

Draft Privacy Notice

Visitors, invited users and individual business contacts | English | v1.0 | 28 October 2026

DRAFT FOR LEGAL REVIEW. Not adopted, executed or accepted by publication. Complete the parties, schedules and required local review before use.

1. Status, operator and contact

DRAFT NOTICE FOR REVIEW, NOT AN ADOPTED PRIVACY POLICY. Before adoption, identify the actual controller/operator, registered address, applicable countries, privacy/grievance representative and functioning request channel. Proposed coordination contact: business@amnayacorp.com. This notice describes the presently reviewed pilot design and intended controls; it must be checked against actual hosting, logs, vendors and operational practices before it is represented as the binding privacy notice. It is not a request for blanket consent.

2. Information and collection routes

Public visits can expose network/request information to hosting providers. The public trade planner calculates locally and produces a download. The longer public onboarding form prepares a profile/download and an email draft; it does not itself submit the profile to the trade API. Its optional remember-draft function stores a profile in the browser's local storage until cleared using the page control or browser settings. An emailed profile is received only when the user sends it, and then travels through the email service.

Invited sign-in uses AWS Cognito and can process email, authentication/MFA information and account events. Do not send passwords or authenticator codes to COTO by email. The workspace sends business names, city/country, role, lot details, agreement terms, authenticated approvals and relevant evidence descriptions/fingerprints to the protected API. Users choose an evidence file locally; the current workspace computes its fingerprint without uploading the file itself. Commercial records may still contain personal data where people are identifiable. Do not submit unnecessary worker identities, identity documents or bank credentials.

3. Purposes, grounds and sharing

Intended purposes are account security, business review, recordkeeping, trade coordination, responding to requests, fraud prevention and legal obligations. Confirm and document the applicable lawful basis for each purpose/jurisdiction, including contract, legal obligation, legitimate interests where available and consent where required. A company's agreement is not automatically consent from every person it names. No claim of universally applicable legal grounds is made in this draft.

Reviewed pilot businesses can see limited lot summaries, including seller business reference, origin, materials, construction, production location and available quantity. Order details are restricted to the contracting businesses and authorized operator access. Operators can review business profiles and attest receipts. Approved vendors, professional advisers and authorities may receive necessary information under appropriate restrictions/legal duties. A finalized vendor list must identify AWS hosting/database/identity services and email providers; no blanket permission for unrelated marketing, sale of personal data or model training is proposed.

4. Storage, security and transfers

The current backend is hosted in AWS US East (N. Virginia), with private encrypted PostgreSQL and separate service permissions. Authentication uses mandatory MFA and short-lived access tokens. The workspace uses session storage for temporary sign-in state/verifier and holds the access token in memory rather than persistent local storage. AWS sign-in may use its own essential cookies; review those provider notices. This description does not promise perfect security, continuous availability or a completed independent audit. Confirm hosting access countries, subprocessors and lawful international-transfer mechanisms before adoption.

Public blockchain writes are currently disabled. If introduced, direct personal data and confidential text must remain off-chain. Even a hash may be linkable data; assess identifiers, access and correction/deletion implications before enabling it. Publishing a hash is not proof that the source is truthful or that a person consented.

5. Retention, requests and choices

Before activation, adopt a retention table covering account data, profiles, contracts/invoices, audit records, correspondence, security logs and backups, with purpose/legal justification, periods and holds. This draft does not invent a universal statutory retention period or promise immediate deletion from immutable records/backups. On closure, offer appropriate export and apply the adopted schedule and applicable rights.

People may request access, correction, deletion, objection, withdrawal of consent where used and other rights available under applicable law through the verified contact. Rights are not identical everywhere and can be limited by lawful recordkeeping needs. Verify identity proportionately; record and respond within applicable legal time limits. Provide the relevant regulator/grievance route after jurisdiction review. Removing a browser draft does not delete an already sent email or server record. Users can decline optional image/story publicity without losing earned remuneration.

6. Children, updates and adoption checklist

The platform is intended for adult business users. It is not designed to collect children's profiles or publicity releases. Escalate inadvertent child data or safeguarding concerns for appropriate restricted handling. Before adoption, complete controller/contact, role and basis mapping, vendor/transfer inventory, retention, rights workflow, cookie/storage review, grievance mechanism, effective date and approval. Review India's phased DPDP commencement and any other applicable regional rules at that time. Material notice changes must be communicated appropriately; a draft publication does not amend an executed contract or manufacture consent.