# A guide to DPIAs

## What is a DPIA:

DPIA stands for Data Protection Impact Assessment, which is an assessment of the risks involved with the personal data processing in a particular project. A DPIA will identify risks and the measures that could be implemented to mitigate against those risks.

A DPIA is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan.

## Why are DPIAs important:

DPIAs are an essential part of your accountability obligations. They are an effective way of ensuring you implement data protection by design and default. A DPIA is important for identifying risks and implementing measures to protect against those risks ensuring that the personal data you hold is secure.

## When is a DPIA required:

DPIAs are a legal requirement for certain types of processing that are likely to result in a high risk to the rights and freedoms of individuals.

To assess whether something is high risk, you should consider the likelihood and severity of the potential harm to individuals.

A DPIA is a legal requirement in the following circumstances:

- Any systematic and extensive profiling with significant effects on the individuals, e.g. automated decision making
- Any large scale use of sensitive data (special category data).

The ICO also requires you to complete a DPIA if you plan to:

- Use innovative technology;
- Use profiling or special category data to decide on access to services;
- Profile individuals on a large scale;
- Process biometric data;
- Process genetic data;
- Match data or combine datasets from different sources;

- Collect personal data from a source other than the individual data subject, without providing them with a privacy notice;
- Track individuals' locations or behaviour;
- Profile children or target marketing or online services to them; or
- Process data that might endanger the individual's physical health or safety in the event of a security breach.

Even if there is no clear indication that the project or data processing may be high risk, it is good practice to carry out a DPIA.

## Who should complete a DPIA:

Whilst your Data Protection Officer (DPO) may lead on the completion of your DPIA, they will need assistance from the person responsible for the project (e.g. the person who would like to carry out the data processing).

For bigger projects or processing activities, there may a team of people who will all be required to assist with completing the DPIA.

If you are signing up to use a service or software, the company may have their own DPIA framework that you could use and adapt. Usually this would cover the company or organisation's technical measures for securing personal information, the type of data they collect, why they collect it, who they share it with and the lawful basis for using it.

You will still need to review the company's DPIA and adapt it if necessary.

## How do we complete a DPIA:

Start by completing the DPIA screening checklist and the assessment tool to establish whether a full DPIA is required.

You should carry out the DPIA process at the start of a project or before the processing commences.

A DPIA will be a working document and will require input from several different stakeholders.

Complete the DPIA template.

## Identifying and mitigating risks:

The point of the DPIA is to identify any risks that may be involved with the particular type of data processing that you are carrying out. As you complete the DPIA template, the risks should become apparent. You should think about any likely harm that may be caused to the individual by the way their personal data is planned to be used.

As you go through, highlight any risks that you identify and add these to the end of the template.

Once you have identified all the risks, you should consider what measures you can implement to mitigate the risks.

The type of mitigation will depend on the type of risk.

## Referral to the ICO:

In most cases, it will be possible to put the appropriate mitigation in place for each risk. If you are still concerned about the risks involved and are unable to implement sufficient mitigation, you will be required to notify the ICO.

If you identify a high risk that you cannot take measures to reduce that risk, you cannot begin the project or processing until you have consulted the ICO.

Please note, if you are required to consult the ICO, it could take eight weeks to receive a response from them and you will not be allowed to proceed with the project until the ICO have given the go ahead.