Evolution of a Profession: the Data Protection Officer (Part 1)

In this first of a three part series, Isobel Murphy, Data Protection Specialist, and Gordon Wade, Data Protection Lead in the Office of the Data Protection Officer at TikTok, Dublin, trace the origins of the position of the DPO and highlight recent guidance concerning their role, tasks and responsibilities

Gordon is speaking on 'Children Front and Centre' at the 17th Annual Data Protection Practical Compliance Conference taking place in Central Dublin and Online on 17th and 18th November 2022. See www.pdp.ie/conferences for further details.

Emerging on a European-wide basis in 2018 with the entry into force of the GDPR, the institution of the Data Protection Officer ('DPO') now occupies a central position in personal data governance within organisations in the EU. Tasked with, among other things, advising the controller/processor on, and monitoring its compliance with, its legal obligations under the GDPR and acting as a point of contact with data protection Supervisory Authorities ('SAs') and data subjects, DPO's have become a cornerstone of EU organisations' accountability for their personal data processing activities and for demonstrating compliance with EU data protection law.

In Part 1 of this article, we track the origins of the position from 1970s Europe to the modern-day privacy professional. We also highlight recent guidance produced by SAs concerning the role, tasks and responsibilities of the DPO. In Part 2, we will discuss recent enforcement actions taken under the GDPR (and their national implementing rules) relating to compliance with the requirement to appoint and properly involve a DPO, alongside relevant case law on the role and position of the DPO. In Part 3, we will share the results from our primary research surveying past and present DPOs and privacy professionals from a diverse range of industry sectors and jurisdictions, and provide insights into how the role of the DPO has evolved and developed over the past number of years (in particular since the coming into force of the GDPR).

Origins of the DPO

DPOs have been a feature of data protection compliance for many years in a number of countries including Germany and Sweden. They were provided for, for example, in the German Federal State of Hesse's Data Protection Act in 1970 (the Hessiche Datenschutzgesetz) which many agree was the first piece of national legislation applicable to the processing of personal information in the world. As described by Professor Spiros Simitis, the German law was regarded as "the father of data protection" in Europe.

The Hessian Data Protection Act applied exclusively to data automatically processed in the public sector and, most pertinent for our purposes, prescribed that a DPO (Datenschutzbeauftragter) be appointed to the State Parliament.

In Sweden, the 1973 Data Act (Datalagen), which was applicable to both public and private sector entities, spoke to the requirement for controllers to appoint one or more persons to assist with investigating complaints from members of the public that the personal data being processed about them were incorrect or misleading. Such appointed person(s) were also required to communicate with the individual on behalf of the controller, informing them of the outcome of the investigation and any steps taken to address the issue.

In 1995, with the adoption of the EU Data Protection Directive ('1995 Directive'), there was for the first time a minimum standard for data privacy and security applicable to all EU Member States. Whilst not requiring the appointment of DPOs by those controllers subject to it, it did contemplate the possibility that some controllers might appoint one. Specifically, Article 18(2) recognised the existence of DPOs in Member State law and practice by allowing Member States to exempt controllers from the obligation to notify processing operations to the relevant national SA if the Member State's law required the relevant controller to appoint "[a DPO] responsible in particular for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive [and] for keeping [a] register of processing operations carried out by the controller, containing [the same information as would otherwise have to be notified to the SA]".

In practice, most EU countries did not adopt a formal legal requirement to appoint a DPO. For example, no such requirement existed under the Irish Data Protection Acts 1988-2003 or the UK Data Protection Act 1998. In its national implementing legislation, Germany elected to formally require that a DPO be appointed in all public authorities, and in certain businesses with 10 or more employees employed in the automated processing of person-

(Continued on page 8)

(Continued from page 7)

al data, regardless of the nature of processing activities carried out. Indeed, Germany's Federal Data Protection Act (Bundesdatenschutzgesetz) made the failure to appoint a DPO, whether otherwise required, a violation of the law and punishable by a maximum fine of €50,000. Germany viewed DPOs as forming part of a hybrid strategy for supervising privacy and data protection compliance: rather than requiring them to inform government supervisors about every aspect of their data processing activities, organisations were exempted from notification duties if they internally appointed a DPO responsible for such supervision. Germany also required its DPOs to be registered with the government, possess a keen understanding of information technology and have a background in law. Elsewhere, Croatia required organisations with data filing systems employing 20 or more people to appoint a DPO. In Italy, entities that handled health-related files in electronic form were required to appoint a DPO and in Hungary, DPOs were mandated for financial institutions.

The 1995 Directive was based on recommendations first proposed by the Organisation for Economic Co-operation and Development ('OECD') in its 1981 Convention for the Protection of Individuals with Regard to Automated Processing of Personal Data ('Convention 108'). Like the 1995 Directive, Convention 108 did not mandate that a DPO be required for certain types of organisations or processing activities but, in Article 10, it did direct signatories to require controllers and processors to "take all appropriate measures to comply with the obligations of this Convention and be able to demonstrate...that the data processing under their control is in compliance [with the Convention]." Guidance was provided in paragraph 87 of the accompanying Explanatory Report to Convention 108, addressing the obligation in Article 10, to the effect that "a possible measure that could be taken by the controller to facilitate such a verification and demonstration of compliance would be the designation of a 'Data Protection Officer' entrusted with the means necessary to fulfil his or her mandate."

DPOs under the GDPR

Today, there exists a mandatory requirement under Article 37 of the GDPR for a DPO to be appointed in three specific circumstances:

- 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 the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

'Public body or authority': The GDPR does not define what constitutes a 'public authority or body'. The European Data Protection Board ('EDPB') considers that national law should determine which entities are covered. In addition to encompassing national, regional and local authorities, many national laws typically also include a range of other bodies governed by public law.

'Require regular and systematic monitoring of data subjects on a large scale': The GDPR does not define what constitutes large-scale processing. According to Recital 91 of the GDPR, it should concern "a considerable amount of personal data [...] which could affect a large number of data subjects". In this regard, the former Article 29 Working Party (replaced by the EDPB) previously recommended that the following factors in particular be considered when determining whether the processing is carried out on a large scale:

- 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.

Despite the absence of a clear definition at EU level as to what may be considered 'large scale' data processing, some assistance may be found in guidance published by individual SAs. For example, in 2018 the Dutch SA (Autoriteit Persoonsgegevens) released guidance on large-scale processing specifically related to the healthcare sector. According to the authority, personal data processing by hospitals, pharmacies, general practices centres and care groups are always considered to be 'large scale'. In contrast, smaller general medical practices, pharmacists working alone and specialist medical care centres only meet the 'large scale' threshold if:

- they have 10,000+ registered patients; or
- more than 10,000 patients are treated on a general basis and all patient files are maintained on a single filing system.

In Germany, the Federal Data Protection Commissioner in its guidance on Data Protection Impact Assessments ('DPIAs') defined 'large scale processing' as data processing operations covering more than 5 million data subjects, or those covering at least 40% of the relevant population.

The UK Information Commissioner's Office ('ICO') has also weighed in on the question of what constitutes 'large scale' for the purposes of the GDPR, stating in guidance ('When do we need to do a DPIA?') that when deciding on whether processing is being/will be conducted on a large scale, organisations should consider the duration, or permanence, of the data processing activity; the number or proportion of data subjects involved; the volume of data and/or the range of different data items being processed as well as the geographical extent of the processing activity.

Helpfully, the ICO provides some examples of what it considers to be 'large scale' processing, including data processing by a hospital, tracking individuals using a city's public

transport system as well as the processing of customer data by banks, insurance companies and phone and internet service providers.

Purpose, role and duties of the DPO

Role: The primary role of the DPO is to independently oversee, audit, advise and guide the organisation with respect to its obligations under applicable data protection laws, rules, regulations and standards (including regulatory guidance). The DPO acts as a kind of internal but independent business partner, providing an essential layer of checks and balances. These checks and balances can include recommending that additional steps be taken before embarking on a processing activity or even to 'think again.'

> ***"In practice, acting independently and avoiding conflicts of interest means that a DPO should have unimpeded access to the organisation's senior leadership."***

Purpose: The purpose of a DPO is to ensure that the organisation to which they are appointed processes the personal data of its data subjects in compliance with applicable data protection laws and, in doing so, acts in the interests of its data subjects. Indeed, such is the importance of the purpose played by a DPO in their organisation's GDPR accountability programme, that there are three separate Articles dedicated to the topic.

Duties: Where a DPO is appointed by an organisation whether by way of GDPR requirement or voluntarily, they should be entrusted with, at least, the following duties:

- advising on the creation of data protection-related policies, processes designed to implement and operationalise those policies, and guides for updating both those policies and processes. This advisory work should include, in particular, consulting on any proposed changes to applicable privacy policies or terms of service, and the adoption of any new policies and procedures relating to the processing of personal data;
- advising and consulting on DPIAs to identify, assess and address personal data protection risks based on the company's functions, needs and processes. To be most effective in this duty, the DPO should be deeply embedded in the risk assessment and review process from early. Enabling the DPO to engage in fact-finding consultation and open dialogue with business stakeholders should ensure that the DPO has the opportunity to provide meaningful feedback and advice;
- planning, supervising and developing data protection training and awareness programmes to educate employees about personal data policies, processes and standard operating procedures. The goal for the DPO in driving data protection training internally is to both build trust in the workforce in the organisation's personal data processing activities and to drive a culture of privacy;
- being the point of contact for the organisation's data subjects and handling and managing data protection-related queries and complaints. In practice, many larger organisations will have a dedicated privacy operations team entrusted with frontline responsibility for handling data subject requests. However, any such team should operate under the supervision and oversight of the DPO;
- engaging and cooperating with regulators on data protection matters, if necessary and in consultation with the applicable legal team. In particular, this includes being closely involved in all matters related to the notification of data breaches (preparation, analysis of incidents, decisions to inform the data protection authority and data subjects and ex-post analysis); and
- providing documented and reasoned opinions and recommendations to the business on personal data related risks.

The DPO may also be assigned additional tasks and duties by law of the requirements of the organisation. Irrespective of the duties they carry out, the DPO will be most effective and efficient in monitoring the organisation's compliance and assigning responsibilities where they have deep and cross-functional involvement, day-to-day, in a wide range of data processing matters.

Status of the DPO

DPOs must, at all times, carry out their tasks with diligence, objectivity, independence, impartiality, integrity, responsibility and honesty, according to their knowledge and expertise. Core to the position of the DPO within its organisation, therefore, are the requirements to act independently in the performance of their task and duties and to avoid conflicts of interest and responsibility in the pursuit of its vision and mission. Related to this, the GDPR mandates that a DPO should not be dismissed or penalised for performing their tasks. For example, if a DPO advises a controller to conduct a DPIA in relation to a new project involving data processing that the DPO considers to be high risk, and the controller disagrees with that advice, the DPO cannot be dismissed for providing this advice. The rationale behind this approach in the GDPR is to help ensure that DPOs are autonomous and independent in their role and should not work in fear of potential dismissal for carrying out their duties.

In practice, acting independently and avoiding conflicts of interest means that a DPO should:

- have unimpeded access to the organisation's senior leadership. A DPO that is positioned with true and effective direct reporting lines to highest management levels will help the DPO influence and guide the organisation's responsible use, management and protection

(Continued on page 10)

(Continued from page 9)

of personal data;

- not receive any instructions from the organisation regarding the tasks of the DPO. The positioning of the DPO as functionally independent will ensure the DPO can carry out their tasks with impartial and unbiased judgement. A DPO should also not be accountable to leadership in the pursuit of their vision and/or mission;
- not take on other roles within the organisation that would create a conflict of interest. Roles which have the potential to undermine a DPO's independence and objectivity would be those that would confer operational responsibility for the personal data processing activities under their supervision (i.e., determining the purpose and means of data processing);
- be provided with adequate resourcing to perform their tasks, which should include access to the DPO's own external legal counsel, separate to that of the business. The DPO may also be provided with appropriate support to staff an 'Office of the DPO' and thus enable the DPO to, at their discretion, delegate their authority and responsibilities; and
- have the freedom to consult, of their own volition, with relevant SAs in respect of matters within the scope of the DPO's remit. In doing so, the DPO should respond diligently to all queries directed to them by a SA and endeavour to maintain a positive and professional working relationship with those SAs.

Part 2 will be published in the next edition of *Data Protection Ireland.*

This article was prepared by the authors in their personal capacities. Any views or opinions expressed herein are strictly the authors' own and do not reflect the views or opinions of TikTok.

Isobel Murphy
and Gordon Wade
TikTok
isobel.murphy@tiktok.com
gordon.wade@tiktok.com