



## Data Protection Impact Assessment – Name of Project

This template is for you to record your DPIA process and outcome. Guidance on how to complete this DPIA can be found in the ICB Data Protection and Security policy. The template follows the process set out in the [Data Protection Impact Assessments (DPIAs) | ICO](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-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.

|  |
| --- |
| Step 1: Identify the need for a DPIA |
| **Identify the need for a DPIA.** You may find it helpful to refer or link to other documents, such as a project proposal. [Click here for guidance on this section.](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how5) |
| * 1. **Explain broadly what your project aims to achieve and what type of processing it involves.**

Text* 1. **Summarise why you identified the need for a DPIA.**

Text |

|  |
| --- |
| Step 2: Describe the processing |
| **Describe the nature of the processing.** You might find it useful to refer to a flow diagram or other way of describing data flows. [Click here for guidance on this section.](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how6) |
| * 1. **How will you collect, use, store and delete data?**

Text* 1. **What is the source of the data?**

Text* 1. **Will you be sharing data with anyone?**

Text* 1. **What types of processing identified as likely high risk are involved?**

Text |

|  |
| --- |
| **Step 2.1: Describe the scope of the processing.**  |
| * + 1. **What is the nature of the data, and does it include special category or criminal offence data?**

Text* + 1. **How much data will you be collecting and using?**

Text* + 1. **How often?**

Text* + 1. **How long will you keep it?**

Text* + 1. **How many individuals are affected?**

Text* + 1. **What geographical area does it cover?**

Text |

|  |
| --- |
| **Step 2.2: Describe the context of the processing.**  |
| * + 1. **What is the nature of your relationship with the individuals?**

Text* + 1. **How much control will they have?**

Text* + 1. **Would they expect you to use their data in this way?**

Text* + 1. **Do they include children or other vulnerable groups?**

Text* + 1. **Are there any prior concerns over this type of processing or security flaws?**

Text* + 1. **Is it novel in any way?**

Text* + 1. **What is the current state of technology in this area?**

Text* + 1. **Are there any current issues of public concern that you should factor in?**

Text* + 1. **Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?**

Text |

|  |
| --- |
| **Step 2.3:** **Describe the purposes of the processing.** |
| * + 1. **What do you want to achieve?**

Text* + 1. **What is the intended effect on individuals?**

Text* + 1. **What are the benefits of the processing – for you, and more broadly?**

Text |

|  |
| --- |
| Step 3: Consultation Process |
| **Consider how to consult with relevant stakeholders.** [Click here for guidance on this section.](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how8) |
| * 1. **Describe when and how you will seek individual’s views – or justify why it’s not appropriate to do so.**

Text* 1. **Who else do you need to involve within your organisation?**

Text* 1. **Do you need to ask your processors to assist?**

Text* 1. **Do you plan to consult information security experts, or any other experts?**

Text |

|  |
| --- |
| Step 4: Assess necessity and proportionality |
| **Describe compliance and proportionality measures.** [Click here for guidance on this section.](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how9) |
| * 1. **What is your lawful basis for processing?**

Text* 1. **Does the processing actually achieve your purpose?**

Text* 1. **Is there another way to achieve the same outcome?**

Text* 1. **How will you prevent function creep?**

Text* 1. **How will you ensure data quality and data minimisation?**

Text* 1. **What information will you give individuals (for transparency purposes)?**

Text* 1. **How will you help to support their rights (in relation to data protection e.g. subject access)?**

Text* 1. **What measures do you take to ensure processors comply?**

Text* 1. **How do you safeguard any international transfers?**

Text |

|  |
| --- |
| Step 5: Identify and assess risks (see Appendix A) |
| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risksas necessary. [Click here for guidance on this section.](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how10) | **Likelihood of harm** | **Severity of harm** | **Overall risk**  |
| **Risk** |  | Rare, unlikely, possible, likely, or almost certain | Negligible, minor, serious, major, catastrophic | Low, moderate, significant, or high |
| **1.** |  |  |  |  |
| **2.** |  |  |  |  |
| **3.** |  |  |  |  |
| **4.** |  |  |  |  |
| **5.** |  |  |  |  |
| **6.** |  |  |  |  |
| **7.** |  |  |  |  |
| **8.** |  |  |  |  |

|  |
| --- |
| Step 6: Identify measures to reduce risk (see Appendix A) |
| **Identify additional measures you could take to reduce or eliminate risks identified as moderate, significant, or high risk in step 5.** [Click here for guidance on this section.](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how11) | **Effect on risk** | **Residual risk** | **Measure approved** |
| **Risk Number** |  | Eliminated reduced accepted | Low, moderate, significant, or high | Yes/no |
| **1.** |  |  |  |  |
| **2.** |  |  |  |  |
| **3.** |  |  |  |  |
| **4.** |  |  |  |  |
| **5.** |  |  |  |  |
| **6.** |  |  |  |  |
| **7.** |  |  |  |  |
| **8.** |  |  |  |  |

|  |
| --- |
| Step 7: Sign off and record outcomes  |
| **FOR DSP TEAM USE ONLY** |
| **Item**  | **Name/date** | **Notes** |
| 1. DPIA submitted to DSPAT
 | Name: Date:  | DPIA reviewed by DSPAT and either returned to author with comments or forwarded to IAO panel. Note advice below.  |
| Summary of DPO / DSP Team advice: |
| 1. Date referred to IAO panel
 | Date:  |  |
| Summary of IAO comments: |
| Residual risks approved by: | N/A | If accepting any residual high risk, consult the ICO before going ahead |
| 1. IAO DPIA panel responses reviewed & accepted by author:
 | Name: Date:  |  |
| Comments: |
| 1. This DPIA will kept under review by:
 |  | The DPO should also review ongoing compliance with DPIA |
| Comments: |
| 1. DPIA approved by DPO:
 |  |  |

 Appendix A

|  |  |
| --- | --- |
| **Risk Matrix** | **Likelihood** |
| **Severity** | **1****Rare** | **2****Unlikely** | **3****Possible** | **4****Likely** | **5****Almost Certain** |
| **5 Catastrophic** | 5 | 10 | 15 | 20 | 25 |
| **4 Major** | 4 | 8 | 12 | 16 | 20 |
| **3 Serious** | 3 | 6 | 9 | 12 | 15 |
| **2 Minor** | 2 | 4 | 6 | 8 | 10 |
| **1 Negligible** | 1 | 2 | 3 | 4 | 5 |
| **Key to Risk Register rating:** |
| Low RiskGreen 0-3 | Moderate RiskYellow 4-6 | Significant RiskOrange 8-12 | High RiskRed 15-25 |
|  |
| **RISK ASSESSMENT:** [using the matrix above] |
| **INITIAL risk rating – step 5**(before any mitigating actions have been implemented) | Severity (example)4 | Likelihood (example)4 | Total (example)16 |
| **CURRENT risk rating – step 6**(at time of writing, taking account of existing controls and mitigating actions) | Severity (example)3 | Likelihood (example)4 | Total (example)12 |