Draft for review · Edition dated 29 November 2026

Renzoire ID Privacy Policy

The information we use to operate your account, what connected apps receive and how you can manage your data.

Scope of this policy

Renzoire Technologies provides Renzoire ID. The service stores account information, verifies sign-in and shares information needed for sign-in with connected apps. This policy covers account registration, profiles, account security and access management.

RenSend messages and documents or workspace data are processed by the relevant apps. For a request about that data, identify the app and, where applicable, the organization.

Information we process

• Registration and recovery. Your Renzoire ID address, username, verified personal email address, address verification information and password hash. We use a separate second-factor email address if you configure one.

• Profile. The name, photo, bio and other fields you provide. Some connected apps can display authorized profile fields.

• Security. Sessions, trusted devices, sign-in methods, password changes and second-factor activity. Session records can include timestamps and browser labels.

• Passkeys. Credential identifiers, public keys and signatures generated by your device. Your device performs biometric checks such as Face ID or Touch ID. Renzoire ID receives a cryptographic confirmation.

• Work access. Assigned apps, organizations, roles, access periods, access requests and invitations.

Why we use this information

We use it to register accounts, confirm addresses, verify sign-in, recover access, share authorized profile details and manage sessions. Service emails deliver verification codes and security notices.

Service records help us detect abuse, investigate outages and restore service. We use the information in a support request to investigate the reported issue and respond.

Information shared with apps and organizations

A connected app receives an account identifier and, depending on its integration and the role, authorized profile fields, role and organization information. Your password, private passkey and recovery codes stay outside the information sent to an app during sign-in.

Authorized organization administrators manage work invitations and access within their role. Hosting, email delivery and support providers may process information needed for their functions. We may also disclose information as required by applicable law.

Sessions, cookies and trusted devices

Renzoire ID uses technical cookies to connect address verification to your browser, keep you signed in and recognize a device you have chosen to trust. Session expiration or cookie removal may require a new sign-in.

You can review or end sessions in security settings. Sign out when you finish using a shared browser. Use the trusted-device option on your own devices.

Data retention and security

Account data supports your profile and sign-in. Verification codes expire after a limited period. Recovery codes expire once used. Generating new recovery codes revokes the previous set.

Some records may remain in security logs and backups after a profile change or sign-out. Retention depends on the purpose of the record, recovery requirements and applicable obligations.

Profile controls and data requests

Account settings let you edit available profile fields, update recovery methods, manage passkeys and end sessions.

To request access, correction, deletion or another action available under applicable law, use the Renzoire Holdings contact page. Include your Renzoire ID address, the nature of the request and the relevant app. We may verify your identity to protect your account. Keep passwords and verification and recovery codes private.

About this edition

This draft is subject to confirmation of the data controller’s details, processing grounds, regions of storage and transfer, retention periods by category and the contact for data requests.