# Appendix 1: DPIA Template

DPIA template

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.

Contents

[Submitting controller details 1](#_Toc71640183)

[Step 1: Identify the need for a DPIA 2](#_Toc71640184)

[Step 2: Describe the processing 4](#_Toc71640185)

[Step 3: Consultation process 7](#_Toc71640186)

[Step 4: Assess necessity and proportionality 8](#_Toc71640187)

[Step 5: Identify and assess risks 9](#_Toc71640188)

[Step 6: Identify measures to reduce risk 9](#_Toc71640189)

[Step 7: Sign off and record outcomes 10](#_Toc71640190)

# Submitting controller details

|  |  |
| --- | --- |
| Name of Controller |  |
| Subject / Title of DPO |  |
| Name of Controller Contact /DPO  (delete as appropriate) |  |

# Step 1: Identify the need for a DPIA – Screening Checklist

|  |  |  |
| --- | --- | --- |
| **To determine whether a DPIA needs to be undertaken review the following questions. If you answer “Yes” to any of the questions you will need to complete a DPIA.** | | |
| **DPIA Screening Criteria** | **Yes** | **No** |
| 1. Does the project involve the processing of personal data? |  |  |
| 1. Does the project plan to carry out any other: 2. evaluation or scoring? 3. automated decision-making with significant effects? 4. systematic monitoring? 5. processing of sensitive data or data of a highly personal nature? 6. processing on a large scale? 7. processing of data concerning vulnerable data subjects? 8. innovative technological or organisational solutions? 9. processing that involves preventing data subjects from exercising a right or using a service or contract? |  |  |
| 1. Will the processing use systematic and extensive profiling or automated decision-making to make significant decisions about people? |  |  |
| 1. Will the processing involve special-category data or criminal-offence data on a large scale? |  |  |
| 1. Will the processing systematically monitor a publicly accessible place on a large scale? |  |  |
| 1. Will the processing use innovative technology in combination with any of the criteria in the European guidelines? |  |  |
| 1. Will the processing use profiling, automated decision-making or special category data to help make decisions on someone’s access to a service, opportunity or benefit? |  |  |
| 1. Will the project involve profiling on a large scale? |  |  |
| 1. Will the project involve the processing biometric or genetic data in combination with any of the criteria in the European guidelines |  |  |
| 1. Will the processing include combining, comparing or matching data from multiple sources? |  |  |
| 1. Will the project process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines? |  |  |
| 1. Will the project process personal data in a way that involves tracking individuals’ online or offline location or behaviour, in combination with any of the criteria in the European guidelines? |  |  |
| 1. Will the project process children’s personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them? |  |  |
| 1. Will the project process personal data that could result in a risk of physical harm in the event of a security breach? |  |  |
| 1. Does the project change the nature, scope, context or purposes of our current processing? |  |  |

|  |
| --- |
| 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

|  |
| --- |
| 1. **Describe the nature of the processing by answering the following questions:** |
| 1. How will you collect the data? |
|  |
| 1. How will you use the data? |
|  |
| 1. Who will have access to the data? |
|  |
| 1. Will you be sharing the data with anyone? Who? Where? Why? |
|  |
| 1. Will you be using any data processors? Who? Where? Why? |
|  |
| 1. Is a Data Sharing Agreement needed? |
|  |
| 1. If the data is being transferred outside of the UK is this covered by an adequacy decision, appropriate safeguards, or exemption? |
|  |
| 1. How long will you keep the data for? |
|  |
| 1. How will you delete the data? |
|  |
| 1. How will you store the data? |
|  |
| 1. What security measures will be / are in place to keep the data secure? |
|  |
| 1. Will any new technologies be used to process the data? |
|  |
| 1. Will you be using any novel types of processing? |
|  |
| 1. Referring to Step 1, what screening criteria identify that the process is likely to be high risk? |
|  |
| 1. Have you produced and attached a data flow map for this processing? |
|  |

|  |
| --- |
| 1. **Describe the scope of the processing by answering the following questions:** |
| 1. What is the nature (type and variety) of the personal data that will be processed? |
|  |
| 1. Will the data include any special category or criminal offence data? |
|  |
| 1. How much data will you be collecting and using? |
|  |
| 1. How often will you be collecting the data? |
|  |
| 1. How many individuals are / will be affected? |
|  |
| 1. How long will the data processing be in effect for? |
|  |
| 1. What geographical area(s) does the processing cover? |
|  |
| 1. **Describe the context of the processing by answering the following questions:** |
| 1. What / who is the source of the data? |
|  |
| 1. What is the nature of your relationship with the individuals? |
|  |
| 1. Would the individuals expect you to use their data in this way? |
|  |
| 1. Do the individuals include children or other vulnerable groups? |
|  |
| 1. How much control will individuals have over their data? |
|  |
| 1. Do you have any previous experience of this type of data processing? |
|  |
| 1. What is the current state of technology in this area? |
|  |
| 1. Are there prior concerns over this type of processing or security flaws? |
|  |
| 1. Is the processing novel in any way? |
|  |
| 1. Are there any current issues of public concern that you should factor in? |
|  |
| 1. Does the processing comply with any UK GDPR codes of conduct (once any have been approved under Article 40) or UK GDPR certification schemes? |
|  |
| 1. Have you have considered and complied with relevant codes of practice? |
|  |
| 1. **Describe the purposes of the processing by answering the following questions:** |
| 1. What do you want to achieve by processing this personal data? What are your legitimate interests? |
|  |
| 1. What is the intended effect on individuals? |
|  |
| 1. What are the benefits of the processing – for you, and more broadly for society as a whole? |
|  |

# Step 3: Consultation process

|  |
| --- |
| 1. **Consider how to consult with relevant stakeholders by answering the following questions:**   *You should seek and document the views of individuals (or their representatives) unless there is a good reason not to.* |
| 1. Describe when and how you will seek individuals’ views – or justify why it’s not appropriate to do so (for example, if consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable). |
|  |
| 1. Who else do you need to involve within your organisation? |
|  |
| 1. Do you need to ask your data processors to assist? |
|  |
| 1. Do you plan to consult information security experts, or any other experts (for example, IT or legal experts, sociologists or ethicists)? |
|  |
| 1. Do you need to carry out a more general public consultation process, or targeted research (for example, if the DPIA covers a plan to collect the personal data of individuals you have not yet identified)? This could take the form of market research with a certain demographic or contacting relevant campaign or consumer groups for their views. |
|  |

# Step 4: Assess necessity and proportionality

|  |
| --- |
| 1. **Describe compliance and proportionality measures, in particular:** |
| 1. What is your lawful basis for processing? |
|  |
| 1. Does the processing actually achieve your purpose? |
|  |
| 1. Is there another way to achieve the same outcome? |
|  |
| 1. How will you prevent function creep? |
|  |
| 1. How will you ensure data quality and data minimisation? |
|  |
| 1. What information will you give individuals? |
|  |
| 1. How will you help to support their rights? |
|  |
| 1. What measures do you take to ensure processors comply? |
|  |
| 1. 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/position/date** | ***Notes*** |
| DPIA completed by: |  |  |
| DPIA signed off by Senior Manager: |  |  |
| Measures approved by IGSSG: |  | *Integrate actions back into project plan, with date and responsibility for completion* |
| Residual risks approved by IGSSG: |  | *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* |
| *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 ongoing compliance with DPIA* |