

Ordo Systems Data Retention and Deletion Policy

How active data, archived attribution, device-local information and backups are handled.

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/data-retention

1. Purpose

This Policy explains how Ordo Systems retains, archives, deletes and de-identifies account and operational information. It should be read with the Privacy Policy and Terms. It does not override a longer or shorter period required by law or agreed in an Order Form.

Ordo Systems retains information only for as long as reasonably needed to provide and secure the service, follow an Organisation's lawful instructions, preserve reliable business and security records, meet legal obligations, and resolve incidents, disputes or legal claims.

2. Retention schedule

Record class	Launch retention rule
Organisation profile, membership and configuration	While the Organisation account is active, then for 30 days after closure, unless earlier deletion is appropriate or longer retention is required.
Fuel operational records	Fuel transactions, receipt metadata, images, statements, reconciliation and reports: while active and for 30 days after closure, subject to authorised deletion and required record integrity.
Trade Plate operational records	Inventory, Borrow and Return history, person or Department attribution, vehicle and licence details, secure-QR lifecycle and reports: while active and for 30 days after closure, subject to authorised deletion and required record integrity.
Unactivated signup	The activation opportunity remains open for 14 days. If activation is not completed, the signup record is quarantined and deleted or de-identified within a further 30 days.
Resolved invitations	Up to 90 days after the invitation is accepted, declined, revoked or expires, subject to a bounded per-Organisation record limit.
Resolved organisation requests without a retained invitation link	Up to 365 days after resolution.
Selected security and audit families	Selected platform, MFA, password-recovery, onboarding and secure-QR failure events: up to 90 days. Other general audit, device, update and operational logs: up to 12 months after creation.
Credentials and live security state	Session, activation, invitation, MFA and recovery credentials expire, rotate or are revoked under the relevant security lifecycle. Related bounded audit records may remain separately.
Device-local information	Account-partitioned working data remains until the relevant local-clear control is used or the platform removes it. Browser data may also be removed by clearing site data; packaged-app data may be removed by clearing app data or uninstalling the app. Sync does not by itself equal backend deletion.

Record class	Launch retention rule
Backups and recovery copies	Removed from ordinary use after active-system deletion and expires within 35 days, unless isolated for an incident, legal hold or required recovery validation.
Support, privacy and complaint records	Routine support records: 24 months after the matter is closed. Privacy requests, complaints and security-incident records: 7 years after final resolution, or longer where reasonably needed to comply with law.

The Organisation remains responsible for exporting and separately retaining records needed for its own tax, accounting, employment, safety, insurance or other legal obligations.

3. Active deletion and archival

An authorised Admin may delete or disable Users, invitations and Departments through available controls. Where a record is dependency-free, Ordo Systems may hard-delete it. Where Fuel, Trade Plate, report, allocation, security, audit or other records depend on it, Ordo Systems may instead:

- remove access and revoke affected sessions, MFA challenges, allocations and unresolved invitations;
- hide the item from active lists;
- retain a disabled or archived reference for historical attribution; and
- limit the retained fields and access to what is reasonably required.

This avoids making business, safety or audit history misleading. Primary Admin and final-Admin protections may prevent a change that would leave an Organisation without authorised control.

4. Local mobile clearing is not account deletion

Clear My Local Mobile Data removes specified device-local Fuel and queued Trade data for the signed-in account. It does not delete backend records, uploaded files, another account's data or quarantined legacy data, and it does not itself sign the User out. A User should sync or export needed information before clearing local storage.

5. User and Organisation deletion requests

A User may request access, correction or deletion through in-app settings, where available, or by emailing support@ordosystems.com.au. Organisation closure must be requested by the Primary Admin or another appropriately authorised representative by emailing support@ordosystems.com.au with the subject 'Organisation closure request'. These routes must also match any in-app and app-store deletion paths.

Before acting, Ordo Systems may verify identity, authority, the affected Organisation and the scope of the request. Removing an individual's login does not necessarily delete records that person created for an Organisation. Those records may remain under the Organisation's authority and this Policy.

Ordo Systems will explain if information cannot be deleted because:

- it belongs to or is controlled by the Organisation and another lawful handling step is appropriate;
- it is needed to preserve a transaction, safety record or historical attribution;
- law, a court or tribunal order requires or permits retention;
- it is reasonably needed for security, fraud prevention, an incident, dispute or legal claim; or
- it remains temporarily in a protected backup or recovery copy.

Where appropriate, Ordo Systems may de-identify information instead of retaining it in identifiable form.

6. Organisation closure and export

On Organisation closure, Ordo Systems will revoke or disable active workspace access and unresolved invitations according to the approved offboarding process. The Organisation should use available in-app export tools or request an assisted export by emailing support@ordosystems.com.au before closure or within the 30-day post-closure export window. Ordo Systems will provide available records in a commonly used electronic format and identify any record class that cannot be exported.

After the applicable period, Ordo Systems will delete or de-identify Customer Data unless retention is required or permitted by law or reasonably necessary for a continuing incident, dispute or legal claim.

7. Backups and service providers

Deletion from active systems may not immediately remove every protected backup copy. Backup data is separated from ordinary use, accessed only for approved recovery or security purposes, and expires under the confirmed recovery schedule. If a backup is restored, deletion instructions are reapplied where reasonably practicable.

Where a service provider processes Ordo Systems data, Ordo Systems applies the relevant return or deletion process under its provider arrangement. Overseas processing is described in the Third-Party Services and Overseas Processing Schedule.

8. Legal holds and changes

Ordo Systems may suspend ordinary deletion for data reasonably required for a legal hold, regulator, court order, incident investigation, fraud prevention or legal claim. Access is restricted and the hold is reviewed; ordinary deletion resumes when the reason ends.

Ordo Systems may update this Policy as the service, providers, retention configuration or law changes. We will publish the current version and effective date and give reasonable notice of a material change where appropriate.

9. Contact

Privacy and deletion requests: support@ordosystems.com.au

Account deletion: in-app Settings

Organisation closure: support@ordosystems.com.au (subject: 'Organisation closure request')