Advice - Data Protection Impact Assessments

Data Protection Impact Assessments (DPIAs) are a tool to help you identify and minimise the data protection risks of existing/new projects. They form part of your accountability obligations under the GDPR, and an integral part of the 'data protection by default and by design' approach.

DPIAs are now mandatory in some cases, and there are specific legal requirements for content and process.

Failure to adequately conduct a DPIA when necessary is a breach of the GDPR and could lead to a financial penalty from the Information Commissioner, in theory up to €10 million.

What is a DPIA?

A DPIA is a 'risk assessment' process designed to help you analyse, identify and minimise the data protection risks of existing or proposed processing of personal data.

A DPIA may concern a single data processing operation or a single DPIA could be used to assess multiple processing operations that are similar in terms of nature, scope, context, purpose, and risks. For example, a group of academies within a MAT/MAC that are each setting up a similar CCTV system could carry out a single DPIA covering the all aspects of processing by these separate controllers.

A DPIA is not a one-off exercise; it is an ongoing process which should be regularly reviewed and reassessed if anything changes, for example if you make any significant changes to how or why you process personal data, or to the amount of data you collect, or if a security flaw is identified.

When do you need a DPIA?

Carrying out a DPIA is not mandatory for every processing operation. A DPIA is only required when the processing is "likely to result in a high risk to the rights and freedoms of natural persons". This mean a high risk to their rights. to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement and the prohibition of discrimination.

A DPIA must assess the level of risk, and in particular whether it is 'high risk'. The GDPR is clear that assessing the level of risk involves looking at both the likelihood and the severity of the potential harm or damage to individuals.

What does 'likely to result in a high risk' mean?

The GDPR doesn't define 'likely to result in high risk'. Given that you wouldn't know whether a high risk exists without doing the DPIA, we recommend that you use the criteria set out in this advice note to determine whether or not to undertake a DPIA.

It is mandatory to undertake a DPIA if you plan to:

- use systematic and extensive automated processing such as profiling that leads to decisions with significant effects regarding individuals;

- process special category (i.e. personal data revealing racial/ethnic origin, political opinions, religious/philosophical beliefs, membership of a trade union and several types of sensitive data such as genetic data, biometric data when the aim is to uniquely identify the data subject, as well as health-related data and data regarding the sex life or sexual orientation of the data subject) or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

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

- use new technologies;
- 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 without providing them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

What is the definition of 'large scale'?

The GDPR does not define what constitutes large-scale.

It is recommended that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:

- the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
- the volume of data and/or the range of different data items being processed;
- the duration, or permanence, of the data processing activity; and
- the geographical extent of the processing activity.

When should you undertake a DPIA?

In practice, the four circumstances when Schools and Academy Trusts would be required to carry out a DPIA are:

- ●Systematic monitoring of a publically available area on a large scale i.e. Audio/video CCTV surveillance of public areas;
- ● Sensitive data or data of a highly personal nature *and* Data concerning vulnerable data subjects i.e. Safeguarding Information;
- ● New technologies: processing involving the use of new technologies, or the novel application of existing technologies; and
- ●Biometric data i.e. Access control/identity verification for hardware/applications (including voice recognition/fingerprint/facial recognition)

as these types of processing are “likely to result in a high risk to the rights and freedoms of natural persons”.

How do you carry out a DPIA?

The DPIA should be carried out prior to processing, although we appreciate that with new legislation in place, you will have to undertake some DPIAs into processing activities which are already taking place.

The GDPR sets out the minimum features of a DPIA:

- ●a description of the nature, scope, context and purposes of the processing;
- ●an assessment of the necessity and proportionality of the processing;
- ●an assessment of the risks to the rights and freedoms of data subjects; and
- ● the measures envisaged to address (i.e. mitigate) the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR.

Who is obliged to carry out the DPIA?

The data controller is responsible for ensuring that the DPIA is carried out. Carrying out the DPIA may be done by someone else, inside or outside the organisation, but the controller remains ultimately accountable for that task.

The controller must also seek the advice of the Data Protection Officer (DPO), where designated and this advice, and the decisions taken by the controller, should be documented within the DPIA.

The controller must where appropriate seek the views of data subjects or their representatives.

Do you need to consult the ICO?

Whenever the data controller identifies any *high risk(s)* and cannot find sufficient measures to reduce the *high risk(s*) to an acceptable level (i.e. the residual risks are still high), consultation with the ICO is required. You cannot begin processing until you have consulted the ICO: you would need to email the ICO and attach a copy of your DIPA.

Please note: The focus is on the *'residual high risk'* after any mitigating measures have been taken. If your DPIA identified a high risk, but you have taken measures to reduce this risk so that it is no longer a high risk, you do not need to consult the ICO.

Once the ICO have all the necessary information, they aim to respond to you within 8 weeks or within 14 weeks if your proposed processing is complex. After which the ICO will provide you with a written response advising you whether the risks are acceptable, or whether you need to take further action. In some cases the ICO may advise you not to carry out the processing because it considers it would be in breach of the GDPR. The ICO also have the power to issue a formal warning or take action to ban the processing altogether.

Action your School/Academy needs to take to carry out a DPIA

This advice note is accompanied by a DPIA template and guidance notes on how to complete the template, which you can use to record your DPIA process and outcome.

You should start to complete the DPIA template in the following instances:

● at the start of any major project involving the use of personal data, or

● if you are making a significant change to an existing process, or

● when you begin to review your existing processing operations

and decide whether you need to do a DPIA, for anything which is likely to be high risk.

Please note, when reviewing existing processing operations only: You do not need to do a DPIA if you have already considered the relevant risks and safeguards in another way, unless there has been a significant change to the nature, scope, context or purposes of the processing since that previous assessment.