Obsequio
Consent-as-a-Service

HOW TO CHOOSE THE RIGHT DPO

Definition of *Data Protection Officer* in English

Data Protection Officer (DPO)

"DPOs assist you to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority"

Essentially, your chosen DPO should be the one to go through your company with a fine-tooth comb, find the gaps, make recommendations, train your staff and monitor it all in the future.

All organisations have been faced with some tough realisations around data protection in the last couple of years. New policies, new procedures, new responsibilities. One of the key questions I get asked every week is "do I need a DPO?" Then, "how do I choose the right one for my business?".

I'm Chris. I used to be the Operations Manager for a large hospitality company. I'm a founder of Obsequio. I'm also a data privacy guy doing audits, training and providing DPO services to a range of companies.

This document will walk you through the things you need to consider in making your decision:

- Do I need a DPO?
- If yes, what type fits me best?

Do I Need a DPO?

This is two questions…. Do I need one? If yes, read on. If I'm not required to have one, under what circumstances should I think about one anyway?

Any company can choose to have a DPO, even if they aren't required to by law. Some companies choose to name a DPO to show their clients and customers that they take Data Protection seriously, or because they work in a sector that requires more data security scrutiny. The GDPR sets out three scenarios where naming a DPO (Article 37) is a legal requirement:

1) *"Where the processing is carried out by a public authority or body, except for courts acting in their judicial capacity".*
   Essentially, if you are an organisation such as a local council, county council, health authority, etc. then you must have a DPO.

2) *"Where 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".*

Some key words here:

a. Firstly, notice that we are focusing only on an organisation's CORE ACTIVITIES. If you have a large number of employees but don't do any systematic monitoring of data subjects in your day-to-day core operations, then it is unlikely you will need a DPO by law. Although, if your company has a large number of employees then it wouldn't be a bad idea to consider having a DPO anyway. After all, employees are data subjects too.

b. Secondly, it talks about LARGE SCALE. The ICO says that large scale could mean activities which "involve a wide range or large volume of personal data, where it takes place over a large geographical area, where a large number of people are affected, or it is extensive or has long-lasting effects." [1] As usual, it's open to interpretation.

c. Finally, REGULAR AND SYSTEMATIC PROCESSING. This is defined really well in an article earlier this year. Regular = reoccurring and Systematic = pre-arranged, organised or methodical. [2]

Putting it all together, we see that if your core activities involve regularly processing and monitoring personal data of people all over the country, continent or world, in a pre-arranged and methodical way, then you should have a DPO. If you're still reading, the above probably isn't you as you'll have one already. If the above is you, and you don't have one, it might be worth giving me a call.

3) *"The core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10."*

This is quite an easy one to summarise. There is a list of data types that are considered Special Category under GDPR: race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation. [3] Article 10 adds Criminal Convictions to this list. [4] If your CORE ACTIVITIES involve processing this type of data on a LARGE SCALE, then you need a DPO.

Remember, you can choose to name a DPO even if you are not required to by law. You may decide that it is worth the small investment to ensure you're compliant. As with everything in business, it's about how much risk you're willing to take. Personally, the peace of mind I get by knowing my business is compliant and secure is worth every penny. I know that even the most malicious customer or ex-employee will have a hard time finding something to complain about. The most important thing to remember is that if you do name a DPO, then you must also update the ICO with their details.

---

[1] *The ICO, [Online]. Available: https://ico.org.uk/for-organisations/business/guide-to-the-general-data-protection-regulation-gdpr-faqs/*

[2] *Swanscan, [Online]. Available: https://www.swascan.com/regular-systematic-monitoring/*

[3] *ICO, The, [Online]. Available: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/*

[4] *ICO, The, [Online]. Available: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/criminal-offence-data/*

How do I Choose a DPO?

You've been through the process of deciding whether you need a DPO and you've decided you do. What next? Well, the first thing to do is consider who CAN be a DPO. Let's look at what the GDPR/ICO says: [5]

1) The DPO must be independent;
2) The DPO must be an expert in data protection;
3) The DPO must be adequately resourced;
4) The DPO must report to the highest management level;
5) The DPO can be a member of staff, or an external contractor.

Nowhere do the regulations specify what qualifications a DPO actually needs, nor do they specify how to judge whether someone is an "expert in data protection" so common sense must prevail. There are also no hard and fast rules on what qualifications a DPO needs and there are a few different types available. Here are your options:

Train Someone in Your Business (Full or Part Time)

There may be someone in your business who would be a good fit for your DPO role. They already know your business, so they could be a powerful DPO in the future. If you can make sure they are well trained and well supported, then training someone internally could be the choice for you. Remember the five points above though. If you do choose the internal route then they must still be independent, an expert, adequately resourced and report to the highest management level. Furthermore, they will probably have their own day job so making them adequately resourced could mean hiring someone to take on some of their other duties.

If you think that an someone internally fits the bill, then you'll need to think about training. Here are your options:

- **Online Training Course.** Online courses are a great start on the road to becoming a DPO, but they're not enough on their own. They are often seen as the quick and cheap option. A good one will teach you the fundamentals of the GDPR, the wording of the regulation and teach you what your company should and shouldn't be doing.
  Pros:
  - A great way of upskilling an existing staff member without the cost of face-to-face courses.
  - The initial investment will be lower than other face-to-face courses or bringing someone with experience in to the business.
  - Huge variety of courses available.

[5] *The ICO, [Online]. Available: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/*

Cons:

- You cannot expect a person to be an expert after one course.
- They will be the same person, just with a bit of regulation knowledge.
- They will not necessarily understand the audit process or how to interpret the regulation and put it into practice.
- It's possible that the course was written by a data privacy expert but, in reality, it's just as possible that they were written by a training team with as much knowledge as your new trainee.
- An online course does not make a person an 'expert'.

- **Face-to-face/Classroom Training.** When delivered by the right person, these courses are a great way of teaching one of your team all they need to know about the regulation. With some real-life examples and specific industry advice, they can be extremely beneficial. They are instructor-led so are much better than any online course. Your new DPO will be able to ask questions specific to your business and will be much more engaged.

  Pros:

  - IF (big if) it is taught by an expert, it means that people new to the role can benefit from the real experience of someone who's done the role before the GDPR.
  - Opportunity for trainees to ask questions.
  - Possible relationship for future investment.

  Cons:

  - After-course support can be lacking.
  - Your new DPO may find themselves with a little knowledge, but no support when things get tricky.
  - The last thing you want is a complaint to the ICO from one of your customers or a disgruntled ex-employee and a DPO who isn't sure what they're doing.
  - You'll probably end up shelling out more money on someone to help them.
  - If the course *isn't* taught by an expert, then your new DPO will come away with as much knowledge as if they'd done an online training course and will again need outside help when things get tricky.

Outsource DPO

A very popular alternative to an internal DPO is to outsource the role to an external supplier. There are a few things to think about when you're looking for an outsource DPO and making sure you make the right choice will define your business.

There are four types of DPO to look out for: The Lawyer, The Marketer, The Cyberist and The Operationalist.

- **The Lawyer.** Normally a qualified lawyer or someone with excellent knowledge of data protection law, spanning back many years before GDPR became a thing. They will be able to give you advice on the strict application on the law and will give a very literal interpretation of the regulation. This is the DPO who will spend much of their time re-writing policies and agreements, bespoke contracts and present you with a list of what needs signing and by whom.

Pros:

- Legal guru so will have an explicit understanding of the law.
- They will give literal guidance on the law and its interpretations.
- Great at counter-arguing supplier and customer contracts and handling the ICO.

Cons:

- Normally disconnected from the real-world operational challenges that new compliance presents.
- Ask yourself if your team would respond well to a training session run by a lawyer.
- How engaged would your teams feel if a lawyer was at the helm?

- **The Marketer.** Normally an ex-marketing expert or someone who still works in digital or direct marketing. This is the DPO who will look at GDPR from the point of view of sending marketing emails. Their primary goal is to find a way to continue to e-market customers and prospects within the constraints of the GDPR.

  Pros:

  - Marketing emails and phone calls are still the number one complaint to the ICO, so their expertise in these areas will be valuable.

  Cons:

  - Can lack experience when it comes to the bigger picture, e.g. not much experience of data protection from perspective of your employees.

- **The Cyber Security IT-ist.** This is the technology-led DPO. The focus will be cyber security and finding technology solutions to assist with the compliance strategy. You can expect some new email and mobile device policies to be near the top of the agenda, along with lots of new acronyms for state-of-the-art security protocols. Because they're driven by IT and IT security, they will try to find an IT solution for everything.

  Pros:

  - Cyber security is a massive risk
  - This DPO will be able to navigate the cyber minefield and advise on the best solutions to plug any gaps.

  Cons:

  - Similar to the marketer, they normally lack experience dealing with the bigger picture.
  - IT is only part of your company.
  - There are also people and offline processes to consider and a business to run.
  - Think about how well your Cyberist would handle training sessions for your teams or complaints from your customers/employees.
  - When was the last time they even saw a paper record so how well could they deal with offline matters?

- **The Operationalist (me).** This is the data protection expert who understands a bit about everything, and more importantly, knows the challenges associated with implementing different solutions. Normally good with process simplification and understands the importance of ongoing staff training. A good one will have experience of dealing with people from every part of a corporation and can tailor training to their needs. For example, the training needs of receptionist

(regular contact with people, one computer, lots of access to personal data records) are very different to the training needs of an on the road Sales Person (regular contact with new people, multiple mobile devices, home-office, paper records). The operationalist can be empathetic to the needs of both and structure appropriate training.

Pros:

- They will understand how processes are simplified.
- It's likely they will be able to visualise best solutions easily and train the right people accordingly.
- As someone with a broad understanding of different parts of the business, they will spend more time making suggestions and training people to do things properly than writing policies from scratch.

Cons:

- Not a legal expert, so may use a few templated documents instead of writing from scratch.

You Choose Not to Have a DPO

Of course, the last option is choosing not to have a DPO (if you don't classify as an organisation that MUST have one). This is perfectly acceptable but remember it does not absolve you or your organisation from your responsibilities under GDPR. You must still do all of the things that a DPO would help you with such as auditing, training, policy writing and checking your cyber security. Somebody in your business MUST still take the lead on all of this. Think carefully about who that will be, because in my experience a lot of people start here and end up coming full circle when they realise how much work could be involved.

In Summary

A lot of **clever owners** of smaller businesses will find someone they can get in the business on a retainer basis and can phone as and when they need their help. If you are a smaller business, then this can work really well. Pay when you need them to help with SARs, policies, training or when you have questions; don't pay when you don't.

For SMEs, the **outsource DPO option is the right choice**. Get someone in to your business initially to find your gaps, action their suggestions and then give a **few hours of commitment** per month to make sure you stay on the right side of the compliance fence.

Remember, you know your company better than anyone else.

Whichever type of person you choose, they must be independent and free from conflict-of-interest. If you are a telemarketing company, for example, then choosing your Head of Marketing is a conflict of interest and should rule them out. Equally, sending someone on a one-day GDPR course and then naming them DPO would be a bad move as they need to be an "expert". Why on earth naïve business owners put their businesses at risk like this, I do not know.

Make sure the DPO you choose is a **real person**. Get someone who will get to know your business properly, and someone understands the sector you work in. I used to be a Recruitment Consultant, so unsurprisingly **a lot of my customers are recruitment agencies**.

My last piece of advice is to **seriously consider the outsource option**. It's a great way of keeping costs down (you'll probably pay for a couple of days a month rather than a full FTE), you'll be able to get an expert in the right field and they'll be able to give you completely independent advice.

As for me, I'm an Operationalist through and through. I am a big believer in getting to know a business properly and looking at using technology solutions only when it brings real value. **My customers benefit** from a DPO who can understand complex processes and suggest improvement from the perspective of Data Protection, as well as operational improvement. **My training sessions cater for everyone** from career executives to apprentices and I get **regular feedback thanking me** for making such a boring subject interesting and engaging. There's nothing better than seeing someone else's review before you make a decision so I've put a few of them on our website, https://www.obsequiosoftware.com/gdpr-pecr-iso-consulting. Take a few minutes to have a read.

Some examples of online courses:

IBITGQ – ibitgq.org
company/ibitgq
IT Governance – itgovernance.co.uk
company/it-governance

Some examples of face-to-face training:

Tim Turner – 2040training.co.uk
tim-turner-845541b3
The International Association of Privacy Professional – iapp.org
company/iapp---international-association-of-privacy-professionals/

Some examples of Lawyer DPOs:

Kristy Gouldsmith, Sapphire Consulting
kristy-gouldsmith

Some examples of Marketer DPOs:

Amanda Williams, Wavemedia UK – wavemediauk.com
amanda-williams-cipp-e-81a4b643

Some examples of Cyberist DPOs:

Nick Baskett, UKGDPR – ukgdpr.org
@UKGDPR
Tom Barker, Agenci – theagenci.com
stuartabarker

Some examples of Operationalist DPOs:

Me, Obsequio Software – obsequiosoftware.com/gdpr-pecr-iso-consulting/
chris-the-ops-guy
Humperdinck Jackman, Euro BPO – eurobpo.eu
humperdinck-jackman-bb43a928

Chris Richardson, Operations Director
Obsequio Software
01223 737288
chris@obsequiosoftware.com

www.obsequiosoftware.com