
# Webinar:
# Deep Dive into the Role of the DPO under the GDPR

Wednesday, 22 June 2016

11:00 AM US EDT

**Use the chat box to ask questions.**

Centre for Information Policy Leadership
Hunton & Williams LLP

Use the chat box to ask questions.

# Webinar Agenda

## Introduction and Overview of the Role of the DPO in the GDPR

- ***Bojana Bellamy, President, CIPL***

## Guest Presentations:

1. **DPO and Accountability *(Nathalie Laneret, Group Data Protection Officer, Capgemini)***
   - **Mandatory and voluntary DPOs: appointment and roles**
   - **Knowledge, skills and abilities of DPOs**
   - **Relationship with European data protection authorities ("EU DPAs")**

2. **DPO Tasks (*Tracy Ann Kosa, Compliance Director, Microsoft)***
   - **Main DPO tasks. Is the DPO role a compliance as well as strategic data governance role?**
   - **"Timely" and "proper" involvement and "access to resources" obligations**

3. **DPO "Independence" and "No Conflict" (*Cecilia Álvarez, European Data Protection Officer Lead, Spain Legal Director, Pfizer)***
   - **DPO independence**
   - **"No conflict" obligations**

## Q&A Discussion

***Common guest topics:***

- ***Natural/Legal persons, internal vs. external, and protected employment status of DPO***
- ***Geographic location of DPO (including Group DPO) viz main establishment/lead authority***
- ***DPO liability (e.g. criminal, administrative and corporate)***

Centre for Information Policy Leadership
Hunton & Williams LLP

Use the chat box to ask questions.

# Mandatory DPO under GDPR

**Mandatory DPO for <u>controllers and processors</u>:**

a) If the processing is carried out by a public authority or body;

b) Core activities (taking into account their scope and/or purposes) involve systematic and regular monitoring of data subjects on a large scale;

c) Core activities involve large scale processing of sensitive data and personal data relating to criminal convictions and offences; or

d) Mandated by Member States.

Use the chat box to ask questions.

# DPO Requirements (1)

- DPO can be an employee, external consultant, or "collective" DPO for an industry association
- May be a single DPO for a group of undertakings
- Name/contact details communicated to EU DPA & publicly available
- DPO selection criteria:
  - ✓ Professional qualities in particular expert knowledge of data protection law and practices and ability to fulfil DPO tasks; and
  - ✓ Necessary expert knowledge level: dependent upon processing operations and the level of protection required for the data.
- DPO independence:
  - ✓ Protected employment status;
  - ✓ No instructions from company on DPO tasks; and
  - ✓ Perform tasks in an "independent manner";
  - ✓ Qualification of the independence criteria – requirement for DPO to report to highest management

Use the chat box to ask questions.

# DPO Requirements (2)

- DPO duties of secrecy or confidentiality
- Duties of organisations towards DPOs:
  - ✓ "Timely" and "proper" DPO involvement in data protection matters;
  - ✓ Support DPO by
    a) Providing "access to resources" necessary to carry out their tasks
    b) Giving access to data and processing operations
    c) Maintaining their expert knowledge
  - ✓ No conflict of interests when DPO undertakes non-DPO tasks.

Use the chat box to ask questions.

# Tasks of DPO

- **Inform and train**: make their organisations aware of their data protection obligations and responsibilities;
- **Advise**: provide organisations advice on data protection laws and in particular advice on data protection impact assessments, risk and accountability;
- **Monitor**: monitor compliance with data protection laws and relevant company policies;
- **Co-operate and consult**: with EU DPAs on relevant data privacy matters (e.g. complaint-handling, investigation etc.)
- **Contact point for EU DPAs**: on processing issues including prior consultation; and
- **Contact point for "data subjects":** Individuals may contact DPO on all processing issues and exercise their GDPR rights.

➢ Overarching DPO obligation to consider the risks associated with the processing operations when undertaking their DPO tasks, taking into account the nature, scope, context and purposes of processing.

Centre for Information Policy Leadership
Hunton & Williams LLP

Use the chat box to ask questions.

# DPO and Accountability

***Nathalie Laneret***

*Group Data Protection Officer, Capgemini*

Centre for Information Policy Leadership
Hunton & Williams LLP

Use the chat box to ask questions.

# DPO and Accountability (1)

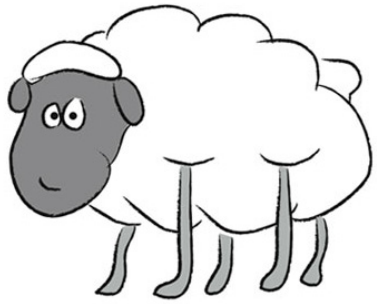
- **Mandatory and Voluntary DPO**
  - **DPO and accountability**
    - ✓ Canadian DPA Accountability Paper (2012)
      https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.pdf
    - ✓ WP 173 on the principle of accountability (2010)
      http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf
    - ✓ WP 153 on elements and principles to be found in BCR (2008)
      http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion recommendation/files/2008/wp153_en.pdf
  - **DPO and risk**
    - ✓ Article 37.1 GDPR (DPO)
    - ✓ Article 35.3 GDPR (DPAI)
  - **DPO and administrative sanctions**
    - ✓ Article 83.4 (a) GDPR
    - ✓ Article 83.2 (k) GDPR
  - **DPO and flexibility**

Centre for Information Policy Leadership
Hunton & Williams LLP

Use the chat box to ask questions.

# DPO and Accountability (2)

- **Knowledge, skills and abilities of the DPO** (Articles 37.5 and 39 GDPR)
  - DPO as legal counsel
  - DPO as compliance officer
  - DPO as IT/security specialist
  - DPO as risk manager
  - DPO as program manager
  - DPO as communication manager



- **Relationship with EU DPAs**
  - Article 39 (d) & (e) GDPR on DPO tasks
  - Article 58.1 & 2 GDPR on investigative and corrective powers of DPA

Centre for Information Policy Leadership
Hunton & Williams LLP

Use the chat box to ask questions.

# DPO Tasks

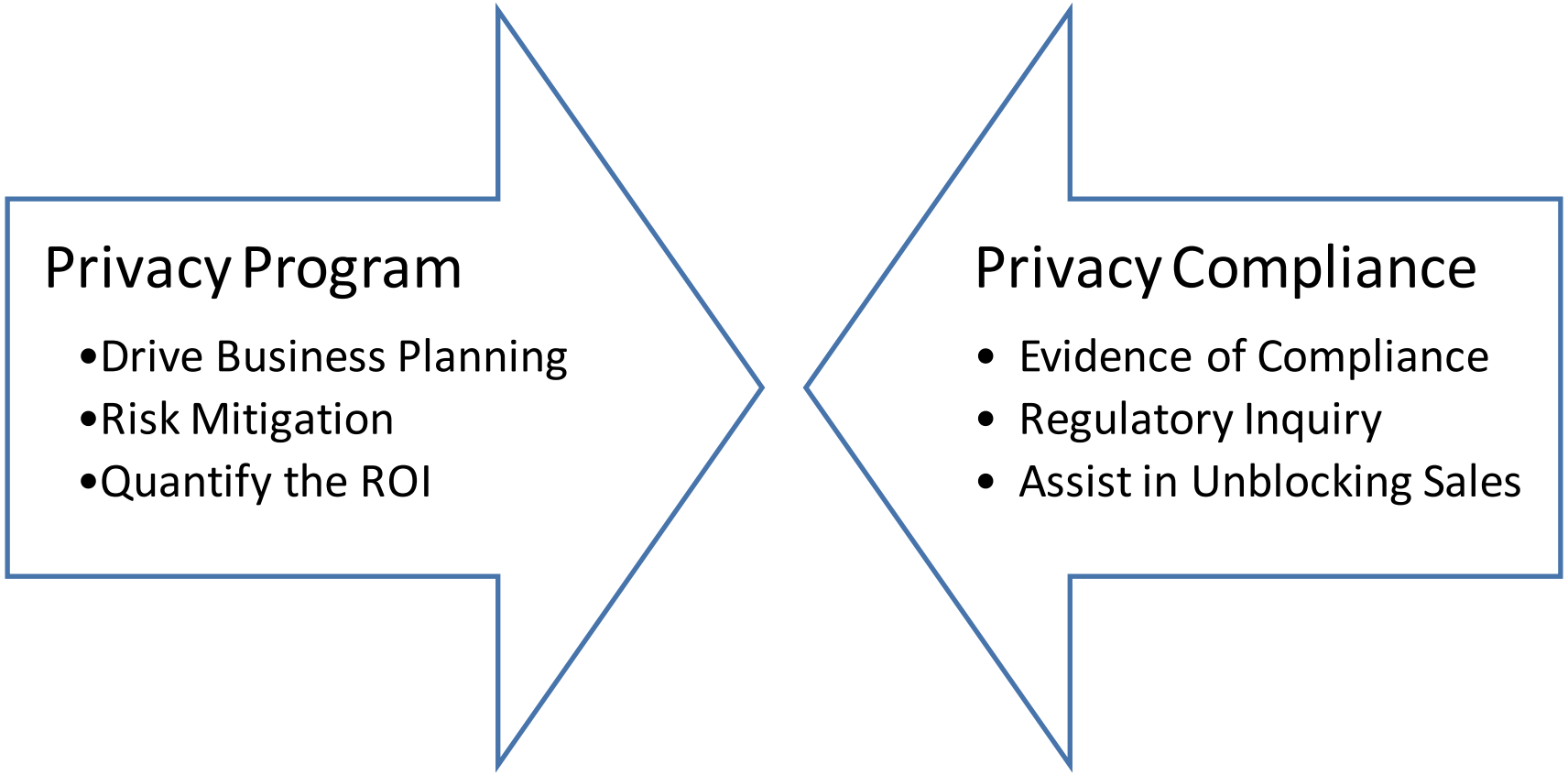
***Tracy Ann Kosa***

*Compliance Director, Microsoft*

Centre for Information Policy Leadership
Hunton & Williams LLP

Use the chat box to ask questions.

# DPO Functions



Use the chat box to ask questions.

# Program Tasks

Centre for Information Policy Leadership
Hunton & Williams LLP

Use the chat box to ask questions.

# DPO Role Details

| # | DPO Accountability | Business Activities | Testable Control for Compliance |
|---|---|---|---|
| 1 | **A company-wide privacy program** | • Business leader as privacy champion<br>• Role specific accountabilities | • Documented R&Rs<br>• Min. qualifications |
| 2 | **Documentation reflecting applicable laws and regulations** | • Feedback cycle<br>• Environmental monitoring | • Requirements database<br>• Documented change management |
| 3 | **Supplier management incorporates privacy** | • Agreements, training, audits | • Standard contract usage<br>• Access commensurate with rating |
| 4 | **Privacy reviews; impact assessments are completed** | • Documented methodology and sign off | • Evidence of completed reviews |
| 5 | **Company-wide privacy training and awareness** | • Role base training developed, updated and delivered regularly | • Training completion records<br>• Distribution of awareness materials |
| 6 | **Privacy is incorporated to incident management** | • R&R are assigned and documented; response plan is implemented, reviewed and tested | • Incident related documentation kept<br>• Notification requirements are documented |
| 7 | **A data inventory of all personal information (employee and customer)** | • Consistent data classification is applied to inventory | • Data inventory<br>• Data classification |
| 8 | **Contributing to risk management for the business as it pertains to privacy** | • Ongoing monitoring and assessment of the business privacy risk | • Baseline privacy risk categories and register |
| 9 | **Requirements are monitored for changes that affect the business** | • Business practices are updated in response to changing requirements<br>• Documentation is updated accordingly | • Current requirements log/tracker |

Centre for Information Policy Leadership
Hunton & Williams LLP

Use the chat box to ask questions.

# DPO "Independence" and "No Conflict"


***Cecilia Álvarez***

*European Data Protection Officer Lead, Spain Legal Director, Pfizer*

Centre for Information Policy Leadership
Hunton & Williams LLP

Use the chat box to ask questions.

# DPO Independence

25.11.2010: Resolution of the **German DPAs** responsible for the private sector on the minimum requirements for the (qualifications and) **independence** of company DPOs:

**Independence Required Under Section 4f(3) of the Federal Data Protection Act**

According to Section 4f(3) of the Federal Data Protection Act, DPOs must be free to the apply their data protection expertise without interference from the company. In order to ensure the DPO's independence, certain of company internal organizational measures are necessary:

- DPOs must be directly subordinate to the data controller's head of management
- DPOs must not be penalized for actions taken to carry out DPO functions, including in cases where the appointment as DPO has been withdrawn
- DPOs are bound to confidentiality about the identity of the data subjects, as well as the circumstances under which they obtained information about a data subject, unless otherwise specifically authorized by the data subject in question

17.12.2012: EPD ***Report on the Status of Data Protection Officers***

The EDPS pointed out in the DPO Role Paper that the appointment of the DPO for a fixed term contributes to ensuring the independence of the DPO. Indeed the longer the mandate, the more this contributes to providing the guarantee that DPOs can carry out their function in an independent manner.

Could we agree?

Use the chat box to ask questions.

# DPO Independence

- A **DPO IS NOT**:
  - a DPA
  - data subjects' representative
  - the CEO!

- A DPO **must** be able to combine **INTEGRITY & LOYALTY**:
  - Knowledge
  - Status
    * high reporting line
    * operational and financial autonomy
  - Protection/no penalties to carry out his/her work properly:
    * Objective reasons to withdraw his/her appointment
    * Protection against individual liability
    * Insurance coverage
    * Others?

Centre for Information Policy Leadership
Hunton & Williams LLP

Use the chat box to ask questions.

# Conflicts of Interest?

- **Internal DPOs**
  - Part-time DPO
  - Board of Directors' Member
- **External DPO**
  - Legal advisors to an organisation also operating as the organisation's DPO
  - Strategic DPO role and advice to several clients of the same sector or engaged in the same transaction

# Q&A Discussion

1. **DPO and Accountability** ***(Nathalie Laneret, Group Data Protection Officer, Capgemini – nathalie.laneret@capgemini.com)***
    - **Mandatory and voluntary DPOs: appointment and roles**
    - **Knowledge, skills and abilities of DPOs**
    - **Relationship with European data protection authorities ("EU DPAs")**

2. **DPO Tasks (*Tracy Ann Kosa, Compliance Director, Microsoft - trako@microsoft.com*)**
    - **Main DPO tasks. Is the DPO role a compliance as well as strategic data governance role?**
    - **"Timely" and "proper" involvement and "access to resources" obligations**

3. **DPO "Independence" and "No Conflict" (*Cecilia Álvarez, European Data Protection Officer Lead, Spain Legal Director, Pfizer – cecilia.alvarez@pfizer.com*)**
    - **DPO independence**
    - **"No conflict" obligations**

***Common guest topics:***
- ***Natural/Legal persons, internal vs. external, and protected employment status of DPO***
- ***Geographic location of DPO (including Group DPO) viz main establishment/lead authority***
- ***DPO liability (e.g. criminal, administrative and corporate)***