**Data Protection Impact Assessment (DPIA)**

A **Data Protection Impact Assessment (DPIA)** is one of the mandatory [suitable and specific measures](https://www.hrb.ie/funding/gdpr-guidance-for-researchers/gdpr-and-health-research/suitable-and-specific-measures-for-health-research/) for the processing of personal data for the purposes of health research in (Regulation 3(1))

It is a procedure designed to determine the risks involved in data processing, retention and collection operations. The aim of a DPIA is to generate mitigation strategies to improve compliance.

It also ensures that appropriate arrangements have been identified for when the research has been completed in order **to anonymise, properly archive or securely destroy that data.**

In summary, a DPIA should:

* Describe the nature, scope, purpose and context of the data processing.
* Assess the necessity of said data use in proportion to compliance measures.
* Identify and assess the risks to individuals.
* Identify any additional measures your organisation could take to mitigate those risks.

DPIA Template

**Title of Study:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Conducting a Data Protection Impact Assessment (DPIA) is in TWO stages.**  **Stage 1 - Identification of the Need for a DPIA through a DPIA Threshold Assessment -** A threshold assessment is a short, initial assessment of a project to determine whether its potential privacy impact requires a DPIA.  **Stage 2: DPIA Exercise.** | | | |
| **Stage 1 - Threshold Assessment**  If you answer yes to **THREE** of the following questions, you must carry out a full DPIA. | | | |
| **No** | **Does your project involve?** | **YES** | **NO** |
| **1** | Evaluation or scoring of personal data (including profiling and predicting)  ***Explanation:*** *e.g. biotechnology firm offering genetic testing to customers in order to predict disease / health risks.* |  |  |
| **2** | Automated decision-making with legal or similar significant effects:  ***Explanation:*** *Processing that may lead to discrimination or exclusion* |  |  |
| **3** | Systematic monitoring  ***Explanation****: including through a publicly accessible place on a large scale e.g. CCTV in a public space* |  |  |
| **4** | Special category personal data or data of a highly sensitive /personal nature e.g. medical records, criminal records, biometrics etc  ***Explanation:*** *All GDPR Article 9 special categories data* |  |  |
| **5** | Data processed on a large scale  ***Explanation****: Minimum of* ***One hundred*** *data subjects involved* |  |  |
| **6** | Matching, merging or combining data sets |  |  |
| **7** | Data concerning vulnerable data subject (including children)  ***Explanation:*** *Where there is power in-balance between the data controller and the data subject e.g. doctor /patients, children, the elderly, employer /employees, person with disabilities* |  |  |
| **8** | Innovative use or applying technological or organisational solutions  ***Explanation:*** *Example will be finger prints or facial recognition, introduction of new technology.* |  |  |
| **9** | Data transfer outside the EU  ***Explanation:*** *Any and all ‘third countries’. This will include the UK in the event of a no deal Brexit.* |  |  |
| **10** | Processing preventing data subjects from exercising a right of using a service or contract  ***Explanation****: Credit screening by banks to decide whether to give credit.* |  |  |
|  |  |  |  |
| **If you have answered yes to at least THREE of the above questions, you must carry out a full DPIA.**  *Please see the DPIA template below.* | | | |

|  |
| --- |
| **Stage 2 – DPIA**  **2**.**1: You are required to document the following:**   * Your privacy management arrangement * Description of your project or research * Mapping of information flows |
| Explain broadly what the project aims to achieve and what type of processing of personal data it involves. You can draw on your answers to step 1- the threshold questions. |
|  |

|  |
| --- |
| **2.2: Describe the Processing** |
| **Project aims**:  Explain broadly what the project aims to achieve and what type of processing of personal data it involves? You can draw on your answers to step 1- the threshold questions. |
|  |
| **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 (data flows) |
|  |
| **Describe the scope of the processing:**  What is the nature of the data?  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 (if any) 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? |
|  |
| **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? |
|  |

|  |
| --- |
| **2.3: Assessment of Necessity and Proportionality of Processing** |
| **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? |
|  |

|  |
| --- |
| **2.4: Consult with Stakeholders** |
| **Consider how to consult with relevant stakeholders:**  Describe when and how you will seek the views of experts e.g. Information Security experts – 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? |
|  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **2.5 Risk Assessment - Identifying Privacy Risks**  This stage involves examining your project to assess what data protection issues may arise, and to identify any risks it may expose individuals to, as well as any data protection-related risks that the project might create for your organisation.  This step should build upon work done at previous stages of the DPIA. The responses to questions in your threshold assessment should act as a guide to the risks which may be possible.  **2.6 Risk Assessment – Identifying and Evaluating Privacy Solutions**  Data Protection solutions are steps which may be taken to reduce the likelihood or severity of data privacy risks being realised. | | | | | | | | | | |
|  |  | **Name of Project:** | |  |  |  |  |  |  | **Risk Register Owner:** |
| **Risk ID** | | **Risk Description** | **Consequence** | **Risk Owner** | | **Current internal CONTROLS  (provide details of how you currently manage the risk)** | **Assessment of Risk** | | | **Describe what further ACTIONS you will take to reduce the Impact/Likelihood and  mitigate the risk.  State who is the risk owner for each action** |
| **Impact** (1,2,3,4,5) | **Likelihood** (1,2,3,4,5) | **Score** |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |



|  |  |  |
| --- | --- | --- |
| 2.7: Document DPIA Outcomes | | |
| **Item** | **Name/date** | **Notes** |
| Measures approved by: |  | Integrate actions back into project plan, with date and responsibility for completion |
| 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: | | |
| Residual risks approved by: |  | If accepting any residual high risk, consult the Data Commissioner before going ahead |
|  |  |  |
| Consultation responses reviewed by: |  | If your decision departs from individuals’ views, you must explain your reasons |
| Comments: | | |
| This DPIA will be kept under review by: |  | The DPO should also review ongoing compliance with DPIA |

Each stage of the PIA process must be documented to ensure compliance.

**2.8 Produce the PIA report**

A PIA report should focus on the needs and rights of individuals whose personal health information is collected, used or disclosed. The report should be easily understood by the public and written in a clear, coherent manner so that the PIA is communicated effectively.

Service providers are not legally obliged to publish PIA reports, however public organisations may benefit from doing so to build a culture of accountability and transparency, and inspire public confidence in the service provider’s handling of personal health information. A summary document might suffice for publication, especially if the full PIA report contains sensitive findings