PROQUEST®
A DIVISION OF ALLIANT

CONSIDERATIONS FOR ATTORNEYS TAKING ON THE DPO ROLE

By Jennifer Groszek

The new requirements for the General Data Protection Regulation (GDPR) went into effect on May 25, 2018. The GDPR is arguably the biggest change to the data privacy regulatory landscape and applies to the processing of individuals' personal data in the EU. This regulation also affects entities based outside of the EU[1]. For example, if you are a U.S.-based company or organization processing the personal data of an individual who resides in the EU, you are subject to GDPR compliance.

At the heart of data protection compliance is the Data Protection Officer (DPO), appointment of which is mandatory for certain organizations. A flurry of activity surrounds this key piece of GDPR compliance as companies/organizations determine whether or not they are obligated to designate a DPO and, if so, whether that person should be an attorney, an internal employee, or an external person. The first step in this discussion requires a determination of whether appointment of a DPO is required under Article 37.[2]

Article 37(1) of the GDPR requires the designation of a DPO when the processing is carried out by a public authority or body (except for courts acting in their judicial capacity); where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; or large scale processing of special categories of data or data relating to criminal convictions or offences.[3] To assist organizations in their compliance obligations, and in determining whether or not they are required to appoint a DPO, the GDPR is supplemented by the Guidelines on Data Protection Officers, issued by the Article 29 Working Party (WP29), an advisory body made up of representatives of the national Data Protection Authorities of each EU Member State.[4] The WP29 Guidelines provide recommendations and further clarification on undefined terms as they relate to the appointment of DPOs.

The next step in the analysis involves identifying who is the best selection to fill the role of DPO. Lawyers and/or law firms are frequently identified as the best candidate to serve as DPOs for their clients. The Guidelines indicate that an organization can appoint an external non-employee as the DPO to fulfill the tasks on a contract basis when the organization has no physical presence within the EU.

While an attorney may be a good fit for the DPO role, the attorney's qualifications and independence need to be thoroughly considered. Further, the tasks of the DPO need to be considered in relation to the attorney's availability. Article 37 as supplemented by the Guidelines provide that the DPO shall be designated on the basis of professional qualities, and, in particular, expert knowledge of data protection law and practices, and the ability to fulfill his/her tasks.[5] Relevant skills and expertise include: expertise in national and European data protection laws and practices including an in-depth understanding of GDPR; understanding of the processing operations carried out; understanding of information technologies and data security; knowledge of the business sector and the organization; and ability to promote a data protection culture within the organization. *Id.*

Article 39 provides that the minimum tasks of the DPO shall include: to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the GDPR and other EU data protection provisions; to monitor compliance with the GDPR, other EU data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35; and, to cooperate with authorities; to act as the contact point for the supervisory authority on issues relating to processing.[6]

Of significance, the role of the DPO is to monitor for compliance and provide advice to the organization/company in an autonomous and independent manner. Therefore, the DPO should perform the role independently. Per the Guidelines, the following safeguards exist to enable the DPO to act independently: no instructions given by the controllers or the processors regarding the exercise of the DPO's tasks; no dismissal or penalty by the controller for the performance of the DPO's tasks; and, no conflict of interest with possible other tasks and duties.[7] Conflicts of interest must be avoided, and, therefore, the DPO should not be in a senior management position or hold a position within the organization that determines the purpose and the means of processing personal data. *Id.* Additionally, a conflict of interest may arise if an external DPO is asked to represent the controller or processor before the Courts in cases involving data protections issues. *Id.* This issue should be evaluated when considering a DPO role for a client.

Another consideration for attorneys contemplating an external DPO role is whether this activity triggers coverage under the law firm's lawyers professional liability policy. The DPO role can be performed by non-lawyers. Therefore, it is necessary to review the lawyers professional liability policy language, specifically the definition of what constitutes a "professional service". The "professional services" definition can vary by insurance carrier and, in some instances, be broad enough to include services performed for others in the Insured's capacity as a lawyer, although such services could be performed wholly or in part by non-lawyers. However, some policies contain a more narrow definition of what constitutes a "professional service." Additionally, serving as a DPO for an entity in which the attorney holds an executive position or has an ownership interest represents not only a conflict of interest but could also potentially trigger the business enterprise exclusion.

In conclusion, the designation of a DPO requires thoughtful consideration of multiple issues, including possible conflicts and coverage implications. It is imperative that an attorney considering this role evaluate whether they possess the professional expertise specific to perform these tasks. Further, one must also consider how performing this role may implicate a potential conflict. Finally, it is necessary to consider whether the actions taken as a DPO are subject to the pending professional liability policy.

[1]https://eugdpr.org/key-changes.html

[2]The Guidelines on Data Protection Officers recommends that controllers/processors document the internal analysis carried out to determine whether or not a DPO is to be appointed to demonstrate that the relevant factors were properly considered. Guidelines on Data Protection Officers ('DPOs') WP 243 rev.01.

[3]See Article 37 of the GDPR.

[4]https://www.whitecase.com/publications/alert/new-eu-guidelines-data-protection-officers.

[5] Guidelines on Data Protection Officers ('DPOs') WP 243 rev.01.

[6] See Article 39 of the GDPR.

[7]Guidelines on Data Protection Officers ('DPOs') WP 243 rev.01.