Zettaset

Data Protection Officer: A GDPR Guide

The much-anticipated General Data Protection Regulation (GDPR) brings massive, necessary changes to data protection in an increasingly vulnerable cyberspace. These modifications touch upon everything from general accountability to data processing to rights to sanctions. The GDPR applies to any and all companies that collect and use the personal data of individuals residing within the EU, regardless of where that company is located in the world.

Included in the GDPR is the requirement that certain companies elect a data protection officer (DPO). This guide will explore everything DPO-related so you have all that you need to make an informed decision in line with GDPR requirements.

The GDPR DPO mandate

Article 37 of the GDPR mandates that specific organizations designate a data protection officer by the time the regulation goes into effect – May 25, 2018. The GDPR also stipulates the position and tasks of the DPO. The data protection officer must be qualified and have "expert knowledge of data protection law and practices." The officer's contact information must be published and communicated to the appropriate independent public authority, as well. Each member state within the EU has its own supervisory authority.

What is a DPO?

Per the GDPR, the title of "Data Protection Officer" is its own unofficial description. A DPO is acts as an assistant to the controller or processor to monitor internal compliance. To put it simply, this means that a DPO ensures that an organization complies with all data protection regulations.

Article 37 also states that the necessary level of expert knowledge "should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor. Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner."

It's not required that a DPO be appointed in-house – the position can be filled by a contractor. Additionally, apart from certain conflicts of interest (such as CEO, CFO, CMO, HR, or IT) DPOs are not prevented from holding another position.

Before we get into the details, however, let's first talk about who needs a DPO.

Who needs a DPO?

The GDPR initially limited the DPO requirement to organizations that have over 250 employees, but the final regulation ultimately did away with size restrictions. Now it applies to small businesses and global powerhouses alike. The GDPR asserts that DPOs are required for companies that fit any (but not necessarily all) of the following descriptions:

You Need to Appoint a DPO if:

The processing is carried out by a public authority or body (excluding courts).

or

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

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.

Several terms need further clarification, and thankfully an independent European committee on data protection and privacy came together to spell things out more clearly. This advisory board was created back in 1996, under Article 29 of the Data Protection Directive, to provide expert advice to the EU regarding data security. Representatives from all EU states call themselves the "Article 29 Data Protection Working Party," or WP29 for short.

The WP29 has defined the following terms as they relate to the GDPR:

- Public authority or body — These include national, regional and local authorities, but under applicable national laws can also cover "a range of other bodies governed by public law." In such cases, the designation of a DPO is mandatory. Sectors such as public transport services, water and energy supply, and road infrastructure are not legally obligated to hire a DPO, though here it is "highly recommended."

  The WP29 stresses that even if the GDPR does not require a company to appoint a DPO, organizations will "find it useful" to voluntarily comply.

- Core activities — These are the essential operations that are critical to achieving the organization's goals. It's important to note that this definition "should not be interpreted as excluding activities where the processing of data forms an inextricable part of the controller's or processor's activity."

  The WP29 offers two examples here. The first is a hospital, whose core activity is to provide healthcare. Since it could not provide its services without processing medical data, the hospital should include data processing as one of its core activities, and therefore needs a DPO. The second example is a private security company. Surveillance is their core activity, which in turn is "inextricably linked to the processing of personal data." As such, this company must also designate a DPO.

  Organizations that use data for support functions (for example, "paying their employees or having standard IT support activities") do not need a DPO because these are considered ancillary functions.

- **Regular and systematic monitoring** — This includes all forms of tracking and profiling on the internet, "including for the purposes of behavioral advertising," but also extends beyond the online environment.

  The WP29 provides plenty of examples here. If an organization's core activities include the following, they are required to designate a DPO:

  - Operating a telecommunications network
  - Providing telecommunications services
  - Email retargeting
  - Profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering)
  - Location tracking, for example, by mobile apps
  - Loyalty programs
  - Behavioral advertising
  - Monitoring of wellness, fitness and health data via wearable devices
  - Closed circuit television
  - Connected devices e.g. smart meters, smart cars, home automation, etc.

- **Large scale** — It is "not possible to give a precise number either with regard to the amount of data processed or the number of individuals concerned."

  The WP29 recommends that the following factors be considered when determining whether processing is being 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
  - The geographical extent of the processing activity

Again, if a organization is a public authority/body, it needs a DPO. If an organization's core activities consist of regular and systematic monitoring of data subjects on a large scale, it too needs a DPO. If the data relates to criminal convictions on a large scale, the processing organization is required to designate a DPO.

What does a DPO do?

The primary task of a data protection officer is to ensure the personal data that is in the possession of a company or public authority/body is processed and protected correctly. The DPO is involved in all issues relating to data protection.

According to the GDPR, the DPO is responsible for:

- Informing and advising the organization of GDPR's provisions so that employees may carry out proper data processing in line with the regulations
- Monitoring GDPR compliance
- Assigning responsibilities, raising awareness, and training staff involved in processing operations and audits
- Providing information regarding the data protection impact assessment
- Acting as the liaison for the supervisory authority on issues relating to processing and consultations

Data protection officers are forbidden from taking instructions from their employer. The GDPR consistently warns that a DPO must act independently, "without instruction" and in the best interest of data protection. This means that in fulfilling their duties, the organization cannot direct the DPO in dealing with a matter — no suggestions

for achieving certain results, no commanding how to investigate complaints, and no instructions to take a certain position on a data protection law issue.

Organizations that are required to appoint a DPO must provide the officer with sufficient resources and cannot fire or punish the appointee "merely for performing their tasks." Necessary resources can be interpreted in a variety of ways, according to the WP29:

- Active support by board members and senior management
- Sufficient time to complete tasks
- "Adequate support in terms of financial resources, infrastructure and staff where appropriate"
- Access to HR, legal, IT, and security
- Continuous training

In some cases, the committee even suggests that a DPO be given a team to work with. From a structure standpoint, DPOs report directly to the highest level of management within a company.

What happens if an organization fails to appoint a DPO?

If an organization meets any of the requirements resulting in the need for a DPO but fails to comply, there are serious repercussions. Non-compliance with the DPO obligation subjects an organization to a fine up to €10 million ($12.2 million) or up to 2 percent of its total revenue.

The WP29 advisory board therefore suggests that all organizations handling large amounts of personal data — whether they meet the GDPR's conditions or not — voluntarily appoint a DPO.

How Zettaset can help

Due to the mounting legal pressure for DPOs to bring their company to GDPR compliance, it's imperative that organizations take proper steps to protect sensitive data. The GDPR notes that if a business has "implemented appropriate technical and organizational protection measures [that] render the data unintelligible to any person who is not authorized to access it," the company would be exempt from the mandate to notify data subjects.

Zettaset's XCrypt™ Data Encryption Platform and products help organizations meet corporate and regulatory data protection requirements, and have been called out as one of the "Top 10 Hot Data Security and Privacy Technologies" by Forbes.

About Zettaset

A leader in data protection, Zettaset's XCrypt™ line of encryption products are optimized for unmatched performance and infinite scalability to address the demanding data protection requirements of today's high-volume compute, storage, and cloud environments.

Zettaset
465 Fairchild Drive, Suite 234, Mountain View, CA 94043 // USA: +1.650.314.7920
Fax: +1.650.314.7950 // sales@zettaset.com // www.zettaset.com