**Data Privacy Impact Assessment (DPIA)**

**PDPPL-02050502E**

**Template for Regulated Entities**

|  |
| --- |
| **National Cyber Governance and Assurance Affairs** |
|  |  |

**Version: 2.0**

**First Published: November 2020**

**Last Updated: September 2022**

**Classification: Public**

**Document History**

|  |  |  |
| --- | --- | --- |
| **Version Number** | **Description** | **Date** |
| **1.0** | Published V1.0 document | November 2020 |
| **2.0** | Published V2.0 document | September 2022 |

**Related Documents**

|  |  |
| --- | --- |
| **Document Reference** | **Document Title** |
| **PDPPL-02050201E** | Principles of Data Privacy Guidelines for Regulated Entities (English) |
| **PDPPL-02050206E** | Data Privacy Impact Assessment (DPIA) Guidelines for Regulated Entities (English) |

# Sample Data Protection Impact Assessment (DPIA) Form

This sample DPIA form is an example that controllers can use to document their DPIAs. It follows the process set out in our DPIA guidelines and should be read alongside those guidelines. Controllers should fill out the template at the beginning of any major project involving the use of personal data, or if making a significant change to an existing process. They should integrate the final outcomes back into any project plan.

|  |
| --- |
| **Details of process ownership** |
| Fill in below the details of which department owns the processing activity, or process that it is a part of. Assign a single owner for the processing activity - the person who would be most accountable for the effective functioning of this process. |
| **Name of division/department** |  |
| **Name of processing activity** |  |
| **Status of processing activity** |  |
| **Project name\*** | \*Add the name of the project or initiative that the processing relates to |
| Add further information here which you may think will be useful to describe the processing activity’s governance and ownership. |

|  |
| --- |
| **Decision on whether to carry out a DPIA or not** |
| Explain broadly what project aims to achieve and what type of processing it involves and why this does or does not require a DPIA. You may find it helpful to refer or link to other documents, such as a project proposal. See DPIA guidelines section 3: When should we perform a DPIA? |
| Either: 1. Summarise why you identified the need for a DPIA - e.g. because you expect to use technology that is relatively new in the industry.2. Summarise your judgement that a DPIA is not required and justification. |

|  |
| --- |
| Details of processing activity |
| Describe the processing activity in this section, in as much detail as is reasonable. Refer to your records of personal data processing for information that might be relevant.  |
| Describe the personal data that will be processed. | In this box you should detail the “what” of the processing activity. Details should include:* What categories of personal data are processed? (name, contact details, family information, etc.).
* What categories of personal data of a special nature will be processed? (racial origin, children’s data, health data, physical data, psychological data, religious beliefs, marital status, criminal records, biometric data).
 |
| Describe the individuals whose personal data will be processed. | In this box you should detail the “who” of the processing activity. Details should include:* Who are the individuals whose data will be collected?
* What is the (estimated) number of individuals whose data will be collected and processed as part of this processing activity, i.e. how many individuals per day/week/month?
* How much control will the individual have of their data?
* Are there any current issues of public concern that you should factor in?
 |
| Describe the nature of processing. | In this box you should detail the “how” of the processing activity. Details should include:* Who will provide the data, i.e. will the personal data for this processing activity be obtained directly from the individual?
* How often does this processing activity take place - constantly, hourly, daily, weekly or monthly?
* Is the data shared with third parties (processors and joint controllers)? If yes, mention the third parties or categories of third parties.
* Does the processing activity involve any cross-border data transfer (data transferred across territories/countries)?
* What are the systems used to process and/or store the data?
 |
| Describe the purpose of processing, including the permitted reason  | In this box you should detail the “why” of the processing activity. Details should include:* What is the purpose of processing? What do you want to achieve?
* What is the intended effect on individuals?
* What is the permitted reason for processing?
 |

|  |
| --- |
| Assess necessity and proportionality |
| Describe measures to ensure necessity and proportionality of processing. |
| Details should include:* How does the processing achieve your purpose?
* Could this outcome be achieved in another less intrusive way?
* How will you ensure that processing is limited to only what is required to achieve your purpose?
* How will you ensure data quality?
* How will you ensure data minimisation?
* Will you ensure an appropriate privacy notice to individuals?
* Will individuals be able to exercise their rights?
* If you are using processors, what measures do you take to ensure processors comply?
* How do you safeguard any international transfers?
 |

|  |
| --- |
| Identify risks and appropriate measures to manage them |
| Describe each risk of damage to individuals subject to the processing and include an assessment of the likelihood of the risk coming to pass and the impact on individuals in terms of the damage it could cause to their privacy or their personal data. |
| Describe the risk event with its cause and nature of potential impact on individuals. | Likelihood of occurrence | Level of impact on (damage to) individuals | Overall risk level |
| Include associated compliance and corporate risks as necessary | Unlikely, possible or likely | Minimal, considerable or serious | Low, medium or high |
| Identify measures you should take to reduce or eliminate these risks identified above. You should be confident that the measures you identify to protect the personal data being processed are commensurate to the risk of serious damage to the individual’s privacy or their personal data.\*You should incorporate the mitigation measures identified into your overall project plan for implementing the processing activity to ensure that they are carried out. |
| **Risk** | **Measure to mitigate risk** | **Residual risk level** | **Measure owner** |
|  |  | Low, medium or high |  |

|  |
| --- |
| Assess the potential for “serious damage” against measures identified |
| Describe how the processing activity could cause serious damage to the individual, and how the potential for this serious damage is mitigated by the risk mitigation actions identified. Provide your rationale for deciding that your mitigation measures are commensurate to the risk to individuals. |
| You must set out how you have decided on the right balance between appropriate protection measures and the risk posed to individuals taking into account:* leading practice including state of the art technology;
* the costs of implementation of various protection measures available;
* the nature, scope, context and purposes of processing (the “what,” “who,” “how” and “why” of processing); and
* the risk of serious damage to individuals.
 |

|  |
| --- |
| Describe how you will demonstrate the data protection principles |
| Describe how the data protection principles (for more information, see the Principles of Data Privacy Guidelines for Regulated Entities) will be demonstrated once all the action plans listed above are implemented. |
| **Principle** | **How we will demonstrate this principle** |
| **Transparency, honesty and respect for human dignity** |  |
| **Data minimisation** |  |
| **Accuracy**  |  |
| **Storage limitation** |  |
| **Integrity and confidentiality** |  |
| **Purpose limitation** |  |
| **Accountability** |  |

|  |
| --- |
| Sign-off |
| Have the DPIA signed off by the staff member responsible for data protection, the head of department/division and the staff who contributed to the DPIA. This signed DPIA should be filed appropriately to enable easy access where required. |
| **Data Protection Leader** |  |
| **Head of Department / Division** |  |
| **Contributing Staff** |  |

**End of Document**