

# PRIVACY AND EU DATA PROTECTION

*Seminar V.*

## The Data Protection Officer (“DPO”)

*prof. dr. Gerrit-Jan Zwenne*



November 8<sup>th</sup>, 2021

1



2

### But first...

A newspaper offers a new special online subscription:

*a 25 percent discount will be given subscribers that consent to the provision of their reading preferences to an advertisement agency*

According to a consumer interest group, the GDPR does not allow this.

What do you think?

3

### Also...

- what are special data and why are the specific rules for such data?
- in the context of purpose specification and purpose limitation, what is the «compatibility test»...?
- what is the accountability principle? how can controllers and processors comply with that principle?

4

## what is a data protection officer or DPO..?

- someone (m/f) in the organization of a controller or processor
- who informs and advises that controller or processor on data protection compliance, and particularly on DPIA's
- **and who monitors compliance with applicable DP-law**
- and cooperates with DPA's and acts as contact-point

*not a committee or commission, but an individual*

*could be an employee, could be from an external organization*

*not part of management(!)*

*but not necessarily a whistleblower*

5

## who should appoint a data protection officer?

- public authority or body (but not courts to the extent...)
- core activities consist of processing operations that require systematic large-scale monitoring of data subjects
- core activities consist of large-scale processing of special data and criminal data

*determined under national law... universities, bar associations?*

*'primary activities, i.e. not relating ancillary activities'*

*key operations to achieve the controller's or processor's goals*

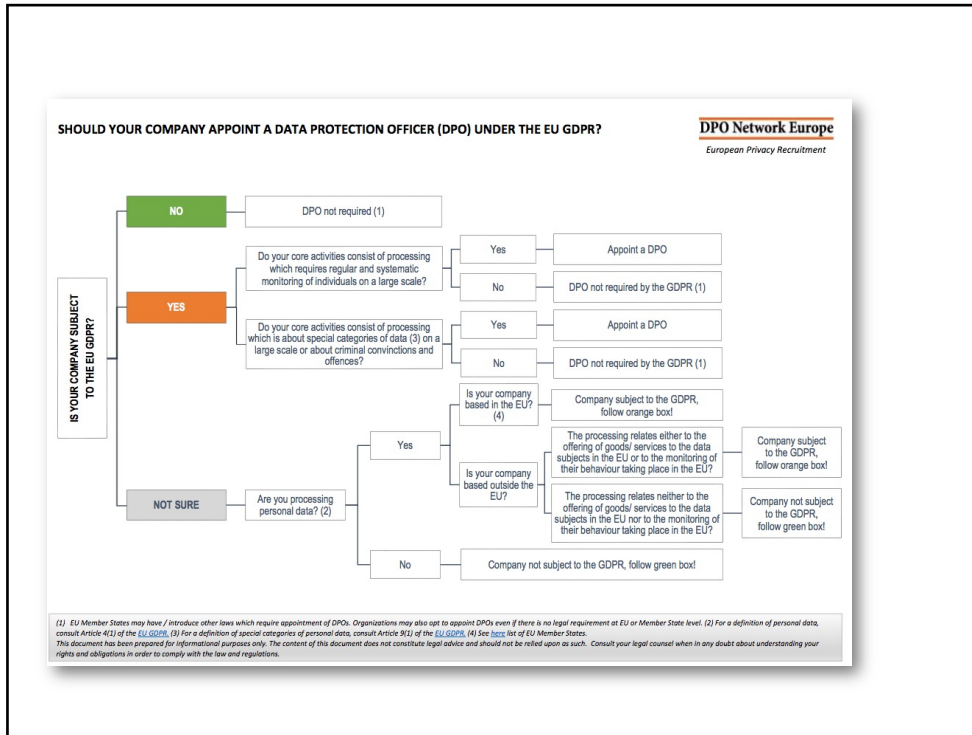
*Therefore, not salary administration, unless that is the core-activity of a processor (e.g. Workday)*

*hospitals, public transport, fastfood delivery, search engines, telco's, banks etc.*

The number of data subjects concerned - either as a specific number or as a proportion of the relevant population

- volume of data and/or the range of different data items being processed
- duration, or permanence, of the data processing activity
- geographical extent of the processing activity

6



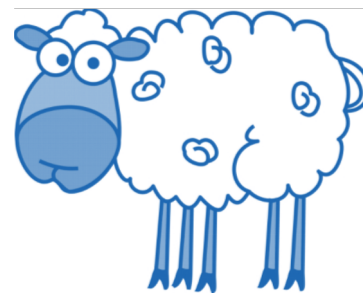
7



8

## the tasks of a data protection officer?

- informing and advising a controller or processor on data protection compliance, and particularly on DPIA's
- monitoring compliance with applicable DP-law
- and cooperation with DPA's and acting as contact-point



9

## what are the requirements for a DPO?



- expertise and professional qualities, and the ability to fulfill his or her tasks
  - on DP-law, on the organization of the controller or processor, on data flows, ICT, etc.
  - all of the above, and well-positioned in the organization of the controller or processor
- independent
  - exclude or provide for solutions in case of conflicts of interest

### QUESTIONS

- *could lawyer working in private practise be a DPO?*
- *is a controller allowed to designate the Data Governance Officer as DPO?*



10

Belgian DPA issues **€50,000 fine** for DPO's conflicting company roles LEXOLOGY

**Belgium, European Union** | May 29 2020

The Belgian Data Protection Authority (**Belgian DPA**) recently imposed a €50,000 fine on a large telecommunications operator (**the company**), for failing to comply with the GDPR in relation to the appointment of their Data Protection Officer (**DPO**). The Belgian DPA decided that the DPO's tasks and duties under the GDPR conflicted with its role as Head of Audit, Risk and Compliance.


**Background**

The company self-reported a data breach to the DPA, which led to a wider investigation into the security of its data processing operations. The investigation focused on three potential breaches of the GDPR: (1) the company's duty to cooperate with the DPA (Article 31 GDPR); (2) the company's accountability obligations (Article 5(2) GDPR); and (3) the DPO was not sufficiently involved in discussions surrounding data breaches (Article 38(1) GDPR) and was not sufficiently independent insofar as the DPO also acted as Head of Audit, Risk and Compliance (Article 38(6) GDPR). The only infringement was found to be in relation to the third issue.

**Legal Issue**

The Belgian DPA found that it is insufficient for a DPO to just be "informed" about a data breach, and that consultation with the DPO is needed as early as possible in the process. However in this case, the evidence indicated that the DPO was appropriately involved in the response to the data breach. In regard to the DPO acting as Head of Audit, Risk and Compliance, the company argued that it only had an advisory role, and did not take decisions concerning the purposes and means of data processing activities. The Belgian DPA disagreed, stating that there was no doubt that the combination of its responsibilities as Head, with its statutory tasks as DPO, led to a lack of independence. The Belgian DPA held this was because the DPO, in its role as Head, was also responsible for the processing of personal data in the context of the organisation's audit, risk and compliance activities. This approach was supported by a decision by the Bavarian data protection authority involving an IT manager

11



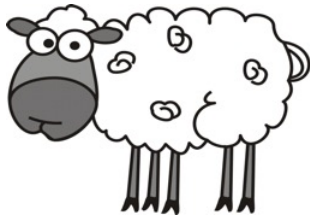
DPO must be in a position to efficiently communicate with data subjects and cooperate with the supervisory authorities

This also means that this communication must take place in the **language or languages used** by the supervisory authorities and the data subjects concerned.

**should have expertise** in national and European data protection laws and practices and an in-depth understanding of the GDPR

knowledge of the business sector and of the organisation of the controller is **useful**.

should also have **sufficient understanding** of the processing operations carried out, as well as the information systems, and data security and data protection needs of the controller.



12

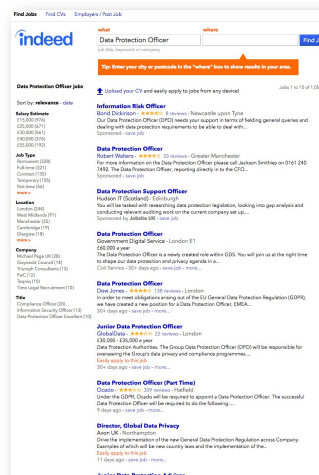


13

## why a data protection officer?

because of

- DPO-obligation (art. 37(1) GDPR)
- accountability-obligation (art. 5(2) GDPR)
- DPA's expectations
- data subjects' expectations
- customers' expectations
- suppliers' expectations
- ...



14

questions?

[g.j.zwenne@law.leidenuniv.nl](mailto:g.j.zwenne@law.leidenuniv.nl)