What are Data Protection Officers?: A Guide to Everything You Need to Know



Data Protection Officers, also known as DPOs, are appointed legal experts who enforce the European Union's (EU) General Data Protection Regulation, or GDPR, within an organization. DPOs aim to inform organizations and help them comply with data protection laws and regulations. Thus, DPOs are essential to fully understanding and complying with the GDPR and supporting an organization's seamless adaptation to the new and fast-changing world of data protection. This article explains what services Data Protection Officers provide, highlighting why it is necessary for organizations to consult with these officers.

What are DPOs?

DPOs are highly qualified legal professionals who are expertly trained on the GDPR and aim to secure an organization's compliance with the regulation. Certified Data Protection Officers are highly skilled professionals who have extensive professional experience, expert knowledge on data protection law, and the demonstrated ability to fulfill the DPO responsibilities laid out in Article 39 of the GDPR.

Each DPO is designated to one or more organizations and can be either internally hired or externally sourced by the organization. While many organizations are not required to hire a DPO, the benefits of hiring a professional far outweigh the costs. Article 37 of the GDPR outlines the three cases where the DPO designation is mandatory:

- When data processing is carried out by a "public authority"
- When the data processor or controllers' "core activities" require large-scale, frequent, and routine monitoring
- When the data processor or controller is involved in "large-scale" processing of "special categories" of data

DPO Expertise and Qualifications

The GDPR does not strictly outline an official path that individuals must take to become a DPO. However, DPOs hold highly influential, specialized, and essential roles in an organization. Thus, the Data Protection Commission issued official guidelines that are important to consider when hiring or training a successful DPO.

- **Level of Expertise**: DPOs acquire a level of expertise that is consistent with the content, sensitivity,

complexity, and size of data that an organization processes. DPOs will also become experts on the processing operations and private policy within their designated organization.

- **Professional Experience**: DPOs possess an in-depth understanding of data protection law, legal compliance, risk management, data security, business procedures, and other technology operations. Additionally, DPOs thoroughly understand Italian, European, and international data protection laws and regulations. There are several ways that DPOs can get this information and experience.
    - **Education**: Obtain at least a Bachelor's degree from an accredited university. Successful DPOs often study law, cybersecurity, business, or computer science
    - **Certification**: Become a Certified Data Protection Officer (CDPO) by taking an official GDPR training course and passing the subsequent assessment

- **Accessibility**: A DPO can assist one or more organizations as long as they are substantially "easily accessible" within the organization, according to Article 37(2) of the GDPR. Being "easily accessible" entails that the DPO must be able to communicate effectively in the language of the supervisory authority, have extensive professional experience, act independently of the organization, be free of any conflicts of interest, and be readily available to accommodate the organization. Additionally, DPOs are the lead contact on all compliance matters and publicize their contact information, in line with Article 37.
- **Service Contract Basis**: DPOs can be hired on a service contract with an external organization if several conditions hold true
    - **Contract Requirements**: The DPO must meet all of

the requirements and responsibilities outlined in GDPR, which includes having no conflict of interest with the organization
- **Employment Protection**: Each employee is protected by the provisions of the GDPR. DPOs are protected from wrongful termination. Employees within the organization are protected from unfair dismissal for carrying out assigned tasks.

In addition, there are more ways current DPOs can illustrate their expert knowledge. Some other ways DPOs can distinguish themselves include:

- The content, difficulty, applicability, and means of the GDPR training assessment taken
- The course of study taken and the standing of the accredited university
- What time the GDPR training was received, and how much business or technology sector experience individuals have since receiving their certificate
- Whether the GDPR training and certification are recognized internationally
- The level of non-technical skills, such as communication and leadership, which reflects one's ability to successfully advise others within an organization

Roles and Responsibilities of DPOs

The primary role of DPOs is to assess all organizational matters related to data processing and consumer protection in a way that is confidential and shielded from external influence. According to Article 38 of the GDPR, DPOs are independent advisors to data processors. They cannot receive tasks or instructions from any supervisor, executive, or

processor within any given organization. Instead, they base evaluations strictly on the organizations' compliance with EU regulations, and their job performance remains confidential to external actors.

As independent reviewers, DPOs are responsible for evaluating all data sharing and collection practices and determining whether they fit in the EU framework. To hold DPOs accountable for their responsibilities, Article 39 of the GDPR outlines the six key responsibilities of DPOs:

- Ensure data processors understand the data protection requirements of GDPR
- Monitor data processors' compliance with the GDPR and their own private policies, including their alignment with key frameworks, proper staff training, raising awareness for data security initiatives, safeguarding processing operations, and conducting necessary audits.
- Advise data processors on areas for improvement and adjust data collection practices accordingly. This can be done by conducting data protection impact assessments, monitoring performance metrics, and tracking compliance with the applicable regulations
- Cooperate with higher authorities, especially those within the European Union
- Remain the data processors' key point of contact on all data protection and GDPR compliance matters, consult data processors on the potential risks of non-compliance, and report any issues related to data processing to higher authorities
- Understand and communicate to data processors the risks associated with data processing operations and practices



Why Consult with a DPO?

There are several reasons why organizations should consult a DPO. For one, GDPR requires many organizations to designate a DPO. Nonetheless, DPOs are advantageous for any organization. As experts on GDPR law, DPOs enhance existing data security practices and act as the first point of contact for all GDPR and data security matters. DPOs can help organizations avoid the harsh fines and penalties associated with GDPR non-compliance.

DPOs can also manage consumer privacy concerns and mitigate the risk of data breaches. Truth be told, data breaches are extremely costly instances, especially for medium to large organizations. In 2024, the average data breach cost rose 10% to over $4.9 million, which is more than 50 times higher than the average annual cost of hiring a DPO. In other words, organizations can save millions by hiring a DPO. By minimizing security costs, DPOs ensure that consumer data is protected and organizations remain compliant with the GDPR. Even in the event of a data breach, DPOs lead investigations into the situation, involve the relevant authorities, utilize their expertise to mitigate the consequences of the breach, and enact the appropriate changes to prevent future breaches.

DPOs also hold their organization accountable to GDPR standards. This source of accountability helps current organizations avoid fines and penalties. In the past, mega corporations such as Meta and Amazon have paid GDPR fines as high as $865 million. DPOs build a culture of transparency, data protection, and compliance within an organization. Even more so, by instilling such values, DPOs, in turn, can enhance an organization's reputation, consumer loyalty, and public trust.

Another reason DPOs are beneficial is their role in monitoring and evaluating third-party vendors. They assess the risk associated with vendors through preemptive measures such as risk assessments. Such risk assessments can help organizations understand the risk linked to vendors' business operations, data security practices, financial stability, compliance with regulations, and overall public image. In the long run, DPOs can inform an organization's strategic decisions about who to partner with.

In summary, DPOs use their expert legal knowledge and training to assist organizations in several ways. These include, but are not limited to, mitigating security risks, reducing the cost of data breaches and maintenance, preemptively improving data security practices, organizing data accurately and safely, increasing transparency, and boosting an organization's reputation.

Hiring A DPO: Internal vs External

After deciding to hire a DPO, the next step is choosing an internal (in-house) or external (outsourced) professional. Internal DPOs are hired and employed directly by the organization. They typically have long-term salary requirements, additional training opportunities, and extended protections against dismissal. External DPOs are hired via a service contract from an external organization. These

professionals typically come at no additional cost beyond the agreed-upon hours and hourly rate.

While organizations can opt for either an internal or external DPO, there are several reasons why an external DPO is a more effective choice for ensuring proper data protection and compliance with the GDPR.

- **Independent Oversight**: Although internal DPOs have pre-existing knowledge of organizational processes and needs, their close association often presents a conflict of interest and a threat to objectivity. An external DPO has minimal bias, no conflict of interest, and can act without constraints as required by Article 38 of the GDPR.
- **Experience**: Internal DPOs' expertise is limited, time-consuming, and costly because they must be regularly trained on both GDPR and an organization's private policy. Conversely, external DPOs bring specialized knowledge from various organizations, are already expertly trained, and are always updated on legal requirements as required by Article 37(5) of the GDPR. External DPOs' vast experience minimizes the costs that organizations otherwise incur from hiring and training an internal officer.
- **Flexibility**: While an internal DPO's expertise is limited to organizational matters and practices, an external DPO's experience stems from in-depth training and exposure to multiple organizations. This broad experience creates greater flexibility, where external DPOs offer a more nuanced perspective on laws and regulations in an industry and draw from numerous perspectives to solve complex problems.

Costs and Benefits of Hiring a DPO

When laying out the total costs and benefits of DPOs, it becomes apparent that hiring a DPO sets an organization up for great long-term success. Although the upfront costs of hiring a DPO can be high, experts suggest that the professionals pay off in the long run by minimizing costs, mitigating the risk of data breaches, avoiding fines for failure to comply with the GDPR, and overall instilling more robust data security within an organization.

- **Costs**: Organizations incur most of these costs upfront. These include costs associated with payment, benefits (internal DPOs only), recruitment, turnover, training, tools (e.g., audits or data assessments), preventative measures (e.g., emails, calls, and communication with regulators), crisis responses, and labor inefficiencies.
    - **Quantifying the Costs**: The costs associated with hiring a DPO depend on the type of DPO, the sector, and the organization's size. Current evidence suggests that hiring and training an *internal* DPO costs anywhere from $40,000 to $150,000, depending on the size and sector of an organization. Hiring and training costs for *external* DPOs are significantly lower because organizations pay the agreed-upon hourly rate with few additional costs. Additionally, there are numerous smaller one-time costs associated with DPO tasks, such as crisis management and compliance assessments, which also depend on the size and sector of an organization.

- **Benefits**: Organizations receive many intangible benefits after hiring a DPO. These benefits range from avoiding future costs of data breaches to lowering the number of data breaches to streamlining data security practices

and policies.

- **Quantifying the Benefits:** In 2024, IBM Security estimated that the global average cost of a data breach was $4.9 million, and the average cost savings from adopting better data security measures was $2.2 million. While the exact benefits vary between organizations, the benefits of hiring a DPO often significantly outweigh the costs.

Conclusion: How to Get in Contact With a DPO

Data Protection Officers are key actors in any organization. Not only do they act as the first point of contact on all GDPR and data protection matters, but their knowledge and expertise make them a valuable resource for pinpointing future business needs and changes to data practices. In short, DPOs' highly skilled and technical role leaves them with a heightened potential to improve efficiency and cut costs in any organization.

A.L. Assistenza Legale hosts a team of lawyers with vast experience working in data protection law and are skillfully trained on GDPR compliance. Our lawyers assist clients in Italy with hiring a DPO and remaining compliant with GDPR requirements. We also work closely with organizations within the US and other foreign nations to move their business operations to Italy and adjust their data practices to be GDPR compliant.

If you have any questions about hiring a DPO, wish to get in touch with a certified DPO, or would like to consult with one of our lawyers, feel free to contact us!

FAQ

Which organizations should hire a Data Protection Officer?
The GDPR states that data processors are required to hire a DPO under certain circumstances, including data processing that (1) is carried out by public authorities, (2) necessitates large-scale monitoring, and (3) consists of large-scale, special categories of data. However, any organization will benefit from hiring a Data Protection Officer because they can mitigate instances of non-compliance and avoid costly data breaches as the leading expert on all GDPR and data protection regulations.

Why is hiring a Data Protection Officer a smart investment to make?
Hiring a DPO always pays off in the long run. Although organizations must pay a salary or hourly rate, a DPO's intrinsic value is very high. To be more specific, experts suggest that the average annual cost of hiring an internal DPO is between $40,000 and $150,000, and the benefits are as high as $5 million. Additionally, a report by IBM Security suggests that various security measures saved organizations over $2.2 million in 2024.

Who holds Data Protection Officers accountable?
DPOs are held subject to the GDPR and are required to cooperate with the higher EU authorities. DPOs are highly skilled, expertly trained officers appointed by the EU. However, they are not immune to penalties or consequences for wrongdoing. If a DPO acts against GDPR, they will face harsh penalties and strict punishment, just as any country in violation of the GDPR would.

What are data protection impact assessments? Why are they necessary?
According to Article 35 of the GDPR, data protection impact assessments are a form of preemptive action over new, high-risk, large-scale, or publicly-accessible data processing

technologies. In other words, data protection impact assessments require data processors to test their processes and technologies ahead of time.

The GDPR explicitly requires organizations to complete these assessments when evaluating (a) personal data that is subject to digital processing or profiling and produces legal effects that impact the consumer, (b) processing “special categories” of data as laid out in Articles 9 and 10, and (c) monitoring publicly available data on a large scale.

These assessments are necessary because they mitigate threats to consumer privacy and examine the lawfulness and compliance of high-risk data processing systems. It is important to use these assessments ahead of time to minimize the future risk of data breaches or GDPR violations.

What does GDPR say about data protection officers?
The GDPR outlines the purpose, goals, tasks, and assignment of DPOs in multiple articles. Article 37 outlines when and where DPOs should be assigned to an organization; Article 38 explains what the position of DPO entails; Article 39 carefully explains the key tasks, goals, and responsibilities of DPOs. Finally, Article 40 shares a general code of conduct for all stakeholders to follow, including DPOs.