**How to use this DPIA template**

Our DPIA template is split into two parts:

**Part 1: DPIA Guidance and Screening Questions.**

This section will help you to identify whether the processing of personal data is (a) necessary and (b) likely to result in a high risk to individuals requiring the completion of a full DPIA. Use the screening questionnaire on the following pages to record the outcome of your DPIA screening exercise.

**Part 2: Full DPIA.**

Where one or more of the mandatory screening questions are answered YES, a full DPIA will be required. (See Part 2 of this template).

If you are unsure whether you need to complete a full DPIA, please return your *completed* screening questionnaire to i-west@bathnes.gov.uk We will review it for you and advise whether a full DPIA is needed.

More information on how to complete a DPIA more generally can be found in [Appendix 1](#apx1).

**What is a Data Protection Impact Assessment?**

A Data Protection Impact Assessment (DPIA) is a risk assessment to help you to identify and minimise data protection risks associated with processing personal data.

Under the UK GDPR it is a legal requirement to complete a DPIA for any processing (use) of personal data that is likely to result in a *high risk* to individuals. This includes changes to existing processes, as well as new projects. You can use this screening questionnaire to determine whether your project/system/processing is high risk and requires a DPIA. The DPIA should be undertaken before processing commences.

It is also best practice to complete a DPIA for any major projects that require you to process personal data, such as the adoption of new information systems and services. As well as meeting the legal requirement, completing a DPIA could help avoid unnecessary costs, help protect your reputation, and provide assurance to stakeholders, such as your Audit & Risk Committee, about the safety of processing.

## Who should complete the DPIA?

The DPIA should be coordinated by the project lead or somebody who has a good understanding of what the processing will involve. Completion of the DPIA is likely to need the involvement of several stakeholders e.g. IT, HR, system provider, and end users, and shouldn’t rest with one person solely.

It is a legal requirement to consult your Data Protection Officer (DPO) regarding the completion of a DPIA. The DPO’s role is to advise on and monitor the DPIA. It is not the DPO’s responsibility to complete the DPIA as they will not have enough knowledge of the project or processing involved.

## DPIA Screening Questions

|  |  |
| --- | --- |
| **Organisation**  |  |
| **Project name** |  |
| **Project manager** |  |
| **Date**  | Click or tap to enter a date. |

|  |
| --- |
| Aim & Purpose of the project / processing  |
| What are you hoping to achieve from this project / change? Why is it necessary? Is it for compliance with a legal obligation or statutory guidance?  |
| The aim of the project is to: enter the aim of this processing.This is: select whether this is new processing or changes to existing processingWithout this project / change: explain what the impact would be if this doesn’t happen.The project / processing is necessary because: explain why the processing is necessary.The legislation / statutory guidance this project supports (if applicable) is: enter legal/regulatory requirements. |

|  |  |  |
| --- | --- | --- |
| 1. **Higher Risk Factors**
 | **Yes** | **No** |
| 1. Will the project involve **large scale processing** of personal data?
 | [ ]  | [ ]  |
| 1. Will the project involve **profiling** or **monitoring or automatic decision making**?
 | [ ]  | [ ]  |
| 1. Does the project involve **special category\* or criminal offence data** or the use of the personal data of **vulnerable individuals (including children)**?

*\*special category data includes: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health information, sex life or sexual orientation.* | [ ]  | [ ]  |
| *If you’ve answered YES to any of the questions above, it is highly recommended that you conduct a DPIA regardless of the mandatory screening questions below. If you decide not to complete a DPIA, then you should retain this form along with a record of your decisions. Please contact the DPO for advice.* |

|  |  |  |
| --- | --- | --- |
| 1. **Mandatory Risk Factors for a full DPIA**

**This project does / will…** | **Yes** | **No** |
| 1. Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
 |[ ] [ ]
| 1. Process special category or criminal offence data on a large scale.
 |[ ] [ ]
| 1. Systematically monitor a publicly accessible place on a large scale (e.g. CCTV).
 |[ ] [ ]
| 1. Use innovative technologies or the novel application of existing technologies (including AI) (e.g. innovative systems, programs, websites, databases etc.)
 |[ ] [ ]
| 1. Use profiling or special category data to make decisions on someone’s access to a service, opportunity, or benefit.
 |[ ] [ ]
| 1. Profile individuals’ personal data on a large scale.
 |[ ] [ ]
| 1. Use biometric data, such as fingerprints and facial features (e.g. for cashless catering, or access controls).
 |[ ] [ ]
| 1. Use genetic data, such as an individual’s gene sequence.
 |[ ] [ ]
| 1. Combine, compare or match datasets from multiple sources.
 |[ ] [ ]
| 1. Use personal data that has not been obtained directly from the data subject without providing a privacy notice to the individual.
 |[ ] [ ]
| 1. Use personal data in a way that involves tracking individuals’ online or offline location or behavior.
 |[ ] [ ]
| 1. Process children’s or other vulnerable individuals’ personal data for marketing purposes, profiling or automated decision-making. Or offering online services directly to children.
 |[ ] [ ]
| 1. Risks physical harm in the event of a security breach.
 |[ ] [ ]

If you answered ‘YES’ to any of the questions in section 3 above, then you must complete a full DPIA (please use **Part 2** of this template).

Please note that it is best practice to complete a DPIA (risk assessment) whenever you undertake a major project involving the use of personal data.

## DPO Review

|  |  |
| --- | --- |
| **DPO Name** | Click or tap here to enter One West representative name. |
| **Date of DPO Review** | Click or tap to enter a date. |
| **DPO Advice** | Click to select. |

**Appe****ndix 1 – Further information**

Crucially, a DPIA needs to:

* Describe the nature, scope, context and purposes of the processing
* Assess necessity, proportionality and compliance of processing.
* Identify and assess risks to individuals.
* Describe any additional measures to mitigate those risks.

A DPIA should be done early in the life of a project. Certainly, before you start the processing, but ideally during the planning and development phases of a project. Importantly, assessing risk this way is a cyclical activity – see the diagram below.



*Figure 1 - DPIA Cycle*

A crucial part of the process involves consulting with your DPO, One West. One West is there to help and ultimately One West will have to sign-off the DPIA.

Note, if you identify a high risk that you cannot mitigate, you may need to consult the ICO. Again, One West will advise you if that is the case and help prepare a question for the ICO.

**Who is responsible for carrying out a DPIA?**

The data controller is ultimately responsible for completing a DPIA although they can allocate the task to someone who would be responsible day-to-day for that processing.  For example, the Head of HR or the Business Manager, who probably know most about the organisation’s HR system, might be given the job.

Importantly, the assessor may also need to work with internal experts, such as the Head of IT, as well as other processors (contractors) and certainly the supplier / vendor to get an accurate view of risk/s.

Again, the assessor can consult with One West while completing the DPIA. For new processes / services the project lead should contact the DPO, as early as possible.

Note it is not the DPO’s responsibility to complete the DPIA. They do not have complete knowledge of the data processing activity. Nonetheless, they may have encountered similar risk while working with other trusts / schools.

This dialogue with the DPO should be recorded as part of the process.