High on the agenda was the evolving role of the Data Protection Officer (DPO). Although their responsibilities are clearly laid out under Articles 37, 38, and 39 of the GDPR, what is perhaps not so clear is how the DPO operates most effectively within the context of a global organisation. To answer this and other key questions around data privacy, we garnered insight from an industry panel which combined legal, consulting, and sector experience at a global level.

THE PANELLISTS
Ashley Winton, Partner, McDermott Will & Emery (Chair)
Noriswadi Ismail, Managing Director, Data Privacy, Ankura
Adrian Leung, Data Protection Officer, Equifax UK
Luke Dixon, Legal Director, Addleshaw Goddard

NOW THAT THE DUST HAS SETTLED, HOW IS THE DPO ROLE TAKING SHAPE?
In the run up to the GDPR coming into effect on May 25, 2018, DPOs were primarily focused on implementation. Systems and processes were still evolving and companies were to some extent still working out how this new role fitted best with the rest of the organisation, from IT and security to strategy and the boardroom. Twelve months on, can we get a clearer picture of how global organisations are managing this new world?

Before looking at differing models it is important to acknowledge that even within the DPO role itself there are tensions. Created to provide a second line of defence, yet often playing a key role in designing, operationalising, and running data privacy programmes, how do they manage this apparent identity crisis? Adrian Leung, Data Protection Officer at Equifax UK, says: “I'm often asked, are you a second line function? Our aspiration is to be a second line, but right now we are more like a 1.5.” Noriswadi Ismail, Managing Director, Data Privacy, Ankura sees it as “two sides of the same coin. The independent oversight role provides valuable insight into the operational side.”

Those two sides of the coin are most useful when a DPO has a good grip of not only the legal requirements but also how they work in more practical and commercial terms within a global organization. At present, many DPOs have a strong legal or technical background but may need help to operationalise the programme. Others do not have the resources, standing, or support within the organization to be fully effective.

So, what is the best answer to this need for multiple skill sets? Adrian describes three phases during the formation of the privacy function: “the design phase, the build phase, and finally the run or BAU phase.” In an ideal world, he believes, one person could be able to work across all three, but other models are being deployed as each phase requires slightly different skills. For example, using an interim DPO to strategise and perhaps also to help initiate the building of the privacy function, then a full-time candidate can be hired to take the role on from there. Another route taken by many companies is for the existing privacy lead within an organisation to step into the DPO role. A 2018 IAPP survey found that almost six in 10 privacy leaders have taken on the DPO role...
duties themselves. On the plus side, the DPO is likely to be well skilled and strongly placed, but on the minus side there may be issues around workload and independence. One thing is certain, however: the multiple demands of the job mean that DPOs are in short supply, with an estimated 75,000 vacancies worldwide and 20,000 in Europe alone.

**HOW ARE GLOBAL ORGANISATIONS DEPLOYING THE DPO ROLE ACROSS MULTIPLE TERRITORIES, SUBSIDIARIES, AND JURISDICTIONS?**

Given the focus on GDPR, it can be easy to forget that many territories both within and outside of the EU already had their own established models around data protection regulation. Indeed, the current DPO role is believed to be firmly based on the German model that precedes it. Existing approaches in, for example, the US and Singapore, alongside emerging legislation such as The California Consumer Privacy Act and India’s Draft Data Protection Bill also need to be taken into account. So, for an organisation with customers across the world, how is data privacy managed?

The key appears to be by combining a global perspective with the need to acknowledge the different requirements within individual countries. Adrian sums this up succinctly as “globally aligned, locally deployed.” By which he means although differences will persist in terms of both regulatory and market pressures, mapping these out within one global framework helps to simplify the problem and create one roadmap for a common journey. Reporting lines are also likely to vary across regions, with some DPOs reporting to the Chief Security Officer, others to the Chief Technical Officer, IT head or even Chief Executive Officer. While a single set of reporting lines may not work effectively across all industries and regions, legacy structures should be revisited as data privacy processes mature and the ‘natural fit’ becomes clearer.

Noriswadi outlined a number of models from a regional perspective, beginning with the US where what they call the Chief Privacy Officer (CPO) operates within a centralised framework. “However, because of GDPR, there is a clear obligation to have a DPO in Europe to act as a key contact,” explains Noriswadi. So, what was a centralised governance model becomes more of a hybrid model. Even in the UK/EU/EEA, where GDPR is the only game in town, there is also something of a hybrid model. Here, Noriswadi has seen companies choose to have a powerful DPO in Germany whose influence extends beyond national borders. This is because, as mentioned, Germany has a very strong history of data protection that predates the GDPR, meaning that organisations are seeking to leverage this strength across EU operations.

Thirdly, there is the global Asian model, which centres around Singapore’s requirement to appoint a DPO based within the country. Given that a global organisation will also want to have a DPO in Europe, companies will need to double up on DPOs, unless they can outsource the Singapore representative to a local legal firm or similar.

Finally, spare a thought for the start-ups which must navigate all the regulatory and organisational complexities that accompany the GDPR, but without the specialist resources available to larger firms. Here, as well as CEO, CFO and head of marketing and sales, a fintech founder may find themselves adding DPO to their job title. In Singapore, this will definitely be the case, with founders automatically being assigned the DPO role by regulators.

**DEFINING THE DIFFERENCES: WHO WANTS TO BE AN EU REPRESENTATIVE?**

As if DPOs do not have enough on their plate, some are coming under pressure to also take on the role of EU representative. The wise choice may be to decline this offer because of conflicts between the roles and issues over liability.

To clarify, the requirement for a business or an entity to appoint an EU representative derives from Article 27 of the GDPR. Put simply, this says that where an entity or an organisation does not have an EU establishment, but it monitors or it sells goods and services into the EU, it is required to appoint an EU representative. And the person appointed must be located in the same territory as at least some of the individuals whose personal data is being processed.

While there may be some territorial issues about a DPO acting as an EU rep – for example, a DPO may be responsible for territories within the EU but, unlike the representative, does not necessarily have to be located there – the main conflict is over differences in the role.
As Luke Dixon, Legal Director, Addleshaw Goddard puts it, “I see the EU representative as being a middleman or a connective tissue between the supervisory authorities, data subjects and so forth within the European Union and the entity which is established outside it. The DPO, on the other hand, is effectively the champion of data protection within an entity, who is there to embed a culture of compliance, train people, act as a consultant for the board, and direct and advise.”

As this suggests, these two roles require differing levels of independence. Article 27 of the GDPR states that the EU representative needs to be authorised, in writing, to act on the organisation’s behalf regarding their EU GDPR compliance, and to deal with any supervisory authorities or data subjects in this respect. “So, you might argue that if you’re applying a written mandate upon a DPO, you might be potentially fettering the autonomy of that person,” explains Luke. In other words, a DPO who is also acting as an EU representative may risk damaging the independence that is key to their role.

When considering a suitable EU representative, companies have a number of options: an employee within a suitably located subsidiary, another related company in the EU, or a service company, law firm, or individual. However, according to the European Data Protection Board’s guidelines on territoriality, EU representatives are subject to the same actions and potential liabilities as the data controller or processor that appoints them. This means that EU representatives could be liable for any failings of their ‘employer’ and makes the role potentially much less attractive unless adequate contractual protections or insurance can be provided.

The best route may therefore be to upskill someone within the organisation who is deployed within an EU territory. Outsourcing options are also likely to be available, but these will need to have specialist skills and understanding, rather than the ‘glorified mailbox’ route that some organisations have taken.

**AND FINALLY, WHAT IS THE BEST PIECE OF ADVICE FOR DPOS?**

We asked our panellists to sign off with some short, snappy words of wisdom for DPOs and their organisations.

Luke focused on the need to keep it simple: “Best practice for DPOs is to be patient, keep it simple, and focus on the practical, commercial needs of the business. GDPR can seem technical and intimidating so upskilling, informing, and training people within the business is key.”

Noriswadi highlighted passion, skill, and creativity: “Only agree to be a DPO if you really want to be one. It’s a role with many demands, so upskill in the areas in which you are less experienced. Finally, communicate in simple language and use creativity to spread the message.”

Adrian’s advice was more specific, referring to the thorny subject of data subject access requests (SARS) and the need to manage them efficiently to avoid potential liability: “Be aware that SARS can come in at different points within an organisation but, wherever they land, the clock may start ticking from that moment. So, get the training and systems in place to identify, monitor, and progress them centrally and efficiently.”

If you would like to discuss any of the subjects covered in this article or find out more about how Ankura can help you manage data privacy within your organisation, please contact Noriswadi Ismail.

**NORISWADI ISMAIL**
Managing Director

+44 207 015 8740
noriswadi.ismail@ankura.com

---

Ankura is a business advisory and expert services firm defined by HOW we solve challenges. Whether a client is facing an immediate business challenge, trying to increase the value of their company or protect against future risks, Ankura designs, develops, and executes tailored solutions by assembling the right combination of expertise. We build on this experience with every case, client, and situation, collaborating to create innovative, customized solutions, and strategies designed for today’s ever-changing business environment. This gives our clients unparalleled insight and experience across a wide range of economic, governance, and regulatory challenges. At Ankura, we know that collaboration drives results.