Data Protection: Implementation

April 2021

1. Data Protection Officer (DPO)

UK GDPR introduces a duty to appoint a Data Protection Officer if you are a public authority, or if you carry out certain types of processing activities. This is the role in an organisation which has responsibility for ensuring that personal data is protected and that the organisation is compliant with the legislation. There should be a degree of independence so the DPO reports direct to the highest management level of the organisation as a part of the organisation's governance. They are part of the enhanced focus on accountability.

Organisations must have a named DPO if they:

- Are a public authority
- Carry out regular and systematic monitoring of data subjects on a large scale as core activities
- Carry out large scale processing of sensitive personal data relating to criminal convictions and offences

Public authority is defined by Freedom of Information legislation and for bodies performing a task carried out in the public interest or in the exercise of their official authority, e.g. the administration of justice, the Houses of Parliament, ministers or a government department, or activity that supports or promotes democratic engagement. There are some exceptions, e.g. parish councils.

Every organisation that processes personal data should have a named data protection lead. If you are unsure, carry out an analysis of your data processing to find out - this analysis is part of your due diligence and accountability trail. An information audit will inform your decision.

It is open to any organisation to appoint a DPO voluntarily. They may be employed in the organisation or with a service contract to fulfil the role. It may also be practical for there to be a shared DPO across related bodies, e.g. a central government department with separate agencies, or a Multi-Academy Trust across a number of schools.

Requirements of the DPO

- Informs and advises the organisation about your obligations to comply with the GDPR and other data protection laws
- Monitors compliance with the Data Protection Act 2018 and UK GDPR

- Has appropriate expertise or experience
- Is the primary Data Protection contact point in the organisation
- Advises on and monitors Data Protection Impact Assessments
- Cooperates with the Information Commissioner's office (ICO) and is the first point of contact
- Can carry out other tasks and duties, provided there is no conflict of interest, so the DPO may hold the asset register and records of the organisation as the central point for ensuring that the organisation is compliant
- Understands and advises on a risk-based approach to data processing in their organisation

UK GDPR advises that a DPO is appointed on the basis of their professional qualities, and in particular, experience and expert knowledge of data protection law. This knowledge could be part of wider, relevant experience within the information field. The skills will be proportionate to the scale and complexity of the data processing in the organisation.

Registration

UK GDPR requires organisations to:

- publish the contact details of your DPO
- provide them in the Privacy Notice, and
- provide them to the ICO

The Data Protection (Charges and Information) Regulations 2018 requires every organisation which processes personal information to register with the ICO and pay a data protection fee. See https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/

2. Data Subject Access Requests

Requests from data subjects [living people whose personal data you hold] are called Data **Subject Access Requests**. DSARs can be made verbally or in writing, on a form or in a letter or email and the subject's identity must be verified for a DSARS response – in other words, you can only send information about somebody, to the person themselves. If a request is made verbally, it is best practice to follow up the dialogue in writing to ensure that the request is documented and a record kept of the request. There is no charge for making a SAR. Note that there are special reasons known as **Exemptions** where you are not required to release the personal information if you are collecting it or using it to meet legal and regulatory responsibilities, e.g. where release might compromise a contract

negotiation or legal proceedings. In all cases you should assess the use of an exemption on a case by case basis and explain the refusal fully.

At all stages of the assessment of each DSAR, take care to document your decision making and approach as that may be relevant to support your assessment if it is challenged or queried in a subsequent complaint. The deadline under the legislation is without delay and at the latest within **one month** of receipt of the DSAR, i.e. 20 working days. This time starts to run from when you have the evidence and can check that the request is valid.

Increased data subject rights, including the end of charging for access to data, might mean more SARs. Your organisation needs to plan how you will recognise and handle DSARs with a documented internal process.

3. Data breach reporting to ICO

A **personal data breach** is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- Access by an unauthorised third party through their direct action or lax internal security procedures or practices
- Deliberate or accidental action or inaction by a member of staff
- Sending personal data to an incorrect recipient, e.g. wrong copy recipients to an email
- USB stick, laptop or phone containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

When a security incident takes place, it must be established whether:

- A personal data breach has occurred
- The nature of that breach
- The steps to be taken in response to the breach

If a breach is not addressed promptly and with the appropriate sense of urgency, then more damage may result. For this reason, there are tight deadlines for reporting and action. A notifiable breach (i.e. a breach that is a risk to the rights and freedoms of individuals) must be reported to the ICO without undue delay, but not later than 72 hours after becoming aware of it. Where this time deadline is not met then reasons for the delay must be explained.

4. Privacy by Design and Data Privacy Impact Assessments (DPIAs)

Privacy by design is an approach to managing personal data that promotes privacy and data protection compliance in all your activities. This ensures that privacy and data protection is a key consideration in the early stages of any activities, including for example a project, and then throughout its lifecycle. For example when:

- building new IT systems for storing or accessing personal data;
- when collecting personal data;
- developing policy or strategies that have privacy implications;
- embarking on a data sharing initiative; or
- using data for new purposes.

You must do a DPIA for processing that is **likely to result in a high risk** to individuals. This includes some specified types of processing. You can use the checklists below to help you decide when to do a DPIA. It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

Checklist for a DPIA

A DPIA should incorporate the following steps:

- Describe the nature, scope, context and purposes of the processing
- Identify the need for a DPIA
- Assess necessity, proportionality and compliance measures
- Describe the information flows
- Identify the privacy and assess the risks to individuals
- Identify any additional measures to mitigate those risks
- Consult with internal and external stakeholders as needed throughout the process

For further information:

- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/
- https://ico.org.uk/for-organisations/guide-to-data-protection/