

Data Protection Impact Assessment

(Website for further details: <https://ico.org.uk/>)

The Information Commissioner's Office has a set guideline in relation to Data Protection, in particular an Impact Assessment with how data is used and stored.

The Impact Assessment will help you identify and minimise risk of data storage and usage

Our DPIA must:

01. Describe the nature, scope, context and purposes of the processing;
02. Assess necessity, proportionality and compliance measure
03. Identify and assess risks to individuals and
04. Identify any additional measures to mitigate those risks



What is a DPIA?

A DPIA is a way for you to systematically and comprehensively analyse your processing and help you identify and minimise data protection risks.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – to individuals or to society at large, whether it is physical, material or non-material.

Data Protection Impact Assessment

(Website for further details: <https://ico.org.uk/>)

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals.

A DPIA does not have to indicate that all risks have been eradicated. But it should help you document them and assess whether or not any remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability and building trust and engagement with individuals.

A DPIA may cover a single processing operation or a group of similar processing operations. A group of controllers can do a joint DPIA.

It's important to embed DPIAs into your organisational processes and ensure the outcome can influence your plans. A DPIA is not a one-off exercise. You should see it as an ongoing process that is subject to regular review.

When do we need a DPIA?

You must do a DPIA before you begin any type of processing that is “likely to result in a high risk”. This means that although you have not yet assessed the actual level of risk, you need to screen for factors that point to the potential for a widespread or serious impact on individuals.

In particular, the GDPR says you must do a DPIA if you plan to:

Use systematic and extensive profiling with significant effects;

Process special category or criminal offence data on a large scale; or

Systematically monitor publicly accessible places on a large scale.

Data Protection Impact Assessment

(Website for further details: <https://ico.org.uk/>)

When considering if your processing is likely to result in high risk, you should consider the relevant European guidelines. These define nine criteria of processing operations likely to result in high risk. While the guidelines suggest that, in most cases, any processing operation involving two or more of these criteria requires a DPIA, you may consider in your case that just meeting one criterion could require a DPIA.

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

Use innovative technology (in combination with any of the criteria from the European guidelines);

Use profiling or special category data to decide on access to services;

Profile individuals on a large scale;

Process biometric data (in combination with any of the criteria from the European guidelines);

Process genetic data (in combination with any of the criteria from the European guidelines);

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') (in combination with any of the criteria from the European guidelines);

Track individuals' location or behaviour (in combination with any of the criteria from the European guidelines);

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.

Data Protection Impact Assessment

(Website for further details: <https://ico.org.uk/>)

You should also think carefully about doing a DPIA for any other processing that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals.

Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data. You can use or adapt the checklists to help you carry out this screening exercise.

DPIA awareness checklist

- ☐ We provide training so that our staff understand the need to consider a DPIA at the early stages of any plan involving personal data.
- ☐ Our existing policies, processes and procedures include references to DPIA requirements.
- ☐ We understand the types of processing that require a DPIA, and use the screening checklist to identify the need for a DPIA, where necessary.
- ☐ We have created and documented a DPIA process.
- ☐ We provide training for relevant staff on how to carry out a DPIA.

DPIA screening checklist

- ☐ We consider carrying out a DPIA in any major project involving the use of personal data.
- ☐ We consider whether to do a DPIA if we plan to carry out any other:
 - ☐ evaluation or scoring;
 - ☐ automated decision-making with significant effects;

Data Protection Impact Assessment

(Website for further details: <https://ico.org.uk/>)

- ☐ systematic monitoring;
- ☐ processing of sensitive data or data of a highly personal nature;
- ☐ processing on a large scale;
- ☐ processing of data concerning vulnerable data subjects;
- ☐ innovative technological or organisational solutions;
- ☐ processing that involves preventing data subjects from exercising a right or using a service or contract.
- ☐ We always carry out a DPIA if we plan to:
 - ☐ use systematic and extensive profiling or automated decision-making to make significant decisions about people;
 - ☐ process special-category data or criminal-offence data on a large scale;
 - ☐ systematically monitor a publicly accessible place on a large scale;
 - ☐ use innovative technology in combination with any of the criteria in the European guidelines;
 - ☐ use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;
 - ☐ carry out profiling on a large scale;
 - ☐ process biometric or genetic data in combination with any of the criteria in the European guidelines;
 - ☐ combine, compare or match data from multiple sources;

Data Protection Impact Assessment

(Website for further details: <https://ico.org.uk/>)

- ☐ process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;
- ☐ process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;
- ☐ process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;
- ☐ process personal data that could result in a risk of physical harm in the event of a security breach.
- ☐ We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.
- ☐ If we decide not to carry out a DPIA, we document our reasons.

DPIA process checklist

- ☐ We describe the nature, scope, context and purposes of the processing.
- ☐ We ask our data processors to help us understand and document their processing activities and identify any associated risks.
- ☐ We consider how best to consult individuals (or their representatives) and other relevant stakeholders.
- ☐ We ask for the advice of our data protection officer.
- ☐ We check that the processing is necessary for and proportionate to our purposes, and describe how we will ensure compliance with data protection principles.
- ☐ We do an [objective assessment](#) of the likelihood and severity of any risks to individuals' rights and interests.
- ☐ We identify measures we can put in place to eliminate or reduce high risks.

Data Protection Impact Assessment

(Website for further details: <https://ico.org.uk/>)

- ☐ We record our decision-making in the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.
- ☐ We implement the measures we identified, and integrate them into our project plan.
- ☐ We consult the ICO before processing, if we cannot mitigate high risks.
- ☐ We keep our DPIAs under review and revisit them when necessary.

Have we written a good DPIA?

A good DPIA helps you to evidence that:

- you have considered the risks related to your intended processing; and
- you have met your broader data protection obligations.

This checklist will help ensure you have written a good DPIA.

We have:

- ☐ confirmed whether the DPIA is a review of pre-GDPR processing or covers intended processing, including timelines in either case;
- ☐ explained why we needed a DPIA, detailing the types of intended processing that made it a requirement;
- ☐ structured the document clearly, systematically and logically;
- ☐ written the DPIA in plain English, with a non-specialist audience in mind, explaining any technical terms and acronyms we have used;

Data Protection Impact Assessment

(Website for further details: <https://ico.org.uk/>)

- ☐ set out clearly the relationships between controllers, processors, data subjects and systems, using both text and data-flow diagrams where appropriate;
- ☐ ensured that the specifics of any flows of personal data between people, systems, organisations and countries have been clearly explained and presented;
- ☐ explicitly stated how we are complying with each of the Data Protection Principles under GDPR and clearly explained our lawful basis for processing (and special category conditions if relevant);
- ☐ explained how we plan to support the relevant information rights of our data subjects;
- ☐ identified all relevant risks to individuals' rights and freedoms, assessed their likelihood and severity, and detailed all relevant mitigations;
- ☐ explained sufficiently how any proposed mitigation reduces the identified risk in question;
- ☐ evidenced our consideration of any less risky alternatives to achieving the same purposes of the processing, and why we didn't choose them;
- ☐ given details of stakeholder consultation (e.g. data subjects, representative bodies) and included summaries of findings;
- ☐ attached any relevant additional documents we reference in our DPIA, e.g. Privacy Notices, consent documents;
- ☐ recorded the advice and recommendations of our DPO (where relevant) and ensured the DPIA is signed off by the appropriate people;
- ☐ agreed and documented a schedule for reviewing the DPIA regularly or when we change the nature, scope, context or purposes of the processing;
- ☐ consulted the ICO if there are residual high risks we cannot mitigate.