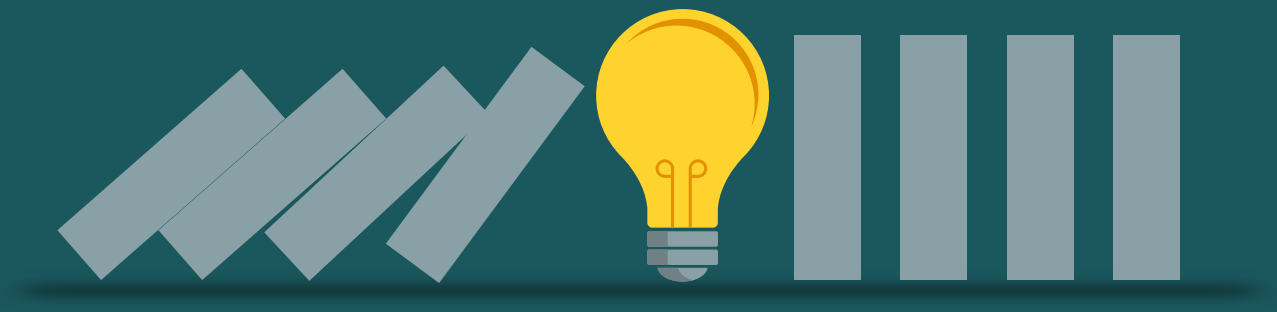
DATA PROTECTION IMPACT ASSESSMENTS QUICK GUIDE

How to manage DPIAs



Contents

Publication date: August 2024

DATA PROTECTION NETWORK

What is a DPIA?

Data Protection Impact Assessments are a useful risk management tool. They're intended to be used in the early stages of a project to help identify and address any data protection risks before they materialise.

A DPIA is a written assessment and a key element of UK/EU GDPRs' focus on accountability and Data Protection by Design. Conducting a DPIA and documenting the outcomes is an important way of demonstrating data protection is being taken seriously.

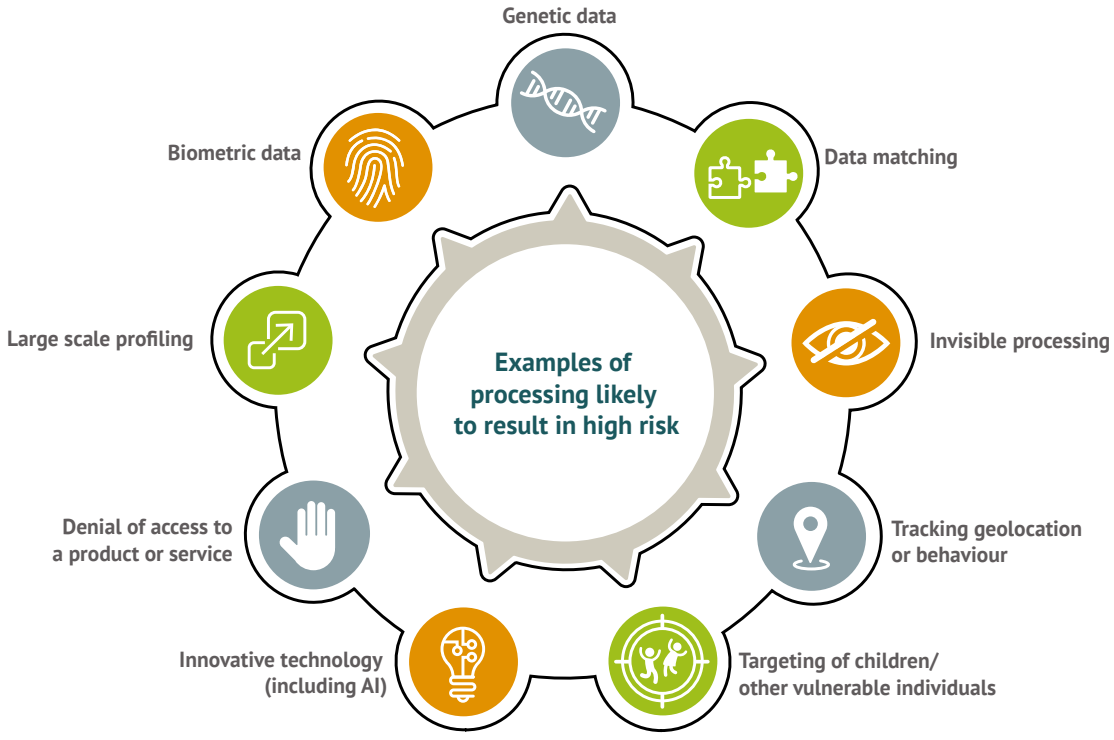
They help us to protect our customers, employees or anyone else whose personal information we're using. As well as protecting the organisation.

When a DPIA is mandatory

DPIAs are legally necessary under UK/EU GDPRs when activities involving personal data are likely to represent a 'high risk' to the rights and freedoms of individuals. Where needed, DPIAs should be conducted before the new processing begins.

The definition of 'processing' includes collecting, recording, organising, storing, adapting, retrieving, sharing and even the act of deleting personal data. Essentially anything we might be doing with personal data.

The UK's Information Commissioner's Office (ICO), in its DPIA guidance, provides examples of the types of activity which are likely to be considered high risk, as illustrated below.



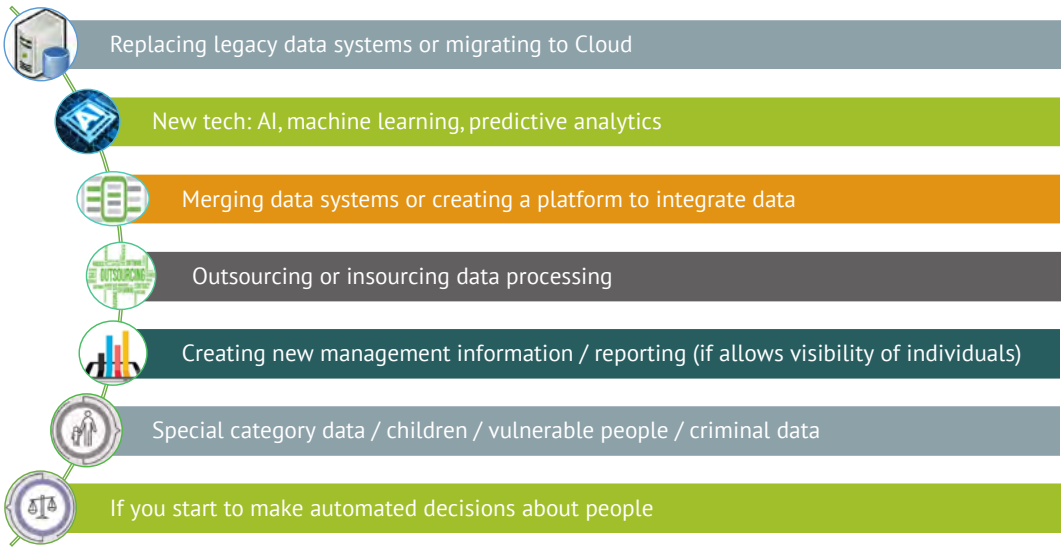
These examples are similar but not exactly the same as examples provided by data protection regulators (Supervisory Authorities) in the European Union.

We need to consider the scope, types of personal data involved and what we're proposing to do. Projects likely to be considered 'high risk' include:

- 'Large-scale' profiling of individuals
- Using biometric, genetic or other special category data
- Matching different datasets
- Use of innovative technology, such as AI
- Tracking people's geolocation or behaviour
- Potentially 'invisible' activities, such as list brokering
- Targeting children or other vulnerable people

There are judgement calls to be made by businesses in assessing 'high-risk' and 'large-scale'. Even when a project doesn't necessarily meet mandatory requirements, a DPIA can be a helpful risk-assessment exercise.

Typical projects likely to need a DPIA



DPIA screening process

It's not always easy working out when a DPIA is necessary, or when it might just be useful. Businesses need to be in control of their exposure to risk, but don't want to burden their teams with unnecessary work, where risks are likely to be minimal.

Lack of clarity around when DPIAs are genuinely needed could lead businesses to carry out far more than needed – whilst others may carry out too few.

This is where a screening process can be an effective and methodical way to identify if a project does or does not require a DPIA.

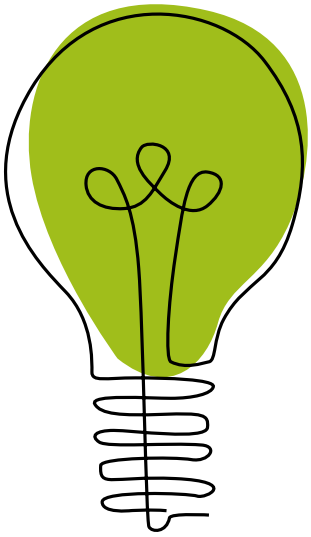
Different approaches can be taken, but a short set of standard questions can be used, which key stakeholders are asked to complete. These can then be assessed by the Data Protection Officer, data protection team or data protection lead.

A screening questionnaire could include:

- The nature and sensitivity of the personal data involved – does it include children's data or special category data such as health information?
- The source of the personal data – did we get data directly from people or not?
- What does the project/activity hope to achieve?
- Will the data be shared with other companies, and/or transferred overseas?
- Could what we're doing be considered particularly innovative, cutting edge?
- Is personal data being used for a new purpose? A purpose that's different from why we originally collected it.

The above is by no means an exhaustive list.

Easy-to-use DPIA process



We're unlikely to reap the benefits using an unwieldly DPIA template full of data protection jargon, with questions people just don't know how to answer.

A straight-forward template which is relatively easy for people to follow, will go a long way to helping to encourage people to engage and complete DPIAs.

The ICO has published a DPIA template, but there's nothing stopping this being adapted to different business needs. A simplified version could also be used for less complex projects.

There are some key elements we need to make sure the process covers to meet the requirements of UK/EU GDPRs.

- ✓ A description of the nature, scope, context and purpose
- ✓ An assessment of the necessity, proportionality and compliance measures
- ✓ Identification and assessment of risks to individuals
- ✓ Identification of additional measures to mitigate those risks.

Teams completing DPIAs need to be able to identify and assess data protection risks. Giving examples of the types of risks to look out for and the types of mitigating actions, can really help to streamline the process. Clear guidelines on how to complete a DPIA are invaluable.

Managing the process

9 key steps to managing the DPIA process

1. Consult with the DPO, privacy team or data protection lead
2. Brief stakeholders and document the new project / activity
3. Identify data protection risks
4. Assess the risks
5. Decide on actions. These may fall into 4 broad categories:

   Treat – take action to control or reduce risk

   Transfer – contract it out or insure against it

   Terminate – eliminate it; stop or change so risks are eliminated

   Tolerate – if risks are considered acceptable
6. Consult with the Regulator (e.g. ICO) if risks can't be mitigated
7. Complete and sign-off
8. Implement action plan
9. Review

DPIA awareness & training

We need to raise awareness of the DPIA requirements; for example meeting with key teams who are most likely to be aware of new projects and investments, such as Legal, Procurement, IT and/or Project teams.

Key team members need to have the skills to conduct a DPIA. A DPO, or data protection lead, can't be expected to do this single-handed. The ICO specifically calls out the need to provide specialist DPIA training.

DPIAs can feel a bit daunting, but the more familiar people are with the process, the risks they should be looking out for, along with the types of measures and controls that could be deployed to protect people's data, the easier it all becomes.

DPIA review

Once a DPIA is completed, review dates help to make sure there's ongoing monitoring and to check if anything has changed.

For example, a new app may have been developed, but six months later there's a desire to improve the functionality by adding new features – does this raise different data protection issues?

Reviewing and asking for feedback on the screening process, DPIA template, guidelines and training can also help to make the whole process more effective.

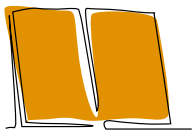
DATA PROTECTION NETWORK

About DPN

Founded in 2014, the Data Protection Network publishes news, insights and guides. Our experienced team regularly deliver bespoke data protection training across all sectors. We advise and support businesses, and frequently carry out data protection gap analysis reviews. The DPN also runs regular webinars where DPOs and other privacy professionals share their experiences and practical tips.

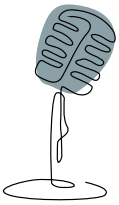
Consultancy

No-nonsense, practical data protection cunsultancy from our experienced team



Articles

News, insight and how-to-guides to support your day-to-day protection work



Events

Expert speakers share knowledge and tips on a range of privacy topics

Training

Down-to-earth data protection training workshops focused on developing your team's skills

Get in touch

Simon Blanchard
simon@dpnetwork.org.uk

Philippa Donn
phil@dpnetwork.org.uk

Sign up for DPN email updates
https://dpnetwork.org.uk/newsletter-sign-up/

www.dpnetwork.org.uk