



Choosing the best *candidate* as your Data Protection Officer (DPO)
Practical guidelines for organisations

May 30th, 2016



Whether compulsory or not it, if information on individuals is relevant for your organization to operate and/or to build your business, you need qualified people to help you in embedding privacy culture in your organization. Indeed, you need to comply with privacy regulations which are complex and not business-friendly and be able to increase the value of this information and the related processes and technologies. Therefore, you need ... a Data Protection Officer (“DPO”) on board!

This is true not only for to private companies but also state agencies, public benefit organizations and many others. To have a DPO is an essential part of your privacy governance which is a clear sign you show to your clients, users or citizens that you care about their personal data, i.e., that you care about them. In addition, a DPO is the best interlocutor that your organization may have with your local data protection authority and may help your organisation cutting red tape.

Can you imagine an organisation working efficiently and responsibly vis-à-vis its stakeholders with no finance, community manager/marketing or HR director? The same applies to the DPO in today’s organisations and, even more, in the near future in a globalized and digital economy and with a complex EU privacy regulation with fines up to 4% of the global annual turnover.

So, who to look for? What to expect from the candidates?

1. Expert knowledge

Pursuant to most current local laws and in the EU regulation that will enter into force in 2018, DPO should have sufficient knowledge to fulfill the role. This is particularly important if you are in one of highly regulated sectors (e.g. healthcare, finance), plan to use data considered sensitive, simply use personal information of any nature as one of the main assets of your activity or wish to use privacy as a competitive advantage.

Therefore, the candidate’s level of expertise of data protection laws and regulations should be among key factors you should consider when choosing a DPO. A DPO should not be a nay-sayer as a general rule. Competent DPOs with expert knowledge is able to overcome the “no” response by suggesting practical yet compliant solution, together with other stakeholders. Only a true expert is able to identify the limited times when a no-go answer is the right thing to do.

This is where experience plays a crucial role. So far there is no school for the DPOs, where graduates receive recognizable certificates. Indeed, to date, there is no “DPO” degree at the University as such but privacy masters and certifications have been and will be proliferating. On the other hand, there are few things better in this world than a DPO who wishes to be up-to-date and invests in his/her self-development. Within this context, which are the criteria to determine that the right expertise is there?

“Privacy on the books” and “privacy on the ground” would be a good combination.

Candidates will probably show you a lot of certificates and diplomas they have gained over the years to show how qualified they are. But how to tell which are valuable and which are not? First thing, you should check is the credentials of the party giving the training and certification. If it is a well known accredited pan-EU or national organization (in some countries even data protection authorities are certifying), you may feel more comfortable. Also, find out the agenda of the training courses. A one day event or certifications obtained mainly as a result of a payment and a very simple exam will not have anyone trained into a reliable DPO.

2. Organisational factors

Another consideration needs to be given when choosing a candidate are privacy needs and the resources that your organisation will be able to allocate to the DPO functions. A DPO will need to cover, by himself/herself (in small organisations) or, otherwise, through his/her own team or ad hoc network within the organization (otherwise), legal, IT and compliance skills. The experience shows that current DPOs have different technical backgrounds and no one seems to be more “perfect” than others. Indeed, the background profile of CEDPO members is diverse: lawyers, IT/Security officers, compliance officers or even marketing managers.

Internal or external DPOs will provide you with different solutions and will need a different level of resources (in terms of salary/professional fees, civil liability insurance, team members, technology, etc.). The appropriate level of resources is one of the elements that would make the DPO successful. In particular, in complex organisations, you will need to think whether the DPO will be assisted or not by other people internally who will complement his/her skills, on a permanent basis (the DPO team) or as required from time to time (an external counsel?).

The DPO’s position within the organization is another point that needs to be considered in choosing the right candidate: will this person be in the legal department, the IT department, or in marketing? For example, depending on type of processing operations you conclude, it could be better to put a DPO within IT structures or processes. This relates more to organizations which have limited data flows and their main concern is security. In case where you use multiple data sources for various purposes with close relations to your income, it could be better to put DPO closer to the business operations.

In any event, if a candidate demonstrates strong skills and reliability and you feel that he/she will meet the main organisation privacy needs, do not dismiss him or her just because of a specific background.

3. Personal qualities: a communicator

In order for DPO to be effective, one should be on ground, not only available to various stakeholders within your organization but proactively looking for opportunities to interact with different departments. Sure, it is possible just to have a person that green lights new projects and updates privacy policies from time to time. But is this all the added value you

look for? In addition, the EU regulation in 2018 will require going beyond a mere compliance function (which will be more complex in any event).

DPO has to face a number of challenges and with different interests at stake. That is why DPO should also show strong communication skills combine with refined diplomacy. A DPO is not (and should not be) a “privacy” activist: with the support of the remaining leaders of the organisation, he/she must play a role of responsible business-enabler and help the organisation to include privacy in the business-decision processes, to not only detect and prevent risks but also create value. In addition, the EU regulation in 2018 will require that his/her reporting line is the highest level of the management and to ensure his/her independence. This will require some kind of “gravity” and leadership skills as well.

So here it is, congratulations, you have found a perfect candidate for your DPO (internal or external)! Now, why not give him/ her the best working environment to ensure his/her success? You should consider:

- How to ensure the DPO independence
- The effective level of resources to be allocated to the DPO
- To establish the appropriate reporting line
- If not a full-time job: how to deal which conflict of interests
- If you are a group of companies and this person will be the EU-wide (single) DPO, which would be his/her network in each establishment

Look for other CEDPO’s publications coming your way, that will deep dive into those matters.



About CEDPO:

CEDPO was founded in September 2011 by European Data Protection Organisations, namely, AFCDP (*Association Française des Correspondants à la Protection des Données à Caractère Personnel*) of France, APEP (*Asociación Profesional Española de Privacidad*) of Spain, GDD (*Gesellschaft für Datenschutz und Datensicherheit*) of Germany, and NGFG (*Nederlands Genootschap van Functionarissen voor de Gegevensbescherming*) of The Netherlands. The Confederation was soon joined by ADPO (Association of Data Protection Officers) of Ireland, ARGE DATEN of Austria and SABI (*Stowarzyszenie Administratorów Bezpieczeństwa Informacji*) of Poland.

CEDPO aims to promote the role of the Data Protection Officer, to provide advice on balanced, practicable, and effective data protection and to contribute to a better harmonisation of data protection law and practices in the EU/EEA.

Contact information

Email: info@cedpo.eu / Website: www.cedpo.eu

