

DATA PROTECTION AND PRIVACY POLICY

Effective Date: This Policy shall be effective from July 1, 2025

Introduction

- (a) we.yan Nigeria Ltd. (“**We**”, “**Our**”, “**Us**”, the “**Company**”) is a financial technology company which operates a multi-functional platform for the purpose of facilitating cross-border payments and a wide range of digital financial services. We are really committed to protecting the privacy and confidentiality of the Personal Data which you disclose to Us.
- (b) Our Data Protection and Privacy Policy (the “**Policy**”) demonstrates our respect for your privacy and explains our information collection and sharing practices, which are in line with the Nigerian Data Protection Act 2023 and all applicable data protection laws in Nigeria (“**Applicable Data Protection Laws**”). Regardless of whether you provide us with your Personal Data via our websites, mobile application or in another manner (e.g., telephone, regular mail or face-to-face interactions, including through our extension agents), we will strive to honor your privacy preferences and process your Personal Data in compliance with Applicable Data Protection Laws.
- (c) This Policy represents the minimum principles and standards applicable and where there is a higher standard or principle of data protection imposed by the Company or any Applicable Law, the higher standard or principle shall apply.

Definition

In this Policy, the following words shall, unless the context requires otherwise, have the following meanings:

Term	Definition
Applicable Data Protection Laws	means any statute, regulation, resolution, rule, enactment, judgement, order, decree, directive, notification, clarification, guideline, policy, requirement or any governmental direction having the force of law and any form or decision or any determination by or interpretation of any of the foregoing by a Governmental Authority, now or hereafter in effect, in each case, as amended, re-enacted or replaced to the extent applicable to the Company;
Customer or User	means any individual within the Federal Government of Nigeria to which the Company provides its products or services;
Data Protection Legislation	means any law, statute, subordinate legislation, regulation, order, mandatory guidance or code of practice, a judgment of a relevant court of law, or directives or requirements which relates to the protection of individuals with regard to the processing of Personal Data including the NDPR and any statutory modification or re-enactment thereof and the NDPR;
we.yan	means we.yan’s web application, mobile application, and digital platform;
we.yan Group	means we.yan, its subsidiaries, affiliates, and related entities wherever located;
Data Subject	means you, the Customer or User of the Service as an identified or identifiable natural person who is the subject of Personal Data;
Jurisdictions	means Nigeria or any other country in which we.yan operates;

Personal 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, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social, or economic identity of that individual;
Personal Data Breach	means a breach of security of a data controller or data processor leading to or likely to lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed;
Governmental Authority	means any regional, national, county, municipal and/or local authority or any governmental, administrative, or regulatory body inside Nigeria having statutory competence to promulgate rules and regulations having the force of law with regard to the Company;
NDPA	means the Nigeria Data Protection Act 2023;
NDPR	means the Nigeria Data Protection Regulation 2019 as may be amended from time to time;
Relevant Information	means information that We require for purposes of providing full access to the Services;
Personnel	means all employees, directors and officers of the Company, including board members, contractors, temporary employees, consultants, trainees, seconded staff, casual workers, agency staff, interns, agents, sponsors, or any other person engaged with the Company;
Processing	means any operation or sets of operations which is performed on Personal Data or sets of Personal Data whether or not by automated means, such as: (a) collection, recording, organization, structuring; (b) storage, adaptation or alteration; (c) retrieval, consultation or use; (d) disclosure by transmission, dissemination, or otherwise making available; or (e) alignment or combination, restriction, erasure or destruction and Process shall be construed accordingly;
Sensitive Personal Information	means data revealing the natural person's race, health status, ethnic social origin, conscience, religious or other beliefs, genetic data, biometric data, political views, trade union membership, criminal records, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the Data Subject; and
Third Party	means a natural or legal person, public authority, agency or other body, other than the Data Subject, data controller, data processor or persons who, under the direct authority of the data controller or data processor, are authorized to Process personal data.

Purpose of this Policy

This Policy is based on the privacy and data protection principles and requirements under Applicable Data Protection Laws. It is applied in view of our overarching desire to comply with the provisions of the Applicable Data Protection Laws, to preserve the confidentiality of your Personal Data and to provide you with our services as effectively as possible within the bounds of the law.

This Policy applies to all Personal Data processed by Us and is part of Our approach towards full compliance. This Policy is applicable to all our services accessed by you, as well as in Our interactions with you, including our processing of your Personal Data. All Our Personnel are required to comply with this Policy.

This Policy outlines how We collect, use, and protect your Personal Data in Our interactions with you and in accordance with Applicable Data Protection Laws.

Purpose of Processing and Lawful Basis

Purpose	Lawful Basis
Processing your Personal Data to provide you with access to our website.	- Where it is in our legitimate interest to manage and run our business efficiently. - Where we have your consent to do so. - Where we have a contract in place with you, requiring our processing of your Personal Data.
Processing your Personal Data to provide you with access to our mobile application.	Where necessary to perform the contract we have with you.
Processing your Personal Data to respond to your inquiries via our support services.	- Where we have your consent to do so. - Where necessary to perform the contract we have with you. - Where it is in our legitimate interest to manage and run our business efficiently. - Where it is necessary to comply with a legal obligation placed on us by an existing law.
Processing your Personal Data is in order to provide you with our services or further to our engagement with you as a vendor or third-party service provider.	- Where necessary to perform the contract we have with you. - Where it is in our legitimate interest to manage and run our business efficiently.
To utilize cookies and to share your information with third parties for advertising purposes.	- Where we have your consent to do so. - Where it is in our legitimate interest to manage and run our business efficiently.
To personalize your experience, improve the Services, and develop new features.	It is in our legitimate interests to manage and run our business efficiently and consider future strategy.
For tax compliance purposes.	Where it is necessary to comply with a legal obligation placed on us by existing law. Compliance with legal obligations for remittance of tax information and related purposes.

Purpose	Lawful Basis

Whenever the processing of your Personal Data is dependent on your consent, We will request and obtain that consent directly from you at the point of data collection. In situations where your Personal Data is accessed through a third party acting on the basis of your consent, We will take appropriate steps to confirm that such consent was given voluntarily by you and was not obtained through deception, coercion, or improper pressure.

By selecting the 'Contact Us' option within Our mobile application, you are expressly agreeing to the collection, storage, and use of your Personal Data in accordance with the provisions of this Policy. If you do not accept the terms of this Policy, you are advised to discontinue use of the mobile application immediately.

It is important to note that you retain the right to withdraw your consent at any time. However, any processing of your Personal Data carried out before the withdrawal of consent will remain lawful and valid based on the consent previously provided.

Data Protection Principles

- (a) We will retain your Personal Data only for as long as is necessary for the purposes set out in this Policy. We will retain and use your Personal Data to the extent necessary to comply with Our legal obligations in accordance with Applicable Data Protection Laws, resolve disputes, and enforce Our legal agreements, policies, and analysis purposes (to strengthen the security or to improve the functionality of Our Service).
- (b) We will ensure that the Personal Data held by Us is accurate, complete, kept up to date and relevant to the purpose for which We collected it. The Company shall take all reasonable action in erasing or rectifying any Personal Data that is incorrect, without delay.
- (c) We will ensure that the Personal Data collected is adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.
- (d) The Company will not use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless it has informed the Data Subject of the new purposes and they have consented, where necessary.
- (e) The Company shall ensure compliance with the principle of collecting data only for specific, explicit and legitimate purposes and not Processing them any further in a manner that is incompatible with those purposes.
- (f) The Company shall process your Personal Data in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Processing of Personal Data

- (a) The Company shall Process Personal Data in a lawful, fair and transparent manner for a specified purpose.

(b) The Company shall be responsible for ensuring its compliance with the principles set out in the Applicable Data Protection Laws. Personal Data shall only be Processed where one (1) of the following conditions is satisfied:

- I. The Data Subject has given Consent to the Processing of his or her Personal Data for one or more specific purposes;
- II. Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
- III. Processing is necessary for compliance with a legal obligation to which the Company is subject;
- IV. Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;
- V. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority; or
- VI. Processing is necessary for the purposes of the legitimate interests pursued by the Company, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, which require protection of Personal Data.

The Personal Data We Collect

(a) We collect and process certain information about you through the services you use, such as our mobile application, when you are onboard as a user, subscribe to Our newsletter as a community member, contact Us via web, mobile application or through social media sites. The specific categories of Personal Data we may collect include, but are not limited to:

- i) **Contact Information:** This includes your name, date of birth, contact address, email address, phone number, professional details, nationality, state or province, and national identity number.
- ii) **Communication Data:** Information related to your interactions with Us, including emails, support inquiries, and any feedback you provide.
- iii) **Financial Information:** This includes your bank account information, bank account name and number, bank verification number, mobile payment number, payment method preferences, and any other information you choose to provide.
- iv) **Usage Data:** We collect data about how you use our mobile application, such as device information.
- v) **Device and Log Information:** We gather information about the devices you use to access our services, including device type, operating system, and unique device identifiers. Additionally, we collect log information, such as IP addresses, browser type, and access times, to improve our digital platform.

- vi) **Geographical Data:** We collect information on your geographical location each time you open and use our mobile application. This enables Us to provide location specific services, support feature flagging, and optimize your app experience. Your location data is processed in accordance with Applicable Data Protection Laws and solely for the purposes described in this Policy.
 - vii) **Other Information:** Any additional information you provide to Us voluntarily or that We collect, such as your potential value to Our program, public information from publicly available sources, including open postings on social media.
- (b) We will always strive to minimize the collection of Personal Data to what is necessary for the intended purpose. Where applicable and required by law, We will obtain your consent before collecting certain categories of Personal Data. Our Personal Data collection is always conducted in accordance with Applicable Data Protection Laws and best practices.
- (c) It is important to note that certain Personal Data may be necessary to provide you with Our services, and refusal to provide such data may impact Our ability to serve you effectively. We are committed to ensuring the security and confidentiality of your Personal Data, and Our data processing activities are conducted in accordance with this Policy and Applicable Data Protection Laws.
- (d) We do not collect, store, transmit, or process your biometric data in any form. We do not retain any record, backup, or copy of your biometric information. As a result, you are entirely responsible for managing access to your device and biometric settings. If you lose access to your device or biometric login, We cannot assist with account recovery, as We have no visibility or control over your authentication method. However, We have a recovery protocol that allows customers to regain access to their accounts where the biometric authentication permanently fails.

Recipients of Personal Data

We may disclose your Personal Data to third parties where necessary for the efficient delivery of our services or in order to fulfil legal, regulatory, or contractual obligations. Such disclosures may be made to the following categories of recipients:

- (a) Our affiliates and international offices;
- (b) Any member of the we.yan Group; and
- (c) Selected third-party service providers and business partners.

Disclosure of Personal Data

The Company shall only disclose Personal Data with Third Parties, where:

- (a) a Third-Party service provider requires the information for the purposes of providing the contracted services;
- (b) the disclosure is required by Applicable Law;
- (c) the Data Subject's Consent has been obtained;

- (d) the Third-Party has agreed in writing to comply with the required data security standards, policies and procedures, and put adequate security measures in place in accordance with the Applicable Laws; and
- (e) the transfer complies with any applicable cross-border transfer restrictions under the Data Protection Legislation; and

Rights of Data Subjects

We have processes in place to ensure that We can facilitate any request made by a Data Subject to exercise their rights under Applicable Data Protection Laws. All staff have received training and are aware of the rights of Data Subjects. Our Data Protection Officer (“**DPO**”) working with other trained staff will ensure that all requests will be considered without undue delay and within one month of receipt as far as possible. The contact details of our DPO are indicated in Clause 15 below.

As a Data Subject, you have the right to:

- (a) request access to your Personal Data (commonly known as a “**Data Subject access request**”). This enables you to receive a copy of the Personal Data we hold about you and to check that we are lawfully Processing it;
- (b) request correction or rectification of the Personal Data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to Us;
- (c) request erasure of your Personal Data. This enables you to ask Us to delete or remove Personal Data where there is no good reason for Us continuing to Process it. You also have the right to ask Us to delete or remove your Personal Data where you have successfully exercised your right to object to Processing, where We may have Processed your information unlawfully or where We are required to erase your Personal Data to comply with local law. Note, however, that We may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request;
- (d) object to Processing of your Personal Data where We are relying on a legitimate interest (or those of a third party) and there is something about your situation which makes you want to object to Processing on this ground as you feel it impacts your fundamental rights and freedoms;
- (e) object when we are Processing your Personal Data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to Process your information which overrides your rights and freedoms;
- (f) request restriction of Processing of your Personal Data. This enables you to ask Us to suspend the Processing of your Personal Data in the following scenarios:
 - I. if you want Us to establish the data’s accuracy;
 - II. where Our use of the data is unlawful, but you do not want us to erase it;

- III. where you need Us to hold the data even if We no longer require it as you need it to establish, exercise or defend legal claims; or
 - IV. you have objected to Our use of your data but We need to verify whether We have overriding legitimate grounds to use it;
- (g) request the transfer of your Personal Data to you or to a third party. In the event, We will provide to you, or a third party you have chosen, your Personal Data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided Consent for Us to use, where We used the information to perform a contract with you or where processing is carried out by automated means;
- (h) withdraw Consent at any time where We are relying on Consent to Process your Personal Data. However, this will not affect the lawfulness of any Processing carried out before you withdraw your Consent. If you withdraw your Consent, We may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your Consent
- (i) ask Us not to continue to Process your Personal Data for marketing purposes

Please note that the specific timeframe for responding to requests may vary depending on the complexity of the request. Within one month of Our receipt of your request, We will either respond or notify you if We require additional time to process your request.

Data Retention Period

We will retain your Personal Data in line with applicable data protection regulations and only for as long as it is necessary to fulfil the purposes for which it was originally collected. Additionally, certain information may be preserved beyond the conclusion of your relationship with us, for legitimate reasons such as record-keeping and archival purposes.

The length of time We retain your Personal Data is influenced by several factors, including:

- (a) the specific reason the information was gathered — for instance, whether it is required to initiate or defend legal proceedings;
- (b) any statutory obligations that mandate the retention of certain categories of data for a legally prescribed period; and
- (c) whether data must be preserved due to ongoing legal action, a court directive, or a regulatory or law enforcement investigation.

Once your Personal Data is no longer required for these purposes, We will securely dispose of or anonymize it. If you would like more information regarding Our data retention approach, please consult the “Contact Us” section on our mobile application.

Cross-border Transfers

We operate systems that may make your Personal Data accessible to members of the we.yan Group around the world and may often transfer your Personal Data to them. Where We share or transfer your Personal Data, We will do this in accordance with Applicable Data Protection Laws and will take appropriate safeguards to ensure its protection. These safeguards may include ensuring that:

- (a) all recipient located in another country operates under a law, binding corporate rules, contractual arrangements, code of conduct, or certification mechanism that guarantees an adequate level of protection for Personal Data; or
- (b) in situations where such mechanisms are not available, transfers will occur only if one of the following conditions is met if:
 - I. you have provided explicit, informed consent to the transfer and have not subsequently withdrawn it, having been advised of any potential risks;
 - II. the transfer is essential for the performance of a contract to which you are a party, or for taking steps at your request prior to entering such a contract;
 - III. the transfer benefits you exclusively, and it would either not be practicable to obtain your consent or it is reasonable to assume you would provide it if asked;
 - IV. the transfer is necessary for compelling public interest reasons;
 - V. it is required for the establishment, exercise, or defense of legal rights; or
 - VI. transfer is necessary to protect your vital interests or of other persons, where you are physically or legally incapable of giving consent.

How we Secure your Personal Data

We take full responsibility for maintaining the confidentiality, accuracy, and security of the Personal Data we process. To achieve this, We have implemented comprehensive security measures aligned with industry standards and best practices, aimed at preventing unauthorized access, use, disclosure, alteration, or destruction of your Personal Data.

Our security framework includes, but is not limited to, the following measures:

- (a) **Encryption:** All Personal Data under our care is encrypted, both in transit and at rest, especially during transfers to authorized third parties, always ensuring its confidentiality.
- (b) **Access Management:** Access to Personal Data is strictly restricted to authorized personnel who require it for their job functions, and these individuals are bound by strict confidentiality obligations.
- (c) **Periodic Security Assessments:** We conduct routine audits and security reviews to identify and address potential system vulnerabilities and strengthen our infrastructure.
- (d) **Data Backup Procedures:** Regular data backups are conducted to prevent loss of information and to facilitate operational continuity in the event of unexpected incidents.
- (e) **Incident Management:** We have established an incident response framework to promptly manage and mitigate any data breach or security threat and, when required by law, to notify affected individuals and regulatory authorities.
- (f) **User Authentication Controls:** Robust authentication protocols are in place to ensure that only authorized users can access systems containing Personal Data.

- (g) **Data Minimization Principles:** We only collect and process Personal Data strictly necessary for defined purposes, thereby reducing the risk of unauthorized exposure or misuse.
- (h) **Anonymization and Pseudonymization:** Where appropriate, We apply anonymization or pseudonymization techniques to safeguard Personal Data and minimize risks.
- (i) **Network Protection:** We deploy advanced network security measures, including firewalls, intrusion detection systems, and secure configurations, to defend against external threats and unauthorized access.
- (j) **Employee Training and Awareness:** Regular training sessions are provided to employees on data protection obligations, privacy principles, and security best practices to foster a culture of data privacy and security compliance.

While We implement rigorous security protocols to protect your Personal Data, it's important to acknowledge that no system can be completely immune from potential risks. We encourage you to take proactive steps in securing your information — such as using strong, unique passwords, safeguarding your login credentials, and reporting suspicious activities promptly.

If a data breach occurs that poses a significant risk to your rights and freedoms, We will notify you and the appropriate supervisory authorities in accordance with relevant legal requirements. Our commitment is to consistently review and enhance our security measures to better protect your Personal Data.

Automated Decision-Making and Profiling

We may employ automated decision-making and profiling processes to provide you with Our services by utilizing algorithms and data analysis to assess the information you provide to Us. The purpose of these automated processes is to make well-informed decisions that enhance our services and ensure they meet your specific needs.

You have the right to object to the use of automated decision-making and profiling processes.

Performance through Affiliates

We may carry out our obligations and exercise our rights under this Policy either directly or through any member of the we.yan Group. Accordingly, references in this Policy to “We,” “Our,” “Us,” or “we.yan” shall, where applicable, be deemed to include any member of the we.yan Group acting on its behalf.

Third-Party Links

Our mobile application may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share Personal Data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy policy of every website you visit.

Cookies

What is a cookie? Cookies are text files containing small amounts of information which are downloaded to your device when you visit a website or use a mobile application. Cookies are then sent back to the originating website or mobile application on each subsequent visit, or to another website that recognises that cookie. Cookies are useful because they allow a website or mobile application to recognise a user's device, preferences and generally help to improve your online experience.

Cookies may be essential for website or mobile application function, for analytics, personalization and/or advertising purposes. By using Our website (when available), you agree that We can place these types of cookies on your device. If you want to restrict or block Our use of cookies, you should do this through the web browser or mobile application settings for each browser you use and, on each device, used to access the internet. Please be aware that some areas of Our mobile application website may not function properly if you restrict or block cookies. However, you can allow cookies from specific websites by making them "trusted websites" in your web browser. You should be able to select cookie preferences within your web browser settings.

Please also note that We have taken measures to ensure that all methods adopted by us to engage automatically with you via cookies do not violate your privacy rights under the NDPA. In the case of cookies, We ensure that they have security protocols and are not vulnerable to abuses by anyone.

.

Contact Us

If you have any questions, concerns, or requests regarding your Personal Data or this Policy, or you would like to exercise one of your data protection rights, please contact Us via:

Email: support@weyan.app

we.yan chat name: "we.yan support"

Right to Lodge a Complaint

If you believe that your data privacy rights have been violated, or you wish to report a complaint to the Nigeria Data Protection Bureau (NDPB), you may contact the NDPB office through the details below

Address: No. 5, Donau Crescent, off Amazon Street, Maitama, Abuja, Nigeria

Helpline number: 09160615551

Website: <https://ndpb.gov.ng/>

Changes to this Policy

We reserve the right to update or modify this Policy to reflect changes in Our data processing practices or legal requirements. We will notify you of any material changes by posting the updated Policy on Our mobile application or by other means of communication, where appropriate. We encourage you to review this Policy periodically to stay informed about how we are processing your Personal Data.

