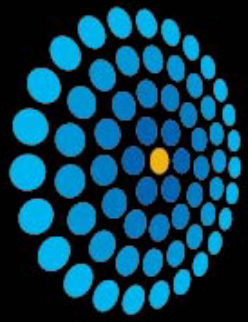


DPO Project Workshop II

10 December 2013

Centre for Information Policy Leadership
Hunton & Williams LLP

Agenda

Arrival and Coffee **09:00 – 0:930**

Introduction and welcome

- Wim Nauwelaerts, Partner, Hunton & Williams **09:30 – 09:40**

Summary of the project, analysis of survey responses and emerging themes **09:40 – 10:40**

Bojana Bellamy, President, Centre for Information Policy Leadership

Coffee **10:40 – 11:00**

Expectations, challenges and opportunities for DPAs when working with DPOs under current national law and the future EU DP Regulation **11:00 – 12:00**

- Albine Vincent, Head of DP Officer Department, CNIL, France
- David Smith, Deputy Information Commissioner, UK
- Wojciech Wiewiórowski, Inspector General for Personal Data Protection, Poland
- Billy Hawkes, Data Protection Commissioner, Ireland

Agenda (continued)

Current corporate practices in appointing and managing the DPO role and how they may change under the future EU DP Regulation **12:00 – 13:00**

- Daniel Pradelles, EMEA Privacy Officer, Hewlett-Packard
- Emma Butler, Senior Director, Privacy and Data Protection, Lexis Nexis
- Daniela Fabian-Masoch, Global Head Data Privacy, Novartis
- Gabriela Krader, Corporate Data Protection Officer, Deutsche Post DHL

Bridging two sessions and conclusions over working lunch **13:00 – 13:30**

- Bridget Treacy, Partner, Hunton & Williams

Rapporteurs

- Rosemary Jay, Senior Attorney, Hunton & Williams
- Naomi McBride, Associate, Hunton & Williams

Centre for Information Policy Leadership
Hunton & Williams LLP

DPO Role Project

Centre for Information Policy Leadership
Hunton & Williams LLP

DPO Project Overview – Addressing the Challenges of a Changing Role

The DPO has assumed an essential role in delivering privacy compliance and has become a critical component of an organisation's privacy management program. Increasingly, new and proposed privacy laws are impacting that role. Companies must recognise the challenges and opportunities presented and explore how to respond.

Project will examine:

- The proposed DPO under the Draft EU Data Protection Regulation;
- Comparative regulatory obligations for the DPO role in current privacy laws;
- Comparative obligations in analogous legislation;
- The potential impact of proposed requirements for the role on existing corporate practices, and management of privacy; and
- Recommendations for dealing with the challenges and opportunities presented by the changed role.

Project Timeline

- September – Completion of initial research and launch of the project at the International Commissioners' Conference in Warsaw
- October to December 2013 – Rolling out DPO Survey and completion of survey analysis and further research
- December 2013 – Workshop in Brussels with key stakeholders
- January 2014 – Interviews with key DPAs
- January to February 2014 – Completion of research papers
- February 2014 – Report from the Centre

Centre for Information Policy Leadership
Hunton & Williams LLP

Proposed Role of the DPO Under the Draft EU DP Regulation

Proposed Role of the DPO Under the Regulation

We examined the requirements for the appointment of a DPO and the nature, function and scope of the DPO role under the Regulation *(see "Initial Discussion Paper: The Role and Function of the DPO in the European Commission's Proposed General Data Protection Regulation*").

This initial discussion paper examined in detail:

- The Requirement for a DPO under the Regulation
- Appointment of a DPO
- Features of the DPO role
- Tasks of the DPO

Centre for Information Policy Leadership
Hunton & Williams LLP

Comparative Analysis of the DPO Role Under Existing Privacy Laws

Obligations to Appoint a DPO under Current Laws

We examined DPO requirements under a number of national data privacy regimes, as well as the OECD Guidelines (*see* "*DPO Requirements Under Selected Data Privacy Laws*").

Conclusions

- Few currently have a mandatory DPO appointment requirement - Germany, South Korea, sectoral U.S. laws, e.g., HIPAA.
- The majority permit either an internal employee as the DPO or an external consultant as the DPO.
- None require the DPO role to be a full-time role, and generally DPOs fulfil a variety of other functions.
- Most laws do not specify the tasks and duties of the DPO, although in some cases these are prescribed by statute (e.g., South Korea).
- Under some laws, the DPO has protected employment status (Germany, Netherlands).
- In one case (Germany), the DPO can communicate confidentially with the regulator without the company's knowledge.

Comparative Roles in Analogous Laws

Comparative Roles in Analogous Areas

We examined potentially analogous roles under other areas of law, in order to draw comparisons or borrow learning from these areas (*see* "*Comparative Table of Analogous Roles*").

Scope - UK and U.S. law in the areas of anti-money laundering, health and safety, environmental reporting, and competition law.

Findings – DPO role is unique

- Mandatory requirements to appoint a designated individual responsible for compliance is not limited to data protection;
- There are no mandatory requirements to appoint an environmental law or competition law officer;
- Only limited comparisons with anti-money laundering laws, which apply to specific sectors, for specific activities only. The remit of the Regulation, which would apply to all sectors and to all processing activities, and the scope of DPO's responsibility are far broader and further reaching; and
- Greater comparisons with UK health and safety laws which, like the Regulation, apply to all sectors and carry high penalties for non-compliance.

Centre for Information Policy Leadership
Hunton & Williams LLP

DPO Role Survey Summary

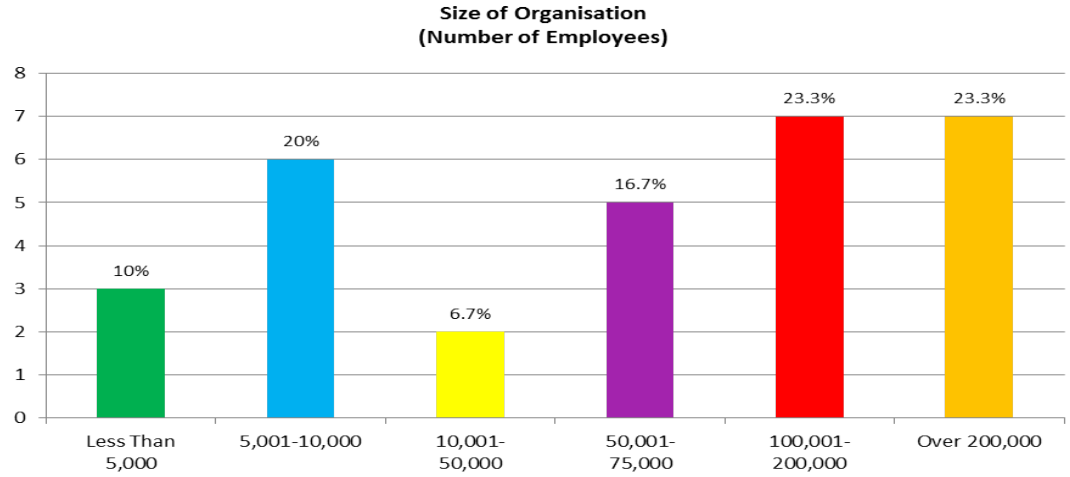
Assessing Current Role and Practices in Light of the Anticipated Changes to the DPO Role

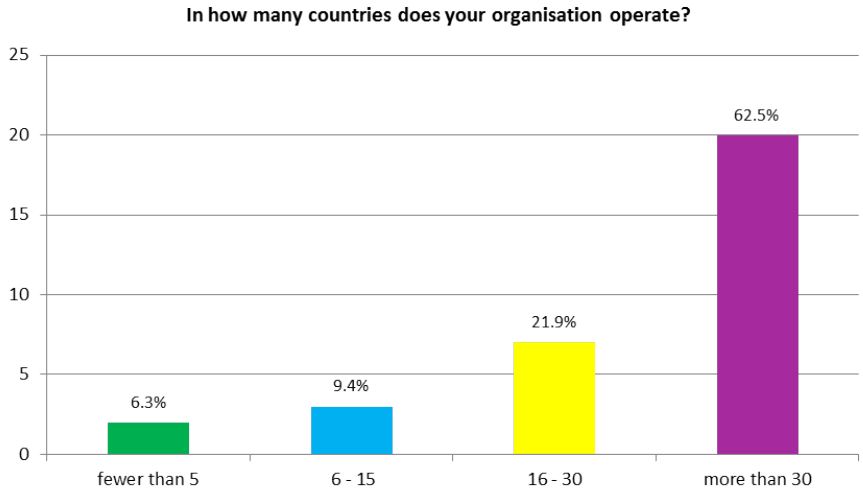
We surveyed 43 practising DPOs/CPOs/global privacy leads ("DPOs") across a range of industry sectors and based in a variety of geographical locations about the role and function of the DPO within their organisation *(see "Report on Survey Results"*).

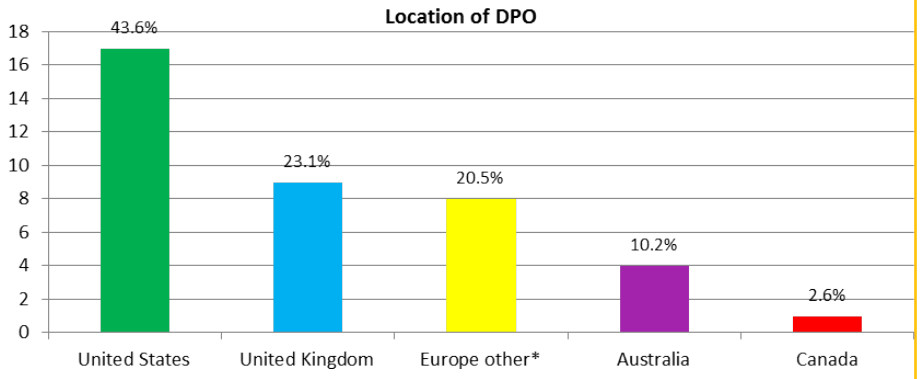
The objectives of the survey:

- Understand current practices and drivers for appointment of DPO, their tasks and responsibilities.
- Assess the impact of the anticipated changes to the DPO role based on the proposed requirements of the Regulation.
- Seek deeper insights on any challenges and changes that organisations will need to make in their current practices to reflect the proposed requirements for the DPO role.
- Seek to understand practical solutions and recommendations on how to manage that change.

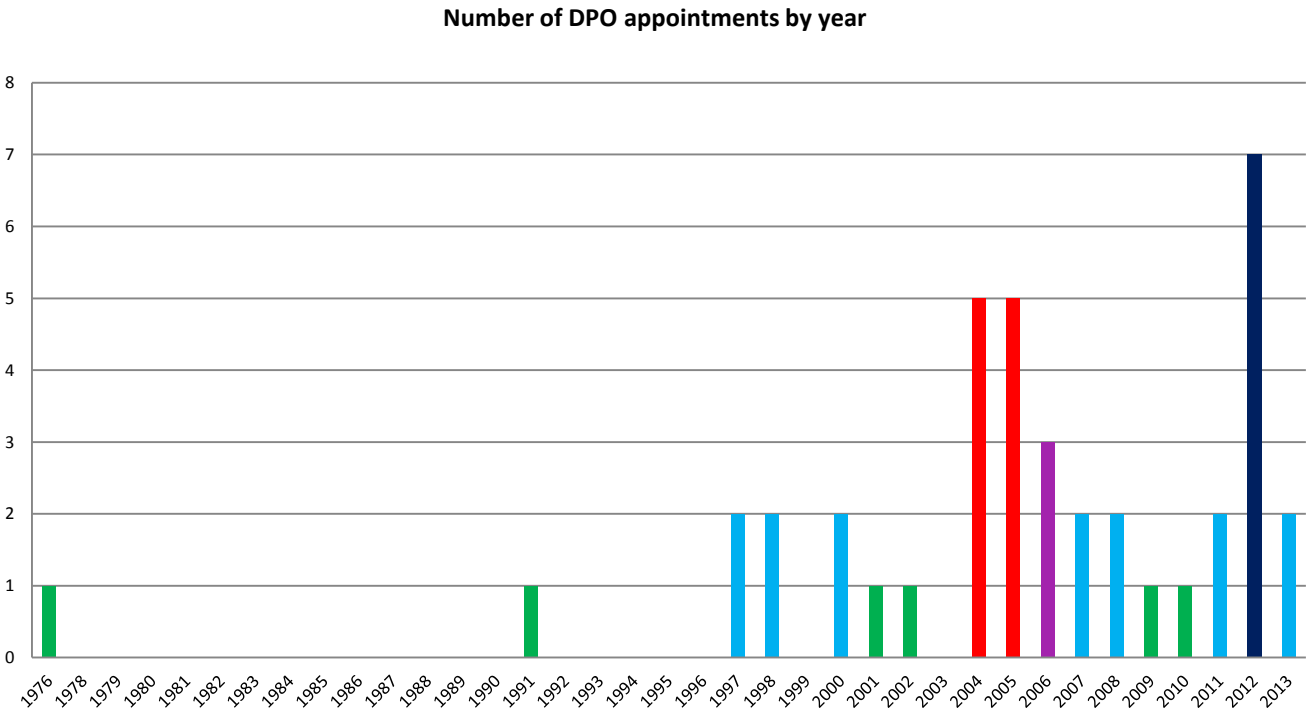
Demographics and Organisational Information





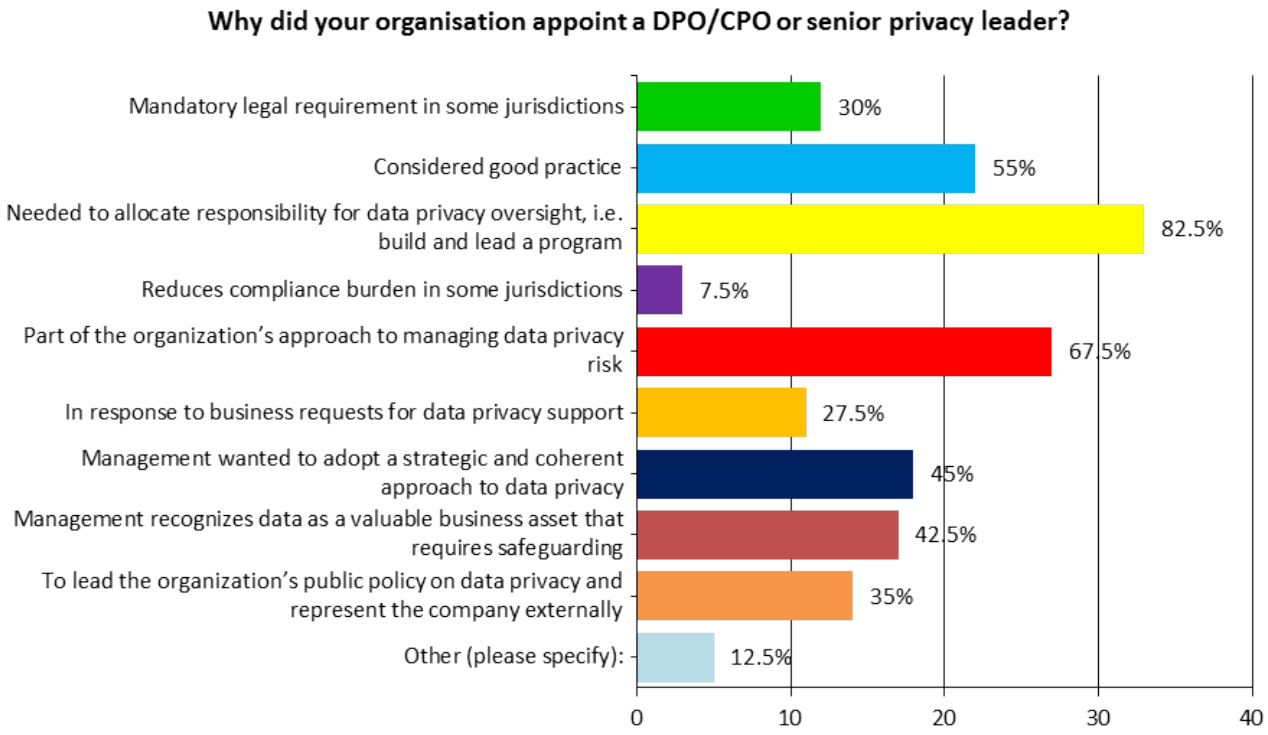


Growth in DPO Appointment and DPO Teams



- Quarter of respondents appointed DPO before 2002 and the majority between 2004-2008.
- Surge in DPO appointment in the past three years.
- Half of respondents hired or assigned additional personnel to their privacy teams in the past three years (great majority between 1-3 people).

Reasons for Appointing a DPO



Despite a lack of legal compulsion, a great majority views the DPO appointment as a cornerstone of corporate accountability and privacy programmes, good corporate practice and a proactive management of data privacy.

Evolving DPO Role and Increasing Responsibilities

Great majority of DPOs already focus on the tasks envisaged in the Regulation

- 87.5% advise their organisation on compliance with applicable laws
- 82.5% oversee the organisation's privacy programme
- 67.5% handle data subject complaints
- 85% provide expert advice following a security breach
- 72.5% maintain relationships with the local regulator

Least number of DPOs perform very operational tasks - 62-67%

- deal with data subjects complaints
- respond and deal with individuals' requests for exercise of rights
- conduct and oversee assessments and verification of compliance

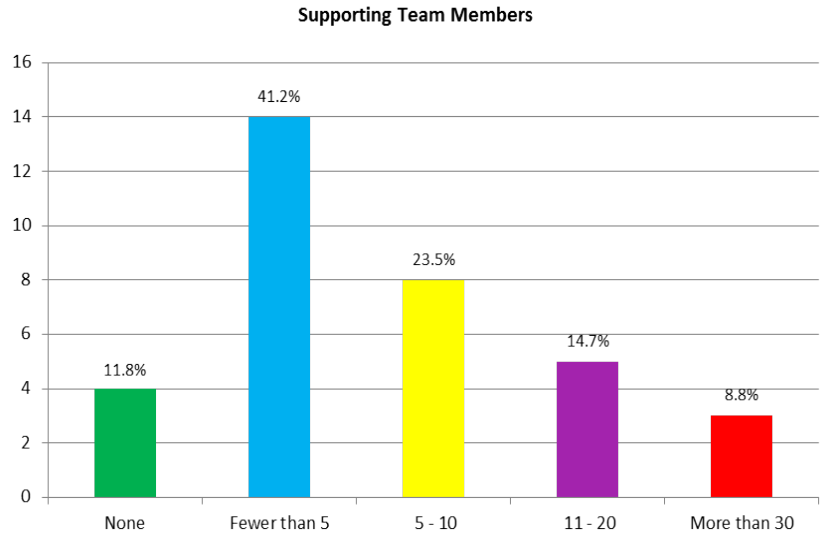
DPO role appears to have transformed over time

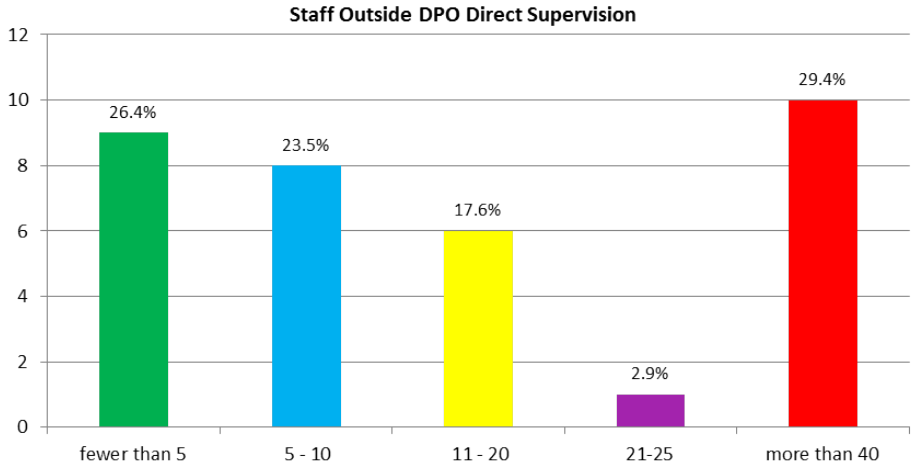
- DPOs are increasingly taking on public policy and external representation tasks
- DPO is increasingly a strategic leader
  - 82.5% consider the setting of strategy and policy as key tasks
  - the Regulation does not prescribe a strategic role, although half of respondents believed it would result in such a role and half thought it would lead to a mid-level compliance DPO role.

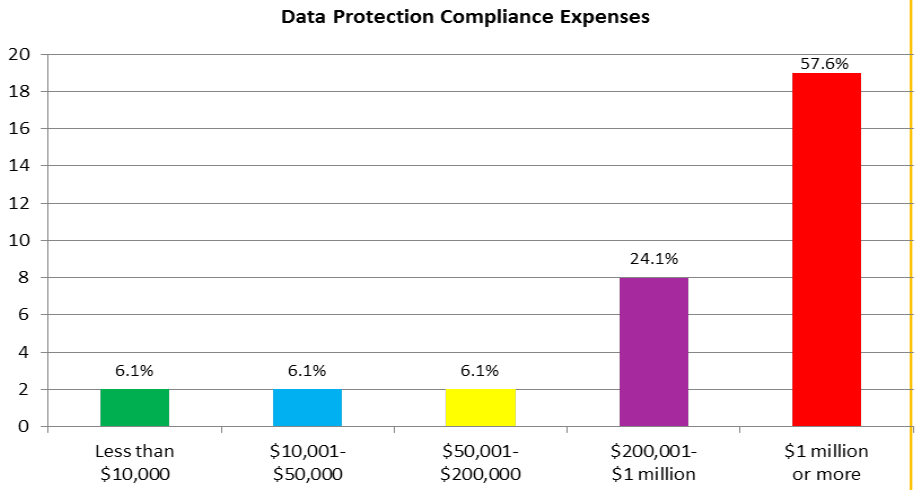
The DPO Role Performed by DPO Team

- 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.
- The Regulation is drafted on the basis that a single individual will fulfil 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 having five or more team members under their direct supervision assisting them in their role as the DPO.
- A privacy team – both central under DPO and decentralised in other parts of organisation – rather than an individual, may be the best way to fulfil such a multi-faceted role.

.


Supporting Team Members
16
14
12
10
8
6
4
2
0
41.2%
23.5%
14.7%
11.8%
8.8%
None
Fewer than 5
5 - 10
11 - 20
More than 30

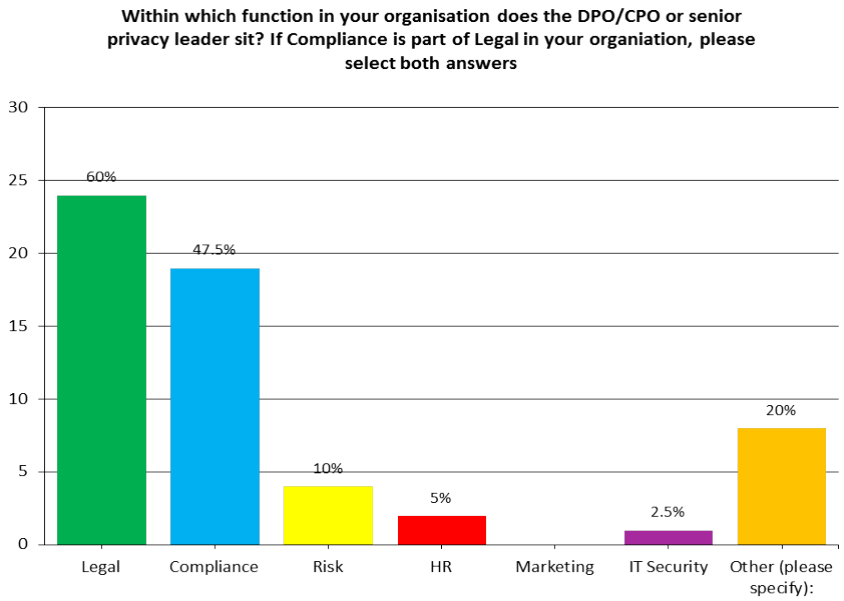

Staff Outside DPO Direct Supervision
12
10
8
6
4
2
0
26.4%
23.5%
17.6%
2.9%
29.4%
fewer than 5
5 - 10
11 - 20
21-25
more than 40

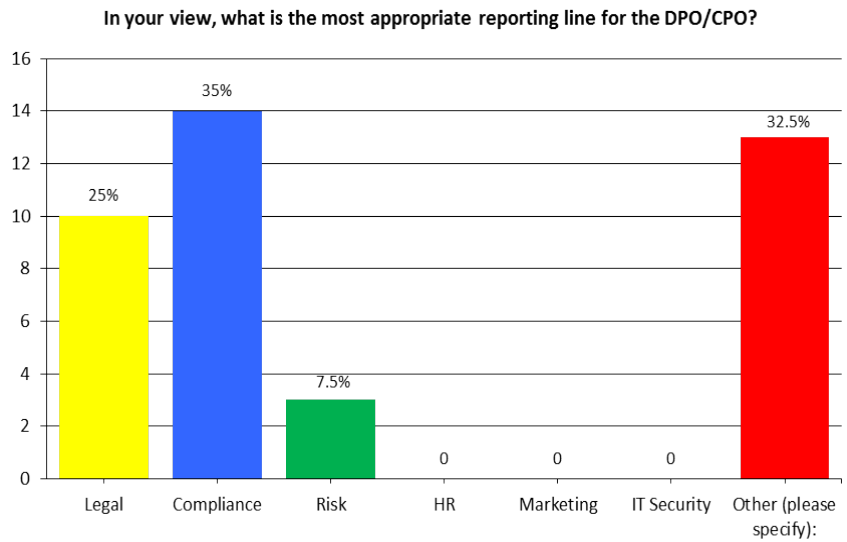

Data Protection Compliance Expenses
20
18
16
14
12
10
8
6
4
2
0
6.1%
6.1%
6.1%
24.1%
57.6%
Less than $10,000
$10,001-$50,000
$50,001-$200,000
$200,001-$1 million
$1 million or more

Independence: Position and Compatible Tasks

The Regulation stipulates that the DPO must report directly to management and not perform any other duties, unless they are compatible with the DPO duties.

- DPO role often sits within legal and/or compliance, yet many respondents appear to suggest an independent, standalone position, reporting directly to senior management (CEO, Board).
- Many senior DPOs performed additional tasks – information governance, ethics /compliance, records management, legal, public policy – some of which may not be compatible.





Independence: Reporting Lines and Not Taking Instructions

The Regulation stipulates that the DPO must not receive any instructions as regards the exercise of the DPO function, and must report directly to management.

- Respondents were divided as to whether their organisation would find this difficult to comply with - 53.8% said yes and 46.2% said no.
- This reflected existing legal requirements in some countries (Germany, France) and many respondents indicated they report directly to management and, given their seniority, do not receive detailed instructions as to how to fulfil their role.
- Some of the identified issues:
  - the conflict for DPO between being integrated within the business, yet being viewed with mistrust as a compliance "enforcer";
  - the inability for any individual within an organisation to be completely independent;
  - in global companies, reporting lines to local management may impede the ability to achieve strong data protection outcomes and an effective privacy programme.
- Emerging themes
  - independence means ability to give free advice, but the ultimate decision lies with business;
  - operational independence to fulfil DPO role, rather than strategical independence.

Protected Employment Status

Under the Regulation, the DPO enjoys protected employment status and cannot be dismissed, except if they "no longer fulfil the conditions required for the performance of their duties."

- Minority of respondents did not perceive difficulties for the organisation:
  - Familiarity with the concept under existing data privacy and other national laws providing for protected status for similar roles.
  - Company's values, code of ethics and non-retaliation policies would prevent any issues.
  - Given strategic importance and highly skilled nature of the DPO role, only a senior and trusted employee would be appointed in the first place.
- Some of the identified issues
  - The concept of protected status is unique, inconsistent with a business having the freedom to make its own decisions and culturally difficult.
  - Need to resolve performance issues.
  - Need to make significant changes to employment practices.
- An emerging consensus - to distinguish between DPOs' dual status as a DPO and an employee and treat the DPO the same as any employee in respect of general employee requirements. Protected employment status could be limited to the DPO tasks only.

Fixed Term of Appointment

Under the Regulation, the DPO would be appointed for a fixed term of 2 years

- 72% considered inappropriate the statutory requirement for a 2-year fixed term
  - Lack of any corporate precedents of fixed term appointment for other similar senior roles.
  - Detrimental to stability, consistency and continuous accountability and compliance in an organisation.

- 28% saw benefits in having a fixed term for DPO
  - The concept supports and interrelates with requirements for independence and protected employment status.
  - It could lead to stability in the role and lack of turnover.

Cooperating and Consulting with Regulators

Under the Regulation, the DPO would be required to cooperate with supervisory authorities and consult with them on his/her own initiative.

- Nearly all respondents already cooperate with regulators.
- Many respondents distinguished the requirement to consult and the requirement to cooperate, seeing the potential for conflicts and tensions to arise from the consultation duty:
  - DPO perceived as a policeman or an extended arm of regulators rather than part of the company's internal compliance framework, resulting in lack of trust, involvement and ultimately effectiveness.
  - Need for change in current organisational practices and culture, and to provide training, guidance and support to DPO.
- 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 - this point would likely merit clarification given divergences under existing national laws.

Avoiding Conflicts of Interests

We asked if the multi-faceted and wide-reaching DPO role would create conflicts of interests for the DPO and the organisation.

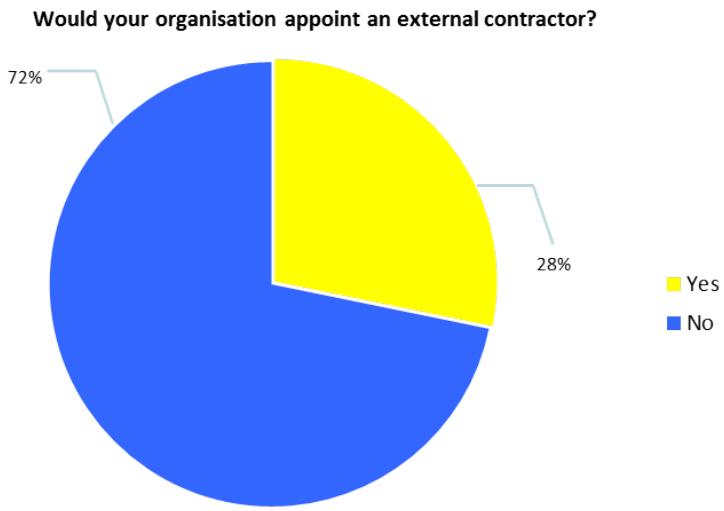
- Many did not have concerns, especially if the role is performed full-time and given their familiarity with other corporate roles that manage to navigate successfully potential conflicts (audit, ethics/compliance, legal).

- Many warned about potential conflict in two specific areas:
  - Conflict is inherent in the DPO role itself if the DPO is expected to perform monitoring and compliance assessment tasks.
  - Consultation duty with DPAs should not be interpreted too broadly and result in the DPO being seen as a policeman and expected to make self-disclosures.

- Emerging themes:
  - Avoiding conflicts of interest is critical to maintaining a strategic and business focused DPO role and preserve the significance, purpose and effectiveness of the DPO role.
  - There is need for careful thinking, further guidance and setting of expectations both from organisations and DPAs, as well as providing guidance to DPOs on how to avoid conflicts of interests.

Internal v. External DPO

We asked survey respondents whether their organisation would appoint an external DPO, and why or why not.



Generally, respondents thought it unlikely their organisation would appoint an external DPO, for a variety of reasons, including:

- an external DPO would unlikely have sufficiently detailed knowledge of the business and processing activities and will be less embedded in the business - could result in less effective compliance and less strategic role for DPO

- business continuity, accountability and whether an external DPO could easily gain the position of "trusted advisor" within the company

- cost

However, an external DPO would work for small organisations/ start ups and may solve the issues of conflicts of interests and challenges presented by DPO's independence and protected employment status.

Discussion