**DATA PROTECTION IMPACT ASSESSMENT TEMPLATE**

Preface

This template is for the recording of your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the [Criteria for an acceptable DPIA](http://ec.europa.eu/newsroom/document.cfm?doc_id=47711) set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan and updates to the Data Asset Register. Please also see the checklist on the final page of this document.

Before You Start

First check whether a DPIA is required at all. If you would answer “Yes” to any of the following, you need to complete a DPIA:

☑️ We are introducing a new process, system or service that will collect or use new personal data, or use existing personal data for something new.

☑️ We’re changing the way we handle personal data currently, or changing who has access to it, or changing when we delete it.

☑️ We are considering sharing personal data with an external organisation, or receiving personal data from an external organisation for some purpose.

☑️ We currently pass personal data to a company or other organisation to do something for us and we’re considering changing that company or organisation.

☑️ We’re going to merge data from more than one source or between more than one organisation.

☑️ There’s some other factor that might affect the privacy or data protection rights of our data subjects (e.g. a change in legislation or external requirements).

This is intended as a guide and is not a comprehensive list – you should still consult the DPIA Process document and relevant legislation.

If you make an assessment that a full DPIA is **not** required, you should keep a record of this decision and the considerations that lead to it for future reference and justification.

If you determine that a DPIA **is** required, please complete this form and submit it in accordance with the DPIA Process.

# 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 high 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’s 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 actually 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 risksas 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 high 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/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 |
| Updates required to Data Asset Register required and made: |  | Update the data asset register to take account of the new/changed data collection/processing |
| 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 on-going compliance with DPIA |
| Signatures (to confirm actions and agreement noted in this document): | Data Process/Product Owner: | Date: |
| Data Protection Officer: | Date: |

**Checklist:**

* Have you completed all relevant sections?
* Have you considered and documented all data processing/collection required and concluded that this is all necessary?
* Have the risks been calculated reasonably and accurately?
* Have you mitigated as much of the risk as possible?
* Have you obtained assurances about sharing of the data and any security arrangements from any third parties?
* Have you communicated how the information will be used to the data subjects concerned?
* Do you have written contracts in place to cover all data-related aspects?
* Have you updated the Data Asset Register, as appropriate?