skillsforcare

The role of the Data Security and Protection Lead

Good practice for meeting your GDPR obligations

November 2020

About this guide

In order to comply with General Data Protection Regulations, social care organisations will need to have someone who is responsible for the protection of data and will champion the principles of good data protection. This person could be a Data Protection Offficer (DPO) or a Data Security and Protection Lead (DPC).

Before reading this guide, you will first need to check whether you need a Data Protection Officer as this is a legal requirement. Please visit our other guide which will help you determine this.

It's important to check first because:

- Having a Data Security and Protection Lead is not the same as a having a Data Protection Officer.
- There are specific requirements for the Data Protection Officer role which are set out in law.
- They will ensure that you're protected against data risks and breaches and that your organisation is compliant with the data protection laws. Their role is outside of the management structure of the organisation itself.

We've confirmed we don't need a Data Protection Officer

Great. You may want to consider appointing or nominating someone to be a Data Security and Protection Lead (DPC).

This guide sets out:

- the role of a DPC
- how you can support them in this role
- what your obligations are under the GDPR

A DPC can help ensure and show that you're adequately protecting personal data within your organisation. A DPO is not a legal requirement and simply best practice.

1. What a Data Security and Protection Lead (DPC) does

A DPC sits within the organisation and operates at service level. Their role;

- Champions good data protection practice.
- Has a suggested set of skills and knowledge in an addition to that person's everyday role.
- May contribute to the service level processes and procedures for processing data.
- Reports to service level management (ie Registered Manager).
- Will be supported and professionally developed by senior managers in their service.
- Makes observations and contributes to senior managers within the service.

The person in the role of DPC needs to be at a sufficient level so they can speak with sufficient authority on the subject to all levels of the organisation. You can either:

- appoint a Data Security and Protection Lead (DPC) or
- incorporate it into someone's role.

The role will have:

- enhanced knowledge and awareness of Data Protection regulations and processes.
- an awareness of the correct processes, to act as a guardian of these and to alert to any possible issues or breaches.
- less responsibility than a DPO (a key function is their ability to know when to advise whether a DPO or Caldicott Guardian's input may be needed.

It's important that organisations do not over-burden the person who holds the DPC role; there needs to be robust discussions and then processes in place stating the 'cut off' points of their role, when senior management will take over or need to be consulted.

Please note: The existence of a DPC does not negate the whole organisation's responsibilities regarding Data Protection or the senior management team's role in setting up, implementing and monitoring Data Protection good practice.

2. How a Data Security and Protection Lead should communicate

The DPC will function as an internal point of information and advice and will escalate any concerns, as appropriate, to the relevant management team.

A DPC must have, or be in a position to develop, a good knowledge their service, which types of personal data their service holds and how this data is used.

3. Getting started in the role

The role of a DPC is not to undertake an audit or full review of the service. This must be undertaken before they take on their role by a suitable member of the management team. Once this is complete, the DPC would monitor, advise and review day to day issues.

Some of the advised organisational changes that are needed to support the DPC would be:

- Update the organisational public-facing privacy policy, including the role of the DPC.
- Know where data is stored and what information you hold
- Put privacy protection policies in place and follow them.
- Examine the data processing activities in the organisation and the lawful basis for this and change or adapt as necessary.
- Delete any data that is no longer needed.
- Flow of data from the organisation.

There is guidance and template policies for this work available **here**.

4. Adding the role to a job description

Use the following duties and responsibilities as a guide when editing job descriptions to reflect the new role:

- To be the first point of contact for GDPR questions and queries.
- To liaise where possible with the DPO in their area when required.
- To provide brief guidance to colleagues regarding data protection impact assessments carried out in their service and/or refer them to the DPO if necessary.
- To escalate difficult questions to the Data Protection Officer or the Information Commissioner's Office.
- To record, collect and advise on actions required regarding Data Portability, Subject Access Requests, Requests for Rectification or Requests for Restriction of Processing (new rights under GDPR).
- To act as a channel of communication between the Data Protection Officer (where there is one) and their service, including management as appropriate.
- To support the Management Team and all the staff to be aware of the requirements of the Organisational Data Protection Policy and the need to abide by the guidance contained therein
- To act as the service's privacy and consumer champion. They should take ownership of compliance and promote it, having a public-facing function representing the interests of Data Subjects (customers, subscribers etc).
- To Champion and promote the data processes in the service to the management and staff teams. For example, the need for a DPC will become acute when an organization is upgrading or changing record systems or implementing new IT systems.
- Promoting data governance and data management in the service.
- To offer advice and assistance when implementing data processes and guidelines, and helping to ensure that they are being followed.
- The DPC should have open access to the senior management team
- To advise on the purposes for which, and the manner in which, any Personal Data is processed. They will advise on establishing practices and policies in line with the organisational Data Protection policies, and with the agreement of the management team.
- To deal with initial Data Protection queries in accordance with the GDPR and organisational policies, ensuring that with management's oversight, that these are appropriately escalated to the DPO or Caldicott Guardian.
- To ensure that the Data Protection principles of the GDPR are followed.
- To advise regarding procedures to ensure security of data e.g. use of computer and removable media, passwords, personal records of staff and users of services, locked cupboards, shredding of paper documents etc. in-line with the policy.

5. Learning and development

It is important to recognise that the role of a DPC is not within the natural skills and knowledge of the average person working within the care sector. It is likely that the person you choose will require an investment by you as the employer into their personal development.

This may mean an investment of time, to engage in learning and understand the organisation's data procedures and practices but may also involve an investment of money, if you choose to pay for their learning and development.

As a base, Skills for Care recommend everyone, including the DPC, completes the e-LfH **Data Security Awareness e-learning** which is freely available for social care providers.

This training is **not mandatory** for social care providers but is a good resource to use to train staff. The level one training is at a suitable level to provide all staff with a good understanding of information governance, data security and their responsibilities under national legislation. This will also satisfy basic training requirements in the Data Security and Protection Toolkit.[1]

Find out how to access this training **here**.

However, in addition to this you may wish for your DPC to have an enhanced level of learning beyond this to fully be prepared and able to fulfil their role.

In order to source this, Skills for Care offer an Endorsed Training Providers list. By passing our quality assurance processes, you can be confident that each training provider below:

- supports excellence
- has good processes in place
- delivers courses that are relevant and fit for purpose
- can prove that the people who've attended their courses are now delivering better care

We would recommend that you choose appropriate training and training organisation from this list. You can take the list of requirements from this guidance and approach a learning provider and they can work with you to match the requirements.

1 For more information on the Data Protection and Security Toolkit, please see https://www.careprovideralliance.org.uk/data-security-and-protection-toolkit.html

Further help and guidance

There are external resources to help your DSPL deal with difficult questions, for example, **The Caldicott Guardian Council** and the **Information Commissioner's Office**.

Keep updated

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.