

Ordo Systems Privacy Policy

How Ordo Systems handles personal information across its organisation, web, mobile and support services.

Effective	08/2026
Version	1.0
Publisher	Shane Tharuka Sarathchandra Keeragala Dewage trading as Ordo Systems
Document	Customer-facing policy
URL	https://legal.ordosystems.com.au/privacy

1. About this Policy

This Privacy Policy explains how [Shane Tharuka Sarathchandra Keeragala Dewage](#), ABN: [83762277110](#), trading as Ordo Systems (Ordo Systems, we, us) collects, holds, uses and discloses personal information in connection with the Ordo Systems service. It applies to our hosted signup and activation flow, organisation accounts, web and mobile applications, support, security and related communications.

We aim to apply privacy practices consistent with the Australian Privacy Principles. Where the Privacy Act 1988 (Cth) applies to Ordo Systems, the rights and obligations under that Act also apply. This Policy does not reduce any right that cannot lawfully be limited.

Ordo Systems is a business operations service and is not directed to children. Organisations decide who they authorise to use their workspace. If you believe a child's information has been provided inappropriately, contact us so we can assess it.

2. Organisations, users and Ordo Systems' responsibilities

An organisation normally decides why its workplace and operational information is entered into Ordo Systems, who may access it, and how long it is needed. Its Primary Admin and Admins manage users, Departments, product allocation and records within their authority. The organisation is responsible for giving staff, contractors and other people any notices and choices required for its use of their information.

Ordo Systems operates, hosts, secures and supports the service; manages authentication and service communications; and handles information for security, legal and service-administration purposes. We also respond to privacy requests that concern Ordo Systems own handling. This operational allocation does not assign technical legal labels that Australian privacy law does not require.

3. Personal information we collect and hold

Category	Examples
Organisation and account	Organisation name, Business Size, Primary Admin and user names, business email, role, Department, invitations, allocations, account status, password and MFA state, recovery and session records.
Fuel Receipts	Supplier or station, date and time, fuel type, liters, price, total and GST, odometer, vehicle registration or stock reference, receipt number, payment label, fuel-card last four, notes, transaction and reconciliation status.
Images and files	Receipt images, uploaded Fuel statements, generated reports and their filenames, type, size, checksum, ownership, upload and lifecycle metadata.
Trade Plates	Plate inventory and status, Borrow and Return activity, borrower or returner name and position, Department, representative comments, vehicle details, timestamps, notes and—where supplied through an authorised workflow—license number.
Reports and history	Generated Fuel and Trade Plate reports, exports, revisions, report settings, delivery status and historical attribution.
Device and technical	Device or installation identifier, app and operating-system details, sync state, IP and request information, session metadata, and bounded device, update and diagnostic events.
Security and audit	Sign-in, MFA, recovery, invitation, access, administrative, secure-QR and security-event records, including actor, time, action, outcome and bounded metadata.
Communications	Support enquiries, privacy requests, complaints, security reports, in-app operational notifications, service notices, optional account-deletion reason or comment, and related correspondence.

Receipt-image review suggestions in the reviewed launch build use a manual/test stub. The service does not send receipt images to an external production OCR provider, and users must review any suggestion before saving. Separate vehicle-registration recognition may process a temporary camera image on the device; the temporary image is deleted after processing, while the reviewed result and bounded recognition evidence may form part of the user's transaction workflow.

4. How we collect information

We may collect information:

- directly from a user during signup, activation, use of the service, support or a privacy request;
- from an organisation, Primary Admin, Admin or another authorised user—for example through an invitation, Department assignment, Fuel record or Trade Plate transaction;
- from a device when a user signs in, synchronises, captures or selects an image, scans a Trade Plate QR, or uses an on-device recognition workflow;
- automatically through essential authentication, security, audit and diagnostic processes; and
- from service providers acting for Ordo Systems, such as hosting, storage, email, app-distribution and support providers confirmed in the current Third-Party Services and Overseas Processing Schedule.

Where a specific permission or consent is legally required, the relevant screen should provide a separate, timely explanation. This Policy is not a blanket consent to every possible use.

5. Why we handle information

We handle personal information where reasonably necessary to:

- create, activate and administer organisation and user accounts;
- authenticate users, enforce roles, Departments, allocations, capacity and MFA controls, and support account recovery;
- provide Fuel Receipt and Trade Plate workflows, synchronisation, images, statements, reconciliation, reports, exports and secure QR resolution;
- send in-app operational notifications, invitations, recovery messages, service notices and reports that an organisation has expressly enabled;
- provide support, investigate defects and maintain service reliability;
- detect, investigate and respond to misuse, security threats and incidents;
- keep appropriate business, security and audit records; and
- comply with law, court orders and lawful requests, and establish or defend legal rights.
- We do not use Customer Data for targeted advertising or sell or trade personal information. The reviewed launch applications contain no advertising or behavioral-tracking SDK. We will update this Policy and provide any required notice or choice before introducing a materially different use.

6. When we disclose information

We may disclose information only as reasonably necessary to:

- the relevant organisation and its authorised users, according to roles and access settings;
- contracted service providers that host, store, transmit, secure, support or distribute the service;
- professional advisers, insurers, auditors or prospective transaction advisers under appropriate duties;
- law-enforcement, regulators, courts or other parties where required or authorised by law; or
- a successor in a genuine sale, merger or restructure, subject to appropriate safeguards and applicable law.

The current provider names, purposes and locations are listed in the Third-Party Services and Overseas Processing Schedule. An organisation should review that Schedule for its own workforce and procurement notices.

7. Overseas processing

Some service providers may store or process personal information outside Australia. At launch, relevant services and providers include: [Render \(with the current staging region in Singapore\)](#), [Cloudflare R2 \(where an Oceania placement preference is not an Australian-residency guarantee\)](#), [GitHub](#), [Uptime Robot](#) and [approved operational tools](#), [Microsoft 365](#), [Postmark email delivery services](#), [Apple](#) and [Google](#). Ordo Systems does not promise Australia-only data residency unless an accepted Order Form expressly says so.

Where Australian privacy law requires it, we take reasonable steps in relation to overseas recipients and remain accountable as provided by law. Detailed provider, purpose, country, location and contract information must be kept current in the published Schedule.

8. Essential cookies, local storage and mobile devices

The web service uses an essential host-only session cookie named Ordo Systems session to keep a user signed in. It is HTTP-only, uses Same Site=Lax, and is marked Secure in production. Packaged mobile clients use a separate native session credential stored through the device platform's secure-storage mechanism. A trusted native session may be unlocked using supported biometrics or an app passcode, subject to server-side validation, expiry and revocation.

Web and mobile clients also use functional local storage for account-partitioned preferences, installation and sync state, and pending or retrievable workflow data. Receipt-image binaries are not retained in mobile local storage; a user may need to reselect an image after refresh. When a user exports a Trade Plate QR artifact on a packaged mobile client, Ordo Systems may temporarily write the export to application cache for native save or share; the temporary application copy is cleaned up after handoff. Other local business data is not represented as being encrypted merely because the session credential uses secure storage.

The reviewed launch experience does not use non-essential analytics, advertising or cross-site tracking technologies. If the public website or app later introduces them, Ordo Systems will reassess whether a separate notice and consent mechanism is required before use.

9. Security

Ordo Systems uses technical and organisational safeguards designed for the nature of the service. These include server-controlled organisation and role checks, MFA for privileged organisation accounts, production HTTPS, private object storage with authorised download controls, session and recovery controls, and bounded security and audit logging. The Security Overview explains the principal safeguards and shared responsibilities.

No system is completely secure. Users and organisations must use individual accounts, protect devices and credentials, keep access current, and promptly report suspected compromise to support@ordosystems.com.au.

10. Retention, archival and deletion

We retain information only for as long as reasonably needed for the service, the organisation's lawful instructions, security, historical record integrity, legal obligations and dispute resolution. The applicable record classes and approved periods are set out in the Data Retention and Deletion Policy.

A user may permanently delete their own account from Profile after confirming the deletion with their password and, where required, MFA. The deletion removes or revokes the user's identity and access, organisation memberships, product entitlements and active sessions. Ordo Systems sends the user a deletion-confirmation email. Relevant organisation administrators may be notified that the member has left.

Deleting a user or Department may remove access but preserve limited disabled, archived or tombstone reference where Fuel, Trade Plate, report, reconciliation, allocation, security or audit records depend on it, or where needed for historical business or audit integrity. Clearing local mobile data affects only specified information on that device; it does not delete backend records, uploaded files or the account and does not itself sign the user out. Organisation closure is a separate process. An authorised representative may request organisation closure through support@ordosystems.com.au. We may verify identity and authority and will explain any information that must or may be retained. Deletion from active systems may not immediately remove protected backup copies, which expire under the approved recovery schedule.

11. Access and correction

You may ask for access to or correction of personal information we hold about you by contacting support@ordosystems.com.au. An organisation Admin may also be able to correct workplace records through Ordo Systems. We may need to verify identity and consult the organisation where its records are involved.

Where the Privacy Act applies, we will handle access and correction requests within the time and on the terms required by that Act. We will ordinarily respond within a reasonable period, tell you if more time is needed, and provide written reasons and complaint options if a request is refused. We do not charge an application fee for access or correction; any permitted access cost will not be excessive.

12. Privacy complaints

Send a privacy complaint to support@Ordosystems.com.au or the postal address below. Describe the concern and the outcome you seek. We will acknowledge it, investigate fairly, and respond within a reasonable period. You may use another legally valid contact method even if email is our preferred channel.

If the Privacy Act applies and you are not satisfied after giving us a reasonable opportunity to respond, you may complain to the Office of the Australian Information Commissioner at oaic.gov.au.

13. Data breaches

We assess suspected privacy and security incidents and take reasonable steps to contain and address them. Where applicable law requires notification—including the Notifiable Data Breaches scheme where it applies—we will notify the relevant regulator and affected individuals as required.

14. Changes to this Policy

We may update this Policy when the service, providers or law changes. We will publish the new version and effective date and provide reasonable notice of material changes where appropriate. We will not treat continued use as consent where specific consent is legally required.

15. Contact

Shane Tharuka Sarathchandra Keeragala Dewage trading as Ordo Systems

ABN: **83762277110**

Address: **64 Damask drive, Tarneit, VIC, 3029**

Privacy: <https://legal.ordosystems.com.au/privacy>

Security: support@ordosystems.com.au

Website: <https://ordosystems.com.au>