From Here to DPO: Building a Data Protection Officer

iapp

Europe's General Data Protection Regulation requires all public authorities in the EU and many private organizations to appoint a data protection officer to help with GDPR compliance. Organizations whose core activities involve processing EU citizens' personal data on a large scale, or who consistently process highly sensitive data, must appoint a DPO, even if they are not located in the EU. Further, the Article 29 Working Party, which interprets the GDPR, has recommended that most organizations err on the side of appointing a DPO, whether or not strictly obliged to by law.

Because of this mandate, the IAPP has conservatively estimated that at least 75,000 DPOs will be needed to manage EU citizens' data around the world.

Who can and should be the DPO? Is it simply a contact name on the website for consumer complaints? Or perhaps slightly more involved, like the agent designated for copyright take-down notices?

In fact, the DPO position is a new professional role with some hefty responsibilities. It must be filled with someone "designated on the basis of professional qualities" with "expert knowledge of data protection law and practices." DPOs work closely with data protection authorities, serving as their contact inside the organization and helping to ensure GDPR compliance. They are expected to train staff on proper data handling practices, keep up with changes in law and technology, and understand how to build, organize, implement, manage, and constantly update data protection programs.

The DPO needs to be a savvy operator who can serve many constituencies, evaluate risk, and prioritize efforts.

It's a big job. Our conservative estimate, outlined below, says that DPOs are likely to need at least 21 hours of training to get to a baseline level of competence for the position.

Let's unpack the DPO's new job description, much of it derived from recent guidance issued by the Article 29 Working Party, and look at how professionals are likely to gain the skills, credentials, and expertise needed to fill this important role.

Understanding the GDPR

The DPO's most significant credential is a solid understanding of the GDPR. This may come more naturally to professionals who are trained in the law, although ability to understand the organization's mission and core operations, and fluency in technology, are also crucial skills.

Organizations collecting and using large quantities of personal data, and certainly those processing sensitive personal data, require a DPO with more experience and expertise than others. So, a hospital, social media site, or mobile fitness app will need a DPO with several years of experience in privacy law and compliance, while a hair salon might not. Large, multi-national organizations will likely need to appoint a DPO with advanced professional credentials, perhaps even a law degree, while smaller organizations may be able to appoint someone who can use on-the-job training time to fulfill the DPO duties.

Regardless of a DPO's educational background, he or she "must have expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR." This means the DPO must be able to read and understand the GDPR's terminology, and as well be familiar with privacy law practice for purposes of implementing its mandates.

The good news is that everyone is more or less in the same position in regard to the GDPR: Because it is a new regulation that has yet to take effect, we are all just learning what it says and what it means. And here's more good news: A whole new community of organizations has created GDPR training, as set forth in the appendix to this paper, to help would-be DPOs get up to speed quickly.

GDPR Training Programs + Professional Certification:
Average Number of Hours: **25**

GDPR Training Programs (no certification):
Average Number of Hours: **17**

DPO Academic Programs:
Average Number of Hours: **78**

Someone assigned or seeking a DPO position can expect to spend at least three days, on average, studying the GDPR and taking a certification exam, and can expect to spend around €1,500. These programs are ideal for people already familiar with data protection principles, or with a legal or compliance background. For those needing to convert to this new profession from an unrelated one, semester-long or year-long programs are launching at academic institutions in Dublin, London and Paris. A student can expect to spend an average of 78 hours and €5,000 for the DPO academic programs.

Privacy Management Skills

GDPR knowledge is necessary but far from sufficient. The DPO also must perform privacy governance tasks. According to the Article 29 Working Party, a DPO must be able to:

- Foster a data protection culture within the organization and help to implement essential elements of the GDPR.
- Advise the controller/processor regarding:
  - Whether or not to carry out a Data Protection Impact Assessment.
  - What methodology to follow when carrying out a DPIA.
  - Whether to carry out the DPIA in-house or whether to outsource it.
  - Whether or not the DPIA has been correctly carried out and whether its conclusions are in compliance with the GDPR.
  - What safeguards (including technical and organizational measures) to apply to mitigate any risks to the rights and interests of data subjects.

The DPO maintains records of processing operations, and will need the professional skill, expertise and demeanor to serve as an advisor on data protection practices throughout the organization. Indeed, the DPO will often answer to the highest levels of management — the CEO and even the Board of Directors — and thus must have solid "soft skills," including the ability to communicate with a wide variety of colleagues and strong personal integrity.

One other notable skill a DPO might need to possess: a way with languages. According to recent WP29 guidance, the DPO "must be in a position to efficiently communicate with data subjects and cooperate with the supervisory authorities concerned. This also means that this communication must take place in the language or languages used by the supervisory authorities and the data subjects concerned." It's difficult to imagine that regulatory authorities expect a DPO at a EU-wide organization to speak every language of the EU, so this may be a further indication that larger organizations should expect to have multiple DPOs for the multiple countries in which they operate and collect EU citizen data.

The Importance of a Privacy Community

The GDPR requires that the DPO be given adequate resources to stay informed, receive ongoing training, and develop and maintain connections with DPOs and privacy professionals around the world who face similar professional challenges. The DPO as liaison between the organization and the data protection authority must also be given considerable independence in deciding how to deal with a matter, what result should be achieved, how to investigate a complaint, or whether to consult the supervisory authority.

One can imagine that being the internal GDPR compliance watchdog could get a bit lonely. By joining a network of privacy professionals and attending events, a DPO can keep abreast of regulatory updates and best practices. The DPO can also reach out to privacy professionals at other organizations to seek advice when confronting new privacy issues.

Finally, the WP29 emphasizes on more than one occasion that the DPO needs a solid understanding of ethical responsibilities. Of course, this question of data ethics might well be the hottest topic in privacy today. It stands to reason that a DPO will need to be in frequent conversation with peers in order to stay abreast of current ethical considerations and ethics issues that arise with new technological developments.

As organizations identify which positions might suitably serve as the DPO, note where conflicts of interest might arise, and create safeguards so that there is space for ethical discussions to take place, it will be vital that they think deeply about this brand-new role and how the person who fills it will be developed and supported.

The only GDPR program that offers privacy management training is the IAPP's Certified Information Privacy Manager (CIPM) program. The CIPM paired with the Certified Information Privacy Professional Europe (CIPP/E) training and certification provides the ideal DPO-Ready package. These programs are available as two separate two-day trainings, or as combined four-day training with exams.

Appendix: A survey of available training options

Host	Duration	Certification
Act Now GDPR Training	1 day/8 hours	No
Act Now GDPR Training + Certificate	4 days/32 hours	Yes (GDPR Practitioner Certificate)
Audit Serve: GDPR Assessment, Implementation and Auditing	2 days/16 hours	No
Brussels Privacy Hub: Implementing the GDPR	2 days/16 hours	No
Copenhagen Compliance: Certified EU GDPR Compliance Foundation Training	1 day/8 hours	Yes
Deloitte DPO Course	5 days/40 hours	No
DLA Piper DPO Training Academy	3 days/24 hours	Yes
Focus on Training	4 days/32 hours	Yes (Certified EU GDPR Practitioner)
Holyrood: GDPR and the Public Sector	1 day/8 hours	No
IAPP CIPP/E + IAPP CIPM	4 days/32 hours	Yes (CIPP/E and CIPM)
ICS: Subject Access Requests GDPR	1 day/8 hours	No
ICS Skills: Data Protection Training	3 days/24 hours	Yes (Data Protection Practitioner Certificate)
Institute of Direct & Digital Marketing	1 day/8 hours	No
IBITGQ GDPR Foundation Training (delivered by IT Governance + Purple Griffon)	1 day/8 hours	Yes (EU GDPR Foundation)
IBITGQ GDPR Practitioner Training (delivered by IT Governance + Purple Griffon)	4 days/32 hours	Yes (Certified EU GDPR Practitioner)
UK Training Worldwide: Preparing for the GDPR	1 day/8 hours	No

DPO Academic Programs

Henley School of Business GDPR Transition Programme	**84 hours**
UC Dublin Institute of Banking Professional Certificate in Data Protection	**30 hours**
Université Paris/ Hogan Lovells Degree in Data Protection	**120 hours**