**What are Data Protection Impact Assessments?**

Data Protection Impact Assessments (DPIAs) are structured assessments of the potential impact on privacy for high risk processes, and help us to identify the most effective way to comply with data protection obligations. The DPIA should form part of the overall risk assessment of the process or project.

A DPIA helps us to:

* Anticipate and address the likely impacts
* Identify privacy risks to individuals
* Foresee problems and negotiate solutions
* Avoid unnecessary costs
* Protect the organisation’s reputation
* Offer assurance to stakeholders
* Meet legal requirements

The DPIA process is not only a legal requirement, but is also an important tool to help you identify and minimise the data protection risks of a project that involves processing personal data.

The DPIA process is relevant to initiatives involving the use of personal data and is particularly important when a new business process or technology initiative involves the collection, recording, sharing or retention of personal data.

The DPIA enables privacy and data protection considerations to be made in the early stages of a project, where any identified problems can be easier to resolve, rather than late or retrospective considerations where solutions can be costlier or delay implementation. A DPIA can also identify whether the project should be continued, when balanced with the rights and interests of persons affected.

The DPIA process will consider privacy in the way individual’s personal data is used. This can involve privacy about: the integrity of the individual, the person, their personal information, their personal behaviour and their personal communications.

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

The responsibility for conducting a Data Protection Impact Assessment (DPIA) lies with the Information Asset Owner (IAO) for a project and is produced as part of the project proposal. The IAO will often be the Project Manager/Lead. When a new project/initiative involving the processing of personal information is being considered, the IAO should contact the Data Protection Officer (DPO) to discuss the proposal. At this stage it may be identified that it is necessary to undertake a DPIA.

The DPIA itself should be completed by somebody who is associated with the business area of the processing activity and who has a good understanding of what the processing will involve. It is unlikely that a DPIA can be completed by one person and is likely to involve a number of stakeholders, for example IT.

It is not the DPO’s responsibility to complete the DPIA, as they will not have enough knowledge of the data processing activity. The role of i-west is to advise and monitor the DPIA and to sign it off when it is complete.

**Review**

The DPIA should be reviewed annually, or wherever the system or method of handling used changes. This may be a significant change to a computer system or a change of policy or legislation.

**What is high risk?**

A high risk is considered to exist when particularly sensitive personal data is processed, a large volume is held, CCTV is in place, or any factor exists where personal data may be breached. High risk can result from a high probability of some harm, or a lower probability of serious harm.

Particularly sensitive data or ‘special category data’ includes:

* race
* ethnic origin
* politics
* religion
* trade union membership
* genetics
* biometrics (where used for ID purposes)
* health
* sex life; or
* sexual orientation

There are separate and specific safeguards for criminal offence data, but they should also be included, for example where processed by HR.

If a high risk is identified that you cannot mitigate, you must consult the Information Commissioner before starting the processing. The ICO will give written advice within eight weeks, or 14 weeks in complex cases. I-west can advise you on this.

There is a legal requirement to consult with the DPO regarding the completed DPIA. If the service is unable to identify a control measure to bring the residual risk to an acceptable level, there is also a statutory obligation to consult with the Information Commissioner’s Office.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Project information** | | | | | |
| **Project name** |  | | | **Document version no.** |  |
| **Author(s)** |  | | | **Version date** |  |
| **Information asset owner** |  | | **Project manager (if different)** |  | |
| **Version no.** | **Version date** | **Summary of key changes** | | | |
|  |  |  | | | |
|  |  |  | | | |
|  |  |  | | | |
|  |  |  | | | |
|  |  |  | | | |

|  |  |
| --- | --- |
| **Do I need to complete a DPIA?** | **Y/N** |
| Will the project involve the collection of new information about individuals? |  |
| Will the project compel individuals to provide information about them? |  |
| Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? |  |
| Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? |  |
| Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition. |  |
| Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them? |  |
| Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private. |  |
| Will the project require you to contact individuals in ways which they may find intrusive? |  |

If you have answered “Yes” to any of the above questions, a DPIA needs to be completed.

|  |
| --- |
| **1. Outline of the project, objectives and benefits** |
| What does the project aim to achieve, including what the benefits will be to the organisation, to individuals and to other parties?  If this is not a new process, but a change to an existing, please describe the proposed changes. |
|  |

|  |
| --- |
| **2. Describe the intended use of personal data** |
| **a) Describe the nature of the processing**  The nature of the processing is what you plan to do with the personal data. This should include:   * How you collect the data * How you store the data * How you use the data * Who has access to the data * Who you will and/or may share the data with * Whether you use any data processors * Retention period(s) * Security measures * Whether there will be any profiling (fully automated decision-making) * Whether you are using any new technologies * Whether you are using any novel types of processing |
|  |

|  |
| --- |
| **b) Describe the scope of the processing**  The scope of the processing is what the processing covers. This should include:   * The nature of the personal data * The volume and variety of the personal data * The sensitivity of the personal data * The extent and frequency of the processing * The duration of the processing * The estimated number of the data subjects involved * The geographical area covered |
|  |

|  |
| --- |
| **c) Describe the context of the processing**  The context of the processing is the wider picture, including internal and external factors which might affect expectations or impact. This might include, for example:   * The source of the data * The nature of your relationship with the individuals * The extent to which individuals have control over their data * The extent to which individuals are likely to expect the processing * Whether they include children or other vulnerable people * Any previous experience of this type of processing * Any relevant advances in technology or security * Any current issues of public concern * Whether you have considered and complied with any relevant Codes of Practice |
|  |

|  |
| --- |
| **d) Describe the purposes of the processing**  The purpose of the processing is the reason why you want to process the personal data. This should include:   * Statutory requirement * Your legitimate interests, where relevant * The intended outcome for individuals * The expected benefits for you or for society as a whole * The impact on the organisation if we don’t do it |
|  |

|  |
| --- |
| **3. Data protection compliance** |
| **Principle 1: Use of personal data is fair, lawful and transparent**  This section makes reference to Articles 6, 9 and 10 of GDPR, to demonstrate the lawful basis for carrying out the activity. If in any doubt, please consult your DPO [i-west@bathnes.gov.uk](mailto:i-west@bathnes.gov.uk) |
| (a) We are relying on the following Article 6 basis for the processing of personal data: (delete lines that don’t apply)   |  | | --- | | **Consent** | | If you are relying on consent, how will the consent be recorded?  How can the individuals withdraw their consent? | | **Necessary for the performance or the setting up of a contract** | | **Necessary for compliance with a legal obligation** | | State the specific set(s) of legislation | | **Necessary to protect the vital interests of a person** | | **Necessary for the performance of a task carried out in the public interest, or in the exercise of our official authority** | | To rely on this condition, the task or function must have a clear basis is law. State the specific set(s) of legislation | | **Necessary for the pursuit of our legitimate interests** | | State your legitimate interests  State what would happen if this processing didn’t happen |   (b) We are relying on the following Article 9 basis for the processing special category data: (delete lines that don’t apply)   |  | | --- | | **NO SPECIAL CATEGORY DATA** | | **Explicit consent** | | If you are relying on consent, how will the consent be recorded?  How can the individuals withdraw their consent? | | **Necessary for compliance with employment, social security or social protection law** | | State which condition of [Schedule 1](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted), Part 1 of the Data Protection Act 2018 is met | | **Necessary to protect the vital interests of a person, where they are physically or legally incapable of giving consent** | | **Processing is carried out by a not-for-profit organisations, and only relates to members of that organisation** | | **The information has been made public by the individual(s)** | | **Necessary for the establishment, exercise or defence of legal claims** | | **Necessary for reasons of substantial interest** | | State which condition of [Schedule 1](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted), Part 2 of the Data Protection Act 2018 is met | | **Necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services** | | State which condition of [Schedule 1](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted), Part 1 of the Data Protection Act 2018 is met | | **Necessary for reasons of public health** | | State which condition of [Schedule 1](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted), Part 1 of the Data Protection Act 2018 is met | | **Necessary for archiving, scientific, historical or statistical research** | | State which condition of [Schedule 1](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted), Part 1 of the Data Protection Act 2018 is met |   (c) We are relying on the following Article 10 basis for the processing of information relating to criminal convictions or offences: (delete lines that don’t apply)   |  | | --- | | **NO INFORMATION RELATING TO CRIMINAL CONVICTIONS OR OFFENCES** | | **We have official authority or statutory functions for law enforcement purposes** | | State what gives you [official authority](http://www.legislation.gov.uk/ukpga/2018/12/schedule/7/enacted) | | **The activity meets the following condition(s) within Schedule 1, Parts 1, 2 or 3 of the Data Protection Act 2018** | | State which condition of [Schedule 1](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted) is met |   (d) Explain how individuals will be made aware of the processing  (e) If your service is subject to the Human Rights Act:   * Will your actions interfere with the right to privacy under Article 8? * Have you identified the social need and aims of the project? * Are your actions a necessary and proportionate response to the social need? |

|  |
| --- |
| **Principle 2: Personal data shall be collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes** |
| (a) If collecting personal data for primary use, explain how you have targeted only the information required  (b) If you are reusing personal data for further use, explain how this secondary use is compatible with the original reason it was collected. |

|  |
| --- |
| **Principle 3: Use of personal data is adequate, relevant and no more than necessary** |
| Explain how the amount of personal data you intend to use is enough to be understood by the audience but no more than the minimum needed to achieve your purpose |

|  |
| --- |
| **Principle 4: Personal data must be accurate and kept up to date** |
| (a) Explain how accurate recording of data will be achieved and how it will be kept up to date, where necessary  (b) Explain any mechanisms that will allow you to amend or append data that is found to be inaccurate |

|  |
| --- |
| **Principle 5: Personal data must be kept in an identifiable format for no longer than is necessary** |
| (a) **Data held in the new IT System:** explain how any automated and / or manual capability to delete data will be used to comply with the corporate retention schedule  (b) **Data held in an unstructured manner (paper, word / excel files etc):** explain how you will use any automated and / or manual capability to delete data in line with the corporate retention schedule  (c) Explain how automatic destruction of individual records can be frozen on request |

|  |
| --- |
| **Principle 6: Personal data must be protected against unauthorised / unlawful use, accidental loss, damage or destruction** |
| (a) Explain any technical security measures that will be put in place to protect the data  (b) Explain how you will make staff aware of any security measures or procedures they will need to follow |

|  |
| --- |
| **Articles 15 – 22: Rights of the data subject** |
| Explain how individual rights (requests for subject access, restriction, rectification, objection, erasure and/or portability) will be managed |

|  |
| --- |
| **Articles 44- 49: Transfers of personal data to third countries or international organisations** |
| (a) Explain where the personal data will be hosted, including the routes of transfer if they leave the UK (for example, while most Microsoft cloud services are based in Europe, the data sometimes goes via America)  (b) If the personal data leaves the UK, explain which of the formal / recognised adequacy measures are in place |

|  |
| --- |
| **Demonstration of compliancy with data protection legislation (accountability)** |
| (a) Explain what (if any) governance documents will be required to support the data processing (eg Information Sharing Agreements, Data Processor contractual clauses etc)  (b) Detail what governance arrangements will be in place to oversee the processing of personal data in a compliant manner |

|  |
| --- |
| **4. Consultation** |
| **(a) The following consultation approach and stakeholder groups were incorporated into the consultation process:** |
|  |
| **(b) A summary of the stakeholder views:** |
|  |
| **(c) The following stakeholder views were taken into consideration and measures to support them have been included in the planned data processing activities:** |
|  |
| **(d) The following stakeholder views were considered, but not reflected in the planned data processing activities:** |
|  |
| **(e) The rationale for not doing so:** |
|  |

\*\*\* Section 5 is for Local Authorities or Health organisations only. For all other organisations, this section can be deleted \*\*\*

|  |
| --- |
| **5. NHS National Data Opt-Out Programme (for processing of records relating to Health and/or Adult Social Care records only)** |
| **(a) How does the processing meet the Common Law Duty of Confidentiality?** |
|  |
| **(b)Will the processing be impacted by the NHS National Data Opt-Out Programme?**  **\*\*\*TO BE COMPLETED BY THE CALDICOTT GUARDIAN\*\*\*** |
|  |

**Risk assessment**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Privacy issue** | *Identify the key privacy risks and associated compliance and corporate risks* | | | *Describe the actions you could take to reduce the risks* | | |
| **Risk to individual** | **Compliance risk** | **Corporate risk** | **Solution(s)** | **Result**  *High, medium or low* | **Evaluation**  *Is the solution a justified, compliant and proportionate response?* |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**Outcomes**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk** | **Approved solution and actions** | **Approved by** | **Completion due date** | **Who is responsible?** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |
| --- | --- |
| **DPIA authorisation** | |
| **Date of consultation with DPO** |  |
| **Summary of DPO advice** |  |
| **DPO advice accepted or over-ruled by IAO** |  |
| **Rationale for over-ruling the DPO’s advice (if applicable)** |  |
| **Date and name of person referring DPIA to ICO (if applicable)** |  |
| **Summary of ICO advice** |  |
| **Date and name of person updating Record of Processing Activity** |  |