TaylorWessing

Data Protection Officer ("DPO") – FAQs

This document gives answers to practical questions regarding the designation and obligations of a DPO pursuant to Articles 37, 38 and 39 of the European Data Protection Regulation ("GDPR"), taking into account the guidelines of the Article 29 Data Protection Working Party and of national data protection supervisory authorities.

1 Who has to appoint a DPO under the GDPR?

All controllers and processors if their core activities include:

Processing operations which require regular and systematic monitoring of data subjects on a large scale.

Examples

- Operating/providing telecommunications networks/services
- Email retargeting
- Profiling/scoring for purposes of risk assessment
- Location tracking
- Loyalty programs
- Behavioural advertising
- Monitoring of data via wearable devices
- Closed circuit television
- Connected devices

Processing of special categories of data or personal data relating to criminal convictions and offences.

Examples

- Data related to:
  - Racial or ethnic origin
  - Political opinions
  - Religious or philosophical beliefs
  - Trade union membership
- Genetic data
- Biometric data
- Health data
- Data concerning sex life or sexual orientation

Please note: Even if a DPO is not necessary according to the aforementioned requirements, it can be useful to designate one on a voluntary basis..

2 Can EU member states adopt national rules for the designation of a DPO?

Yes, according to Art. 37 (4) GDPR. The national specific requirements may even be more restrictive as under the GDPR. In Germany, a DPO needs to be designated under the new Federal Data Protection Act ("BDSG") if

- At least 20 persons are constantly dealing with automated processing; or
- Processing is subject to a Data Protection Impact Assessment (Art. 35 GDPR); or
- Personal data is commercially processed for the purpose of (anonymized) data transfer or for the purpose of market or opinion research.

3 What are the core tasks of a DPO?

- Inform and advise company and its employees in regard to GDPR and EU Member State law and monitor compliance (including assignment of responsibilities, awareness raising, training of staff involved in processing operations, and the related audits)
- Provide advice for data protection impact assessments under the GDPR where requested by company and monitor its performance
- Act as contact point for and cooperate with the supervisory authority on issues relating to data processing
- Act as contact point for data subjects for all issues related to processing of their personal data and to the exercise of their rights under the GDPR
- Direct reporting to the highest management level of the involved company entities

4 What are the obligations of the company when designating a DPO?

The company must ensure that:

- DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data (e.g. regular invitations to meetings of senor and middle management)
- DPO's opinion is given due weight and in case of disagreement reasons for not following DPO's advice are documented
- DPO is promptly consulted once a data breach or similar incident has occurred
- Contact details of DPO are published (internally and externally) and communicated to supervisory authority
- DPO gets support to carry out his/her tasks by providing resources necessary, including i.a.
  - Financial resources, infrastructure and if necessary staff
  - Access to personal data and processing operations
  - Continuous training to maintain his/her qualifications

- DPO acts in an independent manner
  (i.e. DPO does not receive any instructions regarding the exercise of his/her tasks)
- DPO is not dismissed or penalized for performing his/her tasks
  (i.e. no"punishment" for taking a privacy-friendly approach)
- Other duties of DPO do not result in a conflict of interests (conflicting management positions may include Head of Marketing Department/HR/IT/Compliance)
- DPO is bound by secrecy or confidentiality in accordance with EU and Member State law

5 What qualifications are required to be designated as (external) DPO?

The DPO shall be designated based on professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks mentioned above. The necessary qualifications include

- Expertise in European and national data protection laws and practice
- Knowledge of the company's business sector and organization, its processing operations, information technologies and data security
- Ability to promote data protection culture within the company

The DPO can be designated externally based on a service contract.

6 Can a single DPO be appointed for all entities of a company group?

Yes, if the following requirements are fulfilled:

- DPO is easily accessible from each establishment (in order to act as internal and external contact point for group entities as well as for authorities and data subjects)
- DPO can communicate in the language used by supervisory authorities and data subjects concerned

7 Does a DPO have to be designated even if a GDPR EU Representative has already been appointed?

Yes. The supervisory authorities recommend that the representative and the DPO should not be the same person in order to avoid conflicts.

8 What is the risk of non-compliance for the processor / controller?

A violation of the obligation to designate a DPO under the GDPR or national legislation could be charged with a fine up to EUR 10.000.000,- or up to 2% of the undertaking's total worldwide annual turnover of the preceding financial year, whichever is higher.

9 Questions for self-assessment: Does our company need to designate a DPO?

If you can answer most of the following questions with "yes", it is very likely that a DPO needs to be designated for your company.

	Question	Yes	No
	Obligation to designate a DPO	☐	☐
1	Is your company processing personal data as part of the main business activity or in connection with the company's main activity (e.g. not only in an auxiliary function such as providing a standard IT environment or paying employees)?	☐	☐
2	Is your company processing personal data of a large number of data subjects?	☐	☐
3	Is your company processing personal data of a large number of data sets of data subjects?	☐	☐
4	Is your company processing personal data for a long period of time?	☐	☐
5	Is your company processing personal data from data subjects of a large number of countries?	☐	☐
6	Is the processing activity of your company related to the tracking of data subjects, profiling of data subjects or other means of constant, recurring or otherwise regular systematic monitoring?	☐	☐
7	Is your company processing any special categories of data pursuant to Art. 9 GDPR (e.g. health data, data related to ethnic origin, political opinions, religious or philosophical beliefs, genetic or biometric data etc.)?	☐	☐
8	Is your company processing personal data related to criminal convictions and offences?	☐	☐

Your Contacts

Dr. Paul Voigt,
Lic. en Derecho, CIPP/E
Tel +49 (0)30 88 56 36 408
p.voigt@taylorwessing.com

Dr. Axel Frhr. von dem Bussche, LL.M. (L.S.E.)
Tel +49 (0)40 3 68 03 347
a.bussche@taylorwessing.com

Dr. Carolin Monsees
Tel +49 (0)40 3 68 03 347
c.monsees@taylorwessing.com