Customer Onboarding and KYC Policy

This policy explains how CUR-DEV B.V., operating MindSyncr, onboards and verifies individual and business customers, manages fraud and compliance risk, and handles additional verification when reasonably required.

OPERATOR	PRODUCT	VERSION	EFFECTIVE DATE
CUR-DEV B.V.	MindSyncr	1.0	1 August 2026

1. SCOPE AND BUSINESS MODEL

Direct software subscriptions, not a marketplace.

MindSyncr is an AI-assisted productivity and project-management application. CUR-DEV B.V. is the direct provider of MindSyncr and collects payments for access to its own software subscriptions and, where applicable, hosted AI usage, storage, document tools, and integrations.

MindSyncr does not operate a creator marketplace, payment marketplace, money-transfer service, stored-value service, or user-to-user payment system. Customers cannot cash out, transfer, redeem, or exchange subscription access, usage allowances, credits, or features for money or monetary value.

Current sub-merchant position

MindSyncr does not currently onboard sub-merchants, third-party sellers, payout recipients, content creators receiving payments, or other parties that collect money through the platform.

2. CUSTOMER TYPES

Who MindSyncr onboards.

Individual end users

Individuals who create an account and subscribe for their own personal or professional productivity use.

Business customers

Companies, organizations, and professionals that subscribe to use MindSyncr internally. Business customers remain end customers of CUR-DEV B.V.; they are not sub-merchants and are not permitted to resell MindSyncr or collect payments through MindSyncr without a separate written agreement and compliance review.

---

3. STANDARD ONBOARDING

Account creation and verification.

1. **Account information.** The customer provides the information reasonably needed to create an account, such as name, email address, country or region, and account credentials.

2. **Email verification.** MindSyncr may require the customer to verify control of the email address before the account is fully activated or before sensitive account changes are permitted.

3. **Terms and policies.** The customer must accept the applicable Terms of Service, Privacy Policy, Acceptable Use Policy, refund/cancellation terms, and this onboarding policy where presented.

4. **Secure authentication.** Password controls, session security, optional multi-factor authentication, passkeys when available, and additional verification may be used to protect the account.

5. **Payment authorization.** Payments are processed by an approved payment provider. MindSyncr does not intend to store complete payment-card numbers or card security codes. The payment provider may perform its own fraud, identity, sanctions, and transaction checks.

6. **Activation.** Access is provided after required verification and payment authorization are completed. Access may be limited while verification is pending.

4. BUSINESS VERIFICATION

Additional information for organizational accounts.

For a business subscription, MindSyncr may collect or verify:

- legal business name and trading name;
- country of registration and business address;
- company or chamber-of-commerce registration number;
- business website and business email domain;
- name and contact details of the authorized representative;
- proof that the representative is authorized to act for the organization;
- tax or billing information where required; and
- ownership or beneficial-owner information where required by law, a payment partner, or a risk review.

Supporting documents may include a certificate or extract of registration, proof of address, government-issued identification of the authorized representative, or other reasonable evidence of identity and authority.

5. RISK-BASED ENHANCED VERIFICATION

Extra checks are used when the risk justifies them.

Most ordinary individual SaaS customers are onboarded through standard account and payment verification. MindSyncr may request enhanced identity or business verification when reasonably necessary, including when:

- account, billing, identity, device, or location information is inconsistent;
- there are repeated failed payments, unusual purchase patterns, chargebacks, or suspected fraud;
- the customer attempts to conceal identity, impersonate another party, or use unauthorized payment credentials;
- the customer requests unusually high usage, enterprise access, resale rights, or other higher-risk functionality;
- activity indicates prohibited, unlawful, abusive, or security-sensitive use;
- a payment provider, banking partner, regulator, court, or competent authority requires additional information; or
- the customer or transaction presents elevated sanctions, geographic, fraud, or reputational risk.

Enhanced verification may include government-issued identification, proof of address, confirmation of payment ownership, business registration documents, ownership information, source-of-funds information in exceptional cases, or a live/video verification step where supported and proportionate.

6. FRAUD PREVENTION AND ONGOING MONITORING

Verification continues when material risk changes.

MindSyncr and its payment partners may monitor for:

- payment fraud, chargebacks, account takeover, and credential abuse;
- unusual transaction velocity, device changes, or location anomalies;
- misuse of trials, promotions, accounts, or subscription limits;
- attempts to use MindSyncr for prohibited content, unlawful activity, malware, phishing, spam, harassment, or rights violations;
- attempts to enable cash-out, stored value, money transmission, user-to-user payments, or unapproved resale; and
- sanctions or restricted-party concerns where screening is required by law or a payment partner.

MindSyncr may re-verify a customer when account ownership, payment methods, company ownership, authorized representatives, risk profile, or material account information changes.

7. DECISIONS, RESTRICTIONS, AND ESCALATION

Access depends on successful verification and acceptable use.

CUR-DEV B.V. may, where reasonable and lawful:

- request additional information or documents;
- delay activation or restrict particular features while reviewing risk;
- decline a subscription or payment;
- suspend, limit, or close an account;
- cancel or refund a transaction where permitted and appropriate;
- preserve relevant records for disputes, fraud prevention, or legal compliance; and
- report activity to a payment provider or competent authority when legally required.

MindSyncr will not disclose confidential risk controls or information where doing so could enable fraud, compromise security, or violate legal restrictions.

8. RECORDS, PRIVACY, AND SECURITY

Verification data is limited and protected.

MindSyncr collects only information reasonably necessary for account administration, service delivery, payment, security, fraud prevention, dispute management, and applicable legal or payment-partner requirements.

Access to verification information is limited to authorized personnel and service providers with a legitimate need. Reasonable technical and organizational safeguards are used to protect it. Identity and verification records are retained only for as long as reasonably necessary. Where enhanced verification records are collected, they will ordinarily be retained for no longer than five years after the customer relationship ends unless a different period is required for legal, fraud, dispute, security, tax, or payment-partner purposes.

Personal information is handled under the applicable MindSyncr Privacy Policy and applicable data-protection requirements. Customers may be asked to update or correct information that is inaccurate or incomplete.

9. AGE REQUIREMENTS

Paid accounts are intended for adults.

A person must be at least 18 years old, or the age of legal majority in their jurisdiction if higher, to purchase a MindSyncr subscription on their own behalf. An authorized adult or organization may manage an account used by a younger person only where permitted by law and under the applicable terms.

10. SUB-MERCHANTS AND FUTURE MARKETPLACE ACTIVITY

No sub-merchants are currently supported.

MindSyncr does not currently permit customers to sell goods or services, receive payouts, accept tips or donations, monetize content, or collect payments from other users through the platform. CUR-DEV B.V. is the sole publisher and direct seller of MindSyncr access.

If MindSyncr later introduces third-party sellers, creators, partners receiving payments, a marketplace, or sub-merchant functionality, that functionality will not launch until CUR-DEV B.V. has completed a separate legal and payment-partner review. Such parties would be subject to a dedicated KYB/KYC process, ownership and authorization checks, sanctions and fraud screening, prohibited-content review, contractual approval, ongoing monitoring, and any prior approval required by Coda or another payment provider.

11. GOVERNANCE AND POLICY REVIEW

Owned and reviewed by CUR-DEV B.V.

CUR-DEV B.V. is responsible for this policy. The policy will be reviewed at least annually and whenever there is a material change to MindSyncr’s business model, payment flows, customer types, legal obligations, risk profile, or payment-provider requirements.

Questions or verification requests may be submitted using the contact information published on the CUR-DEV B.V. website.