# Privacy impact assessments (GDPR)

**Background**

The GDPR, or General Data Protection Regulation, is a new piece of European legislation which replaced the Data Protection Act (DPA) 1998 on 25 May 2018. A new Data Protection Act 2018 came into force at the same time. The purpose of the DPA 2018 is to apply the GDPR in the UK.

The underlying data protection principles have not changed significantly from those of the DPA – but there is the new principle of 'accountability' (see below). The GDPR also requires organisations to adopt the philosophy of 'Data Protection by Design and Default'. This means that the organisation must be able to demonstrate compliance with the data protection principles. The principles are the backbone of the regulation.

**Processing principles**

The GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency')
- collected for specified, explicit and legitimate purposes ('purpose limitation')
- adequate, relevant and limited to what is necessary ('data minimisation')
- accurate and up-to-date ('accuracy')
- kept in a form which permits identification for no longer than is necessary/archiving ('storage limitation')
- processed with appropriate technical and organisational measures to ensure security of personal data ('integrity and confidentiality').

The GDPR also requires that the data controller must be *responsible for and able to demonstrate compliance with* the principles ('accountability'). This means having the right procedures and processes in place from the point of data collection, so that there is clarity as to the legal basis for data processing at every stage of the life cycle of the data. Organisations have to be able to detect, report and investigate a personal data breach. Reputation management should be considered as part of the process.

**What is privacy by design?**

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. The ICO views privacy by design as an essential tool in minimising privacy risks and building trust. Designing projects, processes, products or systems with privacy in mind at the outset can lead to benefits which include:

- Potential problems are identified at an early stage, when addressing them will often be simpler and less costly.
- Increased awareness of privacy and data protection across an organisation.
- Organisations are more likely to meet their legal obligations and less likely to breach the Data Protection Act.
- Actions are less likely to be privacy intrusive and have a negative impact on individuals.

**Where do privacy impact assessments come in?**

Privacy impact assessments (PIAs) are a tool that you can use to identify and reduce the privacy risks of your projects. A PIA can reduce the risks of harm to individuals through the misuse of their personal information. It can also help you to design more efficient and effective processes for handling personal data.

Privacy impact assessments (PIAs) are, therefore, useful tools to help practices consider and address the privacy risks inherent in processing the data they hold. They are a risk management tool to be used when thinking about how to comply with the data protection principles. They are also about meeting patient and staff expectations about how you keep their personal data safe. The GDPR requires that you carry out a PIA *before* you implement a new system or process for processing data: for example, your accountant always ran your payroll but you decide to do it yourself with a new payroll package bought off the shelf. Or perhaps you want to update your telephone system with call recording. However, assessments should also be part of ongoing processes in your practice and can be carried out when planning any changes to an existing system.

**How do I carry out a privacy impact assessment?**

Conducting a PIA doesn't have to be complex or time consuming but there must be a balance between the amount of time and effort that you put into it in proportion to the privacy risks that might arise.

A PIA should incorporate the following steps.

**Step 1: Identify the need for a PIA.** The ICO has developed a list of screening questions that can be used to help you decide whether you need to produce a PIA or not. The questions can be adapted to suit your practice. If you answer 'yes' to any of the questions then a PIA would probably be required.

- Will the project involve the collection of new information about individuals?
- Will the project compel individuals to provide information about themselves?
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of video recording technology (CCTV).
- Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?

- Is the information about individuals of a kind that is particularly likely to raise privacy concerns or expectations? For example, health records?
- Will the project require you to contact individuals in ways which they may find intrusive?

Once you have identified a need for a PIA as in Step 1 you should access the ICO's *Code of Practice for Conducting Privacy Impact Assessments* for more detailed information regarding the steps set out below.

**Step 2: Describe the information flows.** How will you collect, use and delete personal data? How many people will be affected?

**Step 3: Identify the privacy and related risks.** Annex 3 of the ICO's *Code of Practice for Conducting Privacy Impact Assessments* will help you to identify whether there is a risk that the project will fail to comply with the principles of data protection (it currently refers to the Data Protection Act 1998 but will be amended in due course).

**Step 4: Identify and evaluate the privacy solutions.** Describe the actions you will take to reduce or eliminate risks and note any future actions that might be needed. You will also need to record any risks that you have decided to accept as necessary for the project to continue.

**Step 5: Sign off and record the PIA outcomes.** Approve the PIA at a level appropriate to the project and make the report available to view.

**Step 6: Integrate the outcomes into the project plan.** Ensure that the steps recommended by the PIA are implemented and recorded.

**Step 7: Consult with internal and external stakeholders as needed throughout the process.** Internal and external consultation provides the opportunity for people to highlight their views on privacy risks and solutions that you may not have thought of. Consultation would be ongoing throughout the risk assessment process.

If you follow the suggested methodology then you will be able to show that you have carried out a sufficiently comprehensive process to comply with the GDPR.

If in doubt contact either the Information Commissioner's Office - 0303 123 1113 Option 4 - or MDDUS – 0333 043 4444 – for advice.