

Privacy Policy

Purechem Manufacturing Limited (RC 641774) · TopConnect

Effective 23 July 2026 · Last updated 23 July 2026

1. Who we are and what this policy covers

This Privacy Policy explains how Purechem Manufacturing Limited (RC No. 641774), with its head office at Afprint Compound – 2nd Gate, 122/132 Oshodi–Apapa Expressway, Iyana-Isole Bus Stop, Isolo, Lagos, Nigeria (P.O. Box 2701, Lagos, Nigeria) (“Purechem”, “we”, “us”, or “our”), collects, uses, shares, stores, and protects personal data in connection with the TopConnect distributor mobile application and its supporting services (the “Platform”).

This Policy applies to distributor applicants, approved distributors, authorised representatives of distributor businesses, and other people whose information is submitted through the Platform. Purechem is the data controller for this information. We process personal data under the Nigeria Data Protection Act 2023, applicable NDPC guidance, and other applicable Nigerian law.

TopConnect is a business-to-business service for people aged 18 years or older. It is not directed to children.

2. Plain-language summary

- We collect information needed to review distributor applications, operate accounts, process orders and payments, provide rewards, send service notices, maintain security, and retain business records.
- We do not sell personal data and do not use third-party advertising or cross-app tracking.
- Camera, photo-library, file, and notification permissions are used only when needed for the feature you choose.
- Choosing Delete account signs you out and removes access. You may reactivate within 30 days by signing in.
- After 30 days, your account can no longer be used to sign in. Deleting your account does not erase Purechem's business records, which are retained as required for legal and accounting purposes.
- A request to exercise a legal data right, including an erasure request, is separate and will be assessed under applicable law.

3. Personal data we collect

Identity, age, and contact information

Full name, date of birth, email address and verification status, phone number, profile or distributor photograph when provided, and account or distributor identifiers.

Business and application information

Business or trading name, address, city, state, company or CAC registration number when provided, application status, review and correction history, Purechem notes, salesperson assignment, distributor tier, ERP code, and related classifications.

Account and authentication information

Login identity, email verification, password-reset events, session information, authentication timestamps, security events, account status, deletion or reactivation status, and audit records. Passwords are processed and stored in hashed form by our authentication provider; we do not store readable passwords.

Orders, fulfilment, and commercial records

Cart and order contents, quantities, prices, discounts, special rates, free-of-charge items, order channel and history, status, cancellation, collection and fulfilment events, warehouse and pickup details, balances, statements, ledger entries, revenue and reconciliation records, loyalty points, rewards, redemptions, and adjustments.

Payments and supporting evidence

Bank-transfer reference, date, amount, review status and decision, payment-to-order allocation, and uploaded receipt or proof files. The app does not intentionally collect full payment-card numbers or card security codes.

Communications and technical information

Support messages and files, correction responses, notification records, device push tokens, operating system and app version, approximate network address, crash or error information, timestamps, security telemetry, and app interaction events required to operate, diagnose, improve, and secure the Platform.

4. How we collect personal data

We receive information directly from you, from the distributor business you represent, automatically through your use of the app, from authorised Purechem personnel and business systems, and from service providers that support authentication, storage, communications, security, and Platform operation.

5. Why we use personal data

We use personal data to:

- verify eligibility and review distributor applications;
- create, authenticate, protect, and administer accounts;
- calculate quotes and manage orders, payments, balances, fulfilment, rewards, and commercial records;
- provide support and send requested or operational communications;
- prevent fraud, investigate misuse, preserve audit trails, and protect the Platform;
- comply with tax, accounting, legal, regulatory, and dispute-related obligations; and
- diagnose technical issues and improve Platform reliability.

Depending on the context, our lawful bases include performing or preparing a contract, complying with legal obligations, pursuing legitimate business and security interests, and consent where applicable. You may withdraw consent-based processing, but withdrawal does not affect earlier lawful processing or processing supported by another lawful basis.

6. Push notifications and device permissions

With device permission, TopConnect may send notices about application review, account security, orders, payments, balances, fulfilment, rewards, support, and service changes. You may disable notifications in

device settings, although important account information may still appear in the app or be sent through another appropriate channel.

Camera, photo-library, and file access are requested only when you choose to capture or upload a document such as payment evidence. You can refuse or later change device permissions; the related feature may then be unavailable.

7. Local device storage

The app may temporarily store session information, preferences, cart state, cached content, and other limited data on your device. Protect your device with an appropriate passcode and sign out before giving it to another person. Removing the app may remove local data but does not delete server-held business records.

8. When we share personal data

Information may be accessed by authorised Purechem personnel and affiliated operations where necessary for review, fulfilment, finance, customer support, security, compliance, and administration. Access is limited by role and business need.

We also use service providers for cloud hosting and database services, authentication, file storage, email, push notifications, security, diagnostics, and infrastructure. These providers act under their contracts and applicable law. We may disclose information when required by law, to protect rights or safety, investigate fraud or misuse, resolve disputes, or support a lawful corporate transaction. We do not sell personal data.

9. International data transfers

Some service providers may process or store information outside Nigeria. Where personal data is transferred internationally, we use measures required by applicable law, which may include contractual, organisational, and technical safeguards and an assessment of the receiving environment.

10. Account deletion, access closure, and retention

Voluntary account deletion

If you choose Delete account, access is disabled and you are signed out immediately. During the following 30 days, signing in reactivates your account. If it is not reactivated within that period, your account can no longer be used to sign in.

Retention

Deleting your account does not by itself erase Purechem's records. Your account and business records may be retained as required or permitted by applicable law, including for legal, accounting, tax, and dispute purposes, and are deleted, anonymised, or restricted when no longer required.

Legal erasure requests are separate

You may request erasure or exercise another applicable data right by contacting us. We will assess the request under applicable law, and may retain information where a lawful exception or continuing obligation applies.

11. Your data-protection rights

Subject to applicable law, you may ask for access to or a copy of your personal data, correction of inaccurate information, deletion where legally available, restriction or objection to certain processing, data portability where applicable, withdrawal of consent, and information about significant automated decisions. We may verify your identity and authority before responding.

12. Automated decision-making

We do not intend to make decisions that produce legal or similarly significant effects using solely automated processing without appropriate safeguards. Server-side rules may calculate quotes, discounts, rewards, limits, eligibility indicators, or security signals. Material account and commercial decisions may be reviewed by authorised Purechem personnel.

13. Security and personal data breaches

We use reasonable administrative, technical, and organisational safeguards, including access controls, authentication, role-based permissions, encrypted network connections, managed storage, validation, logging, monitoring, and backups where appropriate. No method is completely secure. If a breach occurs, we will investigate, contain, remediate, document, and notify affected people or regulators when required by law.

14. Children's privacy

TopConnect is not intended for anyone under 18. We do not knowingly approve a child as a distributor user. If we learn that a child's personal data was submitted improperly, we will investigate and take appropriate action.

15. Third-party links and app stores

Third-party websites and services have their own privacy practices. Apple and Google may independently process information relating to app distribution, installation, updates, device settings, and store activity under their own terms and policies.

16. Changes to this policy

We may update this Policy when our practices, Platform, providers, or legal obligations change. The updated date will be shown above. We will provide additional notice through the app or another appropriate channel when a material change requires it.

17. Contact and complaints

Privacy questions and data-rights requests may be sent to purechemtopconnect@gmail.com or addressed to Purechem Manufacturing Limited at the address above. You may also contact the Nigeria Data Protection Commission where you believe your rights have not been respected.