skillsforcare

The role of the Data Protection Officer

Meeting your legal obligations under GDPR

September 2018

About this guide

This guide aims to help social care employers understand their requirements under the General Data Protection Regulations (GDPR) regarding data protection roles and;

- whether you legally need to appoint a Data Protection Officer (DPO).
- Or whether you'd like to appoint a DPO anyway as best practice, or whether you want to appoint a Data Protection Champion (DC) to help you ensure and show you're adequately protecting personal data.

The General Data Protection Regulations (GDPR)

The GDPR took effect on 25 May 2018 and gives individuals more rights with regard to the collection and processing of their personal data. This includes all organisations and businesses that are collecting, storing or processing personal data – including special category data (previously called personal sensitive data.)

Due to the sensitive nature of much of the data that is collected, held, created and shared by health and care organisations, GDPR will have particular relevance to adult social care.

Why GDPR in social care is so crucial

Health and social care organisations are now subject to stricter guidelines on the collection, processing and storage of individuals' data. The penalty for non-compliance with the GDPR is significantly increased from the powers given to the Information Commissioner's Office (ICO) under the Data Protection Act 1998 (DPA).

Social care providers will need to ensure that they demonstrate that they are adequately protecting citizen's information. Social care organisations need to uphold the integrity of individuals' data, as well as ensuring cyber resilience and business continuity in the event of a data breach.

For further guidance on GDPR itself, please see **here**.

For specific guidance for social care organisations please visit our webpage **here**.

The definition of personal data now has been made broader to include: genetic, mental, cultural, economic, social, and sexual identity.

About the role of a Data Protection Officer

The GDPR introduces a duty to appoint a Data Protection Officer (DPO) if you are a public authority, or if you carry out certain types of processing activities. A DPO is a specified role defined in law. Under GDPR, there is a requirement for some organisations to appoint or have access to a Data Protection Officer.

The DPO's responsibilities include audits and notifying the supervisory authorities if there is a breach. They should:

- sit outside the management structure of the organisation
- inform and advise on your data protection obligations
- operate at organisational level
- provide advice regarding Data Protection Impact Assessments (DPIAs)[1]
- ensure that data risks and breaches are identified and mitigated against at organisational level
- assist you in monitoring internal compliance
- report to the highest level of management
- act as the main point of contact with the regulatory data protection authority – the Information Commissioner's Office.

They should not:

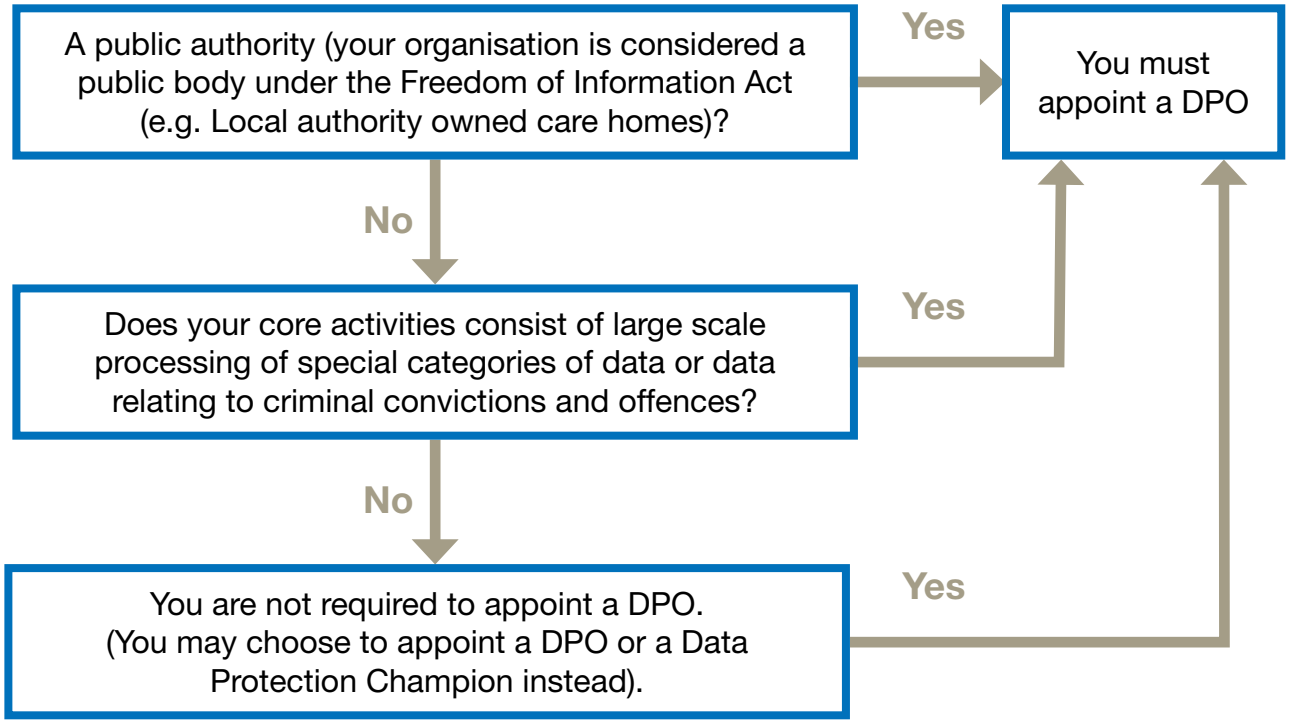
- define the means and purpose of processing data in the organisation.
- receive instructions on how to carry out their tasks relating to data processing

For very small businesses, the responsibility will ultimately fall to the owner or director.

1 For more detail on DPIA's please see;
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Do I need a DPO?

Is your organisation…?



These DPO requirements apply to both data controllers and processors.[2] There is guidance on the Data Champion role here.

Even if you're not legally required to appoint a DPO, you might want to do so anyway.

If you decide to voluntarily appoint a DPO you should be aware that the same requirements of the position apply.

2 For more detail on whether you are a controlling or processing data, please see https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

Important things you need to know about appointing a Data Protection Officer

It will be difficult for many social care providers to appoint a DPO internally because of the position they must occupy in the organisation. The GDPR specifies that they must not receive instructions on how to carry out their tasks relating to data processing, that they cannot be dismissed or penalised for performing their tasks and that they must report directly to the highest level of management.

Additionally, they cannot be the individual who decides the means and purposes of processing data in your organisation. For example, a registered manager plans to bring in a new rota system which would include staff personal details; they couldn't also be the DPO because the decision-making process might conflict with data protection obligations.

What the role involves

A DPO acts as the main point of contact with the regulatory data protection authority – the Information Commissioner's Office (ICO). The role also includes:

- leading the data protection aspect of management/board meetings
- ensuring sound governance and due diligence is in place at all times
- providing advice, support, encouragement to management/board members and other colleagues
- working with any conflicts or concerns within the board/management, supporting members to reach a positive resolution
- ensuring that the voices of people with care and support needs, and their families, are heard and acted upon
- ensuring that appropriate protocols are in place to support information sharing and that they are monitored
- keeping self and relevant organisations up-to-date with, and acting upon developments in national policy.

There is more information about DPOs **here** and **here**.

Questions

My organisation doesn't 'fit' any of those described above. Do we need a DPO?

For all other data controllers and processors other than those cited in the flow chart above, the advice on the requirement for a DPO is currently less clear.

This is because the GDPR does not define what is meant by 'large scale' processing of special categories of data and it is when organisations are processing or controlling 'large scale' amounts of data that the DPO requirement is applied, in addition to the categories stated in the flow chart.

Tip

If you are a larger organisation it is likely that you will need access to a DPO – either in-house or as a consultant.

If you decide you do not need one, then you should document your reasons for this decision.

Having considered the latest guidance, it is up to your organisation to decide whether you need or wish to have a DPO. You may wish to share this function with other organisations, either in-house or as a consultant, using them 'as and when'. If you don't, you should document the reasons why.

You may wish to approach your Local Authority or Clinical Commissioning Group to enquire if their DPO would assist with your service on an ad-hoc basis.

Having looked at all of the above, we do not think we currently need a DPO; what should we doing now to ensure we comply with data protection best practice?

You may decide that you do not need or wish to have a DPO. However it is important that:

- all organisations have a person who is responsible for the protection of data and will champion the principles of data protection as set out in the GDPR
- where there is no DPO, you should appoint a Data Protection Champion as a way of ensuring that you ensure adequate focus, insight and actions on data protection.

However, do not call this person a Data Protection Officer as this is a specific title in law. You can read more about the role of Data Protection Champion in our other guidance. There is more information about DPOs **here** and **here**.

Important note

As with any new regulations, there will now be a period of questioning and testing what is working. Therefore this guidance will be regularly updated to provide social care employers with the most up to date advice. Please re-visit this document regularly for updates and changes.

Useful resources

Data Protection Impact Assessments (DPIA)

A DPIA is a process to help you identify and minimise the data protection risks of a project. This link contains checklists to help you decide when to do a DPIA. **Find out more about Data Protection Impact Assessments.**

NHS digital guidance on GDPR

This policy and guidance is being developed by the national GDPR working group and is aimed at those with senior responsibility for Information Governance. The guidance can be used to learn how to comply with the GDPR and this includes Caldicott Guardians, operational information governance leads and managers, plus all employees.

Access this guidance here

Information Commissioners Office guidance on the role of Data Protection Officer

Accountability is one of the data protection principles of the role of the Data Protection Officer. It makes the role responsible for complying with the GDPR and providing evidence that demonstrates compliance. Employers need to put in place appropriate technical and organisational measures to meet the requirements of accountability. Read more about the role and what is required.

Access guidance from the nformation Commissioners Office here