CYBERPAY LIMITED

DATA PROTECTION IMPACT ASSESSMENT POLICY

1. INTRODUCTION

CyberPay Limited ("CyberPay" or "the Company") is firmly committed to complying with the Nigeria Data Protection Regulation, 2019 and other applicable data protection laws, regulations, rules and principles. This Data Protection Impact Assessment Policy ("**Policy**") describes the minimum standards that must be strictly adhered to whenever CyberPay wishes to conduct a Data protection Impact Assessment in respect of a new or existing project requiring the processing of Personal Data which is likely to result in a significant risk to the rights and freedoms of Data Subjects, unless the specific processing operation is explicitly excluded from a DPIA by the supervisory authority, in this case the National Information Technology Development Agency (NITDA).

This Policy applies to all personal data processing operations by staff members whether temporary or contract, or any agent or third party that is responsible for managing any personal data processing operation of CyberPay.

2. Aims and Objectives

This Policy explains the likely risk involved in data processing procedures and compliance obligations. This Policy is to ensure that CyberPay:

a) remains compliant with all regulatory requirements;
b) adopts best practices in its processing activities;
c) is transparent in its dealings;
d) builds confidence and trust of the public;
e) protects the rights to privacy of all Data Subjects whose Personal Data are within its control;
f) assesses the level of risk and the severity of any impact on individuals;
g) minimizes any potential risks and assesses whether or not remaining risks are justified; and
h) considers compliance risks and the potential harm - to individuals or society and any significant social or economic disadvantage to the business operations of CyberPay.

3. Definitions and Abbreviations

"Data Protection Officer"	means the Data Protection Officer, who is appointed to assist CyberPay monitor internal compliance, inform and advise on data protection obligations, provide advice regarding DPIAs and act as a contact point for Data Subjects and the supervisory authority;
"Data Subject"	means 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;
"DPIA"	means Data Protection Impact Assessment;

"NDPR"	means Nigeria Data Protection Regulation, 2019;
"Personal Data"	means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others;
"Project"	includes but not limited to activities and processing that may have implications on the privacy of Data Subjects. This applies to matters such as employee monitoring, CCTV installation, new methods or procedures for service delivery or information handling, product or solution development, process improvements, IT infrastructure changes, processes and procedures relating to how information is stored or accessed, etc.;
"Processing"	means 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.

4. Responsibilities

4.1. Management and the DPO

4.1.1. The Management team of CyberPay is ultimately responsible for compliance with the NDPR.

4.1.2. The DPO will ensure that data privacy and data protection impact assessment is carried on all new or existing projects (where required).

4.1.3. The DPIA may be carried out internally by the DPO and the Project Management Team or the Company may appoint a licensed Data Protection Compliance Organization (DPCO) to carry out the DPIA either solely or in conjunction with the DPO.

4.1.4. The DPO shall report to the Management of the Company on all matters relating to data privacy and data protection, advice on the review of this Policy and ensure full compliance with this Policy and other ancillary policies on data privacy and protection.

4.2. **Project Management Team**

Project Management Team (i.e. the department managing a new project) shall ensure that any processing activity involving Personal Data is assessed to determine whether a DPIA is required. The Project Management Team should ensure that the report from a DPIA is implemented through-out a project.

4.3. **Risk Management Team and Information Security Officer**

The risk management team (or legal team) and the information security officer of the Company shall, jointly, review the impact of all recommendations in respect of any DPIA conducted by the Company and develop risk elimination measures and safeguards.

5. When to Conduct a DPIA

CyberPay must carry out DPIA prior to the introduction of a new processing activity and in the early stages of a project. The results or recommendations of a DPIA shall be maintained and regularly reviewed and updated to ensure identification of new risks and development of controls throughout the project. Without limiting the generality of the foregoing, CyberPay will conduct a DPIA in the following cases:

- introduction of a new technology (ies) that involves processing of Personal Data;
- to comply with a change in law which may impact on Personal Data of Data Subjects;
- where Personal Data (including sensitive data) was originally collected for a limited purpose but is now intended for reuse for a new purpose(s);
- where there is a transfer of Personal Data outside Nigeria, particularly to countries where there are no adequate data protection laws/regulations;
- where there are changes to existing processing operations that may likely impact on Personal Data of Data Subjects;
- large-scale processing of Personal Data;
- if data processing is used to make automated decisions on Personal Data of Data Subjects;
- where the processing activities include Personal Data of children; and
- when the processing activity is identified as high risk and may pose a potential breach in the rights and privacy of Data Subject.

6. Conducting a DPIA

In order to carry out a DPIA under this Policy, the following shall be taken into consideration:

6.1. **Identifying need for a DPIA:**

6.1.1. Before a DPIA is conducted in respect of any new or existing Project, CyberPay (the Project Management Team and/or the DPO) will conduct an assessment of the Project to identify whether the processing operation requires a DPIA. This will be achieved by each Project Management Team, identifying and completing the checklist for Identifying the need for a DPIA ***(Appendix A)*** which is then forward to the DPO for advice and conclusion on whether or `not a DPIA should be conducted or not.

6.1.2. Where it is determined that there is no need for a DPIA, it should be documented, and the process shall be discontinued.

6.2. **Planning and Scope of the DPIA**

6.2.1. In the event that a DPIA is to be conducted, the DPO and Project Management Team shall plan and detail the scope of the DPIA process.

6.2.2. This activity shall set out the entire details of the proposed processing activity, what information is to be collected and what it is to be used for, how it will be obtained and from whom it will be obtained and disclosed to, who will have access to the information and any other necessary information.

6.2.3. A DPIA Form (**Appendix B)** will be sent to all relevant stakeholders involved in the project for completion and comment.

6.3. **Compliance Measure, Legal Analysis and Risk Identification**

6.3.1. This activity shall be performed by relevant stakeholders of CyberPay such as the Project Management Team, DPO, risk management team (or legal team, as the case may be) etc. They will jointly review the proposed processing operations to determine:

a) the appropriate legal basis for processing;

b) the policy documentation required for the processing;

c) whether the principles of data processing will be complied with if the processing activity or project is carried on;

d) whether there are sectoral laws or regulations or guidelines regarding the processing and their legal impact on the project; and

e) if the NDPR and other relevant laws will be fully complied with.

6.3.2. External stakeholders may also be involved in identifying and analyzing the likely risks from the processing operation.

6.3.3. Where risk is identified in the operation, the risk should be quantified based on its likelihood and severity.

6.3.4. In the event of any ambiguity, CyberPay may seek clarification from the National Information Technology Development Agency (NITDA) or any other successor agency or applicable regulator.

6.4. Risk Identification and Evaluating Privacy Solutions

6.4.1. Once the risks have been identified, all relevant stakeholders involved in the project will make recommendations on the most likely measures and safe guards. Such recommendations may include:

a) Technological and policies measures already in place or to be provided.
b) Procedures and safeguards to mitigate the risk.
c) Documentation and measures relating to personal data protection required to be put in place.
d) Recommendations from previous DPIA which may also be relevant.

6.4.2. In considering relevant recommendation, the effect of the recommendation on the risk(s) and the residual risk(s) must be evaluated. The evaluation outcome will determine whether the risk will be eliminated, modified, avoided, retained etc.

6.4.3. The risk to be retained and its impact must be communicated to the risk management team (or legal team as the case may be) and thereafter the management of CyberPay.

6.5. DPIA Report, Implementation, Monitor and Review

6.5.1. At the end of every DPIA, a report should be prepared and sent to the Company's risk management team or legal team for review. Thereafter, the report should be documented and the identified risks be recorded in a risk register.

6.5.2. The DPO shall supervise and monitor the implementation of the outcome of the DPIA.

6.5.3. The DPO will maintain a central record of all DPIA's conducted by CyberPay.

7. Review

CyberPay shall from time to time amend and review this Policy as best practices, regulations and necessity may require. Whenever this Policy is reviewed or amended, CyberPay shall notify all relevant stakeholders and make it accessible to all employees and relevant third parties.

8. Related Policies and Procedures

This Policy shall be read in conjunction with the following policies and procedures of CyberPay:

a) CyberPay Data Protection Policy (https://www...../)
b) CyberPay Personal Data Breach Management Policyhttps://www...../)
c) CyberPay Employee Data Privacy Noticehttps://www...../)

9. Contact for any Queries

For further information or enquires regarding this Policy, please contact the Company's DPO. The contact details are set out below:

- Data Protection Officer: Nwachukwu Chinedu
- Location: 12 Ologun Agbaje Street, Victoria Island, Lagos
- Phone: 07035736886
- Email: chinedu.nwachukwu@cyberpay.net.ng

CyberPay

APPENDIX A

Checklist for Identifying the Need for a DPIA		
Department/Unit:		**Code No:**
Project:		**Date:**
S/N	**Questions**	**Yes/No/Unsure**
1	Will there be likely risks from the processing activity?	
2	What is the likelihood that the right to privacy of Data Subjects will be breached?	
3	Is there a likelihood that the risk will be high?	
4	Does the activity involve large scale processing?	
5	Will the processing involve the use of technology?	
6	Will the processing activity involve new technologies or innovations?	
7	Does the data processing involve existing personal data?	
8	Does the processing involve processing of sensitive personal data?	
9	Does the data processing involve the Personal Data of children and vulnerable persons?	
10	Does the processing involve a systematic and extensive evaluation of the personal aspects of an individual, including systematic monitoring of public areas on a large scale?	
11	Does the processing involve transfer of data to third parties?	
Comment		
Signed ***[Name and Designation of employee]***		

CyberPay

APPENDIX B

DPIA FORM		
Department/Unit:		**DPIA Code:**
Project Name:		**Date:**
Description of Processing Operation		
S/N	**Questions**	**Responses and Comment**
1	How will the personal data be collected?	
2	What elements of data will be captured?	
3	What is the nature of the Personal Data is collected?	
4	What is the volume and variety of the Personal Data?	
5	Does the data include Personal Data of children or other vulnerable people?	
6	What is the purpose of processing of the Personal Data?	
7	Description of the envisaged processing operation	
8	The extent and frequency of the processing	
9	The duration of the processing;	
10	The number of Data Subjects likely to be involved	
11	The geographical area likely to be covered.	
12	What is the mode of storage?	
13	What is the likely length of storage?	
14	What are the protection measures?	
15	Will a novel type of processing be used?	
16	How will the data be used?	
17	Who has access to the data?	
18	How will the data be deleted and erased?	
19	What is the legal basis of processing?	
20	Any current issues of public concern?	
21	An assessment of the necessity and proportionality of the processing operations in relation to the purposes?	

22	What is the assessment of the risks to the rights and freedoms of Data Subject?	
23	What are the risk mitigation measures being proposed to address the risk?	
24	Is there compliance with relevant codes of practice and law?	
25	Will the data be shared with third parties?	
26	What organization(s) will the data be shared with?	
27	Why will the data be shared with the organization?	
28	Will the data be transferred to a foreign country?	
29	Why is the data being transferred to a foreign country?	
30	Which country will the data be shared with?	
31	Does the country have a data protection law in place?	
32	Is the country on the White List issued by NITDA?	
Signed ***[Name and Designation]***		

a. General Information

Title	Data Protection Impact Assessment Policy
Status	Mandatory
Issuing Department	Legal
Distribution/Target Audience	All employees, including contracted staff CyberPay Limited
Approver	Management of CyberPay Limited
Effective Date	April 2021
Version	1.0

b. Version Control

Version	Last Updated	Reason for Amendment