blancco

WHITE PAPER

EU GDPR: Setting Responsibilities & Expectations for the DPO

INTRODUCTION

The countdown to EU GDPR compliance has begun. By May 25, 2018, any organization that collects or processes data on EU citizens is required to comply with the EU's General Data Protection Regulation (GDPR). This includes any companies that offer goods or services to individuals in the European Union (EU) or any companies that monitor citizens' behavior within the EU.

A replacement for the Data Protection Directive 95/46/ec, the GDPR establishes new requirements for data subject consent, data anonymization, breach notification, trans-border data transfers, the appointment of a Data Protection Officer, data removal and more. Compliance with EU GDPR is no easy feat and the consequences for failing to do so are steep. Organizations found to be in violation of the requirements will be subject to fines of 20 million euros or four percent of their annual global turnover – whichever is higher.

While awareness of GDPR is high amongst IT professionals, our recent study found that 40 percent of global organizations are not fully prepared for GDPR. With so much to do and so little time to do it in, organizations are wondering where to begin.

A good place to start is by appointing a Data Protection Officer (DPO). Doing so will ensure that someone has the responsibility of creating the processes to achieve compliance.

THE REQUIREMENT FOR A DATA PROTECTION OFFICER

Any organization subject to the EU GDPR is required to appoint a DPO if its core activities include personal data processing that:

- Requires large and systematic monitoring of individuals on a large scale
- Concerns special categories of data on a large scale
- Concerns data relating to criminal convictions and offenses

Special categories of data include genetic data, biometric data, data concerning health, sex life or sexual orientation; they also include those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs and trade-union membership. If you think about it, most B2C companies will need to have a DPO.

The DPO is responsible for a number of duties as specified by the GDPR. These tasks include:

- Informing the organization of its obligations to comply with the GDPR and other EU or Member State data protection laws
- Monitoring compliance with the GDPR and other EU or Member State data protection laws, including managing internal data protection activities, training data processing staff and conducting internal audits
- Advising the organization on data protection impact assessments
- Serving as the point of contact for and cooperating with the relevant Data Protection Authority on issues related to personal data processing
- Taking inquiries from data subjects (employees, clients, etc.) regarding the organization's data protection practices and the exercise of their rights under the GDPR

The GDPR also stipulates certain obligations on the part of enterprises to enable DPOs to carry out these responsibilities. Organizations are required to support their DPO by providing the staff, resources and training needed to carry out DPO duties.

Organizations must also provide their DPOs with access to personal data and data processing operations, and ensure that the DPO is involved in all matters related to the protection of personal data in a proper and timely manner. Under the GDPR, DPOs also have the right to conduct investigations, and all controllers have the duty to cooperate with the DPO.

The nature of these requirements helps convey the importance of the DPO role, but perhaps none more so than those regarding the DPO's place within the organization. The DPO must report directly to the highest management level within the organization. DPOs must also work independently, without receiving any instructions on how to carry out their duties. Finally, DPOs cannot be dismissed or penalized for performing those tasks.

The organization is also offered some protection, as the GDPR indicates that DPOs are bound by secrecy or confidentiality regarding the performance of their tasks, and they must ensure that their other tasks and duties do not create a conflict of interest.

DEFINING THE RIGHT DPO SKILLS AND QUALIFICATIONS

There are a number of skills and qualifications organizations should look for when assigning the DPO role. Richard Stiennon, Chief Strategy Officer at Blancco Technology Group, advises organizations to look for someone with a privacy and security background. "Both would be great, but either one is also good," he said. It is also helpful if this person is familiar with regulations and compliance activities, as well as audit requirements.

A professional certification can help fill in knowledge gaps pertaining to privacy laws and security best practices. The Certified Information Systems Security Professional (CISSP) by (ISC)2 is applicable, as well as the Certified Information Privacy Professional (CIPP) by the International Association of Privacy Professionals (IAPP). CIPP covers the history of privacy legislation in a specific region, as well as relevant laws that must be complied with and the existing standards and certifications that can address compliance requirements.

"There are three qualities that effective DPOs must have. They must be strong leaders to lead the privacy team and serve as the liaison to the C-suite. From the perspective of introducing a privacy program and understanding how it contributes to the business, DPOs must also be strategic. Finally, DPOs must be strong communicators so they can communicate what privacy is, why it matters and how to turn it into a strategic advantage in the business."

– Malcolm Crompton, Managing Director, Information Integrity Solutions Pty. Ltd. and former Privacy Commissioner of Australia

The DPO should also have a solid understanding of the way the company operates and its data processing activities, as well as an ability to interpret data protection rules in that context. A DPO needs to be extremely well versed on how the data lifecycle works within the company and understand the technology and processes required to properly manage data across its entire lifecycle. In addition, the DPO must understand

all the different routines when it comes to the customer-facing side of the company, such as where various types of interactions with customers take place and how data is collected from them, both offline and online.

To be successful in the role, a DPO should also possess certain personal and interpersonal characteristics. Because data privacy concerns span operational processes, security protocols and technology solutions and tools, it's vital that the DPO is able to collaborate with various stakeholders and works well across departments.

Admittedly, collaboration can often be a challenge for organizations. One reason is that departments tend to work in silos and have differing interests in collecting and storing data. As our recent EU GDPR research found, only 2 percent of the surveyed IT professionals said their marketing department cares most about data privacy, while 7 percent cite the CTO, another 7 percent cite the legal department and 7 percent compliance. This is where the DPO will play an instrumental role in proving the need for and value of data protection to the various departments within their organizations and subsequently getting them on board. To achieve this, the DPO must have strong communication, negotiation and conflict resolution skills.

Difficult circumstances are likely to come up, and DPOs must be willing to assert themselves to do what is right for the company and its customers. It's also important that DPOs be organized and motivated to carry out the duties of the position. It will be difficult for DPOs to get other stakeholders invested in data privacy if they themselves don't feel passionate about it.

Finally, DPOs should act with the utmost integrity and adhere to ethical standards pertaining to loyalty to the organization, confidentiality, conflicts of interest and using data access on a need-to-know basis. Integrity and transparency will also be vital for the DPO to report data breaches to the Supervisory Authorities, as specified in the EU GDPR.

ASSIGNING DPO RESPONSIBILITIES: YOUR OPTIONS

Organizations have several options when it comes to filling the DPO role. They can establish a new role within the organization and hire a new employee to fulfill those responsibilities. However, if organizations don't have a sufficient budget or bandwidth to hire a new DPO role, they can add the necessary DPO responsibilities into an existing role within the organization as long as the two roles are not in conflict. Finally, a third option may be to outsource the role to a third-party provider, which will cost less than hiring a new executive.

According to our Chief Strategy Officer, Richard Stiennon, companies should first consider whether their primary business is that of a data processor or a data collector before choosing one of these three options. "If you're a company like Yahoo or Google that primarily manages user data, the best solution is to have someone with a DPO title," Stiennon advises. "But if you're a manufacturer whose data records include 1,200 customers who are buyers at other manufacturers, then you're in a good position to outsource the role."

The majority of organizations, however, will be best served by adding the DPO responsibilities into an existing role, such as the Chief Privacy Officer, Chief Information Security Officer, Chief Compliance Officer or Chief Information Governance Officer. As part of these added responsibilities, we would suggest that organizations add DPO into the existing role's title to ensure there is no confusion as to their compliance with this requirement of the EU GDPR. This will also reduce any confusion among auditors and the country's enforcement agencies as to whom they should speak with when reaching out.

There are several benefits to adding DPO responsibilities

to an existing role, driven in part by a general shortage of qualified individuals in the job market. According to research by the IAPP, at least 28,000 DPOs will be required under the GDPR in Europe alone. Grooming an existing employee to take on the DPO role will require a lower investment of time and money – both of which are crucial at this stage of the compliance game.

Another benefit of assigning the DPO role internally is that the existing employee is already familiar with business processes and how the company manages different responsibilities affected by the GDPR. Giving DPO responsibilities to an internal expert provides the company with an in-house advisor who can lead the way and do so right from the start. This is much different from a third-party provider that will serve as more of an auditor function, coming in and checking boxes, or from a new hire who will need several months to learn the business and its processes.

CONCLUSION

The DPO, as required under the GDPR, is intended to help ensure an organization's compliance with GDPR and other privacy laws and regulations. It is just one of many requirements that organizations face in the race to reach compliance. However, assigning this role sooner rather than later will make the compliance process go smoother. Efforts to get up to speed on the requirements, and implement the proper controls and processes can be streamlined through the DPO, who must ultimately be familiar with these elements. Your DPO can actively assist with data subject consent, data anonymization, breach notification, trans-border data transfers, secure data removal and other critical tasks to help ensure that you achieve regulatory compliance by May 25, 2018.

To learn how Blancco Technology Group can help your organization achieve GDPR compliance and provide guidance on establishing the necessary data management processes, sign up for our free evaluation.

ABOUT BLANCCO TECHNOLOGY GROUP

Blancco Technology Group is a leading, global provider of mobile device diagnostics and secure data erasure solutions. We help our clients' customers test, diagnose, repair and repurpose IT devices with the most proven and certified software. Our clientele consists of equipment manufacturers, mobile network operators, retailers, financial institutions, healthcare providers and government organizations worldwide. The company is headquartered in Alpharetta, GA, United States, with a distributed workforce and customer base across the globe.

Blancco, a division of Blancco Technology Group, is the global de facto standard in certified data erasure. We provide thousands of organizations with an absolute line of defense against costly security breaches, as well as verification of regulatory compliance through a 100% tamper-proof audit trail.

SmartChk, a division of Blancco Technology Group, is a global innovator in mobile asset diagnostics and business intelligence. We partner with our customers to improve their customers' experience by providing seamless solutions to test, diagnose and repair mobile assets. SmartChk provides world-class support, pre and post implementation, allowing our customers to derive measurable business results.

For more information, visit our website at: www.blanccotechnologygroup.com

CONTACT US

For Sales & Marketing, Please Contact:
Email: info@blanccotechgroup.com

For Corporate Communications & PR, Please Contact:
Email: press@blanccotechgroup.com