Centre for Information Policy Leadership
Hunton & Williams LLP

Discussion Paper:

The Role and Function of a Data Protection Officer in Practice and in the European Commission's Proposed General Data Protection Regulation

Report on DPO Survey Results

1. Executive Summary

The role and function of a data protection officer ("DPO")[1] are evolving and will underpin data protection compliance under the proposed European General Data Protection Regulation (the "Regulation")[2]. Recognising the critical importance of the DPO function and oversight as a prerequisite for data privacy corporate accountability, many organisations have invested strategically in developing a DPO function, but little is known about how existing DPOs envisage their current role being impacted by, and changing, under the Regulation. As part of the Centre's project to explore the changing role of a DPO, we surveyed 43 practising DPOs from a range of industry sectors and a variety of geographical locations[3], about their role and function. This paper summarises the insights we have drawn from the survey.

While two thirds of survey respondents agreed that there is a disconnect between current organisational practices and the proposals set out in the Regulation, the survey revealed very little consensus in interpreting the future role and function of the DPO, or in assessing the likely impact and change required to implement the Regulation. Several key themes emerged:

- Only a few countries currently mandate the appointment of a DPO, yet there has been marked growth in the number of DPOs that are appointed. The range of tasks that the DPO is expected to undertake has broadened, and the size and resources of the DPO team, and other personnel tasked with data privacy compliance in organisations, are growing.

- The role of the DPO requires a certain degree of flexibility in order to accommodate the needs of different types of organisations, differing corporate cultures, and divergent cultural and legal traditions.

- Some respondents see no tension between this need for flexibility and the prescriptive role and function of the DPO set out in the Regulation. Some were already familiar with a number of these requirements. Others took the view that what is prescribed by the Regulation will be reflected in a multitude of ways in practice.

- Other respondents expressed unease at the rigidity of the DPO provisions in the Regulation. There is concern that some regulators may interpret these requirements literally, resulting in a prescriptive "one-size-fits-all" role for DPOs that will not be appropriate (or workable) for all organisations.

The survey results identify the need for consensus amongst all stakeholders – businesses, public authorities, regulators, and data subjects – to build a shared vision of the role and the function of the DPO. If that is not possible, then there should be acceptance of the fact that the role and function of the DPO can legitimately take many guises. In light of a more harmonised approach to data privacy regulation and compliance across the EU, it is critical to ensure consistency of regulator expectations and the consistent interpretation of the formal requirements of the DPO role.

---

[1] The terms DPO and CPO ("Chief Privacy Officer") are used interchangeably in this paper.
[2] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), published January 25, 2013. Available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last accessed Dec. 3, 2013).
[3] A full breakdown of survey respondents is provided at Annex I.

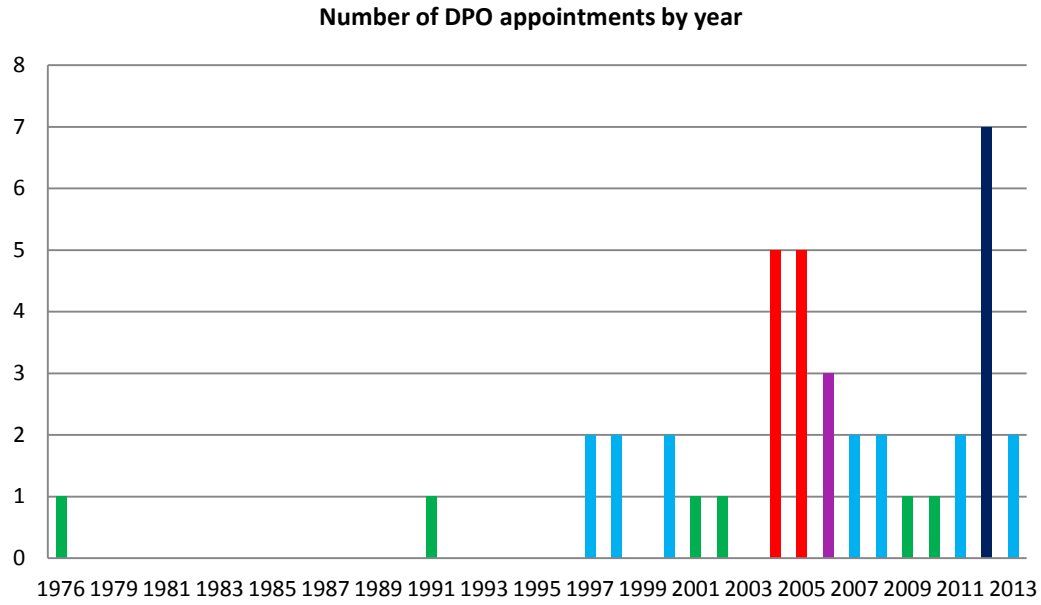
2. The Evolving Nature and Scope of DPO Role

The Regulation mandates the appointment of a DPO in many cases, and prescribes the particular tasks and responsibilities of the DPO. This is in contrast to the current position; under most existing national laws, the appointment of a DPO remains optional.

Notwithstanding the absence of a legal requirement to appoint a DPO in most jurisdictions, our survey responses show that many organisations choose to appoint DPO, for a variety of reasons, and have done so over the last three decades. It appears that while the role of the DPO may have changed and developed over time, the role of DPOs today largely reflects many of the requirements set out in the Regulation.

2.1 Growth in DPO appointments and internal DP resources

We asked survey respondents to state the year in which their organisation first appointed a DPO, so that we could better understand how recently organisations considered it necessary to appoint a DPO. Among survey respondents, the earliest reported appointment of a DPO was in 1976, pre-dating both the 1980 OECD Privacy Guidelines and the 1995 EU Data Protection Directive (Directive 95/46/EC). Just under a quarter of survey respondents appointed their first DPO before 2002, with the majority having appointed a DPO between 2004 and 2008. For many organisations, the role of the DPO was created in the past three years and may not yet be that well-established within the organisation.



The apparent surge in DPO appointments in the past 3 years is confirmed by other data in our survey responses. During this period, almost half of the respondents have hired or assigned additional personnel to their data privacy teams, with a great majority of these organisations adding between one and three additional personnel.

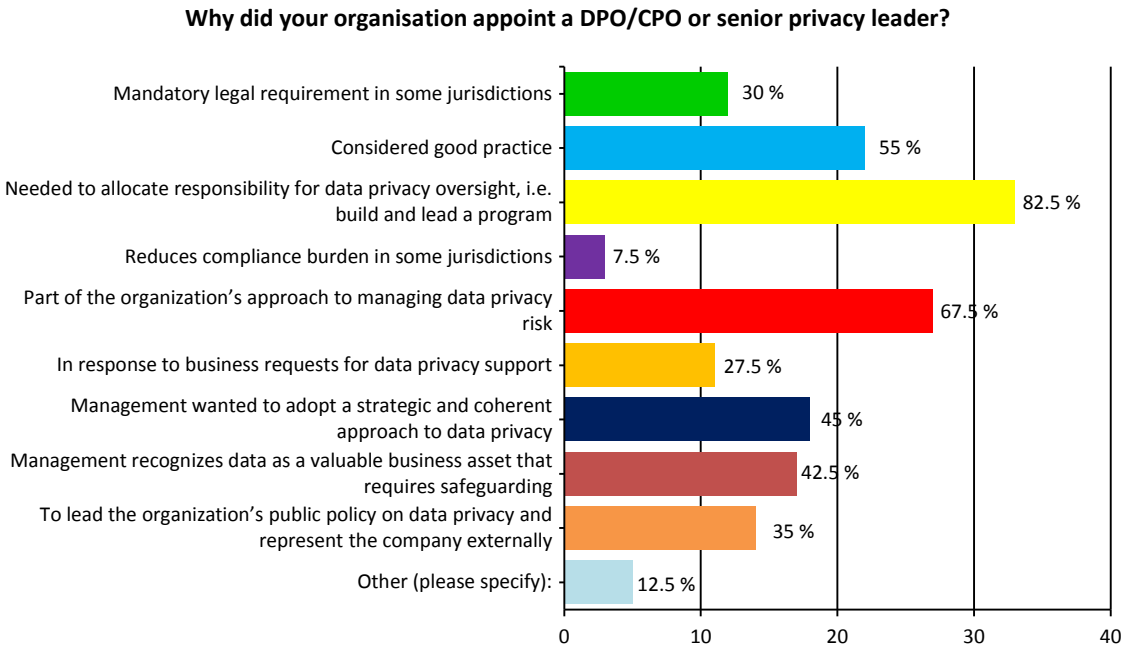
2.2 Reasons for appointing a DPO

Under the Regulation, the appointment of a DPO will be mandatory for many organisations. The exact criteria for appointment will depend on the final text of the Regulation. The Commission proposes appointment based on the number of employees a data controller has or on where its core activities involving the processing of personal data are located.[4] The Parliament proposes appointment of a DPO based on the number of affected data subjects or

[4] Article 35(1)(b) Regulation.

core activities[5]. The Irish Presidency of the Council of Ministers proposed mandatory appointment only where already required under national law (e.g., as is the case in Germany)[6].

Although the appointment of a DPO is optional in most European Member States, in the survey we sought to understand what factors led organisations to appoint a DPO, even when not legally required to do so.



The survey results indicate that the reasons for appointing a DPO are many, and varied. A key factor is the need to allocate responsibility for data privacy throughout the organisation. Other factors appear to include risk management considerations, the desire to adopt a strategic approach to data privacy, and the need to safeguard personal data as a business asset. The last point, in particular, shows that the appointment of a DPO may be linked to commercial considerations and that data protection and the DPO role are viewed strategically, rather than merely as a regulatory compliance requirement. The survey results show also that in at least a third of the companies that responded, the DPO is expected to take the lead on the public policy aspects of data protection, and to represent the company publicly on these issues. The least common reason given for appointing a DPO was to reduce the organisation's compliance burden in some jurisdictions.

There is a clear indication that, despite a lack of legal compulsion, a great majority of organisations view the DPO appointment as a prerequisite for corporate accountability, a matter of good corporate practice and as enabling a proactive, rather than reactive, management of data privacy within the organisation.

2.3 The increasing tasks and responsibilities of the DPO

The Regulation sets out the tasks and responsibilities of the DPO,[7] including: providing information and advice, overseeing and monitoring data protection; maintaining documentation; dealing with data subjects directly; and, consulting and cooperating with regulators. Specific tasks include developing staff training, conducting audits, monitoring the implementation of data

[5] Compromise Text of European Parliament, Amendment 132. Available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bREPORT%2bA7-2013-0402%2b0%2bDOC%2bPDF%2bV0%2f%2fEN (last accessed Dec. 3, 2013).
[6] Article 35(1) of the Compromise Text proposed by the Irish Presidency of the Council of the European Union. Available at: https://www.huntonprivacyblog.com/wp-content/uploads/2013/06/st10227-ad01.en13.pdf (last accessed Dec. 3, 2013).
[7] Article 37, Regulation.

protection by design and default, monitoring data protection impact assessments, and ensuring data security.

In the survey, we asked DPOs to indicate what their role entails currently, in order to understand how similar, or dissimilar, their existing role is compared to the role envisaged under the Regulation. It appears that the majority of DPOs who contributed to our survey are focused on these requirements already. The survey reveals that 87.5% of respondents advise their organisation on compliance with applicable data protection laws and internal procedure, 77.5% advise on the data protection provisions of third-party contracts, and 82.5% monitor legal and policy developments. A high proportion already oversee and monitor data protection compliance: 82.5% provide oversight of the organisation's privacy programme, 70% conduct privacy impact risk assessments, and 65% conduct compliance assessments. 82.5% already develop training and awareness tools and 85% work with the business to build data protection into the design of systems, projects, products and services. 65% already respond to data subject access requests and 67.5% deal with data subject complaints. 72.5% maintain relationships with, or act as a contact point for, the local data protection authority. On the data security front, 70% lead on data breach responses and 85% provide expert advice following a breach.

The survey appears to indicate that of all the tasks enumerated in the survey, very few DPOs actually perform the operational tasks (such as responding to and dealing with data subjects' requests and individuals' complaints, conducting assessments and verifying compliance). This is likely due to the fact that many DPOs have teams and delegate operational tasks to junior team members. Assessing and verifying compliance may be performed by other corporate functions, such as internal audit or dedicated compliance assessment teams, and not exclusively by the DPO. As some respondents indicated in their comments, there may be a conflict where a single DPO or DPO team perform both the oversight and advisory roles, on the one hand, and compliance verification and assessment roles, on the other.

Finally, the scope of the DPO role appears to have transformed and developed over time to include public policy and external representation with regulators, industry and the media. One respondent remarked that "*When [the] position [was] initially created [in 1997], it did not include a public policy component but the role now includes public policy and representing the company externally.*"

2.4 The DPO is evolving as a strategic leader

DPOs who responded to the survey consider that their current tasks and responsibilities largely reflect those outlined in the Regulation. The main departure from the Regulation is that, while the Regulation does not prescribe a strategic role, in practice 82.5% of the DPOs who responded to the survey consider the setting of strategy and policy to be key tasks. Further, the responses summarised in section 2.2 above (on the business drivers for the appointment of a DPO), indicate that, despite the lack of any specific legal mandate, organisations view the DPO as a strategic and business critical role. One respondent noted that their organisation appointed a DPO to "*guide and shape internal business strategy, new business models and innovation, all of which involve the use of personal data*."

We asked survey respondents whether they thought the Regulation envisages the DPO as a mid-level compliance manager, rather than a strategic and senior leader. Responses were evenly split. 50% of respondents either somewhat agreed or strongly agreed that the Regulation envisages the DPO as a mid-level compliance manager and not as a strategic and senior leader. However, 50% of respondents either somewhat disagreed or strongly disagreed with this statement, indicating that they feel the Regulation envisages a strategic leadership role for the DPO.

2.5 The DPO role performed by a team, not a single individual

The Regulation is drafted on the basis that a single individual will fulfill the DPO role; however, the survey shows that in practice the tasks and responsibilities of the DPO may be fulfilled by a team of individuals. Nearly half (47%) of survey respondents indicated that they have five or

more team members under their direct supervision assisting them in their role as DPO, with 15% having between 10-20 team members. 3 DPOs have more than 30 team members. It therefore appears that the tasks of the DPO are not performed by a single person, but by the privacy function within the organisation. Currently, the Regulation does not reflect this possibility.

The diverse structure and composition of current privacy functions reflects the wide range of responsibilities that commonly fall within the DPO role today. A privacy team, rather than an individual, fulfilling the role of DPO may be the best way to staff such a multi-faceted role. The DPO role requires a diverse skill set including technical and legal knowledge, commercial awareness, a deep understanding of the business, and strong communication and public-relations skills. To some extent, the DPO needs to be detail-orientated, understanding the technical aspects of data processing activities and relevant technologies, and how the legal framework and IT security considerations apply. At the same time, the DPO needs to be a big picture thinker, having the vision to look around corners and the ability to view privacy issues within the wider commercial context, thereby helping the business to meet commercial objectives in a compliant manner.

3. Independence of the DPO

The Regulation stipulates that the DPO will perform their tasks and duties independently, will not receive any instructions as regards the exercise of the DPO function, and will report directly to the controller's or processor's management.[8] Further, the DPO enjoys protected employment status under the Regulation, insofar as s/he is appointed for a minimum tenure of two years. The DPO cannot be dismissed during the period of tenure except "if the data protection officer no longer fulfils the conditions required for the performance of their duties."[9] Finally, under the Regulation, the DPO can only perform other duties that are compatible with their DPO duties and that do not result in conflicts of interests for the DPO.[10] In the survey, we sought to explore how DPOs currently discharge their responsibilities, and to what extent they operate independently of the business.

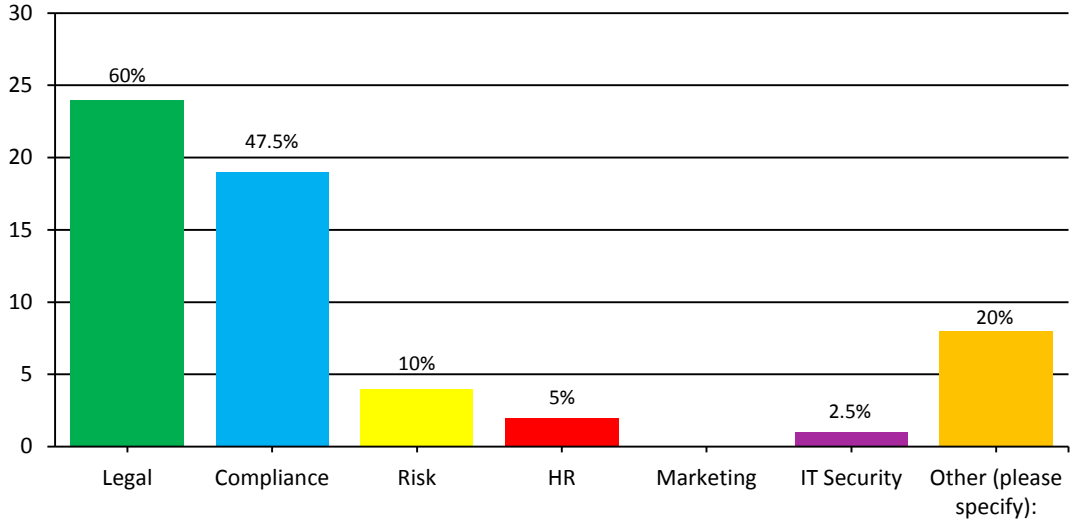
3.1 Position within the organisation and compatible tasks

The issue of independence, and what it means in practice, is not clearly defined today. Some countries seek to ensure functional independence by restricting other roles and responsibilities that the DPO can fulfill. For example, in Germany the role of the DPO is considered incompatible with a number of other roles and responsibilities. The owner of the business, board members and the managing director, as well as those in potentially conflicting functions, such as IT and HR, cannot take on the role of DPO in Germany.[11]

We asked survey respondents to indicate where the DPO function currently sits within their organisation. 60% reported the DPO being in the legal function, and 47.5% within compliance. None were located within the marketing function and few were within IT security (2.5%) or HR (5%).

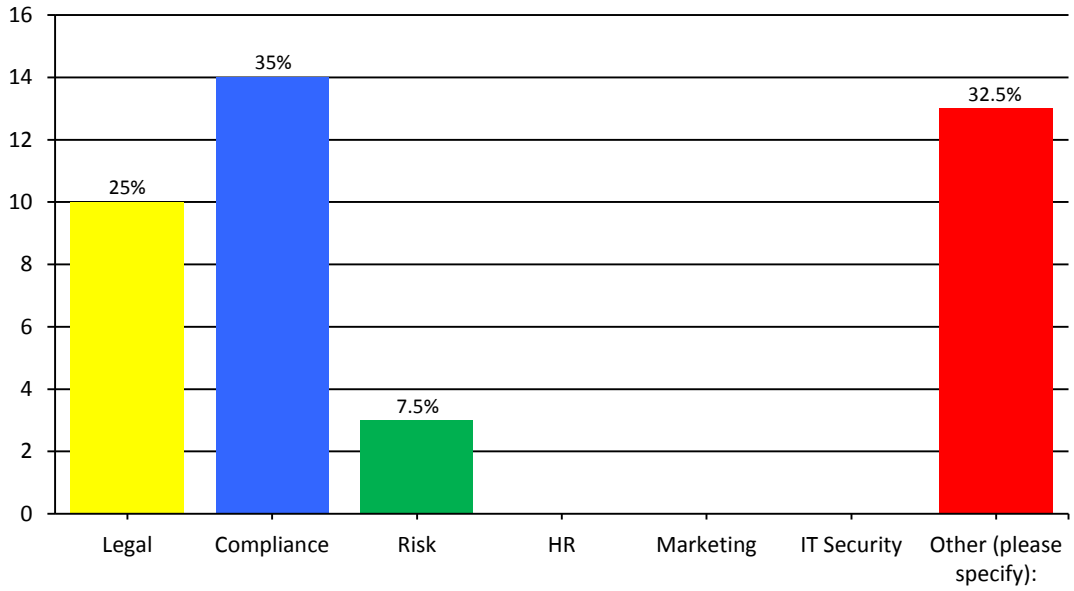
[8] Article 36(2) Regulation.
[9] Article 35(7) Regulation.
[10] Article 35(6) Regulation.
[11] The Federal Data Protection Act, as interpreted by a resolution of the Düsseldorfer Kreis.

Within which function in your organisation does the DPO/CPO or senior privacy leader sit? If Compliance is part of Legal in your organiation, please select both answers



We also asked respondents to indicate where they thought DPOs should be positioned within the organisation. The majority (35%) considered compliance was the appropriate function. 25% considered the legal function to be the most appropriate function, but a significant number of respondents (32.5%) thought that the DPO should be positioned independently, as a stand-alone function, reporting directly to the board or CEO.

In your view, what is the most appropriate reporting line for the DPO/CPO?



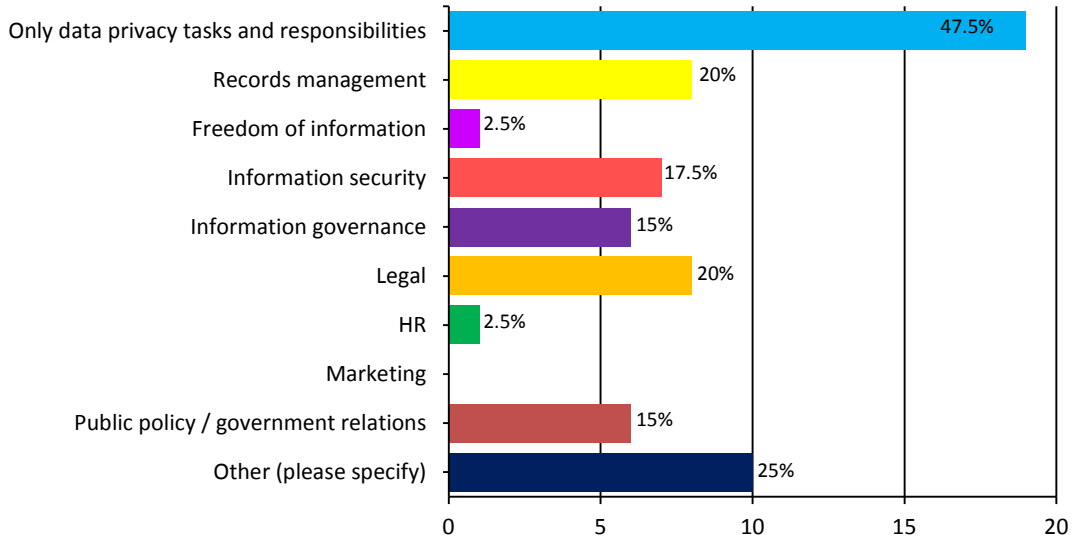
These insights gleaned from respondents' comments confirm what appears to be a growing trend in practice today - the DPO role is often positioned as part of the legal and/or compliance functions. Yet, practising DPOs appear to question this structure, based on the need to ensure the DPO's independence, potentially avoid a conflict of interest and to have a direct line to and visibility of senior management. This may suggest that a more independent, standalone DPO role, reporting directly to senior management, may be better placed to deal with these challenges.

Many respondents considered it important that the DPO has access to the highest levels of management, meaning that the DPO "*could be anywhere with the appropriate authority*". As the Regulation does not stipulate where the DPO should be situated, it allows flexibility for the DPO to sit in whichever function best suits a particular organisation.

Finally, the survey responses reveal that half of the DPOs who responded combine this role with additional responsibilities, such as information governance, records management, information security, ethics and compliance, or other legal duties. This is not surprising, given that many DPOs are very senior executives, entrusted with an array of corporate responsibilities.

Combining the DPO role with other tasks may, however, raise conflict of interests issues for the individual, requiring consideration of whether these additional tasks are compatible with the DPO function, or not. For example, while information governance, or ethics and compliance can be seen as compatible tasks, information security, certain legal functions, audit, IT, or e-discovery responsibility may not be.

What other (non-data privacy) roles and responsibilities does the DPO/CPO have in your organisation?



3.2 Reporting lines and not taking instructions

The Regulation states that a DPO must not receive any instructions as regards the exercise of the DPO function, and must report directly to management. Survey respondents were evenly divided as to whether this proposal would be workable within their organisation.

Some 53.8% of respondents indicated it would be difficult for their organisation to comply with this requirement, for several reasons.

- Some respondents raised the inherent conflict where the DPO is integrated within the business yet, at the same time, is expected to function independently. One respondent commented, "*The success of the DPO relies on me being fully integrated into and involved with the business. I add value by being involved in new projects and programmes from the outset, identifying potential privacy issues and commercial solutions. The requirement for independence would potentially put me in conflict with the business – I could be seen as a compliance 'enforcer' – which would not benefit the business and/or our customers.*"

- Others similarly challenged the notion of independence within the organisation and stressed that the DPO must be seen in the context of an organisation's overall objectives

and strategy. "*No one in an organisation is independent. Not even the CEO, who is responsible towards the Board, who are responsible towards the shareholders. It must be understood that the objectives of the organisation lay down the foundation also for privacy work. The privacy organisation is there to help the business organisation to reach their targets in an ethical, fair and lawful manner. The purpose of the privacy organisation is not to provide the 'No', but the 'know-how'.*"

- Some respondents from global organisations queried whether a direct reporting line to the management of the data controller or processor - usually a European entity - would be effective where the organisation is headquartered outside the EU. For global organisations with a European presence, respondents suggested that a reporting line to local management might not be "*…very sub-optimal in terms of authority, ability to meaningfully impact compliance, effectively limiting the ability to achieve strong, positive data protection outcomes*."

On the other hand, 46.2% of respondents saw no issue with the requirement to report directly to management and not to receive instructions.

- Some respondents noted that this is already a requirement under existing national laws. For example, under German law, the DPO must have a direct reporting line to management.[12] Similarly, under French law, the DPO must report directly to the data controller (i.e., the board) in respect of their DPO duties, and not their usual line manager or the supervisor to whom they report for their non-DPO responsibilities.[13]

- Many respondents indicated that they already report directly to management, and that many organisations already recognise that the DPO needs to be a senior employee, with the freedom to discharge their responsibilities without detailed oversight.

- Finally, some responses demonstrated that there are nuances in what is meant by independence. How we interpret the term in practice and consistently across different jurisdictions will become paramount. One respondent commented, "*Independence is okay if it means they are free to get on with their job and advise the business, with the business making the final decision and taking responsibility. Independence could be an issue if it means that the individual is 'apart' from the organisation and not seen as part of the business.*" They commented further, "*Taking instructions is ambiguous, clearly you can't pressure a DPO to turn a blind eye, but equally, they have to work with the business in terms of priorities...*"

A theme that emerged was that the independence of the DPO should mean that the DPO is free to give their advice - even when unpopular - but that independence should not equate to the DPO making final decisions. Final decisions should rest with the business, having taken the DPO's advice into account: "*If […] the DPO cannot be fired for exercising opinion about privacy matters and making recommendations, that could work. But much of the job is a risk analysis, and [the] boss could override risk calculations.*"

In this regard, one respondent explained that a DPO should have "operational independence" but exercise it in a manner consistent with the business' agreed "strategic direction". They elaborated, "*As the DPO is seen as a subject matter expert, responsible for advising and supporting the business, the DPO receives little instruction from line management in the exercise of his function. However, the DPO, as with all staff, is expected to support company goals and is provided with personal objectives that contribute towards those goals."* Another respondent stressed the need for neutrality, rather than independence, stating that the DPO should "*ensure compliance of the company and […] ensure that group projects can be developed while remaining compliant. If one wants a DPO to have a high level reporting line [the DPO] cannot be expected to be fully independent at the same time. Management always*

[12] The Federal Data Protection Act, as interpreted by a resolution of the Düsseldorfer Kreis.
[13] Article 44 of French Decree No. 2005-1309 of 20 October 2005 implementing the French Data Protection Act, and guidance issued by the CNIL on the role of the DPO, available at: http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Livrets/CIL/Cnil-CIL_V2/index.html (last accessed Dec. 3, 2013).

has expectations. Instead of [requiring] a degree of independence, the EU Regulation should [require] a degree of neutrality in the advice [the DPO] provides."

Operational independence to fulfill the key responsibilities of a DPO role, consistent with company-directed strategy, may be a practical way to ensure independence yet foster integration within a company. This approach to the DPO role does not appear to be incompatible with the provisions set out in the Regulation.

3.3 Protected employment status

A small minority of respondents saw no issue in a DPO enjoying protected employment status and not at risk of dismissal for the performance of their DPO duties. They cited a variety of different reasons in support of this view.

- Some accepted it merely as a fact and a current practice that they are familiar with, noting that this is already the position under existing national law, such as German data privacy law, or other national laws that protect certain company roles. One respondent accepted the idea of protected status as part of the characterisation of a DPO as an extension of the role of the regulator, stating that the protected status "*…would in effect be an extension of the regulator's function, to which we already submit, therefore it would not be a problem*."

- Others noted that their company values and code of business ethics would prevent any issues arising from the DPO's protected employment status. One respondent said that such status would "*…generally fit with our strong policy prohibiting retaliation against an employee for reporting noncompliance with comply policy of law*." A key theme to emerge from the survey is that the DPO role is strategically important, requiring leadership skills, experience and intimate knowledge of the business. Only strong performers and trusted employees would be selected for the DPO role in the first instance, meaning that the protected status may not present an issue in practice. One respondent noted, "*The DPO would not be positioned as a senior thought leader in the organisation if they didn't meet all of the criteria for a senior position*." Similarly, another respondent remarked that: "*A DPO must be an integral part of the management team to be effective. Someone who is not trusted or valued by the management team because s/he is deemed to be a poor performer […] will not be effective.*"

The respondents who rejected the idea of protected employment status did so for a variety of reasons.

- For some, the concept of protected status is a unique requirement and inconsistent with a business having the freedom to make its own decisions as to how it conducts itself and ensures legal compliance. One respondent remarked, "*This approach is completely out of touch with how modern corporations work.*" Another considered it "unreasonable" and that "*The organisation should be setting the requirements of the position, not a regulation.*" Another similarly noted, "*An organisation should be free to manage its own employment practices within the law, without mandatory protection of employment status.*" Further, one respondent noted that the protected status could have the unintended consequence of companies choosing candidates close to retirement, in order to maintain a degree of flexibility for the company.

- The primary concern respondents appeared to have, however, is how to resolve performance issues in the context of protected employment status. Many respondents expressed similar views in this regard: "*It would be challenging as the organisation needs to be able to still enforce general expectations on employees – work quality, performance, and meeting general expectations – that could be easily conflated with the issues that a DPO would be attending to in privacy*" and "*I think this is a very bad idea, and something that incentivises unethical behaviour. It is not good that an employee has no obligation/pressure to support the fulfilment of the organisation's business strategy and ways of working.*" Or as one respondent put it "*it is unlikely that the organisation*

would allow a poor performer to stay in position because of this (protected employment status)".

- Some respondents expected that their organisations would have to make significant and difficult changes to their employment practices, such as the amendment of standard employment contracts, for the DPO role; placing the DPO outside the standard company bonus schemes that relate to individual or company performance; reconsidering the company's headcount reduction schemes; and adapting their performance management process.

- Others cited cultural challenges for their organisations in accepting protected employment status, and predicted that company management would reject such a notion.

As with independence, the comments appear to indicate that a solution for aligning the requirements of protected employment status with the DPO role could lie in distinguishing between the DPO's dual status as a DPO and as an employee (or external consultant) of the company. A DPO should have operational independence in carrying out the duties of a DPO (albeit consistently with the overall strategic direction of the business), and should not fear reprisal from management – including, ultimately, dismissal – for performing the DPO role. Yet the DPO would be expected to meet the general requirements of any other employee: "*A DPO should have the same status as any employee, in that they can be dismissed if they are a poor performer, gross misconduct and so on.*" Or as another respondent put it: "*The DPO cannot be fired for acting on privacy issues, but will otherwise be treated just as any other senior executive – including targets and behavioral requirements!*"

It may be a sufficient safeguard if the DPO cannot be removed from the role merely for carrying out the DPO's duties, even when the DPO's decisions may at times be unpopular. Again, it may be useful to learn from existing national law requirements. Under French law, the company must notify the data protection authority (the CNIL) of any change affecting the DPO's functions and cannot terminate the DPO role without having informed the CNIL in advance. A similar requirement in the Regulation would prevent a company from summarily dismissing the DPO from their role (e.g., merely because of unpopular advice) and it would also prevent the company from summarily withdrawing the DPO's resources and changing their role, following which it could claim that the DPO was failing to fulfill the role (i.e., potentially a form of constructive dismissal).

Finally, a respondent had an interesting insight which may be helpful in solving what appears to be a conflict for organisations when dealing with a non-performing DPO, *"… a DPO who isn't an effective communicator or doesn't understand commercial considerations, isn't fulfilling the conditions required* (by law for the DPO role) *anyway and should be disciplined and ultimately dismissed."*

3.4 DPO fixed term of appointment

72% of respondents considered it inappropriate for the Regulation to specify a fixed term of appointment for the DPO.

- Some explained that an organisation should have the flexibility to make its own determination and that there are no corporate precedents for fixed term appointments. The DPO role should not be different from any other senior corporate role, such as in legal, compliance, audit, or accounting, none of which have a prescribed term of tenure. *"(T)to make a difference a DPO needs to be in a role for a certain length of time, however, I don't think it should be a prescribed period – it will depend on each organisation as to what is appropriate and required.*" Similarly, fixed term appointments would be unrealistic from both the organisation's and the individual DPO's perspective. "*…why should an organisation have to recruit a different DPO simply because the existing DPO has reached the end of tenure. Conversely, why should the DPO have to leave and search for similar role elsewhere?"*

- Many responses seem to indicate that the complex and challenging nature of the DPO role, the need to preserve consistency and stability in an organisation, and the need to ensure continuous accountability and compliance would argue against a fixed term of employment for the DPO. *"Individuals with fixed terms will solve for short term outcomes, not long term positive data protection outcomes. It lessens accountability of the DPO to data subjects and to the organisation"*. In the words of another respondent *"Privacy laws, industry standards and the technologies they guide and govern are ell evolving at a very rapid pace. This dizzying speed makes the DPO role a challenging one, and one better suited to someone who can learn and develop in the role for more than two years."*

- Others suggested that setting a minimum term of DPO employment might be better than fixing the length of the term. A specified fixed term does not appear to offer any particular benefits.

A minority of respondents (28.2%) saw benefit in having a fixed term.

- Some saw this as helping business continuity and stability- "(it) *helps to create stability and ensure we don't have constant turnover*" and it "…*would allow some stability in the role, however, if there was a performance issue – especially with an external contractor – it may cause some operational difficulties.*"

- The requirement for a fixed term also supports and interrelates with the concepts of the DPO's independence and protected employment status. A fixed term would *"assist the officer in executing their role without fear or favour"* or, in the words of another respondent, it would *"allow him to step down (by denying the re-appointment) if the board doesn't cooperate!"* As indicated in sections 3.2 and 3.3 above, survey participants appear to support the view that the minimum term and protected status of the DPO would not apply where the employee's general performance in unrelated areas is poor.

4. Cooperation and Consultation with Supervisory Authorities

Under the Regulation, the DPO would be required to consult on their own initiative and cooperate with data protection supervisory authorities.[14] The majority of survey respondents did not anticipate any issue with this, although quite a few sought to distinguish the requirement to consult from the requirement to cooperate.

- Nearly all respondents stated that their organisation and DPO already cooperate with the regulator and many viewed cooperation with regulators as "key" for the DPO. Also, organisations in the financial sector appear to be more used to regular interaction with regulators generally.

- Many respondents queried whether the requirement to consult with the supervisory authority on a DPO's own initiative might result in significant tensions and potential conflicts of interests for the DPO and the organisation. In particular, the DPO might feel obliged to over-report to avoid possible future criticism from a regulator. Several respondents felt that conflicts of interests would lead to diminished trust between the organisation, the individual and the regulator. One respondent considered it "…*problematic to ask the DPO to become a policeman and 'tell tales' on the organisation [as] they would not be trusted and respected by staff and they would never be able to get honest answers about what the business is doing*." Or as another respondent put it *"The DPO is caught between a rock and a hard place and has to do a very difficult balancing as to not deny his statutory duties nor violate his loyalty requirements towards his company."* This again points to the need for there to be a working and practical balance between independence on the one hand and intimate involvement in the business on the other.

[14] Article 37 Regulation.

- One respondent said that any conflict of interests should be avoided and called for clarity on the issue of whether the DPO is seen as an "extended arm" of the supervisory authority or part of the company's internal compliance framework.

- Currently, the position varies between Member States. Under French law, a DPO must first raise all issues with the data controller before contacting the CNIL, and must inform the data controller of any communications with the CNIL. In contrast, under German law, the DPO is not required to inform the data controller of communications with the regulator, and is bound by confidentiality obligations that would prevent the DPO from giving any details to the regulator that would lead to the identification of data subjects or information provided by data subjects (without the data subjects' consent). The current text of the Regulation does not indicate whether communications with the supervisory authority must be open and transparent, or whether any obligations of confidentiality would attach. Given the existing divergences under national law, this point would likely merit clarification under the Regulation, as otherwise the expectations of supervisory authorities in different jurisdictions could differ. In the absence of clarification, the DPO's relationships with supervisory authorities may be difficult, especially if a group DPO is appointed to liaise with multiple supervisory authorities across Member States.

- Several respondents saw challenges and anticipated changes in current organisational practices if a DPO were to be allowed to consult on their own initiative with regulators. It will be critical to have a DPO with "*appropriate judgment who is able to carry such a degree of independence and initiative".* Also, companies need to be aware, understand and control regulatory interactions. One respondent indicated that their "*DPO is not currently authorised to have any independent contact with government officials."* Finally, it will be necessary to provide training and guidance to the DPO and ensure that they work with the company's government relations, legal department and other stakeholders when preparing to consult with regulators. Some respondents pointed to the need for familiarity with multiple and different privacy requirements, and also local language skills, which may be hard to achieve.

- One respondent cautioned against the consultation duty becoming a mechanical and superficial, tick box exercise due to time pressure on the DPO and lack of sufficient resources from regulators to support such an intensive relationship.

5. Avoiding Conflicts of Interests

We sought to understand whether the multi-facetted and wide reaching role of the DPO, as envisaged under the Regulation, would create conflicts of interests within the organisation and for the individual DPO.

Many respondents did not see any new issues with the envisaged scope or duties for the DPO, particularly where the role is performed on a full time basis. Also, some respondents pointed out that other roles within companies perform similar duties, such as internal audit, legal and ethics and the compliance function and manage to navigate potential conflicts of interests. Conflicts of interests can be avoided by involving others to oversee the privacy programme, such as internal or external auditors.

On the other hand, many respondents warned against the potential for conflicts of interest, especially in relation to two specific areas:

- Some respondents saw conflict inherent in the role itself and the tasks the DPO is required to perform. Independent compliance, monitoring and audit functions are key. It is essential to split the monitoring and assessment role from the DPO tasks and have compliance and audit perform those tasks. Having such "ethical walls" within the company is essential, but may be hard for smaller enterprises to achieve.

- Many felt that conflicts of interests would arise where the consultation tasks of the DPO are interpreted broadly, and will depend on how the role is perceived by the DPO, the organisation and data privacy regulators. If the DPO is seen as a policeman in an

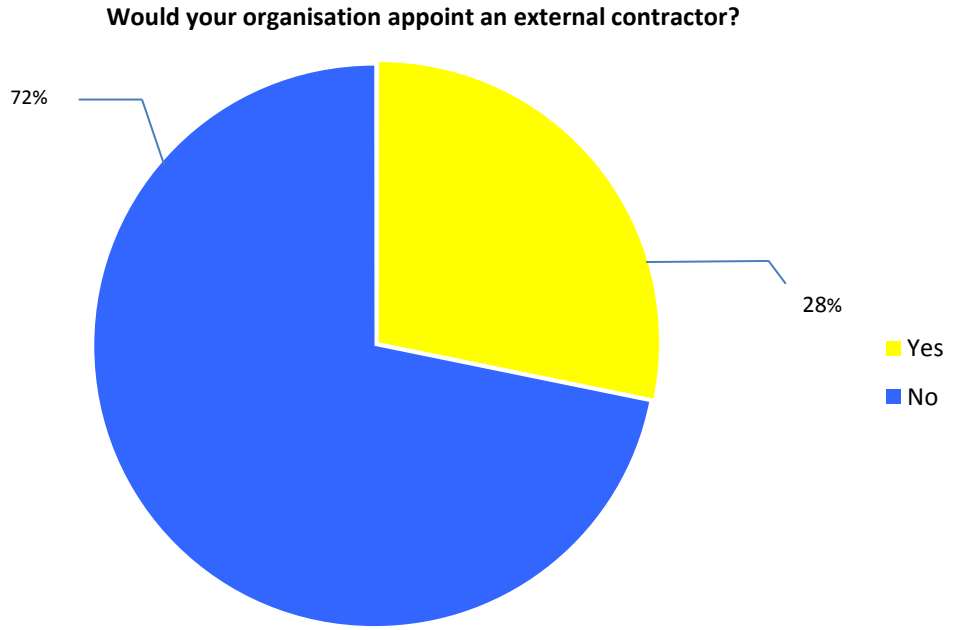
organisation and expected to make self-disclosure and report compliance problems, that likely would create conflicts of interest. In the words of one respondent: "*The key question is whether the view of the DPO is that their first duty is to the organisation, or to be a police officer for data protection regulators. The latter view would create a high potential for conflict.*"

- Several respondents felt that careful thinking is required to set expectations for the DPO and the role, in order to avoid these potential conflicts of interest and preserve the significance, the purpose and the effectiveness of the DPO role. *"Serving as essentially an agent of the DPA within the organisation will set up the DPO role as being basically adverse to the organisation, which is likely to result in isolation and minimisation of the DPO role."* These conflicts of interests would result in the DPO under the Regulation being focused more on compliance, as their ability to provide risk based advice and support to the business would be curtailed.

Insights from respondents point to the need for careful thinking both on the part of the organisation and on the part of data protection regulators, and the need to consider and provide further guidance on how to avoid and manage any potential conflicts of interest for the DPO. In the words of one respondent, there should be no conflicts in the scope and the nature of the DPO role *"if the individual has the appropriate profile, experience and collaborative mindset and if he/she is supported by the organisation and the regulators. There is a need of paradigm change on both sides: Companies & Regulators."*

6. External v. Internal DPO

The Regulation allows for the appointment of an internal or external DPO.[15] We asked respondents whether their organisation would appoint an external DPO, and if not, why not.



Most respondents thought it unlikely that their organisation would appoint an external consultant, for a variety of reasons.

- The primary concern was that an external DPO would unlikely have sufficiently intimate knowledge of the business and its processing activities to be able to advise properly and perform the DPO role effectively: "*An external contractor does not know the business as well as is needed and has no investment in doing so.*" An external DPO may result in

[15] Article 35(8) Regulation.

less effective compliance and a less strategic role for the DPO, as the individual would not be embedded in the organisation and benefit from internal relationships and knowledge. "*An external DPO would have difficulty staying informed of all of the product and operational developments and details within the company that involve personal data.*" This last comment is significant. The mere fact of approaching an external DPO for advice assumes that the company has already understood and identified the privacy issues arising on a particular project but, in practice, the business may not appreciate that data protection advice should be sought. This can arise where business stakeholders fail to appreciate that privacy restrictions apply beyond obvious personal identifiers, such as name and address.

- Many respondents also raised cost concerns over external DPOs which, in their experience, are expensive. One respondent commented that they usually cross-checked the advice of the external DPO with outside specialist counsel in any case, further increasing the cost.

- Respondents also raised concerns relating to the continuity, internal accountability, and whether an external DPO could easily gain the position of "trusted advisor" to the company. One respondent noted that "*…employees may potentially feel uneasy to share information about the more confidential practices*." The benefit of having an internal DPO is that the DPO is part of the business, is a colleague, and – hopefully – is working towards shared goals along with the rest of the business. Again, this emphasises the point that the DPO should perhaps have operational independence, but follow company strategy.

On the other hand, respondents also felt that an external DPO could be a feasible option and that the external DPO has a place and a role to play.

- Small organisations and start-ups would benefit from an external DPO. In particular, this would ensure that they have the required level of data privacy expertise and knowledge, that they would not otherwise have within their organisation.

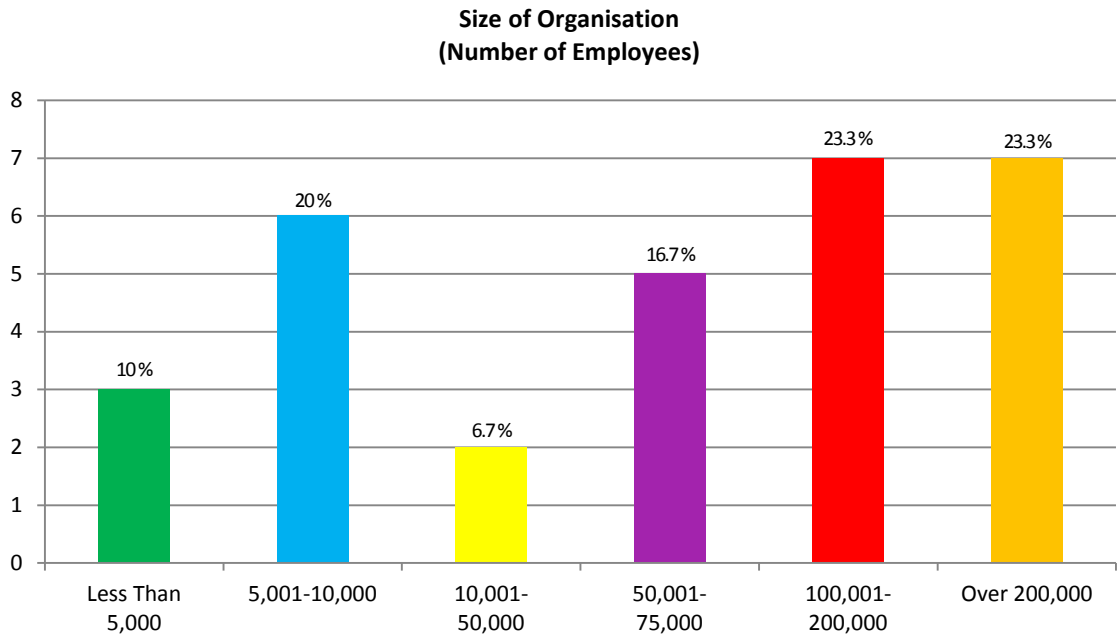
- It may also solve the issues of conflicts of interests and challenges presented by the requirements for independence and protected employment status for the DPO. One respondent even contemplated real benefits from having a combination of an external DPO and internal DPO. *"A key role of the DPO today is to advise the business, taking into account the company's risk appetite and business objectives and the risks… associated with ….non-compliance. Although some aspects of DP obligations are clear, many are in fact are "grey" and its' necessary to take a risk based approach to advising the business on how to proceed… Having an outsider carry out the role would allow that individual to focus solely on the statutory requirements of the role, i.e. monitoring compliance and reporting to executive. That would allow the company then to have an internal DPO who can advise and support the business…."*

Annex I

Survey Respondents: Demographics and Organisational Information

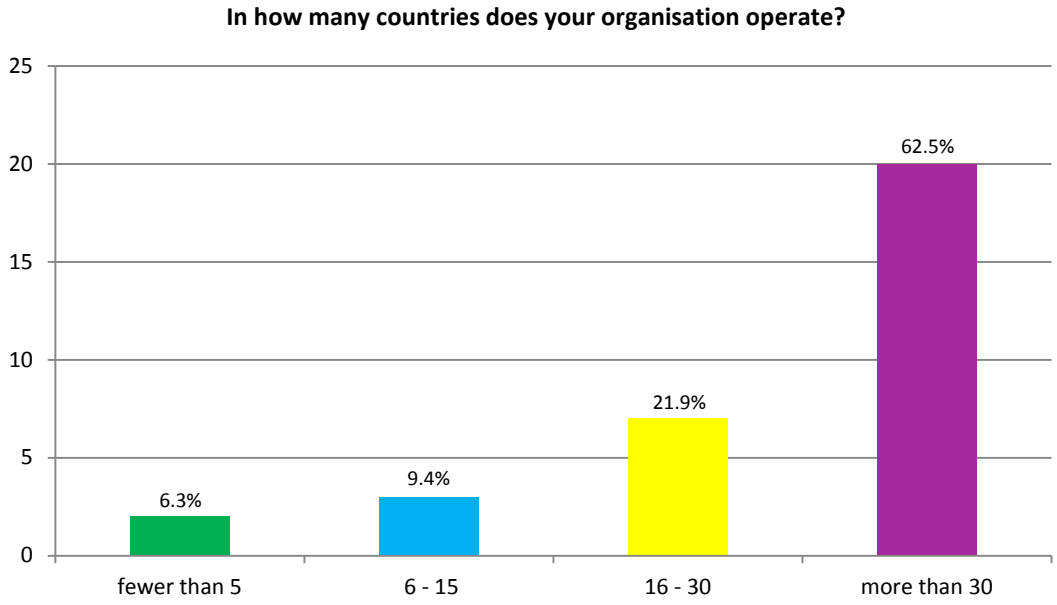
1. *Size of Organisation*

The DPOs that responded to the survey belong to organisations of varying sizes (by number of employees):



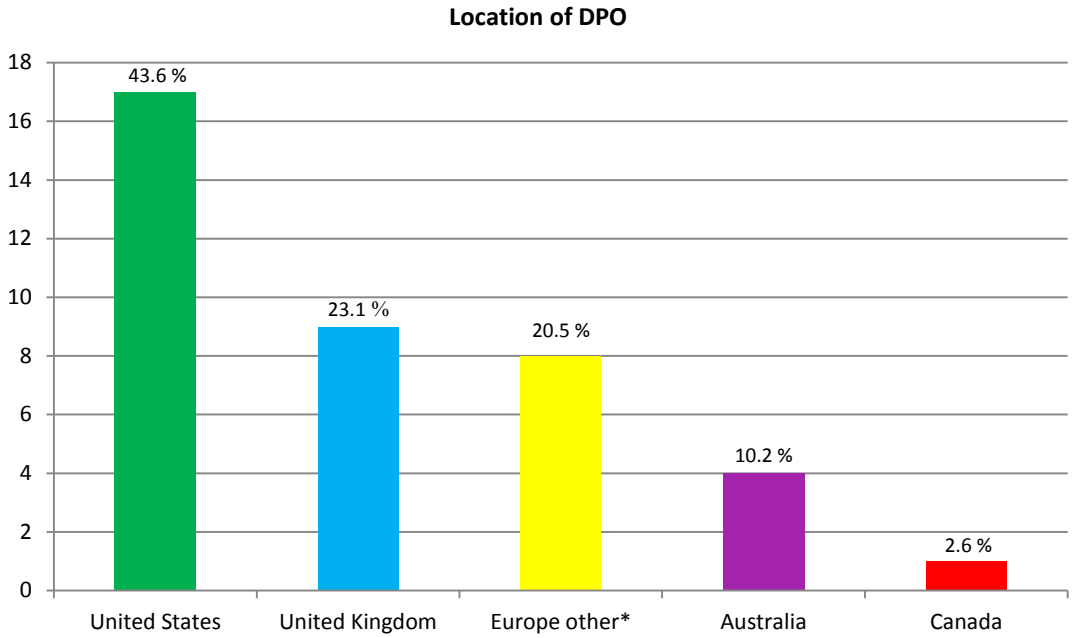
2. *Geographical Reach of Organisation*

The DPOs that responded to this survey belong to organisations having the following geographical reach:



3. *Location of DPO*

We asked survey participants to indicate where their DPO/CPO or global privacy leader is located:

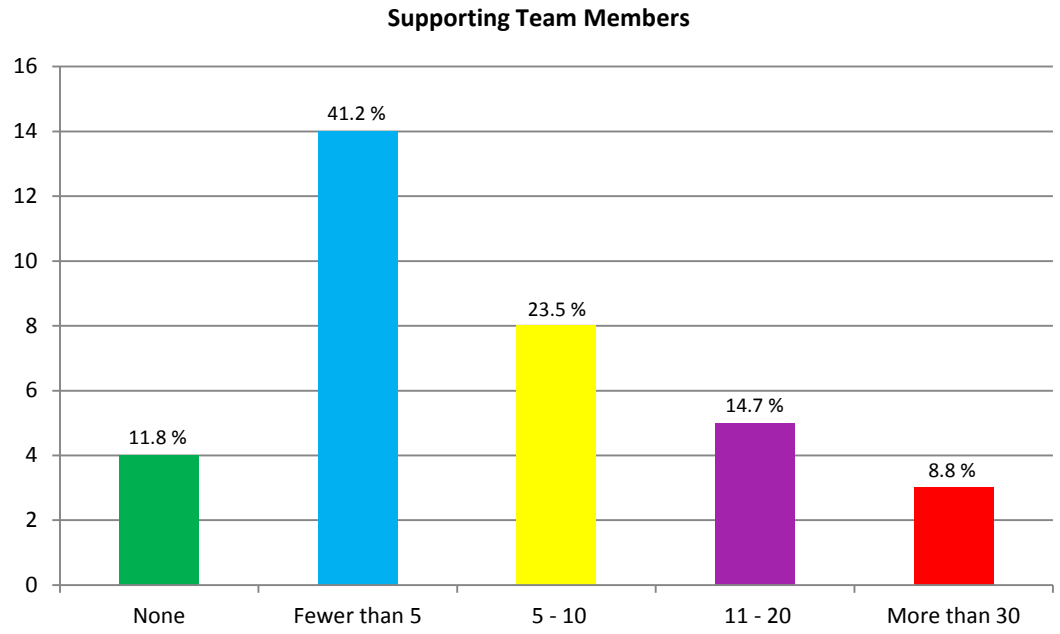


*Other European countries represented: 3 in France, 3 in Germany, 2 in Switzerland

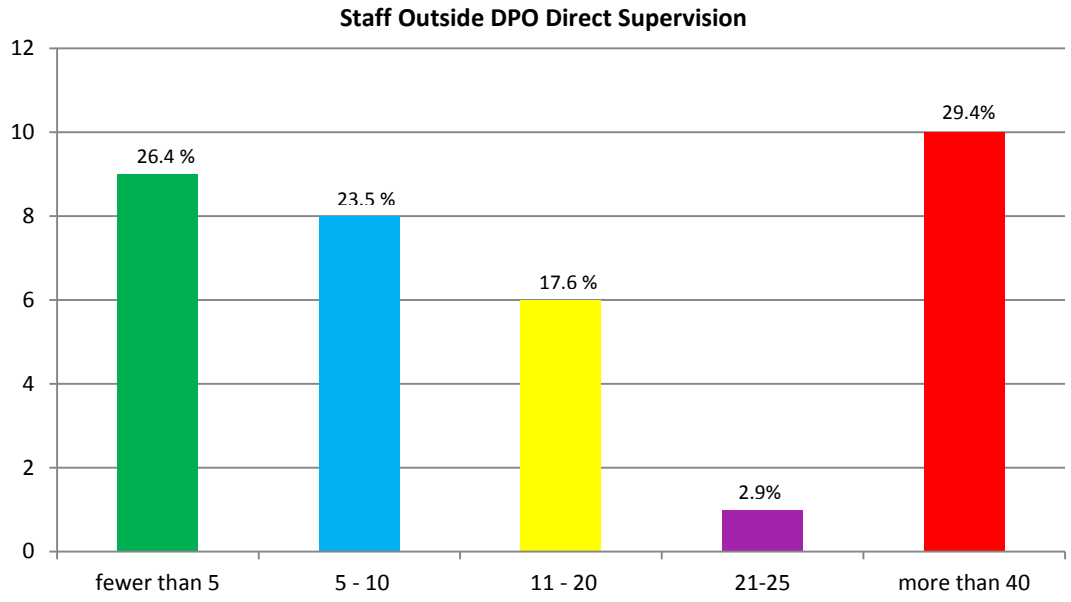
4. *Resources*

We asked survey participants to identify the human and financial resources available to the DPO in their organisation.

Number of supporting team members:



Number of other staff outside the DPO's direct supervision with data privacy responsibilities:



Additional data privacy personnel hires (or assigned responsibilities to existing personnel) in the past year:

- Almost half the organisations that responded to this question (15) hired or assigned additional personnel to data privacy in the past year
- The majority of these organisations indicated that they appointed 1-3 additional personnel in the past year
- One fifth of organisations who responded to the question did not hire, or assign any additional personnel.

Budget for data protection compliance in the past year (including outside counsel fees, internal resources, security upgrades, etc.):