

APPENDIX A

What is a Data Protection Officer?

A Data Protection Officer is the person who is in charge of ensuring the Council is compliant with any laws and regulations relating to data protection.

A DPO is the key to understanding the new regulations and helping ensure the Council does not break the law. They will provide guidance and practical advice, explain necessary processes, and put safeguards in place to prevent Councils falling foul of the GDPR.

Identifying requirements for a Data Protection Officer

Advice from the Information Commissioner's Office (ICO) states the following:

- The GDPR introduces a duty for you to appoint a data protection officer (DPO) if you are a public authority, or if you carry out certain types of processing activities.
- DPOs assist you to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.
- The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.
- A DPO can be an existing employee or externally appointed.
- In some cases several Councils can appoint a single DPO between them.

Key tasks of the Data Protection Officer

Essentially, the DPO will hold responsibility for all things relating to data protection. Their role covers everything from providing information and advice, to monitoring compliance and being the first point of contact for authorities.

The General Data Protection Regulations details the minimum tasks that a DPO should carry out. It's important to note that these are only the minimum requirements and responsibilities and that the DPO's duties could vary dramatically depending on your Council's needs and size.

The DPO's tasks will be to:

- Inform and advise the controller or the processor and the employees about data protection provisions
- Monitor compliance with the General Data Protection Regulation, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits
- Provide advice where requested on data protection impact assessments
- Cooperate with the supervisory authority
- Act as the first contact point for the supervisory authority and individuals whose data has been processed"

The primary job of the Data Protection Officer is to work with everyone in an Council to ensure that the company is fully compliant with all GDPR legislation.

In practice, this means:

Guidelines, policies and procedures

The DPO will be responsible for providing guidelines on the GDPR and best practice for compliance throughout the Council. They will need to check existing policies and procedures, and provide new ones that adhere to the new data protection regulations. Responsibility will fall on them for a procedure to correctly deal with subject access requests made by individuals.

Staff & Councillor training (new and existing)

The DPO will advise on training for staff and Councillors and can provide that training

Council Liaison

The DPO should act in an advisory role, liaising with the Council to ensure compliance is followed at each stage of processing.

In order to fulfil the task of monitoring compliance, the DPO will need to conduct regular reviews of all processes and oversee the implementation of necessary changes. They will be regularly checking the activities of data controllers and processors and need to offer their expert advice on Privacy Impact Assessments (PIAs). In general, if there is anything relating to data protection in a Council, the advice of the DPO should always be sought.

Employers' duties to the DPO

Whilst the Data Protection Officer has a wealth of responsibilities, employers also have some legal duties to the DPO.

Under the GDPR, an employer should support their DPO at all times, with the responsibility to 'provide resources necessary to carry out those tasks, and to maintain his or her expert knowledge.' That could mean the provision of facilities, staff and a training budget. Employers all need to put an adequate chain of communication in place to allow a DPO to report back directly to the highest level in the Council – i.e. the Clerk and the Council.

Employers need to ensure that DPO's have the freedom and independence to do their job. They must not be hindered in their tasks, and cannot be dismissed or penalised for performing their duties.

Preparing for the new regulations

It is clear that the GDPR brings with it a mountain of tasks and requirements for any council. A Data Protection Officer can take some of those responsibilities away and provide protection and safeguards for your council.

DATA PROTECTION OFFICERS

67 Designation of a Data Protection Officer

- (1) The Controller must designate a data protection officer, unless the controller is a court, or other judicial authority, acting in its judicial capacity.

- (2) When designating a Data Protection Officer, the Controller must have regard to the professional qualities of the proposed officer, in particular:
 - (a) the proposed officer's expert knowledge of data protection law and practice, and
 - (b) the ability of the proposed officer to perform the tasks mentioned in section 69.
- (3) The same person may be designated as a Data Protection Officer by several Controllers, taking account of their organisational structure and size.
- (4) The Controller must publish the contact details of the Data Protection Officer and communicate these to the Commissioner.

68 Position of Data Protection Officer

- (1) The Controller must ensure that the Data Protection Officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.
- (2) The Controller must provide the Data Protection Officer with the necessary resources and access to personal data and processing operations to enable the Data Protection Officer to:
 - (a) perform the tasks mentioned in section 69, and
 - (b) maintain his or her expert knowledge of data protection law and practice.
- (3) The Controller:
 - (a) must ensure that the Data Protection Officer does not receive any instructions regarding the performance of the tasks mentioned in section 69;
 - (b) must ensure that The Data Protection Officer does not perform a task or fulfil a duty other than those mentioned in this Part where such task or duty would result in a conflict of interests;
 - (c) must not dismiss or penalise the Data Protection Officer for performing the tasks mentioned in section 69.
- (4) A data subject may contact the Data Protection officer with regard to all issues relating to:
 - (a) the processing of that data subject's personal data, or
 - (b) the exercise of that data subject's rights under this Part.

- (5) The Data Protection Officer, in the performance of this role, must report to the highest management level of the Controller.

69 Tasks of Data Protection Officer

- (1) The Controller must entrust the Data Protection Officer with at least the following tasks:
- (a) informing and advising the Controller, any processor engaged by the Controller, and any employee of the Controller who carries out processing of personal data, of that person's obligations under this Part,
 - (b) providing advice on the carrying out of a data protection impact assessment under section 62 and monitoring compliance with that section,
 - (c) co-operating with the Commissioner,
 - (d) acting as the contact point for the Commissioner on issues relating to processing, including in relation to the consultation mentioned in section 63, and consulting with the Commissioner, where appropriate, in relation to any other matter,
 - (e) monitoring compliance with policies of the Controller in relation to the protection of personal data, and
 - (f) monitoring compliance by the Controller with this Part.
- (2) In relation to the policies mentioned in subsection [\(1\)\(e\)](#), the Data Protection Officer's tasks include—
- (a) assigning responsibilities under those policies,
 - (b) raising awareness of those policies,
 - (c) training staff involved in processing operations, and
 - (d) conducting audits required under those policies.
- (3) In performing the tasks set out in subsections [\(1\)](#) and [\(2\)](#), the Data Protection Officer must have regard to the risks associated with processing operations, taking into account the nature, scope, context and purposes of processing.