BHBIA Ethics & Compliance

Data Protection Requirements

Data Protection Officer

Introduction

This guidance sets out to explain both what you need to know, and what you need to do, to determine whether your organisation needs a Data Protection Officer (DPO).

The BHBIA's Ethics & Compliance Committee is providing this guidance as general information for its members. It is not legal advice and should not be relied upon as such. Specific legal advice should be taken in relation to any specific legal problems or matters. Whilst every reasonable effort is made to ensure the information is accurate, no responsibility for its accuracy or for any consequences of relying on it is assumed by the BHBIA.

What you need to know

When a Data Protection Officer needs to be appointed

Under the General Data Protection Regulation (GDPR) and the UK Data Protection Act (DPA) 2018, data controllers and data processors **must appoint a DPO if - as a core activity - you carry out large scale systematic monitoring of individuals or large scale processing of special categories of data**. Special categories of data is what was previously referred to as 'sensitive' data and includes health data.

How to interpret this requirement

It is important to decide whether your organisation - as a core activity - is involved in either:

- large scale regular and systematic monitoring of individuals OR
- large scale processing of special categories of data

Core activities are the key operations necessary to achieve the controller's or processor's goals.

'Regular' monitoring, 'systematic' monitoring and 'large' scale processing are not defined within the GDPR/DPA 2018.

Regular is however interpreted by the Article 29 Working Party (WP29) now the European Data Protection Board (EDPB) as:

- Ongoing or occurring at particular intervals for a particular period
- Recurring or repeated at fixed times
- Constantly or periodically taking place

Systematic is interpreted by the WP29 (now the EDPB) as:

- Occurring according to a system and/or
- Pre-arranged, organised or methodical and/or
- Taking place as part of a general plan for data collection and/or
- Carried out as part of a strategy

Systematic work would include online tracking and profiling such as using cookies for behavioural marketing purposes (but systematic is not limited to online work). Other examples quoted include:

- Loyalty card schemes
- Tracking of health or fitness through wearable devices
- Behavioural advertising

Large scale processing - the WP29 (now the EDPB) recommends that the following factors are considered when deciding whether the processing is carried out on a large scale:

- Number of data subjects (as a specific number or a proportion of the population)
- Volume of data and/or the range of different data items being processed
- Duration, or permanence, of the processing
- Geographical extent

If a supplier or data processor does not process large volumes of personal data for one client company but has many such clients then this would constitute large scale processing.

Examples of large-scale processing quoted include processing of:

- Patient data in the regular course of business by a hospital
- Personal data for behavioural advertising by a search engine
- Data (content, traffic, location) by telephone or internet service providers

Examples that do not constitute large-scale processing include processing of:

- Patient data by an individual physician
- Personal data relating to criminal convictions and offences by an individual lawyer

The UK Market Research Society has stated that:

> **"*In a research context panel providers, opinion pollsters or audience measurement researchers will almost certainly need to appoint* [a DPO] *in light of the type and scale of their data. On the other hand, freelance independent qualitative researchers are unlikely to need to, as the volume of data and number of subjects whose data they process is likely to be relatively small*."**

If you have more than one office

It is possible to appoint a single DPO for a group of undertakings (i.e. a controlling undertaking e.g. the head office and its controlled undertakings e.g. subsidiary companies), as long as the:

- DPO is easily accessible from all the different locations
- DPO's contact details are published and have been communicated to the supervisory authority.

The DPO does not have to be based at the 'main establishment' i.e. the place within the EU where the main data processing decisions are made, although in many cases they will be.

If you are based outside the European Union (EU)

Remember the GDPR applies to organisations based outside the EU (this is referred to as the 'extra territorial effect'). If your processing of personal data relates either to offering of goods and services to individuals in the EU or to monitoring of behaviour taking place in the EU, you may be required to appoint a DPO (depending on the criteria described earlier).

Much of the following information has been copied from the UK Information Commissioner's Office (ICO) *Overview of the General Data Protection Regulation (GDPR)* with only minor edits to remove information that is irrelevant to healthcare market research and data analysis – https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/accountability-and-governance/

What the tasks of the DPO are

The DPO's minimum tasks are to:

- Inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor compliance with the GDPR and other data protection laws – collect information to identify processing activities, analyse and check the compliance of processing activities and provide information, advice and recommendations to the organisation
- Advise on data protection impact assessments
- Train staff and conduct internal audits
- Be the first point of contact for supervisory authorities and individuals whose data is processed and able to communicate effectively with them
- Any prioritisation of activities should reflect the data protection risks inherent in them.
- DPOs are NOT personally responsible in cases of GDPR/DPA 2018 non-compliance, the controller or processor is.

What data protection law says about employer duties

You must make sure that:

- The DPO reports to the highest management level of your organisation i.e. board level.
- The DPO operates independently and is not dismissed or penalised for performing their task.
- Adequate resources are provided to enable DPOs to meet their GDPR/DPA 2018 obligations. There is further detail on the necessary resources within section 3.2 of the Guidelines on Data Protection Officers ('DPOs'), Article 29 Data Protection Working Party, Adopted 13 Dec 2016.

Allocating the role of DPO to an existing employee

Yes. As long as the duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests. For example, if the DPO holds a position that allows them to determine the purposes and means of processing personal data this will be a conflict of interests, so a hands-on project director could not be a DPO.

You can also contract out the role of DPO externally.

You may appoint a single data protection officer to act for a group of companies, taking into account their structure and size. ESOMAR provides a DPO service for members through ESOMAR Plus. This service will be based on a partnership between ESOMAR and a network of specialist data protection lawyers. It will be a modular service that can be tailored to the company's structure and resources. To find out more go to https://www.esomar.org/utilities/esomar-plus

DPO qualifications

The GDPR/DPA 2018 does not specify the precise credentials a DPO is expected to have. It does require that they should have professional experience and 'expert' knowledge of data protection law. This should be proportionate to the type of processing your organisation carries out, taking into consideration the level of protection the personal data requires.

The UK Market Research Society (MRS) has said that "*an individual with experience within the research sector is important for research organisations*".

What you need to do

The following information has been largely sourced from the *Do you need to appoint a data protection officer*, GRBN News, April 24, 2017

http://grbnnews.com/do-you-need-to-appoint-a-data-protection-officer/

You must:

Decide whether to appoint:

- Decide if you need to appoint a trained DPO and document analysis,
- If you decide to appoint someone on a voluntary basis (if for example you are uncertain or believe even if there is no mandatory requirement it would benefit your organisation) then decide whether you want to call them a DPO or not. If you give them the title voluntarily you must comply with all the other DPO requirements
- If you decide not to appoint a DPO then document your internal analysis as evidence for the regulator showing that you have taken all relevant factors taken into account. Failure to appoint a DPO where required can lead to significant fines.

Pre appointment:

- Determine whether to appoint as an employee or outsource
- Analyse the required skills and expertise and start recruiting
- If using an external DPO then draft an appropriate contract
- Allow the DPO to work autonomously, report to the highest management level and provide adequate resources
- Identify any potential conflicts of interest

Post appointment:

- Publish contact details of the DPO (although not necessarily the name) and provide contact details of the DPO to the Data Protection Authority

Additional Sources:

Guidelines on Data Protection Officers ('DPOs'), Article 29 Data Protection Working Party, 13 Dec 2016
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

The UK Data Protection Act 2018 http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf

GDPR In brief (No. 4) Data Protection Officer, MRS, April 2017
http://www.mrs.org.uk/pdf/MRS%20GDPR%20In%20Brief%204.pdf

Updated by the BHBIA's Ethics & Compliance Committee August 2020

British Healthcare Business Intelligence Association
Ground Floor, 4 Victoria Square, St. Albans, Herts AL1 3TF
t: 01727 896085 • admin@bhbia.org.uk • www.bhbia.org.uk

A Private Limited Company Registered in England and Wales