The Role of the DPO under the GDPR
NGFG Meeting - Utrecht

Paul Jordan

Thursday, January 19, 2016

Overview

- General DPO requirements under the GDPR: legitimacy of the DPO role
- IAPP International Research in Privacy

Mandatory Data Protection Officer

Data Protection Officers Art. 37–39

Data Protection Officers (Art. 37–39) are to ensure compliance within organisations (and supply chains). They have to be appointed for all public authorities and for companies where the "core activities":

- **regularly and systematically monitor** data subjects on a large scale, or
- **process on a large scale** special categories of data (Art. 9 and 10).

Data Protection Officers

Nature and challenges

- The DPO is similar but not the same as a Compliance Officer as they are also expected to be proficient at managing IT processes, data security (including dealing with cyber-attacks) and other critical business continuity issues around the holding and processing of personal and sensitive data. The skill set required stretches beyond understanding legal compliance with data protection laws and regulations.
- Monitoring of DPOs will be the responsibility of the Regulator rather than the Board of Directors of the organisation that employs the DPO.
- Usually, the DPO will need to create their own support team and will also be responsible for their own continuing professional development as they need to be independent of the organisation that employs them, effectively as a 'mini-regulator.'

DPD

SECTION IX NOTIFICATION
Article 18 Obligation to notify the supervisory authority

1. **(…)**
2. **Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:**
   - **(…)**
   - **Where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:**
     - for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive
     - for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2), thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

Article 20 Prior checking
1. **(…)**
2. **Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.**

GDPR

SECTION 4 DATA PROTECTION OFFICER
Article 37 Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:
   a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

   b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

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

Data Protection Officer

Qualifications

Art. 37 (5): *'The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.'*

- Certifications: CIPP/E (EU data protection legislation), CIPM (data protection practices, PIAs, Program mgt)
- Log book documentation
- Further qualifications

Data Protection Officer

Responsibilities (Art. 39)

- **Counsel** the entity in regard to applicable data protection laws
- **Monitor** compliance with applicable data protection provisions and with internal policies, including the assignment of responsibilities
- **Awareness-raising** and **training** of staff involved in the processing operations
- Conduction of data protection **audits** and [D]PIAs
- **Cooperate and communicate** with the responsible regulatory authority

Data Protection Officer

New: Data Protection Risk Management

(**Art. 39 (2)**): '*The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.*'

Data Protection Officer

Positioning in the company (Art. 38)

- (1) Proper and timely involvement in all relevant aspects to be ensured by the controller
- (2) Support by sufficient resources and access to data and systems and allowance of further qualification
- (3) Independence of instructions and protection against sanctioning by controller as employer
- (4) Point of contact for data subjects
- (5) Professional secrecy and interest protection

Outsourcing the DPO?

Shared and external DPOs

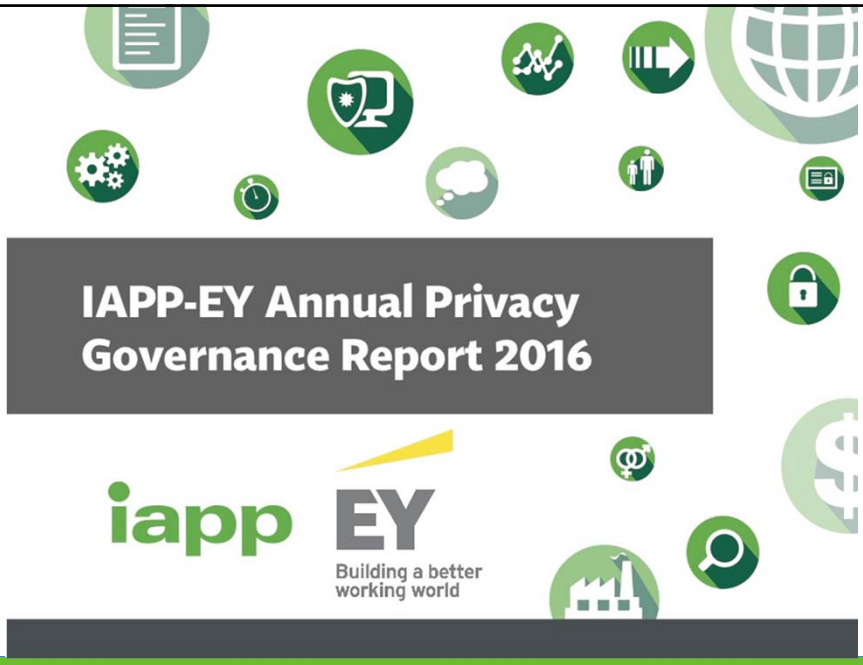
(Art. 37 (2)): 'A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.'

(Art. 37 (6)): '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.'

CPO vs. DPO

Considerations

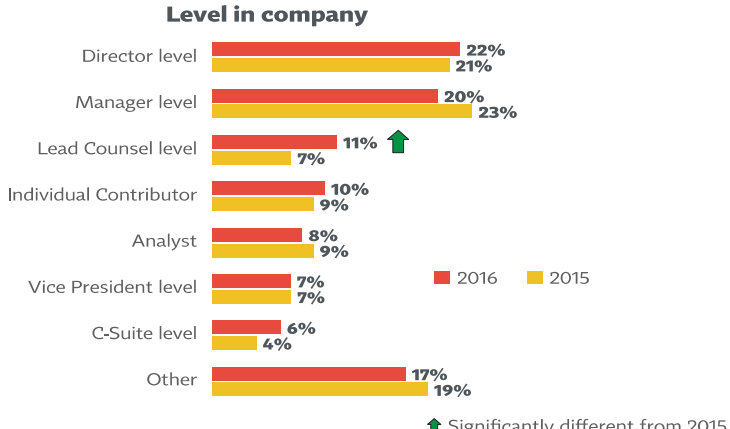
- Is this mandatory DPO the lead data protection and privacy voice in the organisation?
- Does the DPO's role in working with the regulator make it difficult for the DPO to engage in high-level strategic conversations?
- Would appointing external counsel as DPO create conflict when working with the lead privacy voice in the organisation?
- Remember Art. 38 (3): *'The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks.'*



iapp

As in 2015, privacy professionals are most likely to be directors or managers

- However, this year's wave sees a statistically significant increase in the proportion at the Lead Counsel level, to 11%



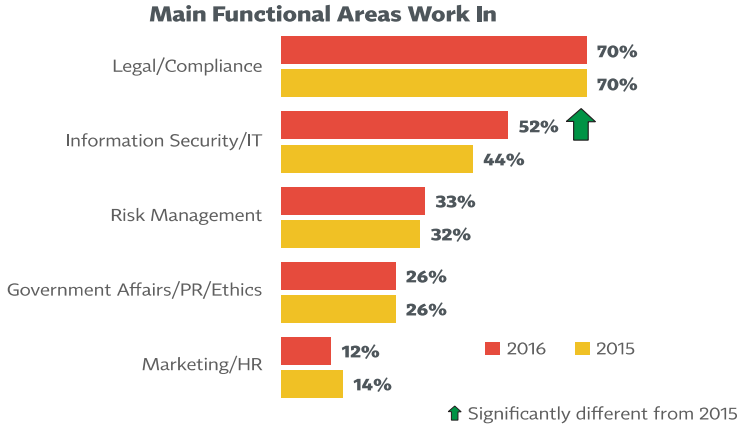
C1: Which of the following levels best describes your position in your company?

IAPP-EY Annual Privacy Governance Report 2016 Background on Companies and Individuals 6

iapp

We saw in 2015 that professionals work across a range of functional areas, and that's still the case

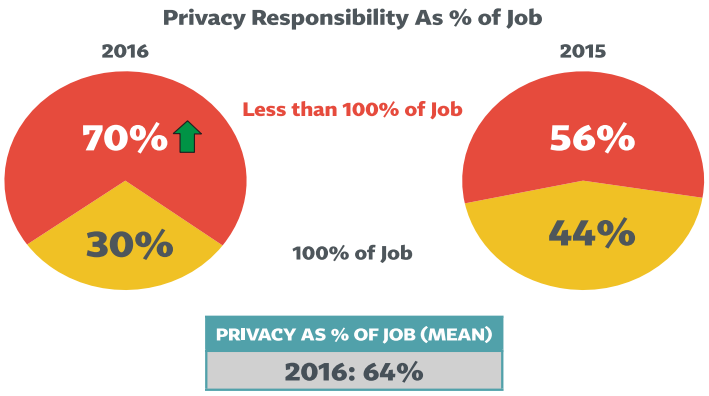
- Legal/compliance is the most commonly mentioned area, although there's also been an increase in those who say they're involved in IT



C3: Which of the following functions best describe the areas you regularly work in at your company?

Looking at in-house professionals, we see a drop since 2015 in those saying privacy makes up 100% of their job

- Just 30% say they're dedicated full-time to privacy, vs. 44% a year ago



Note: Different question structure
2016: D1: About what percentage of your work at your company is made up of privacy responsibilities?
2015: D1: Would you say that privacy responsibilities make up 100 percent of your work at your company or less than 100 percent?

DIRECTORS AND HIGHER

Staff increases are expected for all privacy roles, and virtually no one expects staffing cuts

- By how much will staff increase? Respondents expect to add 7%-11% more staff, all told

Expected Employee Change in Coming Year

	% Saying Increase	% Saying Decrease	% Saying Stay the Same	Net % Change
Full time privacy, in privacy program	37%	2%	61%	+11%
Part time privacy, in privacy program	25%	1%	75%	+7%
Full time privacy, in other units	24%	0%	76%	+8%
Part time privacy, in other units	39%	2%	60%	+11%

F2: In the coming year, do you expect the number of employees in each of these categories to increase, decrease, or stay the same? If increase or decrease, please enter your estimate of the percentage change you expect.

IAPP-EY Annual Privacy Governance Report 2016 Privacy Group Characteristics: Structure **23**

www.iapp.org

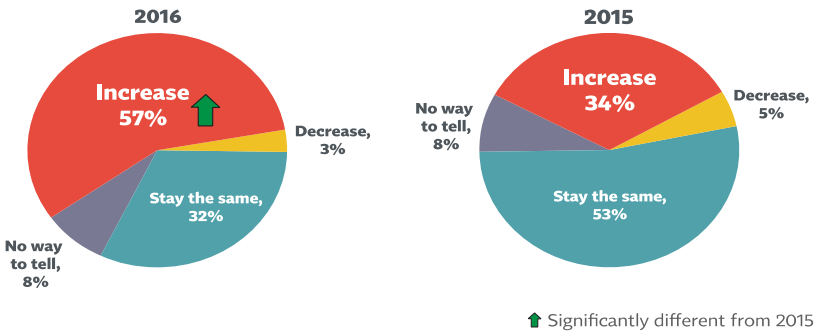
17

DIRECTORS AND HIGHER

2016 sees a sharp jump in those saying their privacy budget will increase next year

- In 2015, 34% expected an increase; in 2016, it's 57%

In Next 12 Months, Privacy Budget Will…



F5: In the next 12 months, you expect your company's privacy budget will …

IAPP-EY Annual Privacy Governance Report 2016 Privacy Group Characteristics: Structure **28**

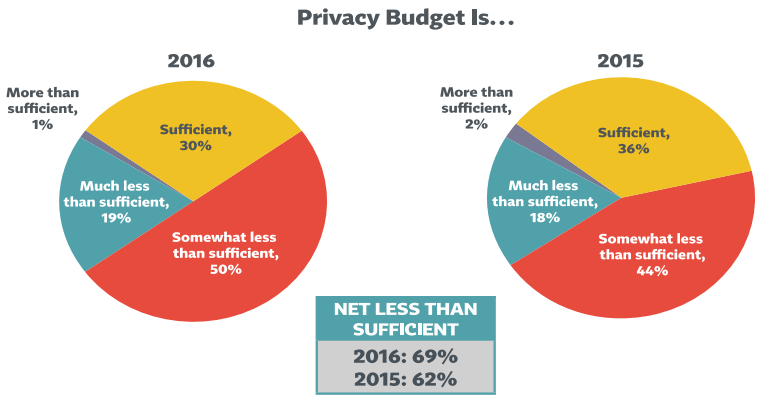
www.iapp.org

18

DIRECTORS AND HIGHER

As in 2015, about two-thirds feel their current privacy budget is not sufficient for their needs

- The "insufficient" proportion is up directionally from 2015, 62% to 69%



F6: In your opinion, your company's privacy budget is … to meet your privacy obligations

IAPP-EY Annual Privacy Governance Report 2016 Privacy Group Characteristics: Structure 29

www.iapp.org

19

The most commonly taken steps to prepare for GDPR are developing training and accountability frameworks

- About a third each say they're preparing by boosting their privacy budget or privacy staff

J8: What, if anything, is your organization doing to prepare for the GDPR?

IAPP-EY Annual Privacy Governance Report 2016 Cross Border Data Transfer 97

www.iapp.org

20

Who are the IAPP

- Founded in 2000
- Largest independent privacy association in the world
- Leading platform for the privacy industry
- More than 26,500+ members in 87 countries
- 552 Corporate members
- Boston, Brussels, Toronto, Mexico City and Singapore



www.iapp.org

Setting the industry standard

IAPP certification is the global standard for privacy and data protection professionals.

- Launched more than 12 years ago, the CIPP has become the preeminent credential in the field of privacy and educates on privacy laws and regulations
- The CIPM training demonstrates how to embed privacy into an organization through process and technology

Now ANSI/ISO Accredited*

*CIPM, CIPP/E, CIPP/US, CIPT

CIPP CIPM CIPT

www.iapp.org

Connecting the industry

More than a professional association, the IAPP provides a home for privacy professionals around the world to share experiences—working to promote career readiness and improve job effectiveness.

www.iapp.org

opportunities

LEARN

NETWORK

CERTIFY

www.iapp.org

THANK YOU!