Data Protection Officer

Contractors

How to pick the right one and not get ripped off by the cowboys

Tim Turner

December 2017

Introduction

The General Data Protection Regulation (GDPR) is a new version of EU Data Protection law to replace the 1995 DP Directive, and in turn our Data Protection Act 1998. Despite the Brexit vote, the Government seems committed to adopting the GDPR, and a Data Protection Bill is currently making its way through Parliament to give effect to some of GDPR's provisions. We will still be EU members when GDPR can be enforced, and adopting it may also help in our admittedly limited hopes of a simple data sharing relationship with the EU after Brexit.

One of GDPR's innovations is a requirement for some to appoint a Data Protection Officer (DPO) with specific responsibilities. The DPO is an independent expert, providing advice and monitoring compliance, as well as liaising with the Information Commissioner (ICO). She or he can be a salaried officer or a contractor – it's up to the organisation. Many have a DP or IG lead who more or less carries out the GDPR tasks already, and my advice to those organisations is to grow up and anoint that person as DPO forthwith. Making a senior person with limited DP knowledge your DPO because you don't trust a junior may be unlawful and it's certainly daft.

The DP market is turgid with nonsense right now. One self-styled DP expert claims to have 20 years of experience, despite never having held a DP job (he also claims to be a Facilities Management expert, which makes a bow with a lot of strings). Another was suddenly a GDPR consultant after completing a training course that lasts 8 hours. Training providers are recruiting candidates with no experience, enticing them with claims about how much money they will earn as consultants. Seeking a DPO service in this environment is like entering a circus – you want a skilled acrobat, but you're surrounded by clowns.

There is no DPO approval process. There is no independent, accreditation body, no Institute of Data Protection, and nothing from the ICO. There is something called the 'GDPR Institut' but it's a Swiss-based outfit with no official or legal status in the UK, the less said about which the better.

I've been a DPO in 3 organisations, and a trainer and consultant on Data Protection issues since 2005, first on the side, and since 2011, full time. I write a DP blog, I tweet about it, and I write stuff like this. I've spent a year talking to and annoying a variety of people to see what they know and where they came from. There are fine folk out there, some long established, some new but with the right skills and approach. And there are also some idiots. This guide is intended to help you weed out the dross, and find the right DPO for your organisation.

Tim Turner
December 2017

1 The DPO role

1.1 Do we need one?

Article 37 of the GDPR requires some organisations to have a data protection officer. The GDPR's demands are a tall order; though the list of tasks is familiar to many people with a Data Protection or Information Governance background, the independent fashion in which the GDPR DPO operates is different.

When I was DPO in the last decade, I had direct access to senior management because that was what they wanted. But Chief Executives come and go and the approach changed with them. This GDPR DPO role is designed to avoid this problem – though they must give risk-based advice tailored to their employer's circumstances, the DPO's independence (and the requirement to consult them) is mandatory.

Three types of organisation must have a DPO:

- Public authorities, i.e. in the UK, this is every organisation covered by FOI (either FOI 2000 or FOISA 2002)
- The organisation's core activities involve processing on a large scale special categories of data or data relating to criminal convictions or
- The organisation's core activities require regular and systematic monitoring of data subjects on a large scale

The public authority test is easy because it is binary – either you're covered by one of the UK's FOI Acts, or you're not. The other two tests are subjective. The Article 29 Working Party (A29 WP), composed of representatives from Data Protection Regulators and the EU itself, issued guidance about DPOs in April 2017. If you're wondering if you need a DPO, you have to read that document, so do that now!

The flaw in the A29 WP guidance is the analysis of 'large scale'. They throw out factors – volume of data, geographical extent – without coming to a conclusion. There are a number of possible reactions to this problem – you could decide that if the A29 WP can't make up their minds, neither can you (which is a bad idea), or more constructively, you could decide that whatever answer you come up with, it won't be a disaster.

If you decide that you do need a DPO and it turns out that you didn't, appointing a good DPO still gives you the benefit of an independent professional, advising you on risky legislation. It's not that bad. On the other hand, if you decide that you don't need one and then guidance or an ICO decision suggests that you're wrong, it is unlikely that the ICO will enforce on you if you have documented your rationale. Enforcement is likely only where a breach can be traced back to the lack of proper advice (i.e. advice that would have been sought from a DPO), or where you

ignored more specific advice from the ICO that doesn't currently exist. The ICO doesn't have the resources or the moxie to second guess a data controller's DPO decision without a big breach forcing them into it.

Whether you need a DPO is a risk-based decision. Read the A29 WP guidance (nothing published by the ICO adds anything), then roll the dice.

1.2 Do we need an employee or a contractor?

If you do need a DPO, the next question is whether you should employ someone, or use a contractor. The text of the GDPR is neutral: "*The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.* A recital states that data protection officers, whether or not they are an employee of the controller "*should be in a position to perform their duties and tasks in an independent manner*". The DPO contractor is arguably independent, and if you let them to carry out their role properly, you should be able to meet that requirement. Separately, there should be no conflict of interest between the DPO's role and any other tasks that they carry out for the organisation. Avoiding a conflict of interest is arguably easier if you use an external DPO.

A29 WP say that a DPO contractor can combine the expertise of different people under a lead consultant, so in theory, you could benefit from a team that includes a lawyer, an IT security expert, a former DPO, a policy guru and an auditor if you find the right provider. That's a big 'if' though, as many consultants have been working on DP for a short period of time, and offer one of the above if you're lucky. If this guide has one overall message, it's this: **don't take any claim at face value**.

1.3 What should the DPO do for us?

The primary DPO role is giving advice on DP issues. The DPO is your expert on the legislation and how applies to you. You seek their advice when you receive a subject access request, when the police want information in relation to an crime, or when you need to work out whether to inform the ICO or the affected public about an incident. The DPO has to be available immediately and capable of thinking on the spot.

The DPO also monitors your organisation's compliance – not just the law itself, but other relevant legislation and your own policies and procedures. They have to be someone you trust with access to your premises, your files, your data and your staff. The relationship between you and your DPO is ongoing, even if they are a contractor. Swapping from one to another will mean losing insights and specific knowledge they gain by working with you, and starting again with someone else. If your DPO is in it for the short term, they're useless.

A DPO is not a project or change manager. You might well need someone with change or project management skills to get things lined up, but May 2018 is not a cliff-edge deadline. If you haven't completed everything you need to by then, it's not the end of the world. The DPO is an advice-giving, monitoring role – if the person you're dealing with know is focussed on setting up structures and processes, they're not the right person to be the DPO. You might need two people – DPO and project manager – and if you do, find someone who is a good project or change manager and match them with your DPO.

1.4 Basic checklist – do not use anyone who cannot pass these tests

- The company has a Data Protection notification – they should have '*Consultancy and Advisory Services*' as part of it. Go here and check their company name https://ico.org.uk/esdwebpages/search

- They have transparency information on their website for any mailing list, newsletters, 'whitepapers' or other information-gathering tools.

- The website should clearly identify who owns and runs the company. If they are a limited company, the company number should be clearly displayed on the website. It's illegal for a company not to display their company number (some consultants are sole traders, and legitimately won't have a company number).

- Individual consultants should be named on the company's website. A company claimed to be the 'UK's leading GDPR consultancy' only a month after being set up, but there was no information on who the consultants were. You should be able to find out the professional background of the people who want to be your DPO before you ever speak to them.

2 Look at the company

Although some companies hype up the GDPR as a revolutionary change, it is not. The six GDPR principles are similar to six of the eight principles in the DPA / 1995 Directive. Even elements that seem new, like incident reporting and impact assessments, have been mainstream good practice for a decade. Long story short: GDPR is not new. It is not a revolutionary change unless you haven't properly complied with Data Protection up to now – if that's the case, just about the worst person to guide you through it is someone who is as new to the subject as you are.

2.1 Positives

2.1.1 Experience

Ideally, the company should have DP experience well before GDPR was a reality. GDPR was agreed in December 2015 – look for someone with experience from before then. Some parts of GDPR are new but most of the alleged innovations have roots in the current legislation or its application. Even the so-called 'accountability principle' which some consultants tout as requiring a massive culture change is simply a requirement to have measures in place to make Data Protection compliance work.

2.1.2 References

The company should offer testimonials or references about Data Protection work from named existing clients in your sector. Make sure that you can speak to clients without interference from the DPO, and check whether there are any connections between the referee and the DPO. A DP 'expert' tweets endorsements from clients that turn out to be companies he also runs – make sure that the endorsement is genuine.

2.1.3 Methodology

Your consultant should have clear processes for implementing Data Protection practices. For example, how to implement a Data Protection by design approach that incorporates concepts like pseudonymisation and retention limits into your systems and routines, how to deal with disclosures to third parties, how to process a subject access request and so on.

2.1.4 Insurance

They should have professional indemnity insurance in case their advice is flawed – especially if it leads to enforcement action being taken. Cover for claims in the millions of pounds isn't remotely unusual for a professional indemnity policy. Be wary if they don't have one, even if they're willing to take one out on request. It's also wise to expect public liability insurance in case of mistakes and slip-ups when working in your premises or with your equipment. Depending on the nature of their work – especially if they are likely to be working on rights requests or complaints on your behalf – you

should also expect cyber liability insurance to cover them against hacking and similar threats.

2.1.5 Enthusiasm

Data Protection is not boring. It is about people – the data that identifies and defines them, and the decisions that people make with that data. Your DPO should be enthusiastic about making it work. You don't want a zealot who values Data Protection above all else, but such people are rare. DP is based on flexible principles rather than fixed rules, so people who enjoy working on the subject are unlikely to be dogmatic and inflexible. If you get the sense that your DPO thinks the subject is boring or technical, drop them like a stone. On the other hand, if you get someone who wants to get stuck in, who enjoys working on subject access requests, who wants help your staff, that makes up for other deficiencies.

2.2 Bad signs

2.2.1 GDPR r us

A company with 'GDPR' in its name means it was set up recently. Experienced people may have moved jobs to create a new company with 'GDPR' in the name, but don't assume that 'GDPR' is a good sign. It's likely to be an indication of limited experience.

2.2.2 Newbies

A company has been registered for a short time also indicates limited experience. If your contractor is a limited company, Companies House will tell you how long they've been running: https://www.gov.uk/get-information-about-a-company. Input the name of the company and you can see when it was incorporated.

The 'People' tab on Companies House shows what businesses a director has been involved in before. A history of involvement in Data Protection is a good sign. But if your potential DPO is more experienced in marketing, IT security, bead-making or international scrap metal (they're all out there), you should be cautious. If the director has a track record of failed companies, what does that say about their reliability and ability to support you in the medium to long term? Someone who transitioned into Data Protection since 2015 has quite possibly jumped on a bandwagon. Ask them what they offer in lieu of experience.

2.2.3 FINES! FINES! FINES!

Any company that predicts massive fines doesn't have a positive message about their product and is probably useless. The ICO has confirmed that an emphasis on fines is 'fake news' and the Deputy Commissioner Simon Entwistle said in November 2017 that the ICO wouldn't be routinely putting extra zeros on the penalties they issue now. More importantly, the GDPR itself says that any penalty must be 'proportionate' as well as effective. You

shouldn't want a DPO who gives you the advice you want to hear, but they should equally offer you a positive prospectus.

2.2.4 Poor knowledge

Look at the company's website and see if you can spot any of these basic errors – remember, these are supposed to be experts, so they shouldn't be making errors like these in any of their materials. Data Protection is a precise business – cases are won and lost on the interpretation of a single word or phrase. Someone who thinks that the details don't matter is on the wrong track, and will give you bad advice.

- It's the General Data Protection Regulation (not *Regulations*), although it might be more reassuring if they talk about Data Protection.
- Consent is not required to process personal data – if they say it is, they're idiots. Walk away.
- The 'Data Controller' is the name for the organisation as a whole, not a specific member of staff. The only way that a person can be a data controller is if they are a sole trader; if your DPO company thinks the Data Controller is a person, they don't know what they're talking about.
- The fines are a maximum – there is no indication that any DP regulator will automatically fine at the top level
- There are two levels of penalty – the maximum fine for not reporting a breach to the ICO is €10 million or 2%, not the higher rate.
- The Data Protection Officer does not have personal liability

2.2.5 Compliance

Avoid anyone who promises to make you 'compliant'. The GDPR has not been implemented properly yet, and the Data Protection Bill is still making its way through Parliament as I write. Full compliance is a pipe dream.

3 Look at the DPO candidate

3.1 Are they relying on a qualification, rather than experience?

I am a trainer. I've been teaching DP qualifications since 2008. I wrote and taught a certificated Data Protection course for three years. I have every incentive to tell you that qualifications are magic. They're not.

One training provider's qualification – made up of both basic and advanced components – involves just 8 hours of distance learning modules. That's the whole of Data Protection boiled down to just over a normal working day. A person cannot gain the GDPR's 'expertise in Data Protection law' in eight hours. It's bollocks.

If your DPO candidate touts a qualification, ask how long the course was, what it covered, and what the exam or test was like. The longer and more demanding it was, the more faith you can put in it. If the assessment was solely multiple-choice questions, forget it. Data Protection is a complex subject that requires the ability to understand and communicate difficult ideas and choices. It cannot be reduced to 70-odd tick boxes.

3.2 What if they say they are 'GDPR Certified'?

They're not. There is no such thing. GDPR Certification involves a processing activity being assessed and then approved by a certification body. That certification body needs official approval – in the UK, this will be delivered by the ICO or the UK Accreditation Service. GDPR does not provide for certification of people or products, and the UK has no privacy seals or kite marks process. Even GDPR certification – which won't apply to people – won't start until 2018 at the earliest. 'GDPR Certified' is a hoax.

Nobody offers a course free of issues. Courses run by the British Computer Society (BCS) offer an independent marking process. Competing training companies run the courses according to the BCS syllabus, but the exams marked independently. However, the exam itself requires rote learning and a phenomenal memory. A good DPO has the sense to consult the source text rather than relying on the Rain Man total recall that successful BCS candidates must possess. The International Board for IT Governance Qualifications (IBITGQ) also exists, but only accredits courses by one UK company (the same company that set the IBITGQ up and registered its website). Make of that what you will. The International Association of Privacy Professionals operate a popular and successful Certified Information Privacy Professional qualification, but the content is not specific to the UK.

Many training companies run their own certificated courses (including one I wrote and delivered). Most have their merits, no course will turn a novice into an expert. Completing a course does turn a person into a DPO – if it did, rather than paying consultants rates, why not pay for a member of staff to go on a course?

3.3 Knowledge and experience

3.3.1 Do they have experience of being a Data Protection Officer, IG Manager, IG Officer?

You **must not** pay anyone to be your DPO if they have not done some kind of Data Protection work before. Let someone else be their guinea pig. The ideal candidate offers you recent DP experience in your sector. You may decide to compromise on it being recent, and you might compromise on it being in your sector, but hiring someone with neither is a significant concession. They must have done at least some of the following tasks:

- Handled subject access requests (i.e. liaised with the applicant, decided what information should be provided and what should be redacted)
- Handled Data Protection complaints (e.g. accuracy of personal data, data being shared with people that the subject didn't want it to be shared with)
- Dealt with requests for personal data from third party organisations (e.g. the police, insurance companies or solicitors)
- Written – or at least advised on – privacy notices or fair processing statements
- Carried out an impact assessment on a new project or idea
- Investigated a data security incident
- Liaised with the Information Commissioner's Office

3.3.2 Do they understand other DP and privacy legislation that affects your sector?

GDPR isn't the only thing your DPO needs to grasp – can they demonstrate their understanding of other laws that are relevant to you. Some of the other laws you should consider include:

- Data Protection Bill (soon to be Data Protection Act 2018) – NB this one is non-negotiable
- Common law duty of confidentiality
- Human Rights Act 1998 (especially Article 8 Privacy)
- Regulation of Investigatory Powers Act 2000 (if you do covert investigations)
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (if you do direct marketing by any method other than post)

4 Questions to ask your prospective DPO

There should be an interview where you get a sense of what these people are like, whether they have a balance of expertise and pragmatism, and fundamentally, whether you will get along with them. I've included three sets of questions for you to try – practical questions about their approach, DP questions to test their knowledge, and finally, some scenarios for them to respond to.

4.1 Practical questions

Ask questions about the methods they will use to support your organisation:

- What is your method for conducting a data protection impact assessment?
    - You're looking for someone who understands that a DPIA is about risks to individuals' rights, not ticking boxes relating to the GDPR principles.

- Ask them to tell you about the most challenging Data Protection issue they've ever faced, and how they dealt with it

- Ask for a practical example of what would constitute a breach of the first, second or third DP principle – steer them away from the more obvious areas of data subject rights or breach notification.

- Ask them to explain – in plain English – Data Protection by Design, and to give you a practical example of how your organisation might implement it. You're looking for someone who understands the need to incorporate a wide variety of DP controls into the way that you run things and make decisions. It isn't just about encryption.

- If you're likely to be doing marketing or fundraising, ask them questions about consent for marketing – they should be able to tell you about the implications of PECR (and its replacement, the ePrivacy Regulation, which may or may not arrive in 2018). If they talk about marketing and don't mention PECR and ePrivacy, don't trust them.

- How will you monitor our compliance with the GDPR and ensure that we have proper oversight for all our activities? What access will you need?

- How many other clients do you have, and what guarantees do you have that you will have capacity to give us what we need?

- What security measures do you have for communications with us, and data that you provide to us?

    - Think about both electronic communications and the storage of your documents and equipment in their premises / vehicle / home

- Do you have provision for annual leave / cover for the main consultant?

- Why do you want to be our DPO?

4.2 DP questions

The problem with these questions is that you may not be in a position to judge the quality of the answers. To be frank, I don't want to give you the answers here because some of the cowboys might be reading this document (hello and up yours if you are), but what you should get is a sense of how fluent and well-prepared they are. Someone with expertise in Data Protection law and practise will not struggle to answer these questions, and they need the ability to put their answers into words that you can understand. If they can't do both, what are you paying them for?

- Can you sum up GDPR in 5 minutes for the total beginner?

- Can you explain SSL for us?

- What is the difference between encryption and pseudonymisation?

- Can you give us an example of profiling?

- What do you think the biggest risks for us as an organisation are?
    - NB: an answer solely about fines or security is a sign that the person doesn't really understand Data Protection

- Ask them to explain situations where it would be appropriate for your organisation to pseudonymise personal data before using it or sharing it.

- What lessons do you think we can learn from the Information Commissioner's enforcement on the charities?

- What do you think the implications of the [*choose one from the following that might suit your organisation*] are for our organisation?
    - Optical Express Appeal (marketing, consent, third parties)
    - Supreme Court Named Person Case (justification to use sensitive personal data)
    - Verso case (consent and data sharing)
    - Breyer case (European Court decision about whether IP addresses are personal data)

    - Durant case (2003 case about the significance of personal data and where the focus of personal data lies; probably superseded by GDPR's personal data definition)
    - Southampton City Council (use of CCTV surveillance)
    - Jala Transport (ICO fine on a small business)

- What do you think the implications of the [*choose one from the following stories that might suit your organisation*] are? Feel free to pick your own cases – read the tabloids or your local paper and you are likely to find stories of people losing data, suffering because of inaccurate data, or publishing information that they shouldn't.
    - Equifax (hacking attack)
    - Uber (question of jurisdiction, question of whether Uber breached Data Protection by keeping the hack secret)
    - University of East Anglia (sending emails to multiple people by mistake)
    - Home Office letters to European citizens about deportation (citizens had the right to remain so data was inaccurate)

- What is the biggest challenge in the Data Protection Bill for our organisation?

- Explain one of the exemptions in the DP Bill that you think might be relevant for our work

- What steps do you advise us to take now to prepare for the GDPR – what should we do now, and what should we put off?

4.3 Test scenarios

- We have gathered a large database of marketing contacts over many years through a mixture of opt-in, opt-out and we don't know. We can separate off the opt-in because they are recent, but everything else is a mess. Our Chief Executive wants to expand, and hopes for a big marketing push next year. The ICO says that you cannot use email to ask people to opt-in to email marketing, and we can't afford to write to them all. What should we do?

- A member of staff had a file full of sensitive information about the health of several staff members in their car when it was stolen. We don't want to tell the Information Commissioner as the member of staff is quite senior and it could expose them to a lot of negative scrutiny. What can we do?

- A police officer rings us at work and asks you to confirm whether a person still lives at that address – officers are about to raid the premises and want to make sure they are not going to kick the wrong door down.

5 How do we decide?

Your chosen DPO is your advisor, your auditor, your expert, your friend. It's a tall order, and you may well have to compromise somewhere. I've mentioned **experience** a lot here, but you might find someone who's new to the sector but they're immersed in the subject, their instincts are good and they're not selling bullshit.

Choose someone who offers practical, helpful advice. Choose someone with communication skills, with insight into the legislation, who has a track record of having done it before, or a good reason why they don't but you should hire them anyway. It doesn't matter if they have long experience of being a consultant – your DPO will be doing a practical series of tasks for you, supporting you in your work, and someone who has been a DPO, or a deputy or part of a DP / IG team will be just as well placed to do the work. I got one DPO job mainly because I clicked with the boss. In another role, I was by far the most qualified and experienced candidate, and I was spectacularly unsuccessful from the first day until I left. There's no harm in trusting your instincts (as long as you've done your research).

Just don't pick a plank with a smart haircut and a shiny suit who claims to be certified. You serve better than that, and better than that is out there.

Acknowledgements

A variety of people provided me with questions and issues when writing this guide. My gratitude goes out to them all. Bilal Ghafoor and Jon Baines very kindly read a draft version of the guide and gave me feedback – amongst other constructive comments, both of them thought it was too long. They were right and it's still too long but you should see the awful stuff that I cut out. This should not be taken as their endorsement of the guide and the views expressed within it, for which I bear sole responsibility, including any mistakes and those mean things I said about you.

About me

I have been working on Information Rights since 2001, when I got a job at the Information Commissioner's Office. I did not want to become a Data Protection specialist, I just wanted a permanent job. My time at the ICO was short and undistinguished but it put me on the DP path. Since then, I have been a DPO in two different councils (Derbyshire and Wigan) and an NHS body (the now defunct Manchester Primary Care Trust). In 2006, a training company asked me to do some courses for them because they had seen me speak at a conference, and my employer at the time (Wigan) graciously allowed me to do so in my spare time.

Since 2011, I have been a full-time trainer and consultant for myself and for several training organisations. In 2018, for the first time, I will be working solely for myself with no ties to any training or consultancy organisation. Because I don't have an employer to embarrass, I write a noisy and provocative blog about Data Protection and I tweet disrespectfully about data protection and privacy issues. I do something on LinkedIn, but I don't really know what the point of it is beyond annoying other consultants until they block me.

I hope you found this guide useful; if you think it would have been worth paying for, making a donation to any mental health charity would be a lovely gesture. If you have any feedback, especially if it helps you to choose your DPO, I am more than happy to hear from you. If you would like training, advice or consultancy on Data Protection, please contact me using the details below.

2040 Training Limited, Courthill House 60 Water Lane Wilmslow Cheshire SK9 5AJ
Email: tim@2040training.co.uk Telephone: 07508341090
Twitter: @tim2040 LinkedIn: Tim Turner
Registered in England - Company Number: **6682698** – VAT Number: **155713606**