UK GDPR – data protection impact assessments (DPIA)

The GDPR, or General Data Protection Regulation, is a piece of European legislation which replaced the existing Data Protection Act (DPA) 1998 on 25 May 2018. A new UK Data Protection Act 2018 also came into force on the same day. The purpose of the UK Data Protection Act 2018 is to apply the GDPR in the UK, and is now commonly referred to as 'UK GDPR'.

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 UK GDPR.
- Actions are less likely to be privacy intrusive and have a negative impact on individuals.

This is where data protection impact assessments come in.

Reducing privacy risks

Data protection impact assessments (DPIA) are a tool that you can use to identify and reduce the privacy risks of your projects and systems of working. A DPIA can reduce the risks of harm to individuals arising from the misuse of their personal information. It can also help you to design more efficient and effective processes for processing personal data.

DPIAs are, therefore, useful tools to help organisations consider and address the privacy risks inherent in processing the data they hold. They are a risk management tool to be used when considering how to comply with the data protection principles. They are also about meeting patient and staff expectations regarding how you keep their personal data safe. The UK GDPR requires that you carry out a DPIA before you implement a new system or process for processing data: for example, you want to update your telephone system with call recording.

However, assessments should also be part of ongoing processes in your organisation and can be carried out when planning any changes to an existing system.

Conducting a DPIA doesn't have to be complex or time consuming and the amount of time and effort that you put into it should be proportionate to the privacy risks that might arise.

A DPIA should incorporate the following steps:

Step 1: Identify the need for a DPIA

The ICO has developed a list of screening questions that can be used to help you decide whether or not you need to produce a DPIA. The questions can be adapted to suit your organisation. If you answer 'yes' to any of the questions then a DPIA 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 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 DPIA, follow the steps 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
The ICO's guide to DPIAs will help you to identify whether there is a risk that the project will fail to comply with the principles of data protection (in the section *Have we written a good DPIA?*)

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 DPIA outcomes
Approve the DPIA 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 DPIA 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. This could include raising queries with MDDUS.

By following this methodology you will be able to show that you have implemented a sufficiently comprehensive process to comply with the UK GDPR.

Common Pitfalls

- Organisations fail to carry out a proper risk assessment on the impact that the new system or process might have on data protection. This could increase the risk of a data breach.
- Under the UK GDPR, non-compliance with DPIA requirements can lead to fines imposed by the ICO. Non-compliance could include: failure to carry out a DPIA when it is required; carrying out a DPIA in an incorrect way; or failing to consult with the ICO where required.

Key points

- Follow the ICO's guidance to determine whether you need to carry out a DPIA.
- Remember, you don't need to spend a large amount of time on a DPIA for a small project – the amount of time and effort that you put into it should be proportionate to the potential privacy risks.

Further guidance

- ICO. *Data protection impact assessments*: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

MDDUS GDPR checklist and guidance sheets: https://www.mddus.com/training-and-cpd/training-for-members/gp-risk-toolbox/gdpr