Data Protection Impact Assessment

This template is used to review and record our DPIA processes and outcomes.
It follows the process set out in the ICO's DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.
We complete a DPIA at the beginning of any major project involving the use of personal data on a large scale, or if we are making a significant change to an existing process that involves high risk to individuals' rights and freedoms. We will integrate the final outcomes into our project plan and implement them.

BASIC INFORMATION

Organisation:		**Manager Name:**	
Assessment Date:		**Initial to confirm completion:**	

Step 1: Identify the need for a DPIA

Outline what the project aims to achieve and what type of processing it involves. Where appropriate refer or link to other documents, such as a project proposal. Summarise why we identified the need for a DPIA.

<type here>

Step 2: Describe the processing

Describe the nature of the processing: how will we collect, use, store and delete data? What is the source of the data? Will we be sharing data with anyone? Where appropriate refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?

<type here>

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 we be collecting and using? How often? How long will we keep it? How many individuals are affected? What geographical area does it cover?

<type here>

Describe the context of the processing: what is the nature of our relationship with the individuals? How much control will they have? Would they expect us 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 we should factor in? Are we signed up to any approved code of conduct or certification scheme (once any have been approved)?

<type here>

Step 3: Consultation

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

<type here>

Step 4: Assess necessity and proportionality

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

<type here>

Step 5: Identify and assess risks

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote/ Possible/ Probable	**Severity of harm** Minimal / Significant / Severe	**Overall risk** Low / Medium / High
<type here>			
<type here>			

Step 6: Identify measures to reduce risk

Identify additional measures we could take to reduce or eliminate risks identified as medium or high risk in step 5

Risk	**Options to reduce or eliminate risk**	**Effect on risk** Eliminated/Reduced/Accepted	**Residual risk** Low/Medium/High	**Measure approved** Y/N
<type here>				
<type here>				

Step 7: Sign off and record outcomes

Item	**Name/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 ICO before proceeding.
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing should proceed.

Summary of DPO advice: <type here>		
DPO advice accepted or overruled by:	<name>	If overruled we must explain our reasons:
Comments: <type here>		
Consultation responses reviewed by:	<name>	If our decision departs from individual's views we must explain our reasons:
Comments: <type here>		
This DPIA will be kept under review by:	<name>	The DPO should also review ongoing compliance with the DPIA