Spatial

The PIA process set out in this document is based upon the Privacy Impact Assessment Handbook; version 2.0, published by the Information Commissioner's Office (www.ico.gov.uk) and is tailored to the needs of Spatial.

In accordance with the Data Protection Act 2018, all data is up to date with all changes known to be in force on or before 30th January 2023

What is a DPIA (Data Protection Impact Assessment)?

A DPIA is a way to analyse our processing and help us identify and minimise data protection risks systematically and comprehensively.

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.

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 any remaining risks are justified.

DPIAs (Data Protection Impact Assessment) 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 is 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 UK 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.

When considering if your processing is likely to result in substantial risk, you should consider the relevant European guidelines. These define nine criteria of processing operations likely to result in elevated 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).

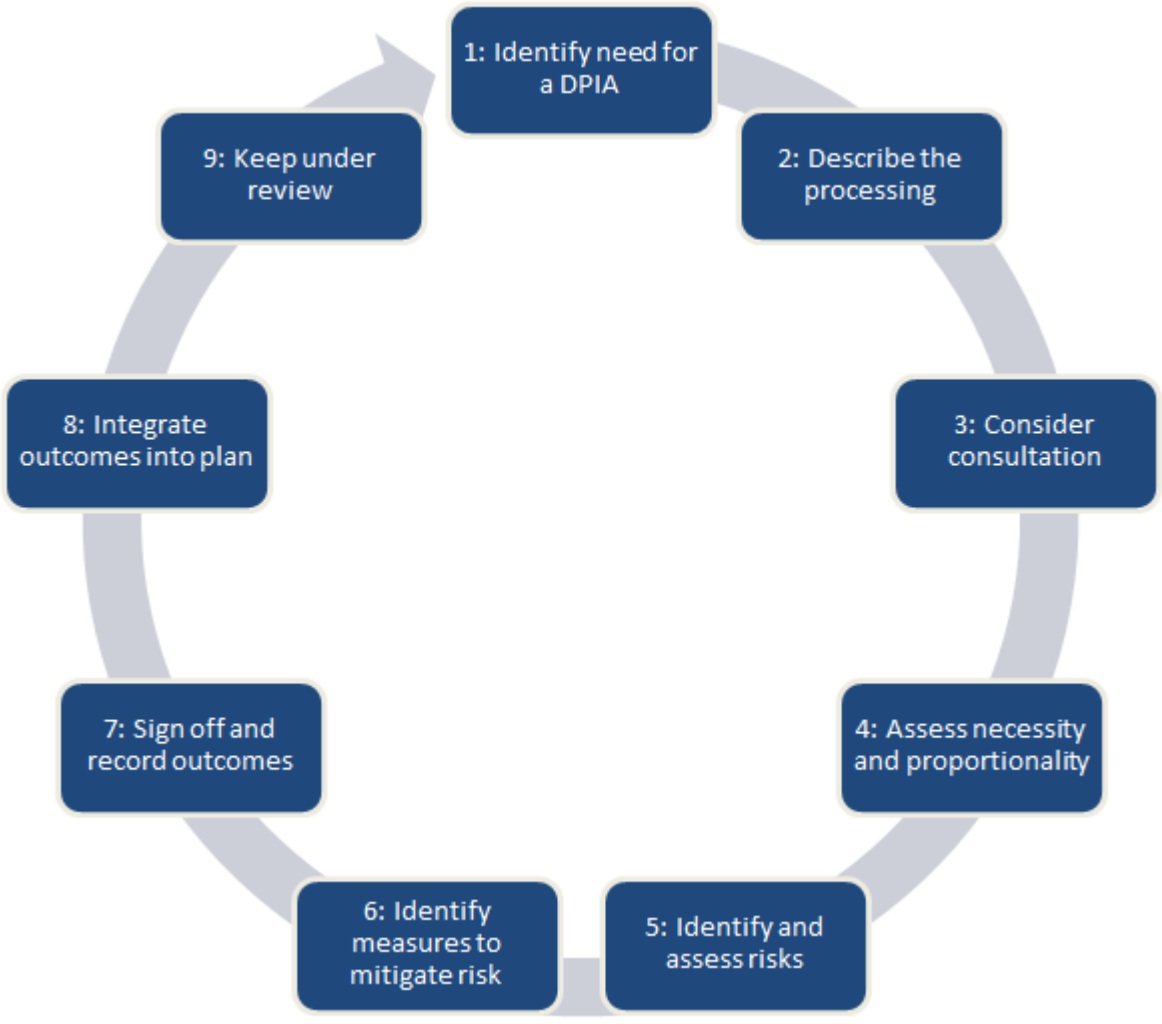
- match data or combine datasets from various sources.
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') (in combination with any of the criteria from the European guidelines).
- track individuals' location or behaviour (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.

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 substantial 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.

How do we carry out a DPIA?

A DPIA should begin early in the life of a project, before you start your processing, and run alongside the planning and development process. It should include these steps:



You must seek the advice of your data protection officer. You should also consult with individuals and other stakeholders throughout this process. The process is designed to be flexible and scalable.

\Although publishing a DPIA is not a requirement of UK GDPR (General Data Protection Regulations), you should actively consider the benefits of publication. As well as demonstrating compliance, publication can help engender trust and confidence. We would therefore recommend that you publish your DPIAs, where possible, removing sensitive details if necessary.

Do we need to consult the ICO?

You do not need to send every DPIA to the ICO and we expect the percentage sent to us to be small. But you must consult the ICO if your DPIA identifies a substantial risk and you cannot take measures to reduce that risk. You cannot begin the processing until you have consulted us.

Ian Flanagan
CEO
01.09.25

DPIA template

Start to fill out the template at the start of any major project involving the use of personal data, or if making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely substantial risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it is not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks, as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible, or probable	Minimal, significant, or severe	Low, medium, or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or substantial risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA