CASSIE SYRENIS

Data Protection

The requirements of a Data Protection Officer

The challanges faced and opportunities created

Tash Whitaker, a leading Privacy Specialist, informs for Syrenis, on the subject of the increasing importance for the requirement of Data Protection Officers and why they are so crucial to have within your organisation.

Introduction

An early morning email alert from LinkedIn beeps on my phone: "58 new Data Protection Officer roles you may be interested in". That's in addition to the 30 or so I was alerted to yesterday. The demand for Data Protection Officers (DPOs) is growing exponentially, but a quick look through the job descriptions shows me that the role is still highly misunderstood. Requirements in today's (mainly private sector) adverts include:

> "An understanding of GDPR… with, desirably, an appropriate qualification"
> "Basic IT knowledge … and previous use of Microsoft Office",
> "reviewing contracts for the DP bits"
> " Some knowledge of Data Protection legislation"...
> ...as well as roles being combined such as
> " Group Data Protection Officer, UK Head of Compliance and MLRO"[1].

These descriptions show little understanding of the role as it should be on paper; let alone the challenges faced by the DPO in reality on a daily basis.

In order to understand the role and the challenges, it is necessary to look at two main sources; the General Data Protection Regulation (GDPR) itself, and the accompanying Article 29 Working Party Guidance in Data Protection Officers, revised and adopted on April 5th 2017 (WP29). These documents clearly breakdown when a DPO is needed, the skills and expertise required, their position in a company and the tasks that they are required to perform.

[1] MLRO – Money Laundering Reporting Officer

Requiring a DPO

According to Article 37 (1) of the GDPR, a controller or processor must appoint a DPO under the following circumstances:

01 the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

02 the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

03 the core activities of the controller or the processor consist of processing on a
04 large scale of special categories of data … or personal data relating to criminal convictions and offences…

It's safe to assume that all the companies currently advertising for a DPO role have therefore looked at this article and ascertained that they wish to appoint a DPO, as they fulfil one of the three criteria. It may also be, that the company has chosen to appoint a DPO without fulfilling this criteria, because they see it as the right thing to do for their customers. In fact, the WP29 actively encourages this. When that is the case, it is important that the company realises that the "voluntary" DPO is still subject to the conditions for his or her appointment, position and tasks as set out in the GDPR.

If a company doesn't appoint a DPO, the WP29 recommends that they should document how and why they have come to that decision. I tend to recommend that clients revisit this analysis on an annual basis or if there are significant changes to the services that they provide, or the data processing carried out.

If a company does not need to appoint a DPO, and does not make a voluntary designation, they should still have someone responsible for overseeing their data protection activities. However, they should not call that position a DPO, their role should be clearly communicated as having responsibility but not the title. This is often the reason we see job adverts like the ones mentioned above; those tasks/requirements are needed by the business, but they are not those of the designated DPO.

Expertise and skills of the DPO

This is where so many companies fall down in understanding who they should be recruiting as a DPO. Back in 2017, Thomas Shaw, an EU lawyer wrote that;

"The two professions best suited to carry out the role of the DPO are experienced privacy- and technology-focused lawyers and IS auditors licensed as certified public accountants or chartered accountants" [2].

I, and many others, judging by the feedback on the article, fundamentally disagree with this. At no point does the GDPR suggest that the DPO should be a lawyer. In fact, there have been multiple instances where lawyers have been criticised for providing potentially negligent advice [3], including by the Direct Marketing Association and by lawyers themselves. Don't get me wrong, there are some brilliant lawyers out there, but my personal experience has shown them at times to be too risk adverse and that they can lack an understanding of the business drivers; instead I see them as a valuable business partner of the DPO rather than a DPO themselves.

Article 37 (5) of the GDPR does however state that the DPO must have "expert knowledge of data protection law and practices and have the ability to fulfil the tasks referred to in Article 39" (I'll come onto those!) This is then backed up by recital 97 and WP29 making clear that the level of expertise should be proportionate to the complexity and type of data being processed and that the DPO should have an understanding of the processing carried out and the needs of the controller. In other words, they should fully understand the business for which they are a DPO.

The general recommendation I give to DPOs is that they should ideally hold one of the recognised qualifications such as CIPP, C-DPO or ECPC-B DPO etc. However, I see them in most cases as a tick box exercise and have I expanded on my thoughts in a previous article. [4] Only last week I saw a contact go from no knowledge to CIPP/E in the space of four days – does that give them "expert knowledge"? There is very little that can really substitute knowing the laws, understanding the guidance and any supervisory authority action, and then combining it with business knowledge and stellar communication skills to influence the business.

The expertise of the DPO is not static, and the WP29 recommends that they undergo regular training. This can be a challenge. There are plenty of qualifications and training sessions that are springing for new DPOs but very little ongoing training. I find that I have to spend at least two days of my week reading articles and staying up to date with the most recent court cases and guidance. Webinars that offer CPD points are generally still aimed at those new to the profession, and again, whilst they tick a nice box, the opportunity to learn more is very limited.

[2] https://iapp.org/news/a/what-skills-should-your-dpo-absolutely-have/
[3] https://www.lawgazette.co.uk/news/lawyers-warned-over-potentially-negligent-gdpr-advice/5069473.article
[4] https://www.linkedin.com/pulse/data-protection-courses-qualifications-bit-honest-review-whitaker/

Position of the DPO

When looking to designate a DPO into your organisation, there are a few things that should be considered. Firstly, the DPO is there (according to Article 38) to be "involved, properly and in a timely manner, in all issues that relate to the protection of personal data". WP29 makes it clear that this does not mean that DPO is there to do all the operational work, but instead to be consulted and informed in order to facilitate compliance. This is echoed in the required tasks that they must carry out (again, later…).

The DPO must be given the appropriate resources to carry out their tasks and must not have conflicting priorities. I see this conflicting priorities as key. It is very tempting for a company to combine roles eg MRLO or Head of Compliance. Unless that person is Superman or Super-woman, there is no way that there are enough hours in the day to fulfil the requirements of more than one of these roles. Multiple roles may also lead to conflicts of interest, something else that is highlighted in Article 38, "[the DPO should] not receive any instruction regarding the exercise of tasks" and there must be an assurance that any tasks outside of those designated in the GDPR "do not result in a conflict of interest". WP29 calls out specifically senior management roles as a potential conflict, as well as any role who may be called to represent a controller or processor in court regarding data protection matters.

If there is a perceived conflict, then it is important that the controller documents how this conflict is to be avoided. I have a number of clients who use an external DPO precisely to ensure that there is absolutely no conflict in place. It is particularly important in a smaller business or a start up where employees wear multiple hats.

The DPO must also be positioned in the company so that they report directly to senior management. In the case of an external DPO, they need to have a line of communication to senior leadership at all times. If a DPO isn't heard then they cannot fulfil the tasks designated to them under Article 39 and they cannot succeed in their role.

The tasks of the DPO

This is an area where there is much discussion amongst data protection professionals. The GDPR is clear that there are a set of tasks that the DPO must fulfil, but this does not preclude him/her from carrying out other tasks, as long as they do not conflict with those designated by the GDPR.
So, in short, the Article 39 tasks are:

- Inform and advise the controller/processor of their obligations under the GDPR
- Monitor compliance
- Provide advice on data protection impact assessments
- Co-operate with the supervisory authority
- Be the point of contact as needed for the supervisory authority

I would add to this the WP29 guidance that the DPO should be an intermediary between relevant stakeholders (eg supervisory authorities, data subjects and business units within and organisation).

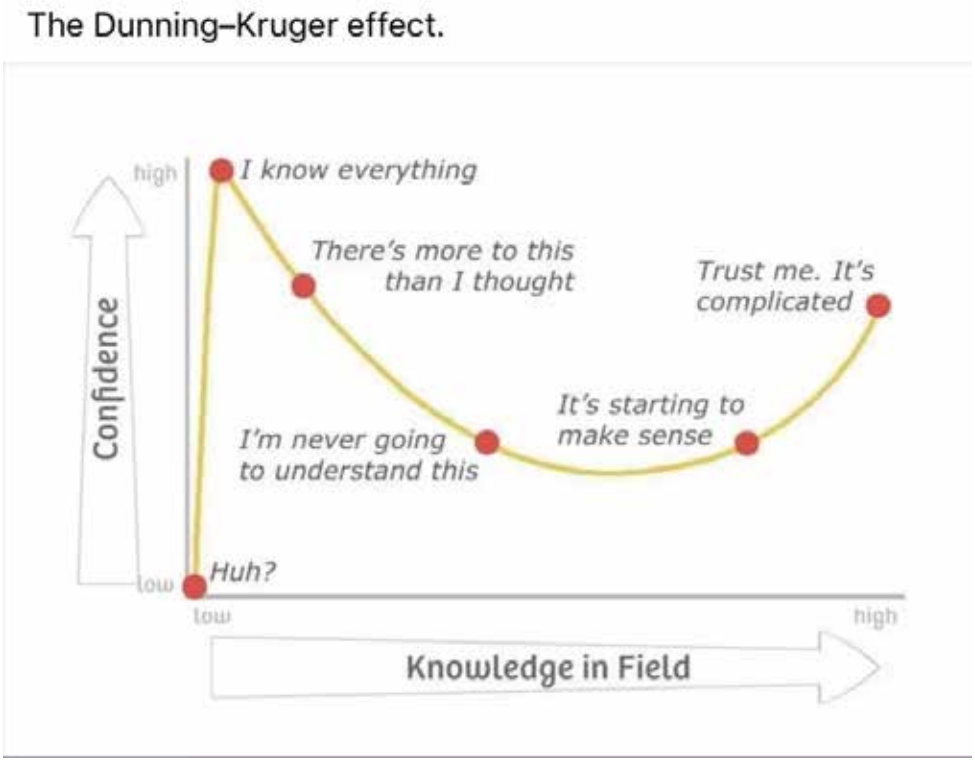
The debate arises from the fact that it is rare for a DPO to only carry out the Article 39 tasks. Most companies have budget constraints that mean that a DPO often ends up "doing" as well as "advising". For some areas, this presents no issue. For example, a DPO maintaining the Article 30 Record of Processing is called out by WP29 as something that the DPO may need to in order that they can monitor compliance and informing and advising the entity. However, there will be situations where being too deep in the day to day operations does cause an issue. The WP29 sets out how a DPO may be involved in doing a data protection impact assessment. The involvement is pretty onerous, but does not go as far as suggesting that the DPO should be the one carrying out the assessment or making the final decision on whether or not processing should be carried out. This is for a couple of reasons; firstly, if you are the employee carrying out the operational work, then you are creating a potential conflict of interest, as you are ultimately policing your own activities. Secondly, the WP29 guidance reminds us that the DPO "does not have decision-making powers extending beyond their tasks pursuant to article 39". The role of the DPO is to advise. If a controller disagrees with the advice provided then that should be documented, but it is the controller who ultimately makes the final decision not the DPO.

This leads nicely to the fact that it is the controller or processor who is ultimately responsible for compliance with the regulations, and not the DPO personally. If the DPO carries out the tasks assigned as per the GDPR, then that DPO cannot be removed from their job, even if the controller/processor does not agree with advice given, or decides to disregard it, resulting in a noncompliance situation. [5]

[5] If you didn't do your tasks, or you messed up in some other way, you absolutely can be fired – you are not invincible!

Final thoughts

As I mentioned, demand for DPOs is rising and businesses are recruiting at an unprecedented rate. But I am not totally sure that these entities are clear on who they should be recruiting and what that role should be. Likewise, I see the same with some professionals who already hold the title of DPO. For some it has become a nice shiny title to add to their previous one of "Head of Marketing" or "Business Development Leader". I don't see knowledge being in place, or the appropriate teams/resource being provided as often as I would like. Companies getting the job description wrong are likely to recruit people who are unsuited to the role and they will be none the wiser until it is too late. The old adage of "knowing enough to be dangerous" and the Dunning-Kruger effect springs to mind on a daily basis.



There are some companies getting this right, primarily in the public and regulated sectors. They are entities who have had data protection embedded into their DNA for much longer than the implementation of the GDPR. However, we have also seen that getting it right doesn't assume a guaranteed level of protection. The recent ransomware attacks on Travelex and Maastricht
University are enough to make any good DPO worry. We know that whilst we carry out our tasks as we should, we are also bound by Article 39 to do it according to a risk-based approach. That approach has to include the type of data, the complexity of processing and therefore perceived risk. That means lower risk work can fall through the cracks. We are only human. Not only that, but many a DPO will provide the correct advice, but then watch the controller/processor view that advice in the grand scheme of corporate priorities and make a contradictory "business decision". The final decision could well seem valid at the time, but is usually the one that results in the later data breach. These decisions may well be documented by the DPO but that doesn't help the impacted data subject. I am fortunate in the role that I have as a DPO-as-a-service that my clients all have a strong culture of compliance, a want and need to do the right thing, and trust the advice I give. But I'm not naive. As a DPO I know that none of us can ever know as much as we need to, and the bad actors out there have way too much time on their hands and too much incentive to ever give up. I believe the most important thing that a DPO can do beyond these tasks is to continue to educate themselves; be aware of what people in the organisation are doing or planning on doing .and be aware of what is happening out there in the industry and bring the two together.

An "understanding of GDPR" and "previous use of Microsoft Office" are nowhere near the level of skills and knowledge needed by a DPO. If you are looking for a DPO role, avoid adverts like that at all costs. Look for the ones that tell you that you will report to the board, that you will be autonomous in your role, you will have the resources needed to fulfil your tasks, that you will have the relevant expertise and experience and most of all, you will be listened to. A DPO who isn't listened to is just an expensive chair filler.