

INTERNET PRIVACY AND EU DATA PROTECTION

Seminar VIII.

The Data Protection Officer (“DPO”)

prof. dr. Gerrit-Jan Zwenne

November 4th, 2020



1

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?

2

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?

3

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, but could also be someone from an external organization

not part of management(!)

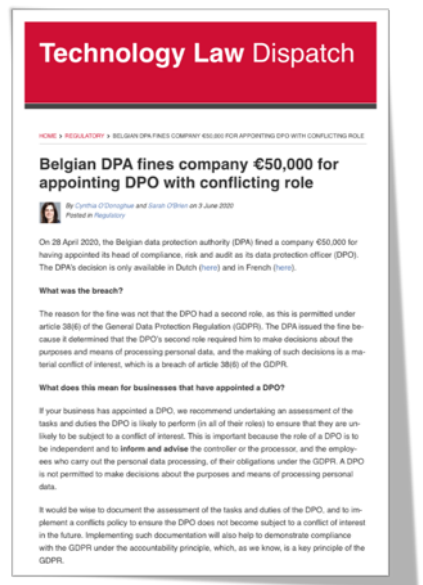
but not necessarily a whistleblower!

4

conflicts of interest?

- draft processor agreements and privacy policies?
- data breach notifications?
- ...?

- DPO may fulfil other tasks and duties
- controller or processor must ensure that any such tasks and duties do not result in a conflict of interests



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 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)

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

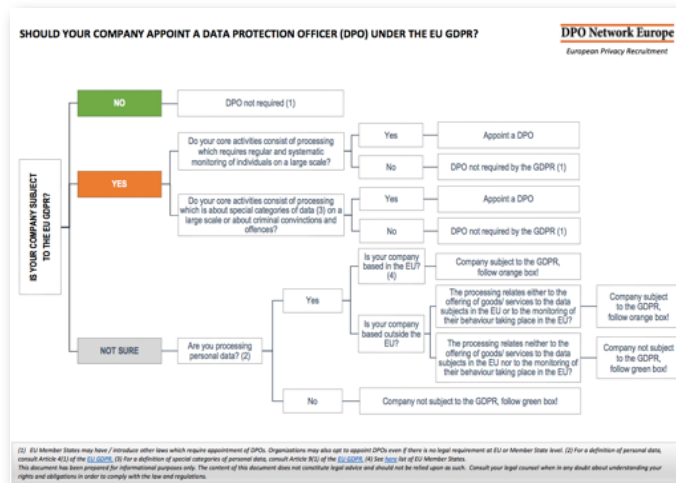
hospitals, public transport, fastfood delivery, search engines, telco's, banks etc.

6

in the context of the DPIA-
requirement of art. 35.1 GDPR

91. [...] The processing of personal data
should not be considered to be on a large
scale if the processing concerns personal data
from patients or clients by an individual
physician, other health care professional or
lawyer

7



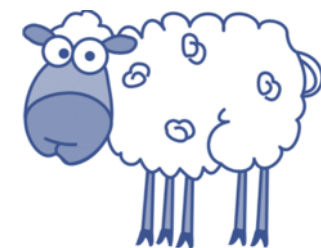
8



9

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



10

what are the requirements for a DPO?



- expertise and professional qualities, and the ability to fulfill his or her tasks
- independent

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

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?*



11



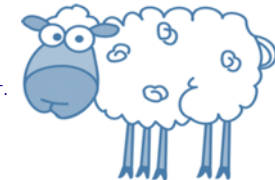
DPO must be in a position to efficiently communicate with data subjects and cooperate with the supervisory authorities

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

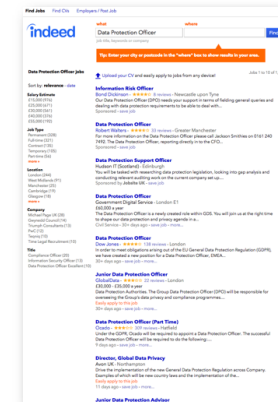


13

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

15