

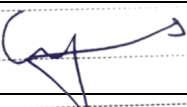

PRINCEPS CREDIT SYSTEMS LIMITED

DATA PROTECTION POLICY



DOCUMENT INFORMATION

Version	Date	Owner(s)	Author	Description	Effective Date
1.0	April 2025	IT; Legal and Compliance	Ekene Ugbede	Creation	June 2, 2025

REVIEWED BY

S/No	Name	Designation	Signature	Date
1.	Efosa Ehigie	CIO		April 15, 2025
2.	Oluwatoyosi Adetula	COO/Executive Director		April 15, 2025

APPROVED BY

S/No	Name	Designation	Signature	Date
1.	Oluwatoyosi Adetula	COO/Executive Director		May 15, 2025
2.	Peter Atuma	Executive Chairman		May 15, 2025

1.0 POLICY STATEMENT

- 1.1 Everyone has rights with respect to how their Personal Data is handled. In the course of our activities, we will collect, store and process personal information about our staff, service providers, suppliers, customers, consultants, business partners and third parties in respect of our business operations as well as the various services we render or receive, or otherwise.
- 1.2 We are committed to treating all Personal Data in a responsible manner, in compliance with all applicable laws, including the Nigerian Data Protection Act 2023 (“**NDPA**”), regulations made pursuant to the NDPA, and any regulations or guidelines made by an applicable industry regulator as it relates to data protection, as may be enacted or amended from time to time.
- 1.3 Data protection is key for us, consequently, we require a firm adherence to this policy. The regulatory sanctions and the potential penalty exposures for any non-compliance are also quite dire, including the risk of reputational damage. Hence, any breach of this policy will result in disciplinary action.

2.0 FEATURES OF THIS POLICY

This policy outlines our rules on data protection and the crucial legal conditions that must be satisfied in relation to obtaining, handling, processing, usage, storage, transfer and destruction of Personal Data.

3.0 DEFINITION OF DATA PROTECTION TERMS

“Automated Decision-Making” means a decision based solely on automated processing by automated means, without any human involvement.

“Automated Processing” means any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal attributes of an individual, and may include analysing or predicting aspects concerning that individual’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements (E.g. profiling).

“Biometric Data” means Personal Data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of an individual, which allow or confirm the unique identification of that individual, including without limitation by physical measurements, facial images, blood typing, fingerprinting, retinal scanning, voice recognition and *deoxyribonucleic acid (DNA)* analysis.

“Consent” means any agreement of a data subject which is freely given, specific, informed, and which clearly indicates, whether by a written or oral statement or by an affirmative

action, that the data subject agrees to the processing of Personal Data relating to him; or relating to any individual on whose behalf he has the permission to provide such Consent.

“Data Privacy Impact Assessment” (DPIA) refers to the tools and assessments used to identify and reduce the risks attached to a Data Processing activity.

“Data Subjects” for the purpose of this policy, includes all living or identifiable individuals whose Personal Data we receive or hold. A data subject need not be a citizen or resident of Nigeria.

“Data Controllers” are the people or organisations who, alone or jointly with others, determine the purposes, means and manner in which Personal Data is processed. We are Data Controller of all Personal Data we possess relating to our staff or third parties in the course of or for the purpose of our business. Other parties are also Data Controllers in respect of those Personal Data they possess and share with us.

“Data Processors” include any person or organisation who processes Personal Data on behalf of at the direction of a Data Controller or another Data Processor. It includes suppliers, service providers, consultants or third parties who handle Personal Data, whether on our behalf or not.

“Data Protection Officer” (DPO) refers to the person who is primarily responsible for data protection and privacy practices of our Company and for our Company’s compliance with relevant Data Protection Laws. The Data Protection Officer may be an employee of the company or engaged by a service contract.

“Data Protection Laws” means all applicable laws that relate to data protection in Nigeria and any other country having competent jurisdiction in the course of our business, and includes the Nigeria Data Protection Act 2023 (**“NDPA”**), regulations made pursuant to the NDPA and any regulations or guidelines made by an applicable industry regulator from time to time with respect to data protection.

“NDPC” means the Nigeria Data Protection Commission.

“Personal Data” or “Data” means any information relating to an individual, who can be identified or is identifiable, directly or indirectly, by reference to an identifier such as a name, an identification number, phone number, address, email address, location data, date of birth, an online identifier or one or more factors specific to the gender, nationality, physiological, genetic, psychological, cultural, social, or economic identity of that individual. Personal Data includes Sensitive Personal Data and pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. It may be stored electronically, on a computer, on a cloud system, or in certain paper-based filing systems.

“Processing” means any activity that involves use of Personal Data. It includes any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing by transmitting, disseminating or otherwise making available, aligning, combining, restricting, erasing or destroying data.

“Pseudonymisation” means replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be specifically identified without the use of additional information which is meant to be kept separately and secure.

“Sensitive Personal Data” includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life, biometric or genetic data, and Personal Data relating to criminal offences and convictions. Sensitive Personal Data can only be processed under strict conditions and will usually require the explicit consent of the person concerned.

4.0 DATA PROTECTION PRINCIPLES

4.1 In accordance with the principles of data protection, we will ensure that Personal Data is:

- (a) processed fairly, lawfully and in a transparent manner.
- (b) collected and processed for specified, explicit, related, and legitimate purposes.
- (c) adequate, relevant and limited to the minimum necessary for the purposes for which it was collected or further processed;
- (d) retained for a reasonable or lawful period, and no longer than is necessary to achieve the lawful bases for which it was collected or further processed.
- (e) accurate, complete, not misleading, and kept up to date where necessary and practicable, in relation to the purposes for which it was collected or further processed.
- (f) processed in line with applicable law and the Data Subjects' rights.
- (g) processed and stored using appropriate technological and organisational security measures to ensure the security and confidentiality of Personal Data.
- (h) transferred to another country only where adequate security measures, protection and safeguards have first been put in place; and

- (i) is subject to the exercise by a Data Subject of its Personal Data rights under the applicable Data Protection Laws.

5.0 FAIR, TRANSPARENT AND LAWFUL PROCESSING

5.1 We will process Personal Data in a lawful, fair and transparent manner. We intend to ensure that Personal Data is properly processed without negatively impacting on the Data Subject.

5.2 We will indicate the purpose for which the data is to be processed by us, our contact information - our identity, place of business and means of communicating with us; who we will share it with, how long we will keep the data, whether it will be subject to international transfer, and what legal safeguards are in place to protect it; the existence of automated decision-making, including profiling, the significance and envisaged consequences of such processing for the data subject, the rights of the data subject, such as the right to access; to object to such processing or the data being used.

5.3 We may refrain from indicating such information, where such information has already been provided to the Data Subject and where we have evidence of same; or where the provision of such information is impossible or would involve a disproportionate effort or expense.

5.4 What is lawful processing?

5.4.1 For Data Processing to be lawful:

- (a) The consent of the Data Subject must have been obtained.
- (b) The processing should be necessary for our legitimate interests or that of any other applicable Data Controller (or party to whom the data is to be disclosed), provided that such interests are not prejudicial to the interests or fundamental rights of the Data Subject.
- (c) The processing is necessary for the performance of a contract with the Data Subject, or to take steps at the request of the data subject prior to entering into a contract.
- (d) The processing is necessary to meet our legal obligations to the Data Subject or third parties.
- (e) The processing is intended to protect the vital interest of the data subject or another person.
- (f) The processing is necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the Data Controller or Data Processor.

- 5.5 We will process Personal Data in accordance with any of the applicable lawful circumstances outlined above. We require our collaborators, business partners, suppliers, service provider and vendors who act as Data Controllers or Data Processors to ensure that they comply with the applicable lawful basis set out above in respect of any such data in their custody or which they obtain or have access to.

6.0 CONSENT

- 6.1 A Data Subject consents to the processing of their Personal Data if they expressly agree to the processing, by a statement or positive action.
- 6.2 Silence or inactivity of the data subject is not consent.
- 6.3 Consent must be in the affirmative. It may be provided by a clear statement in writing, orally, or through electronic means, or ticking of appropriate boxes, but not based on a pre-selected confirmation or pre-ticked box. Where practicable, evidence of consent, or opt in, should be captured and recorded where consent is given or being relied upon.
- 6.4 Data Subjects must be able to withdraw their consent to any processing at any time and such withdrawal must be honoured as promptly as possible.
- 6.5 Similarly, where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available, where practicable, and systems should be in place to ensure such revocation is reflected accurately in our systems.
- 6.6 Where we intend to process Personal Data for a different and incompatible purpose which was not disclosed when the data subject first consented, a further or distinct consent of the data subject should be obtained.
- 6.7 When Sensitive Personal Data is to be processed, the explicit consent of the data subject to such processing will be required.

7.0 LIMITED PURPOSES

- 7.1 Personal Data may only be processed for the specific purposes notified to the Data Subject when the data was first collected or for any other purposes specifically permitted by law. This means that Personal Data should not be collected for one purpose and then used for another.
- 7.2 Personal Data may only be used for a new purpose if related to or compatible with the original purpose. Where it is for an entirely different and unrelated purpose, the Data Subject should be informed of the new purpose and their consent obtained before any processing occurs; or the Personal Data may be processed under any other applicable lawful basis.

8.0 ADEQUACY

- 8.1 We must ensure that Personal Data is sufficient for the disclosed purpose and collected only to the extent required.
- 8.2 Any Personal Data which is not relevant or necessary for the disclosed purpose should not be collected.

9.0 ACCURACY

- 9.1 Personal Data must be accurate, relevant and kept up to date. Reasonable steps must be taken to verify the Personal Data or ensure that the Personal Data is correct. This may be done at the point of collection and at intervals afterwards to ensure that such data remains accurate or up to date.
- 9.2 Where Personal Data is suspected or found to be inaccurate, incorrect, incomplete, misleading or out of date, steps must be taken to correct or update such data where practicable.

10.0 STORAGE LIMITATION

Personal Data should not be kept in a form which permits the identification of the Data Subject longer than is necessary for the purpose or that is permissible by applicable law. This means that data should be properly and carefully destroyed or erased from our systems, or that of other applicable Data Controllers whom such data is shared with, when it is no longer required. However, where a law or accounting or regulatory or other relevant reporting requirement requires such data to be kept for a specific or minimum period, such data should be kept for such period and may be deleted or erased upon the satisfaction of that timeline requirement.

11.0 THE RIGHTS OF A DATA SUBJECT

The rights of a data subject include the right to:

- (a) Confirm whether or not Personal Data concerning them is being processed. And if so, the right to access such data along with relevant information such as the purposes of processing, categories of Personal Data, recipients, and storage period.
- (b) Request access to their Personal Data held by the Company or by a Data Controller through the Company.
- (c) Request the rectification or correction of inaccurate, incomplete, outdated, or misleading Personal Data concerning them.

- (d) Request the erasure (right to be forgotten) of Personal Data where:
 - (i) the data is no longer necessary for the purpose it was collected or processed
 - (ii) consent is withdrawn (and no other legal basis applies)
 - (iii) the Data Subject has objected to processing and there are no overriding legitimate grounds for processing such Personal Data.
- (e) Object to the processing of their Personal Data, including profiling and processing for direct marketing purposes.
- (f) Restrict the processing of their Personal Data in specific circumstances, such as where the accuracy of the data is contested or where processing is unlawful but the Data Subject requests a restriction instead of an erasure.
- (g) Withdraw consent to processing at any time, where consent is the legal basis for processing.
- (h) Receive their Personal Data in a structured, commonly used, and machine-readable format, and to transmit that data to another controller (right to data portability), where technically feasible.
- (i) Be notified of a Personal Data breach that is likely to result in a high risk to their rights and freedoms.
- (j) Challenge any processing that they believe is unlawful, disproportionate, or not aligned with the stated purposes.
- (k) Lodge a complaint with the Nigeria Data Protection Commission or any other competent supervisory authority.
- (l) Not be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significant effects; unless necessary for entering into or performing a contract between the Data Subject and a Data Controller, or authorised by law, or authorised by the consent of the Data Subject.

12.0 SECURITY, INTEGRITY AND CONFIDENTIALITY

- 12.1 We will ensure that appropriate technical and organisational security measures are put in place to secure Personal Data against unlawful or unauthorised access, processing, use, and against accidental loss, alteration or damage.
- 12.2 We will ensure that measures are put in place to maintain the security of all Personal Data throughout its life cycle, from the point of collection, processing, usage, storage, transfer, to

the point of destruction. We must require that Personal Data may only be transferred to a third-party Data Processor where such third party agrees to comply with our procedures and policies, and where such third party has similarly established adequate security measures for the protection of such data.

- 12.3 The measures put in place to ensure data security are aimed at guaranteeing the following:
- a. Confidentiality: Only people who are authorised to use the data can access it.
 - b. Integrity: The data should be accurate and suitable for the purpose for which it is processed. Consequently, we require our customers, service providers, business partners and other stakeholders to ensure that they only provide us with accurate data.
 - c. Secure Availability: Authorised users must access data securely when needed for legitimate and authorised purposes.
- 12.4 Appropriate safeguards may include entry controls, encryption and Pseudonymisation where applicable. Personal Data users must ensure that the devices used in accessing or processing data are operated in such a way that they do not display such data to passers-by and that they log off from their devices left unattended. Secure lockable lockers, drawers and cabinets should also be utilised when dealing with hardcopy Personal Data and proper methods of disposal for destruction utilised to ensure that destroyed data is irretrievable, inaccessible or unusable.
- 12.5 We will continually develop, maintain, review, test and enhance our safeguards and the integrity of same - in consideration of the nature of our services or other relevant service, the identified risks, the volume of Personal Data that we process or possess, our resources, and other factors as we may consider necessary from time to time.
- 12.6 Our staff, service providers, business partners and customers must ensure full adherence to our security measures and actively protect against any unlawful or unauthorised processing of Personal Data, and against the unauthorised access, accidental loss of or damage to Personal Data. No one is permitted to attempt to or actually bypass, break into or circumvent our systems or security measures.
- 12.7 We will also endeavour to put in place appropriate back-up and disaster recovery solutions to ensure continuity, minimal risk of loss and any relevant mitigation in the unlikely event of any necessitating event.
- 13.0 DEALING WITH A DATA SUBJECT'S ACCESS REQUEST**
- 13.1 A formal request from a data subject for information that we hold about them must be made in writing.

13.2 A Data Subject's access requests will be addressed free of charge, except where it is manifestly unfounded or excessive, in which case we shall:

- (a) charge a reasonable fee considering the administrative costs of providing the information or communication or taking the action requested; or
- (b) write a letter to the Data Subject declining such request, depending on the nature of such request and where legal reasons or limitations exist to reasonably decline such requests, and copy the Nigeria Data Protection Commission (the **"NDPC"** or **"Commission"**) on such occasions.

14.0 PROVIDING INFORMATION OVER THE TELEPHONE

14.1 In dealing with telephone enquiries, staff should be careful about disclosing any Personal Data. In particular, our staff must:

- (a) check the caller's identity to make sure that information is only given to a person who is entitled to it.
- (b) suggest that the caller make such request in writing if there is any doubt with respect to the caller's identity and where such identity cannot be checked or confirmed.
- (c) refer to their line manager or the relevant Data Protection Officer for assistance in difficult situations. It is important that no one should be harassed or bullied into disclosing personal information because of the risk of disclosing such information to the wrong person.

14.2 When in doubt, please exercise caution. You must satisfactorily verify the identity of any individual who requests for any data under any of the rights listed in this policy or available in law. Do not disclose any Personal Data without proper verification or authorisation.

14.3 You may immediately forward any request from a Data Subject you receive, to the appropriate department, where it is not ordinarily handled by your business function.

15.0 TRANSFER

15.1 We may transfer Personal Data across borders by transmitting; transferring to; viewing or accessing that data in a different country.

15.2 We may transfer Personal Data to another country if:

- (a) The NDPC has issued an "adequacy decision" confirming equivalent protection under Section 42(2) of the NDPA, on the enforceability of data subject rights, independent supervision, and international commitments in respect of such country; or

- (b) The transfer uses an NDPC-approved cross-border data transfer instrument (CBDTI), such as standard contractual clauses (SCCs), binding corporate rules (BCRs), or certifications; or
- (c) The data subject provides explicit consent after being informed of the risks (e.g., lack of redress mechanisms in the recipient country); or
- (d) The transfer is necessary for
 - (i) A contract involving the Data Subject as a party;
 - (ii) Public interest;
 - (iii) Legal claims - the establishment or defence of legal claims; or
 - (iv) The protection of the vital interests of a Data Subject or other persons (particularly where the Data Subject is physically or legally incapable of giving consent - including without limitation, welfare, livelihood or medical emergency situations).

Such transfer of data will comply with NDPA safeguards, including data minimization and encryption.

15.3 Where Personal Data is to be transferred from Nigeria to an international organisation or a foreign country not covered by an NDPC adequacy decision under Section 42(2) of the NDPA, the Data Subject's explicit consent must be obtained. Prior to seeking consent, the Data Subject shall be:

- (a) Informed of specific risks arising from the transfer (e.g., lack of enforceable rights, absence of an independent supervisory authority, or potential government access to data);
- (b) Notified of the absence of alternative safeguards (e.g., adequacy decisions or approved cross-border data transfer instruments); and
- (c) Provided a clear option to withhold consent.
- (d) Such consent must be:
 - (i) Freely given, specific and documented;
 - (ii) Withdrawable at any time; and
 - (iii) Reaffirmed if the risks materially change.

16.0 REPORTING A PERSONAL DATA BREACH

16.1 In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data, we will promptly assess the risk to the Data Subjects' rights. Where appropriate, we will notify the affected Data

Subjects promptly as soon as we become aware of any such breach affecting them, if high-risk, or any applicable regulator - the NDPC, within 72 (seventy-two) hours of discovery, where such breach is likely to result in a high risk to the rights and freedoms of a data subject.

17.0 ACCOUNTABILITY

We will:

- (a) Integrate our data protection policies and the need for compliance with the applicable Data Protection Laws into our contracts and other relevant business documents;
- (b) Organise trainings for our staff from time to time in respect of data protection.
- (c) All staff must participate in all such mandatory trainings.
- (d) We will also conduct audits, tests and otherwise review our systems and processes from time to time to assess and ensure that adequate governance controls and resources are in place to ensure the proper use and protection of Personal Data.

18.0 RECORD KEEPING

- 18.1 In accordance with the relevant Data Protection Laws, we will keep relevant records of our Data Processing activities. These may also include records of consents obtained or withdrawn, where applicable.
- 18.2 The records may also include the name and contact details of all other relevant Data Controllers in respect of the Personal Data we use or share, descriptions of the Personal Data types, data subject types, processing activities, processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, transfers, retention period and a description of the security measures in place. Data maps may be created to reflect such details together with the relevant data flows.

19.0 DATA PRIVACY IMPACT ASSESSMENT (DPIA)

- 19.1 Where it is likely that the processing of Personal Data may result in a high risk to the rights and freedoms of a data subject by virtue the nature, scope, context, and purposes of such use or processing, a Data Controller will, prior to the processing, carry out a data privacy impact assessment.
- 19.2 Data protection impact assessment is a process designed to identify the risks and impact of the envisaged processing of Personal Data.

- 19.3 We will implement appropriate technical and organisational measures to ensure our processing of data complies with data privacy principles. This may also be referred to as privacy by design.
- 19.4 We will assess what measures we could implement by taking into account the modernity of such measures, cost of implementation; the nature, scope purposes of the processing; and the possible risks or impact on the rights and freedoms of Data Subjects in respect of the processing.
- 19.5 A data protection impact assessment should include:
- (a) a description of the processing, its purposes; and the legal basis or legitimate interest pursued by the Data Controller, Data Processor, or third party for the processing of such data;
 - (b) the necessity and proportionality of the processing in relation to its purpose;
 - (c) the risk to the rights and freedoms of the data subject; and
 - (d) the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of Personal Data, taking into account the rights and legitimate interests of a data subject and other persons concerned.

20.0 DIRECT MARKETING

- 20.1 Where Personal Data is processed for direct marketing purposes, the data subject shall have the right to object, at any time, to the processing of Personal Data concerning the data subject, which includes profiling to the extent that it is related to such direct marketing.
- 20.2 A data subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible and the Personal Data shall no longer be processed for such purposes.
- 20.3 Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

21.0 SHARING PERSONAL DATA

- 21.1 We may share the Personal Data in our possession with third parties, such as our service providers where:
- (a) They need to know such information for the purpose of providing contracted services or for the performance of any contract we enter into with them or you.
 - (b) Sharing the Personal Data complies with a privacy notice, policy or disclosure made known to the Data Subject, or complies with a lawful basis further to this policy.
 - (c) The third party has agreed to comply with the Data Protection Laws, required data security standards, policies and procedures and put in place adequate security

measures for the protection of the data. We reserve the right to audit third-party compliance with this policy and to suspend and/or terminate contracts for any potential, suspected or actual violation.

- (d) The transfer complies with applicable Data Protection Laws and any cross-border transfer restrictions.
- (e) A fully executed written contract is in place which contains the relevant data protection clauses, and which requires the compliance of such party with the Data Protection Laws.

21.2 We may share Personal Data with any affiliate or member of our group, group holding company and subsidiaries.

22.0 POLICY REVIEW

22.1 We may review this policy from time to time to bring same in line with improvements and advancements and to optimise its effectiveness in achieving its objectives.

22.2 Without prejudice to the preceding provision, we may also undertake a yearly review of this Policy.

22.3 All staff, customers, business partners, suppliers, consultants, service providers and all parties whom we engage with are encouraged to read our policies regularly to be aware of their contents, and to also offer your feedback, recommendations, inquiries and enquiries in respect of this Policy.