This document is purely for guidance and does not constitute legal advice or legal analysis. It is intended as a starting point only, and organisations may need to seek independent legal advice when renewing, enhancing or developing their own processes and procedures or for specific legal issues and/or questions.
Data Protection Impact Assessment

You must carry out a Data Protection Impact Assessment (DPIA) where the type of processing of personal information envisaged, is likely to result in a high risk to the rights and freedoms of natural persons.

The types of processing needing a DPIA may include circumstances where you plan to:

- Process **special category data** on any scale;
- Systematically monitor a publicly accessible place;
- Systematically monitor employee activities, including the monitoring of the employees' workstation, internet activity etc;
- Use innovative technology;
- Carry out any form of profiling;
- Process either biometric or genetic data or in a combination of both;
- Combine, compare or match data from multiple sources;
- Process personal data in a way that involves tracking individuals' online or offline location or behaviour;
- 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;
- Use automated decision-making to make decisions about people.

You can consider carrying out a DPIA for any project involving the use of personal data.

**DPIA process checklist**

- Describe the nature, scope, context and purposes of the processing;
- Ask any third-party companies who are part of the change/introduction of a new process (data processors) to help understand and document their processing activities and identify any associated risks;
- Consider how best to consult individuals (or their representatives) and other relevant stakeholders;
- Check that the processing is necessary for and proportionate to your purposes and describe how you will ensure compliance with data protection principles.
Do an objective assessment of the likelihood and severity of any risks to individuals’ rights and interests;

Identify measures you can put in place to eliminate or reduce high risks;

Implement the measures you identified and integrate them into your project plan;

Consult the JOIC before processing, if you cannot mitigate risks, especially any high risks;

Keep your DPIAs under review and revisit them when necessary.

Have you written a good DPIA?

A good DPIA helps you to evidence 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

Have you;

- Explained why you needed a DPIA, detailing the types of intended processing that triggered its preparation;

- 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 you have used;

- Set out clearly the relationships between all parties using the personal data 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 you are complying with each of the Data Protection Principles under DPJL and clearly explained your lawful basis for processing (and special category conditions if relevant);

- Explained how you plan to support the relevant information rights of your 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 your consideration of any less risky alternatives to achieving the same purposes of the processing, and why you didn’t choose them;
Given details of stakeholder consultation (e.g. data subjects, representative bodies) and included summaries of findings;

Sought the advice of your data protection lead in your organisation;

Attached any relevant additional documents you referenced in your DPIA, e.g. privacy notices, consent documents;

Agreed and documented a schedule for review;

Consulted the JOIC if there are residual risks you cannot mitigate.