CyberInsecurity News™
WHAT LAWYERS NEED TO KNOW

SHOULD A GC TAKE ON THE ROLE OF DATA PROTECTION OFFICER?

Spurred by new rules, companies are hiring for the position, but it isn't always easy to find candidates with the right skills.

BY R. JASON STRAIGHT

DECEMBER 1, 2018

By now, few general counsel are unaware that the European Union's General Data Protection Regulation (GDPR), which became enforceable on May 25, can penalize their companies for mishandling personal data related to people in the EU. With penalties of up to 4 percent of global revenue, privacy risk has become a board-level issue for companies that conduct a significant amount of business in Europe.

Many companies have sidestepped the GC's office and assigned accountability for GDPR compliance to a separate and independent Privacy Office, or have given IT primary responsibility for ensuring data protection compliance. But is this the best approach? Should the GC ultimately be responsible for GDPR compliance, or is an independent privacy function more appropriate?

In answering this question, it may be helpful to start by looking at how the GDPR defines the role of the data protection officer, or DPO. While any company that processes data pertaining to individuals in the EU must comply with the GDPR, only certain ones are required to appoint a DPO. Article 37 of the GDPR states that a company must designate a DPO in the following circumstances:

1. Where the processing is carried out by a public authority;
2. Where the core activities of the company require regular and systemic monitoring of EU data subjects on a large scale; or
3. Where the core activities of the company involve processing, on a large scale, special categories of personal data (e.g., data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership, genetic data, biometric data or information pertaining to sexual orientation).

UnitedLex

www.cyberinsecuritynews.com

The GDPR provides limited guidance on how to define "regular and systemic monitoring" or "processing on a large scale," so companies have done their best to interpret the requirement on a case-by-case basis. If the obligation to appoint a DPO is not clear-cut, companies should think twice before designating a DPO, because by doing so, that subjects them to additional obligations.

The GDPR requires companies to ensure that the DPO is "involved, properly and in a timely manner, in all issues which relate to the protection of personal data." The DPO is also responsible for supervising all GDPR compliance activities, such as data mapping, risk assessments, consent tracking, policy updates, training, etc.

Finding the Right Skills

The first challenge for companies that opt to appoint a DPO is to identify the most appropriate spot on the org chart for the position. The unusually broad range of attributes that the role requires does not allow for a natural fit in most organizations. Guidance from regulators suggests that anyone holding a senior management (i.e., C-Suite) position in a company is likely to have a job-function conflict that would prevent them from being designated as the DPO. Anyone who makes decisions about how the company collects and processes personal data as part of their normal role in the business will be conflicted out of the role. The responsibilities of the GC must therefore be closely examined before determining that a DPO designation is appropriate.

Article 3[Office1] 8 of the GDPR emphasizes that the DPO must be able to operate independently, "with direct reporting to the highest management level," and must be "available to be contacted by data subjects." In addition, Article 38 states that the DPO "shall not be dismissed or penalized by the controller or the processor for performing his [or her] tasks." This requirement can be tricky to navigate if the DPO is an employee with other responsibilities at the company. Arguably, you have granted a significant level of job security to anyone designated as DPO.

Article 39 provides a brief list of the DPO's tasks. Some are internally focused, such as monitoring compliance and providing advice regarding the organization's data protection impact assessments (DPIAs). Other tasks involve communications with data subjects in order to respond to requests and assertions of rights. And finally, the DPO is required to serve as the point of contact for the appropriate governmental supervisory authority, and is charged with maintaining "due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing." These tasks are fairly well suited to management by the legal function.

When we look at the guidance that the GDPR provides on the qualifications that the DPO must possess, the case for designating an in-house lawyer for the role is not as clear. While the GDPR does not cite specific credentials, it does require that the DPO have an understanding of the processing operations carried out by the data controller and of the information technologies and data security deployed by the data company. This requirement can get a traditionally trained lawyer out of her comfort zone fairly quickly.

Industry-specific business expertise: The DPO must also be a credible leader who can draw upon knowledge of the business requirements and cultural subtleties of the organization and its industry in order to demonstrate knowledge of the company's sector and related risks. In addition, the GPDR requires the DPO to have the ability to promote a data protection culture within the organization. To be sure, most GCs have a very deep and granular understanding of their company's operations as well as its sector. But driving cultural change in the organization? That usually falls to someone else.

Expertise in data-related compliance and privacy-related risk mitigation: In addition to the duties and qualifications cited above, the DPO must be able to fully understand national and European data protection laws and practices, including an in-depth understanding of the GDPR. The DPO must cooperate with the supervisory authority and act as a point of contact, should any complaints or concerns arise. The DPO must also support and monitor the creation and maintenance of processing activities carried out on behalf of a controller in a manner consistent with GDPR. And finally, the DPO must oversee incident and breach response management activities as needed, and as defined by Articles 33 and 34 of the regulation. These requirements are right in the wheelhouse of many in-house counsel.

GC or Not GC?

In short, the DPO role requires a skill set that encompasses very high levels of executive, technical, legal and business expertise. That's a tall order for even the most seasoned GC, especially considering the potential for conflicts of interest when the role is assigned to an existing employee. The regulation makes clear that independence and credibility are key components of the DPO function, and are especially important when you consider the level of accountability required of the role in the event of a breach or other incident that could compromise the personal data of customers or employees. That level of expertise, integrity and singleness of purpose may be difficult for an internal employee to rise to when he/she is already employed by the company whose data management practices are being monitored.

To be sure, the role of the GC as an adviser to the executive team may be broadly consistent with the obligations of a DPO. However, consider a scenario where the GC is overseeing litigation involving the company's processing of personal data, or is making decisions about what personal data the company is comfortable sharing with third parties. What if the GC's performance is measured in part by the outcome of these decisions? Would that not create a conflict with the obligations of the DPO? [Rita Heimes, who is the DPO and GC of the IAPP, talks about this issue in our related article.]

Many organizations are looking at utilizing an external DPO service that leverages personnel with expertise in a range of disciplines. Why? Finding a single individual with working knowledge of information governance, data mapping, data flow analysis, network architecture, cross-border data transfer, cloud computing, critical cybersecurity controls, encryption, incident response and data breach management is a challenge—whether you are looking internally or externally.

The advantage of engaging a DPO as a service provider (and, to be clear, my company, UnitedLex, offers this service to companies looking to outsource the role) is that such a provider can

support the DPO function with a team of people collectively possessing the requisite skills. Moreover, it is a much more cost-effective option for organizations that do not require a full-time DPO, as they only pay for what they need from the role. Many of these services are structured to provide a fixed number of hours per month to carry out DPO responsibilities.

An external DPO may not be the ideal solution for all companies, but given the complexity of the DPO role, the shortage of qualified privacy experts and cost constraints, it is an attractive option for many organizations.

The next question for organizations opting to engage outside help is: Who should provide oversight and day-to-day guidance for the DPO? Notwithstanding the independence requirement, the DPO will need a consistent contact point at the company to discuss complex GDPR interpretation questions, as well as a starting point for discussions about data protection risks.

For organizations that already have an internal privacy function with an established leader, the DPO would naturally take day-to-day direction from the privacy office. However, the GDPR also requires the DPO to have direct access to the senior level of management, so a mechanism for escalating above the privacy office is critical. For organizations that do not have a formal privacy office, the GC is often in the best position to provide support and oversight to the DPO role. Even GCs conflicted out of performing the DPO role themselves are typically able to understand the DPO's mandate and effectively assist the DPO in ensuring ongoing compliance with the GDPR. After all, it is the responsibility of every GC to help the company avoid legal risks.

The Bottom Line

Absent additional guidance from data protection regulators, decisions on appointing a DPO (or not) and identifying the appropriate person will remain murky. In many instances, the GC will emerge as the most qualified candidate. But organizations must ensure that the DPO duties do not conflict with the GC's other obligations. In addition, the GC must have the requisite knowledge of data protection law as well as deep familiarity with the company's business processes that involve EU personal data. Companies struggling with these decisions are advised to explore the option of using an external expert for the role instead.

R. Jason Straight is Senior Vice President of Cyber and Privacy Risk Solutions and Chief Privacy Officer at UnitedLex. (You can read our interview with him here.) He has been managing information security risks, data breach incidents, data privacy obligations and complex information governance challenges for more than a decade. As a Certified Information Privacy Professional and recognized domain expert, he frequently writes and speaks about topics relating to data privacy, cybersecurity, data breach response and computer forensics. He began his career as an attorney at Fried, Frank, Harris, Shriver & Jacobson.