what degree is the primary service or product offering based on processing of personal data?

In a recent Danish parliamentary report it was suggested that the degree to which the primary service or product offering is based on the processing of personal data is decisive. While still abstract, if adopted more broadly, such consideration could prove useful in determining whether a processing activity is inextricably linked to the core activity.

What added value does the processing contribute to the organisation's core activity?

An alternative approach is to look at whether an activity is inextricably linked by looking at it from a 'value added' perspective.

In this respect it arguably does not matter whether in principle the core activity could be carried out without processing personal data or whether other similar organisations manage without. If an organisation decides to initiate a scheme which entails the processing of personal data which creates significant value for the core activity, then arguably it becomes inextricably linked to its core activity as a result.

Whilst each case will be fact specific, and so a different answer may result for what otherwise appears to be the same processing by a similar organisation, some illustrative examples of how we see this distinction are in the box below.

Activity	Is it ancillary or inextricably linked?
Use of CCTV by a shopping centre for security purposes	Ancillary, unless in the particular case customer or tenant demand requires it
Use of CCTV by a train operator	Inextricably linked
Recording of medical information by a company for HR purposes	Ancillary
Recording of medical information by a charity to provide services to the individual	Inextricably linked
Targeting of global customer base with a long-term behavioural advertising campaign by a consumer products organisation	Inextricably linked

Finally, it is worth bearing in mind that the first draft of the GDPR contained a mandatory obligation for all companies to appoint a DPO. The current wording therefore reflects a compromise position, tying the need to appoint a DPO to the risks posed by certain types of data processing. The initial position may therefore indicate that data protection authorities will adopt a strict approach when assessing the need to appoint a DPO.

In addition, we consider that the ICO is likely to favour a purposive, rather than restrictive, interpretation of "core activity" given that the legislative rationale behind mandatory DPO appointments is to ensure that organisations conducting high-risk processing, including the monitoring of individuals on a large scale, comply with the terms of the GDPR and protect the rights of individuals.

Voluntary appointments

Many organisations are considering appointing an individual with a similar role to a DPO on a voluntary basis. Doing so is in line with the recommendations of the A29WP. A DPO acts as an anchor point in respect of an organisation's ongoing compliance efforts and, with the support of management, can help promote a culture of awareness. In addition, increased focus on data protection means some organisations consider it to be a parameter of competitiveness, and appointing an individual to deal with it underlines the organisation's efforts in this respect.

However, according to the A29WP, if an individual is given the formal title of "Data Protection Officer" the GDPR requirements apply irrespective of whether the individual was appointed on a voluntary basis. The most significant implications being that the individual cannot easily be made redundant and that their genuine independence must be ensured. Whilst this position is not expressly found in the GDPR, we recommend for voluntary appointments that a different title such as "Head of Data Privacy" be adopted instead.

Who should be the DPO?

The GDPR stipulates that DPOs must be appointed:

"on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks"

The nature of a DPO's tasks, ranging from monitoring compliance to training of employees, therefore requires the individual to possess many traits. When appointing a DPO, factors such as

personal qualities, professional qualifications, knowledge of the business and their positioning within the organisation should also be given due consideration.

It is not specified what qualifications a DPO must possess in order to be deemed an expert in data protection law. The recitals of the GDPR provides for some flexibility by stating that it depends on the "*… data processing operations carried out and the protection required for the personal data being processed*".

The A29WP is clear that a DPO needs an in-depth understanding of the GDPR. In addition, organisations may want to appoint a DPO familiar with the rules on direct marketing since distinct, and to some extent overlapping, rules apply in this respect.

Expert data protection knowledge

There has been uncertainty as to whether an individual who has a working rather than specialist knowledge of data protection law can be appointed as a DPO if supported by others who possess such knowledge.

The wording of the GDPR seems to suggest that a third party cannot be relied upon to bridge a gap in the DPO's knowledge. However, while a DPO's ability to carry out their tasks is conditional on at least some level of data protection knowledge, such a strict interpretation would make it virtually impossible to recruit individuals who are up to the task – few have all relevant qualifications themselves. In our view, it is therefore acceptable to have a senior person appointed as a DPO who, whilst having a working knowledge, is not himself fully versed in data protection, but who is supported by subject experts who report to him. This seems to be acknowledged by the A29WP which refers to the "*set up [of] a DPO team (a DPO and his/her staff)*" and, in the context of an external DPO service provider appointment, describes the benefits of "*individual skills and strengths [being] combined so that several individuals, working in a team, may more efficiently serve*" an organisation.

Appointment of a GC as DPO

The DPO must be positioned within the organisation at a level which ensures the effective supervision of processing of personal data which makes the DPO easily accessible and provides for a direct line of communication to "*the highest management level*". In practice, organisations will most often prefer to appoint a DPO whose ability to deal with management has been tried and tested.

Many organisations have therefore said they would prefer to designate their GC as DPO. After all, a GC will often have a respected position within the organisation, report to the highest level of management, have an in-depth knowledge of the business and may even be "an expert" in data protection law. A GC thus often possesses many of the sought after traits.

However, the DPO is required to be independent in carrying out their role. It must therefore be ensured that the GC's other duties do not result in a conflict of interest when they start to act in this capacity as DPO which entails scrutinising the organisation's data processing activities. A conflict could arise, for instance, if the GC has a decisive say in determining the organisation's strategy and operations in respect of data processing since those very decisions may need to be challenged.

The A29WP notes that such a conflict is most likely to be faced by any person holding a senior position in management (i.e. as a CEO, COO or CFO), a Head of HR, Marketing or IT, or a lower level employee who makes decisions about how and for what purpose personal data is processed. They do not, however, make any comment about a GC and, as such, subject to the points above, in our view there is no automatic bar on the GC also being the DPO.

Conclusion

Despite the A29WP guidance, there is still plenty of uncertainty with respect to DPOs and guidance from the ICO would be beneficial, just as data protection authorities in some other jurisdictions have published their own views on this topic.

Over time market practice will no doubt develop but, until there is clear precedent, organisations will need to make their decisions about the DPO to the best of their ability on the basis of legal advice. We hope that in the meantime data protection authorities will grant some leeway to organisations that are finding their way.

This article was written by Rebecca Cousin and Oliver Howley. Slaughter and May advises on all aspects of data protection and privacy, including GDPR compliance audits. If you would like further information, please contact Rebecca or your usual Slaughter and May advisor. Further publications are available on our website.

Rebecca Cousin
T +44 (0)207 090 3049
E rebecca.cousin@slaughterandmay.com

Oliver Howley
T +44 (0)207 090 3595
E oliver.howley@slaughterandmay.com