SendUs Customer & Recipient Privacy Policy

Customer bookings, delivery recipients and SendUs–SafeDrive data flows

SendUs Customer & Recipient Privacy Policy

1. Controller and scope

SendUs is operated by SafeRoads Technology Services, trading as SafeRoads Tech, RC: 8726781, Nigeria. We act as controller for the purposes described here. Support contact: support@sendus.com.ng. Effective date 20th November 2026.

This notice covers customers, business representatives, senders, pickup contacts and recipients using or receiving SendUs delivery services, including recipients who do not have an account. The SafeDrive Driver Privacy Notice covers drivers' trip recording, verification, safety analysis and rewards. A driver who also books a parcel is covered by this notice for that booking.

Our privacy contact receives privacy requests and escalates them to the person responsible for data protection. Details of any legally required DPO or EEA representative are published in the Contact and Processing Schedule attached to this notice. We do not claim either appointment has already occurred.

2. Information and sources

Account information: name, phone number, email, business details supplied for a business account, authentication records and preferences. We receive it from you or an authorised business administrator.

Delivery information: sender and recipient contact details, pickup and destination addresses, parcel description, handling instructions, order reference, price, status and timestamps. We receive it from the person arranging the delivery, the assigned driver and fulfilment records. Include only information needed to transport the item; do not disclose unnecessary medical, financial or identification details in instructions.

Delivery progress and proof: assigned-driver location during the job, route/distance records relevant to the delivery and the proof actually captured, such as a delivery code, signature or photograph. Proof must be limited to the handoff, not unrelated faces, private documents or parcel contents.

Payment records: amount, currency, transaction reference, payment method identifier, status and refund record returned by the payment provider. The attached schedule states the provider and whether any additional payment information reaches SendUs; no claim that SendUs stores or never receives full card details is made without that verification.

Support and incident records: messages, attachments, feedback and information necessary to investigate a query or incident, received from the people involved. A report is an allegation to investigate, not an established fact.

Technical records: app/device version, operating system, IP address, access times, authentication/security events and crash information needed to operate the service. The attached schedule lists additional SDKs and identifiers, if any. This notice does not authorise collection of calendar contents, contact lists, microphone recordings, biometric templates or advertising profiles.

3. Why we use information and the lawful basis

Account and customer-requested delivery: we use account, order, payment, tracking and necessary support information to perform our contract with the customer or take steps the customer requests before a contract. This basis does not cover unrelated advertising or everyone named in a booking.

Non-account recipients and pickup contacts: we use necessary contact, address and delivery information under legitimate interests in completing the requested delivery and coordinating the handoff. We assess necessity and balance those interests against the person's rights. We do not treat the sender's contract as the recipient's contract.

Security, fraud investigation and proportionate delivery evidence: we use relevant technical, order, proof and incident records under legitimate interests in protecting users, parcels and our systems. We document necessity and balancing and limit access to people who need the information.

Service diagnostics: we use necessary crash and security records under legitimate interests in keeping the app functional and secure. Non-essential analytics or device tracking requires a separate choice where law requires it.

Mandatory records and disclosures: we process only the information necessary to meet an identified legal obligation. The attached schedule identifies applicable recordkeeping obligations. Where GDPR applies, reliance on Article 6(1)(c) requires an applicable EU or Member-State legal basis; Nigerian law alone is not automatically that basis.

Optional marketing: we use your selected contact details only after a specific opt-in for promotional communications. You can withdraw through the unsubscribe control or privacy contact without losing ordinary delivery access. Non-account recipient details supplied for a delivery are not added to marketing lists by default.

Genuine emergencies: we disclose necessary information to protect vital interests where that legal condition is met. Routine monitoring is not justified as an emergency.

Where sensitive information is necessary to investigate an incident, we first establish the additional condition required by the applicable sensitive-data rules. Contract acceptance is not sufficient by itself.

4. Permissions, customer location and tracking

Customer device location is optional for locating an address and is accessed only for the disclosed location feature after permission. This policy does not authorise continuous customer background tracking.

Camera or selected-photo access is requested for the upload you choose. Delivery notifications are separate from optional promotional notifications. Refusing an unrelated permission does not prevent you receiving a parcel or making a privacy request.

Delivery participants receive only the tracking information necessary for their job. Access is restricted to authorised accounts or protected, time-limited links; authentication and expiry are specified in the attached schedule. Customers do not receive a driver's unrelated or off-duty journey history.

Device permissions can be changed in device settings. Removing a permission limits the dependent feature, not all account functions. Closing an app does not itself erase information already lawfully retained.

5. Recipient notices and required information

A recipient need not open an account to receive a delivery, ask a privacy question or exercise rights. We provide the required notice about indirectly supplied information before collection unless a legal exception applies. The attached schedule identifies the actual recipient-notice channel. A sender's instruction to inform the recipient does not remove our own duty.

Where GDPR Article 14 governs, its information requirements and deadlines also apply: generally within one month and at first communication or disclosure if earlier, unless an applicable exception permits otherwise.

A usable pickup/destination and appropriate contact information are necessary for delivery. Optional photos, marketing choices and unrelated profile fields are not. If a required detail is missing, we explain why the affected booking cannot proceed.

6. Sharing and SendUs–SafeDrive integration

Assigned drivers receive the necessary pickup/recipient names, operational contacts, addresses and parcel instructions. Customers and authorised recipients receive the appropriate assigned-driver identification, job status and delivery progress. The schedule states whether telephone numbers are masked and how post-job access ends.

SafeDrive and SendUs exchange driver eligibility/verification status, job assignment, active-delivery location, delivery proof and necessary settlement/support information. This does not authorise unrestricted merging of personal-trip histories or disclosure of driver identity documents, bank accounts or raw safety records to customers. The attached schedule confirms the operator of both apps and any separate controller arrangement.

Business customers receive their own order and reconciliation information, not unrelated customer histories. Where a particular merchant service genuinely makes SendUs a processor, a separate processing agreement governs that activity; the label does not automatically cover all SendUs operations.

Contracted providers support hosting, maps, authentication, messaging, payments, security and support. Their roles and processing locations appear in the attached schedule. Processors receive written purpose, confidentiality, security, assistance and deletion obligations. Independent controllers are identified with their own notices.

Authorities, courts, insurers and professional advisers receive proportionate information only under an established legal basis. We assess the scope and validity of requests. A business transfer requires confidentiality, an appropriate basis and required change-of-controller notice. This notice does not authorise selling personal data, advertising-audience sharing or insurer access to journey histories; any proposed new purpose requires assessment, safeguards and advance disclosure.

7. Matching, profiling, pricing and significant decisions

Booking details, driver eligibility, availability and location support assignment. The attached schedule states the actual matching method and factors. Before using a safety score to affect job access or priority,

we explain that effect to drivers and implement the required legal safeguards. Customer fraud flags are evidence for investigation, not automatically conclusive proof.

Matching: assignment is rules-based on distance and availability. Candidate inputs may include driver availability, pickup proximity, vehicle suitability and service area.

Pricing: factors used such as distance, vehicle category, parcel requirements and handling fee. SendUs does not use surge pricing, personalised pricing or a person's inferred willingness to pay unless that is genuinely implemented and lawfully disclosed.

Security: actual fraud will be flagged and temporary restrictions and verification steps will follow. Some actions are automated but they will receive meaningful human review.

We do not make a final account termination or similarly significant adverse decision solely through automation under this policy. A trained reviewer assesses disputed significant outcomes and can change the decision. A future change to solely automated significant decision-making requires a permitted legal condition, meaningful explanation, applicable safeguards and notice before use.

8. Retention, deletion and security

The attached Retention Schedule states the actual period and trigger for each category. We do not keep identifiable information merely because storage is inexpensive or for undefined future opportunities. Raw location, proof, accounting records and security logs have distinct purposes and retention decisions.

When a period of 180 expires after account deletion, we delete or irreversibly anonymise the information unless an identified legal duty or documented claim hold requires specified records to remain. Held records are restricted to that purpose and reviewed when the matter ends. Pseudonymisation is not anonymisation. Backup deletion and restored-data handling follow the stated backup cycle.

Account closure starts the applicable closure/deletion process; it does not automatically remove mandatory tax records or evidence necessary for a live claim. We explain any refusal to erase data and the available challenge route.

Account details will be deleted upon close such as personal information; delivery records and proof will be retained for accounting and legal basis; raw precise location will be deleted; invoices/payment/tax records will be retained for accounting and legal basis; support/incident/security records will be retained for legal basis; marketing consent/suppression evidence will be retained for business basis.

We maintain risk-appropriate technical and organisational protection. The attached schedule states verified controls, not untested security claims. Absolute security is not guaranteed. We investigate incidents and meet applicable regulator and individual notification duties. Nigerian and GDPR notification rules are assessed separately; the incident process addresses applicable 72-hour regulator deadlines and high-risk individual notification requirements.

9. Your rights and complaints

Subject to applicable conditions, you can request information, access and a copy, correction, deletion, restriction, eligible portability, objection to legitimate-interest processing, withdrawal of consent and protections relating to significant automated decisions. You can object to direct marketing at any time. Withdrawal does not invalidate earlier lawful processing.

Contact our privacy email; account closure requests are also accepted there. We verify identity proportionately and do not require an account or payment of delivery charges to exercise rights. Requests are normally free; a lawful refusal or permitted fee is explained with complaint rights.

We respond within the applicable deadline. Under GDPR, the normal period is one month; a permitted extension of up to two additional months for complexity or volume is explained within the first month. Any shorter binding Nigerian requirement applies where relevant.

You can complain to the Nigeria Data Protection Commission through https://ndpc.gov.ng/. Where GDPR applies, you can contact a competent supervisory authority, including in your habitual residence, workplace or location of the alleged infringement. Court remedies remain available. Our internal contact process is not a waiver of regulatory rights.

10. Children and changes

SendUs account holders must be at least 18. A delivery involving a child recipient requires a lawful, safeguarded arrangement and appropriate adult involvement; we do not treat an age rule as permission to ignore child data already received.

We notify material policy changes through a suitable direct or in-app channel and update the effective date. New consent-dependent uses require fresh consent. Publishing a revision is not permission to disregard the purpose for which information was collected.

11. Complaints, policy changes and current framework

Complain directly to the NDPC through https://ndpc.gov.ng/, or use the competent EEA authority where GDPR applies. Statutory court remedies remain available; internal support is not a mandatory barrier. Material changes receive appropriate notice and new consent-dependent uses require fresh choice. Version 1.0, effective 20th November 2026.

This notice follows Nigeria's NDPA 2023 and GAID 2025. GAID Article 3 ceases NDPC application of NDPR 2019 as a regulatory instrument while preserving prior actions. GDPR coverage depends on Article 3 scope, not citizenship alone.