[*Company Logo*]

|  |
| --- |
| DATA PROTECTION IMPACT ASSESSMENT (DPIA) POLICY |

**DOCUMENT CONTROL**

|  |  |
| --- | --- |
| **Version:** |  |
| **Date of version:** |  |
| **Document Author:** |  |
| **Approved by:** |  |
| **Document Owner:** |  |

**REVISION HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| **VERSION** | **REVISION DATE** | **REVISED BY** | **SUMMARY OF CHANGE/SECTION REVISED** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**DATA PROTECTION IMPACT ASSESSMENT (DPIA) POLICY**

1. **INTRODUCTION**

This policy sets out [*Name of Company*]’s systemic approach to DPIAs. [*Name of Company*] needs to collect personal data to effectively carry out its everyday business functions and activities as well as also providing the products and services typically offered by its business type. Such data is collected from employees, customers, suppliers and clients and may include (but is not limited to), name, address, email address, date of birth, IP address, identification numbers, private and confidential information, and sensitive personal data. In addition, [*Name of Company*] may be required to collect and use certain types of personal data to comply with the requirements of the law and/or statutory bodies. However, [*Name of Company*] is committed to processing all personal data in accordance with the Nigeria Data Protection Regulation (NDPR), and any other relevant data protection laws and codes of conduct (herein collectively referred to as “the data protection laws”).

To ensure that the method of collecting personal data and the storage within the database is secure, all systems must be tested against the Data Protection Impact Assessment (DPIA). DPIAs are required for assessing risks within [*Name of Company*]’s processes for handling of personal data, especially when the processing poses a risk to the rights and freedoms of individuals especially regarding their personal data. DPIAs also need to be revisited periodically and involve key players within our organization.

1. **DEFINITIONS**

|  |  |
| --- | --- |
| **TERM** | **DEFINITION** |
| Data Controller | The Data Controller is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; |
| Data Protection Officer (DPO) | The person within the organisation who is responsible for ensuring that the organisation is compliant with the NDPR; |
| Data Protection Laws | Means for the purposes of this document, the collective description of the NDPR, The 1999 Nigerian Constitution as amended and any other relevant data protection laws that [*Name of Company*] complies with; |
| Data Subject | Any person, who can be identified, directly or indirectly by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. |
| Personal Data | Is any information relating to Data Subject; |
| Processing | Is any operation or set of operations which is performed on personal data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. |
| Profiling | Is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. |
| Supervisory Authority | National Information Technology Development Agency; |

1. **OBJECTIVES OF THE DPIA POLICY**

To ensure that all risks are identified, and where possible eliminated in the system that collects and stores personal data.

1. **RESPONSIBILITIES**

[*Name of Company*] is the Data Controller and the Management, as governing body for internal operations is ultimately responsible for compliance with Data Protection Laws. [*Name of Company*] will take the appropriate measures to ensure privacy by design and to protect the rights of the Data Subjects whose personal information is in their purview.

1. **DATA PROTECTION IMPACT ASSESSMENTS**

A Data Protection Impact Assessment (DPIA) is a process whereby potential privacy issues and risks are identified and examined from the perspective of all stakeholders and allows [*Name of Company*] to anticipate and address the likely impacts of new initiatives and put in place measures to minimise or reduce the risks. As the use of technology, the collection and storage of personal data grows, the need to ensure that it is properly managed and maintained increases.

It is a requirement of NDPR that a Data Protection Impact Assessment (DPIA) is carried out in certain circumstances. This section will explain when a DPIA should be done and how it should be carried out. It is the responsibility of the Regular Process Owner to carry out a DPIA. As part of the process, the Data Protection Officer must be consulted but it is not the Data Protection Officer who carries out the DPIA.

The impact assessment covers not only the protection of Personal Data but broader privacy of individuals and therefore could also be referred to as a Privacy Impact Assessments (PIA). The procedures in this section are designed to minimise the risk of harm that can be caused by the use or misuse of personal information by addressing data protection and privacy concerns at the design and development stage of a project conducted by the Data Controller. Conducting a DPIA should benefit [Name of Company] by managing risks, avoiding unnecessary costs, avoiding damage to reputation, ensuring legal obligations are met and improving the relationship with stakeholders. The term “project” is used in a broad and flexible way and is intended to include any plan or proposal by [*Name of Company*]. Examples of the types of projects that need a DPIA are:

* A new database storing and accessing Personal Data;
* A data sharing initiative where two or more groups seek to pool or link sets of Personal Data;
* A proposal to identify people in a particular group or demographic and initiate a course of action;
* A new surveillance system such as CCTV;
* A new database where the data is captured by form.

[*Please note that the foregoing are mere examples and are not exhaustive*]

1. **WHEN DOES A DPIA NEED TO BE DONE?**

A DPIA should be completed as part of the initial phase of a project or at the point of creating an asset or process that involves Personal Data to ensure that risks are identified and taken into account before the problems become embedded in the design and cause higher costs due to making changes at a later stage. Also, if there is a change to the level of risk involved in the Processing of an existing project/asset/process, a review should be that a Data Protection Impact Assessment be carried out. In the context of this guidance, a project could include the development or enhancement of any activity, function, or processing such as a system, database, programme, application, service or scheme. The time and effort put into carrying out the DPIA should be proportionate to the risks.

1. **WHAT TO DO DURING A DPIA**

This section is for those projects/assets/processes which include the use of any Personal Data. If it involves the processing of Personal Data, then you should start by completing the screening questions (Annex A – Step 1) on the DPIA form in the annexure to this document. If the answer to all these questions is ‘No’ then the remainder of the assessment does not need to be completed. If the response to any of the screening questions is ‘Yes’, it is recommended that you should go on to complete Part 2 of the impact assessment form.

Once Step 1 and if required Step 2 are completed, the DPIA form is to be attached to the asset and stored alongside the project’s documentation.

1. **THE DPIA PROCESS**

Once the risks are identified and outcomes and actions agreed, it is important that the person leading the DPIA ensures that the necessary actions are implemented. As the project develops or the asset/process is launched and embedded, the privacy risks should continue to be assessed to ensure that adequate protections remain in place.

Once the DPIA process has been completed, the outcomes will be recorded in a register maintained by the Data Protection Officer. The register will record each risk, explain what action has been taken or will be taken and identify who is responsible for approving and implementing the solution.

1. **POLICY REVIEW**

This Policy will be reviewed as required and at least every [*2 years*]by the Data Protection Officer and select members of the [*Name of Company*]’s management team.

**ANNEXURE**

Annex A: Example Form for DPIA

|  |  |
| --- | --- |
| Asset/Process/Project title |  |
| DPIA Author |  |
| Contact Details |  |
| Asset/Process Owner or Project Sponsor |  |
| Faculty/Directorate |  |
| Date created |  |
| Date of last review |  |

Step One - Identify the need for a DPIA

**Screening Questions**

|  |  |
| --- | --- |
| Screening question | Yes/No |
| Does your data processing involve evaluating or scoring individuals (including profiling and predicting)? |  |
| Does your data processing involve automated decision-making that may have a significant effect on an individual? |  |
| Does your data processing involve systematic monitoring? |  |
| Does your data processing involve special category or criminal Personal Data? |  |
| Does your data processing involve processing Personal Data on a large scale? |  |
| Does your data processing involve datasets that have been matched or combined? |  |
| Does your data processing involve the Personal Data of vulnerable people? |  |
| Does your data processing involve the use or application of innovative technological or organisational solutions? |  |
| Does your data processing involve the transfer of Personal Data outside of Nigeria? |  |
| Does your data processing prevent individuals from exercising a right or using a service or contract? |  |

If ‘yes’ has been answered to any of the questions in step one, please proceed to Step 2 as a full DPIA will be required.

**Step Two – Full DPIA**

Context

Outline the asset/process/project – what is the purpose, what does it aim to achieve and what are the benefits.

|  |
| --- |
|  |

**Describe the information flows**

Include the nature of the data, how it will be collected, accessed, stored, shared and retained including reference to IT. It may be useful to refer to a flow diagram or another way of explaining data flows.

|  |
| --- |
|  |

**Identify and assess the privacy risks**

List key privacy risks

|  |  |  |  |
| --- | --- | --- | --- |
| Risk ID | Privacy risk | Impact | Likelihood |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Identify and approve controls**

List the actions to be taken to reduce the identified risks and the expected outcome of those actions, e.g. is the final impact on individuals after implementing each solution a reasonable and proportionate response to the aims of the asset/process/project?

|  |  |  |
| --- | --- | --- |
| Risk ID | Control(s) identified | Expected outcome |
|  |  |  |
|  |  |  |

**Assign responsibility for implementing controls**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk ID | Controls | Responsible Officer | Deadline for implementation | Completion Date |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Reassess and accept the risks**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk ID | Privacy risk | Impact after control | Risk Accepted by | Likelihood |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Consultation**

Provide details of any consultation which has taken place.

|  |
| --- |
|  |