ONTIER

16th May 2017
#11

Index

DATA PROTECTION OFFICER

Under the GDPR, certain Data Controllers and Data Processors will be required to appoint a Data Protection Officer ("DPO") in order to facilitate internal compliance with the provisions of the regulation. A DPO is a person (either an employee or an external consultant), responsible for, in an independent manner, monitoring compliance with the GDPR, providing information and advice to the organisation on privacy and data protection matters and liaising with the respective supervisory authority.

Current situation

Directive 95/46/EC does not currently require organisations to appoint a DPO. Notwithstanding this, many organisations have developed the practice of appointing someone responsible for privacy and data protection matters.

In some member states (in particular Germany), the decision to appoint a DPO may have some practical advantages, namely the exemption to file a registration regarding a data processing before the relevant supervisory authority.

What's new?

The obligation to appoint a DPO does not apply to every organisation. Under Article 37(1) of the GDPR, the regulation only requires the appointment of a DPO in three specific cases:

a) where the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

b) where 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) where the core activities of the Data Controller or the Data Processor consist of processing on a large scale of special categories of data (being personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation) and personal data relating to criminal convictions and offences.

Recital 97 of the GDPR specifies that the **core activities** of a Data Controller 'relate to primary activities and do not relate to the processing of personal data as ancillary activities'. Under the Article 29 Working Party ("WP29")'s Guidelines on Data Protection Officers, core activities should be considered as the key operations necessary to achieve the Data Controller's or Data Processor's goals, and also include "activities where the processing of data forms as inextricable part of the Data Controller's or Data Processor's activities."

The concept of **large scale processing** is not defined under the GDPR. However, the WP29, in its Guidelines on Data Protection Officers, recommend that the following factors should be considered to determine whether or not a processing is carried out on a large scale:

• The number of data subjects concerned - either as a specific number or as a proportion of the relevant population;
• The volume of data and/or the range of different data items being processed;
• The duration, or permanence, of the data processing activity; and
• The geographical extent of the processing activity.

A group of undertakings can appoint a single DPO provided that he or she is “easily accessible from each establishment”. This means the DPO must be easily contactable not only within the organisation but also by data subjects and by the supervisory authority.

The DPO should be appointed on the basis of their professional qualities, namely he or she must have expertise in data protection laws, a solid understanding of the GDPR and the ability to fulfil the tasks referred to in the GDPR, which are, at least, the following:

a) to inform and advise the Data Controller or the Data Processor and the employees who carry out processing of their obligations pursuant to the GDPR and to other EU or member state data protection laws;

b) to monitor compliance with the GDPR, with other EU or member state data protection laws and with the policies of the Data Controller or Data Processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

c) to provide advice where requested as regards the data protection impact assessment and monitor its performance;

d) to cooperate with the supervisory authority; and

e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation with the supervisory authority (if required), and to consult, where appropriate, with regard to any other matter.

The DPO should be involved in all issues relating to the protection of personal data and the organisation should provide the necessary resources that allows the carrying out of their duties and to access to information and data processing operations.

The exercise of the above tasks are to be performed in an independent manner so the DPO should not take any instructions from the Data Controller or the Data Processor on how to deal with a specific matter. An important cornerstone of this principle is the prohibition of the Data Controller or the Data Processor to dismiss or penalise the DPO for performing their tasks.

The DPO is also bound by secrecy and confidentiality concerning the performance of his or her tasks in accordance with EU or member state law but will not be prohibited from contacting or seeking advice from the supervisory authority and may consult the supervisory authority on any other matter, where appropriate.

What to do to adapt?

If an organisation is:

a) a public authority or a body; or

b) its core activities consist of either regular and systematic monitoring of data subjects on a large scale; or

c) processing sensitive personal data special categories of personal data on a large scale,

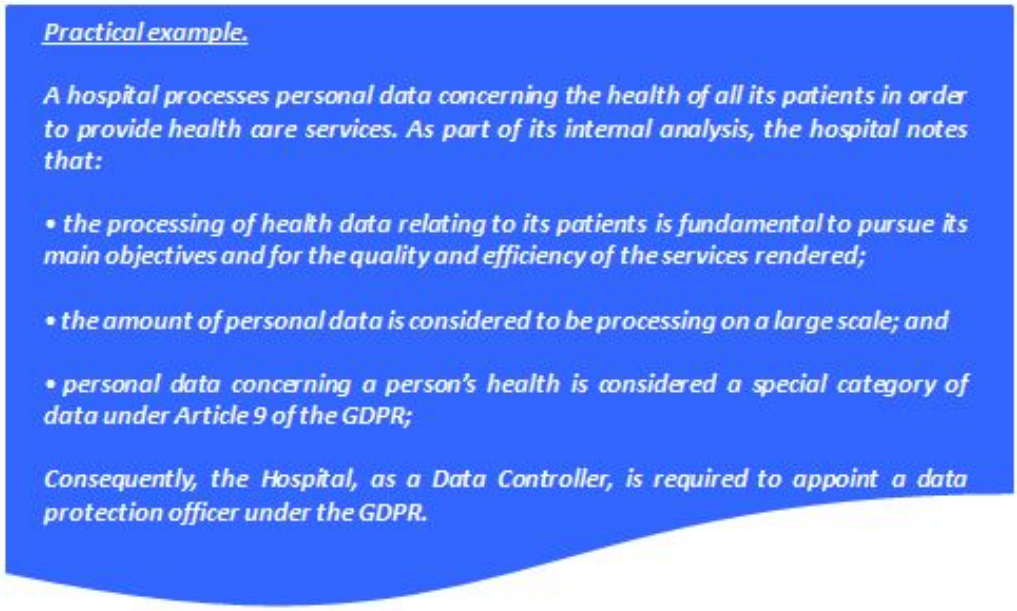
then, according to the GDPR, it will be mandatory to appoint a DPO.

The WP29 in their Guidelines on Data Protection Officers recommends that, unless it is obvious that an organisation is not required to appoint a DPO, Data Controllers and Data Processors should document their internal analysis to determine whether or not a DPO is to be appointed. This will demonstrate that the relevant factors have been properly taken into account.

Additionally, Data Controllers and Data Processors are also obliged to appoint a DPO whenever it is required by either EU or member state law.

Even when it is not required by the GDPR, Data Controllers and Data Processors may appoint a DPO on a voluntary basis. The WP29 considers that the requirements under the GDPR shall apply to the appointment of a DPO on a voluntary basis, as if the appointment had been mandatory.

To appoint a DPO may be considered good practice, in any case.



Practical example.

A hospital processes personal data concerning the health of all its patients in order to provide health care services. As part of its internal analysis, the hospital notes that:

• the processing of health data relating to its patients is fundamental to pursue its main objectives and for the quality and efficiency of the services rendered
• the amount of personal data is considered to be processing on a large scale; and
• personal data concerning a person's health is considered a special category of data under Article 9 of the GDPR.

Consequently, the Hospital, as a Data Controller, is required to appoint a data protection officer under the GDPR.

TEAM

Joaquin Muñoz Rodríguez (Spain)
Pablo Uslé Presmanes (Spain)

Derek Stinson (UK)
Paula Enríquez (UK)

Ana Rocha (Portugal)
Joana Cunha de Miranda (Portugal)

Luca Pardo (Italy)
Giulio Ciompi (Italy)

Read more:

about us

Share on:

Linkedin Twitter

Subscribe:

our Newsletters

Contact us:

Website | LinkedIn

Rua Vitor Cordon Nº 10A - 1249 - 202 Lisboa | Portugal
Tel. (+351) 213 223 590 / Fax (+351) 213 223 599

Rua Pedro Homem de Melo, n.º 55, 8º piso - 4150 - 599 Porto | Portugal
Tel. (+351) 223 190 888 / Fax (+351) 220 924 945

PORTUGAL / **SPAIN** / **U.K** / BOLIVIA / / BRAZIL / CHILE / CHINA / COLOMBIA

USA / **ITALY** / MEXICO / PERU / VENEZUELA
