Information Governance Alliance

# THE GENERAL DATA PROTECTION REGULATION: GUIDANCE ON THE ROLE OF THE DATA PROTECTION OFFICER

Information Governance Alliance IGA

# Contents

# 1 Introduction

The EU General Data Protection Regulation (GDPR) was approved in 2016 and will become directly applicable as law in the UK from 25th May 2018. The current Data Protection Bill, which will become the Data Protection Act 2018 (DPA18), fills in the gaps in the GDPR, addressing areas in which flexibility and derogations are permitted.

The GDPR will not be directly applicable in the UK post Brexit but the DPA18 will ensure continuity by putting in place the same data protection regime in UK law pre- and post-Brexit, equivalent to that introduced by the GDPR which will continue to be applicable throughout the EU member states.

The Bill does not replicate all the provisions of the GDPR but cross-refers to the relevant provisions as appropriate. When the GDPR and DPA18 come into force, it will therefore be necessary to view the DPA18 and the GDPR side by side in order to see the complete picture of all the data protection legislation. This guidance note only refers to the relevant provisions of the GDPR and will therefore need to be updated to refer to the relevant provisions of all the data protection legislation, once the DPA18 comes into force. The guidance will also be kept up to date in light of any relevant guidance issued from Government and the ICO.

The GDPR requires that public authorities appoint a Data Protection Officer. This role is key to ensuring that organisations comply and can demonstrate that they comply with the Regulation.

### In this guidance

The word **must** is used in this document to indicate a legal requirement.

The word **should** is used to indicate that, in particular circumstances, there may exist valid reasons not to follow the guidance, but the full implications must be understood and carefully considered before choosing a different course.

The word **may** is used to indicate a discretionary activity for data controllers. This includes decisions where a permissive legal power is available. Under UK law, data controllers which are public authorities are additionally required to act in accordance with public law principles and to exercise their discretion reasonably and fairly, subject to judicial review, so again such organisations will need to understand the full implications and be able to justify their actions and decisions.

## 2 Key messages

1) Health and social care organisations that are public authorities must appoint a Data Protection Officer (DPO)

2) Public authorities include:
   a) General Practices and other providers of NHS funded primary care services
   b) NHS Trusts and Foundation Trusts
   c) health commissioners
   d) local authorities
   e) arm's length bodies

3) Other controllers or processors must also appoint a DPO where they EITHER:
   a) process special categories data on a large-scale OR
   b) perform regular and systematic monitoring of data subjects on a large-scale.

4) This is an essential role in facilitating 'accountability' and the organisations ability to demonstrate compliance with the GDPR

5) Organisations are responsible for making sure that the DPO is provided with adequate resources

6) Organisations must have procedures in place to make sure that the DPO is consulted on all data protection matters at an early stage (as part of privacy by design and default)

7) Organisations must ensure that the DPO role is independent, free from conflict of interest and reports directly to the highest management level of the organisation – there are specific roles that the DPO cannot perform in conjunction with this new role (see the EU guidelines mentioned at 4.1)

8) The DPO must have expert knowledge of data protection law and practices and the ability to acquire detailed understanding of the organisation's business, the purposes for which it processes, or intends to process personal data

9) A DPO may be directly employed by an organisation, or appointed as an external consultant

10) A single DPO may be appointed by a group of organisations provided all of the criteria for the role are met and provided the DPO is easily accessible from each organisation. A DPO team with a nominated contact for each organisation is acceptable. In cases of several public authorities, a single DPO may also be designated, taking into account their organisational structure and size.

# 3 The requirement to appoint a Data Protection Officer

## 3.1 Public authorities

The GDPR requires that public authorities appoint a DPO. The GDPR does not define a public authority and this is left to national legislation. The Data Protection Bill defines organisations that are public authorities under the Freedom of Information Act 2000 (FOIA) as public authorities for the purposes of the GDPR and DPA18. These will include, for example:

- NHS funded health provider organisations
  - NHS Trusts
  - NHS Foundation Trusts
  - GP Practices
  - Dentists
  - Opticians
  - Community pharmacies
- Commissioners
  - Clinical Commissioning Groups
  - NHS England
- Arm's length bodies
  - National Institute for Health and Care Excellence
  - Care Quality Commission
  - NHS Improvement
  - Public Health England
  - NHS Digital
- Local Authorities
- NHS Shared Business Services
- Universities
- Department of Health, including its executive agencies (i.e. Medicines & Healthcare products Regulatory Agency (MHRA) and Public Health England (PHE)

## 3.2 Systematic monitoring and special categories

Commercial organisations that provide data processing services to health and social care organisations are not public authorities under the FOIA. However, they also must appoint a DPO where the core activities of the controller or processor:

**37(1)(b) '…require regular and systematic monitoring of data subjects on a large scale…', or**

**37(1)(c) '…consist of processing on a large scale of special categories of data…'**

Commissioning support and e.g. risk stratification activities are likely to fall into one or both of these categories, so the organisation that provides these services (if they are not already required to do so) must appoint a DPO. Health and social care organisations should make sure that contracts with data processors include provision for DPOs.

Where the core activities of health or social care providers that are not public authorities falls in to one of the two categories above, they must appoint a DPO.

# 4 The role of the Data Protection Officer

## 4.1 The organisation's responsibilities – the position of the DPO

The DPO is an essential role in facilitating 'accountability' and the organisations ability to demonstrate compliance with the GDPR. The organisation must appoint a DPO whose job description is compliant with GDPR requirements (see section 6) and in particular must ensure:

- that the DPO role directly reports to the highest management level of the organisation – **this does not necessarily imply line management at this level, but direct and unimpeded access to the senior management team**
- that the DPO role is provided with adequate resources: financial and human resources, and is supported in maintaining his or her expertise
- that the DPO has proven 'expert knowledge of data protection law and practices', the ability to perform the tasks specified in the GDPR, and sufficient understanding of the organisation's business and processing
- that information governance and related policies address
  - organisational accountability
  - DPO reporting arrangements
  - timely involvement of the DPO in all data protection issues
  - compliance assurance: privacy by design and default
  - advising on where data protection impact assessment is required
  - the DPO's role in incident management.
- that the DPO does not receive any instruction regarding the exercise of his or her tasks, and is protected from disciplinary action, dismissal or other penalties
- that where the DPO performs another role or roles, that there is no conflict of interest
- that the contact details of the DPO are published in the organisation's transparency information for subjects and are communicated to the ICO.

It is important to consider EU Guidelines that:

**'[t]he DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case'**

and further:

**'As a rule of thumb, conflicting positions may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing'**

So positions that involve the authorising or commissioning of IT or manual records management systems are likely to meet the criteria for determining the purposes and the means of processing.

DPOs may be shared by multiple organisations that are 'public authorities' taking into account organisational structure and size, and may be either a member of staff or may fulfil the tasks on the basis of a service contract, provided there is no conflict of interest. A DPO team with a nominated contact for each organisation is an acceptable approach.

## 4.2 The qualities and tasks of the DPO

The DPO shall be designated on the basis of professional qualities and, in particular:

- expertise in national and European data protection laws and practices and an in depth understanding of the GDPR
- sufficient understanding of the processing operations carried out, as well as the information systems and data security and data protection needs of the organisation
- demonstrable ability to fulfil his or her tasks.

The principal tasks of the DPO from the GDPR are:

- to provide advice to the organisation and its employees on compliance obligations
- to advise on when data protection impact assessments are required and to monitor their performance
- to monitor compliance with the GDPR and organisational policies, including staff awareness and provisions for training
- to co-operate with, and be the first point of contact for the Information Commissioner
- to be the first point of contact within the organisation(s) for all data protection matters
- To be available to be contacted directly by data subjects – the contact details of the data protection officer will be published in the organisation's privacy notice
- to take into account information risk when performing the above.

# 5 Data Protection Officer – core job description

The table below highlights key components of the role of the data protection officer mapped to the relevant Articles of the GDPR. Whilst this is not in itself a job description, it is intended to assist organisations in developing job descriptions by including all the essential components.

| POSITION IN THE ORGANISATION | ARTICLE |
|---|---|
| The data protection officer reports to [line manager], who will oversee the strategic direction and context of the work of the role. | Not applicable – reporting to the highest management level does not necessarily mean Board or executive team membership |
| The data protection officer reports directly to the [Board / CEO / Chair / nominated accountable officer in each organisation supported] in matters relating to data protection assurance and compliance, without prior oversight of [line manager]. | Art. 38(3) – independence and reporting to highest management level |
| In performing his or her tasks the data protection officer must not receive specific direction from [line manager]. | |
| The data protection officer acts under contract to the [organisation or group of organisations – if applicable]. | Art. 37(6) – staff member or contractor |
| **RESPONSIBILITIES** | **ARTICLE** |
| • To provide support, advice and assurance of compliance across [organisation or group of organisations]. | Art. 37(1), (3) – scope of responsibilities |
| • To maintain expert knowledge of data protection law and practices and how they apply to the business of the organisation(s). | Art. 37(5) – professional qualities and expert knowledge<br>Art. 38(2) – organisation's responsibility to ensure DPO maintains his or her expert knowledge |
| • To be the first point of contact within the organisation(s) for all data protection matters. | Art. 38(1) involved properly and in a timely manner in all issues relating to data protection |

| RESPONSIBILITIES | ARTICLE |
|---|---|
| To support programmes of work from inception to ensure that data protection is addressed by default and in the design of new systems and information processes. | Art. 25 – Data protection by design and default |
| • To manage [the data protection team – as applicable depending on the size of the organisation]. | Art. 38(2) – resources and training |
| • To ensure that the team are deployed appropriately and that they are appropriately trained and maintain their expertise. | |
| • To be available to be contacted directly by data subjects – the contact details of the data protection officer will be published in the organisation's privacy notice. | Art. 38(4) contact for data subjects<br>Arts. 13(1)(b), 14(1)(b) – contact details for DPO in fair processing information |
| • The data protection officer will ensure that appropriate confidentiality is maintained in the performance of his or her tasks. | 38(5) confidentiality regarding performance of tasks |
| • In performing his or her tasks as [other role] the data protection officer must ensure that DPO responsibilities are not influenced in any way, and should a potential conflict of interest arise report this to [line manager / highest management level] | 38(6) conflict of interest |
| • To develop or advise senior management on the development and establishment of policies, procedures and other measures to ensure compliance with the GDPR, including but not limited to:<br>– records of processing activities<br>– data protection by design and default<br>– data protection impact assessment<br>– fair processing | 39(1)(a) inform and advise organisation and staff of responsibilities |
| • To monitor compliance with these measures and provide reports to the [highest management level] | 39(1)(b) monitor compliance<br>Art. 38(3) – independence and reporting<br>Art. 39(1)(c) |

| RESPONSIBILITIES | ARTICLE |
|---|---|
| • To support programmes and initiatives that involve the development of new or innovative information processes on the need for data protection impact assessment | |
| • To support and advise programmes and initiatives in conducting data protection impact assessments, and to assure the proposed mitigations | Art. 35 – Data protection impact assessment<br>Art. 36 – Prior consultation |
| • To consult with the Information Commissioner's Office (ICO) where proposed processing poses a high risk in the absence of proposed mitigations | Art. 38(2) – resources and training |
| • To ensure that [the data protection team] operates effectively in supporting these function | Art. 39(2) due regard for risk |
| • To take account of the risks associated with processing in the performance of his or her tasks | |
| • Provision of specialist advice to the organisation on compliance obligations | Art. 39(1)(c) – provide advice where requested regarding DPIA, and monitor performance |
| • Provision of advice to projects and business change initiatives on when data protection impact assessment is required | Art. 35 – Data protection impact assessment |
| • Development of materials to support staff in conducting data protection impact assessment, and implementing | |
| • To be the first point of contact for the ICO. | Art. 39(1)(e) contact point for the supervisory authority |
| • To cooperate with the ICO in any matters relating to data protection compliance including provision of evidence of compliance, and in relation to breach management. | Art. 39(1)(d) cooperate with the supervisory authority |

| KEY RESULT AREAS | ARTICLE |
|---|---|
| At a high level, the key result area is to ensure that the organisation can demonstrate compliance with all the requirements of the GDPR. Key components of this include, but are not limited to | Art. 5(2) – principle of 'accountability'<br>Art. 24(1) – technical and organisational measures to ensure and to be able demonstrate compliance |
| • Policies and procedures that comprehensively address the requirements of the GDPR, and that are available and current | |
| • Information provided to patients or service users are fit for purpose, up to date, and signpost to procedures that address subjects' rights under the GDPR | |
| • A database that holds and can provide on request details of all processing activities with the data required by the GDPR | |
| • Evidence that privacy by default and design principles are incorporated in all processing | |
| • Evidence that data protection impact assessments are conducted in appropriate circumstances, and that their conclusions mitigate risk and are assured | |
| • Routine documented reports to the [highest management level] on the organisation's state of compliance. | |

## Sources and further reading

CEO Briefing Note – Changes to Data Protection legislation: why this matters TO YOU (Information Governance Alliance, June 2017)
https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance

Overview of the General Data Protection Regulation (GDPR) (V1.5.0, Information Commissioner's Office, 03 February 2017)
https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

Preparing for the General Data Protection Regulation – 12 steps to take now (Information Commissioner's Office)
https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

Guidelines on Data Protection Officers ('DPOs') (Article 29 Working Party, 13 December 2016)
http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083