Compliance Program Policy

This policy explains how CUR-DEV B.V. governs compliance risk for MindSyncr across customer onboarding, payments, acceptable use, AI-generated content, privacy, security, complaints, providers, and enforcement.

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

1. PURPOSE AND SCOPE

A proportionate compliance process for MindSyncr.

This policy describes the risk-based compliance process maintained by CUR-DEV B.V. for MindSyncr. It applies to MindSyncr's product offering, customer onboarding, payments, acceptable use, user-generated and AI-generated content, privacy, security, complaints, third-party providers, and enforcement.

> **Private-alpha position**
>
> MindSyncr is currently in private alpha. Management oversight and manual review apply now. Operational controls required for public paid subscriptions must be enabled and tested before public commercial launch.

2. BUSINESS MODEL AND COMPLIANCE BOUNDARIES

Direct software subscriptions, not payment intermediation.

MindSyncr is an AI-assisted productivity and project-management application. CUR-DEV B.V. is the direct publisher and seller of MindSyncr access. Payments are intended to cover subscriptions and, where applicable, hosted AI processing, storage, document tools, and integrations.

MindSyncr does not currently:

- onboard sub-merchants, third-party sellers, creators receiving payouts, or other payment recipients;
- provide money transmission, stored value, cash withdrawal, user-to-user payments, or exchangeable virtual currency;
- permit access, usage allowances, or platform features to be redeemed for cash or monetary value; or
- operate a marketplace for goods, services, gifts, tips, donations, or investment products.

MindSyncr is not a financial institution or money-service business, and this policy is not represented as a financial-institution AML program. CUR-DEV B.V. nevertheless applies proportionate fraud, identity, sanctions, content, privacy, security, and payment-partner controls where applicable.

3. GOVERNANCE AND RESPONSIBILITY

Compliance is owned by CUR-DEV B.V. management.

Management is responsible for:

- approving and reviewing compliance policies;
- assessing material product, payment, customer, content, privacy, and security risks;
- reviewing escalated accounts, transactions, complaints, and suspected violations;
- coordinating with providers, advisers, regulators, or competent authorities where appropriate; and
- ensuring corrective actions are recorded and followed through.

During private alpha, these responsibilities are performed through documented management review. A dedicated compliance role or specialist support may be appointed as scale, geography, or legal requirements increase.

4. RISK ASSESSMENT

Material changes are reviewed before launch.

Compliance risk is reviewed before material launches and when MindSyncr changes its:

- payment model, pricing, subscription plans, credits, or usage allowances;
- supported countries, customer types, or distribution channels;
- AI providers, hosted models, document capabilities, or external connectors;
- marketplace, sharing, collaboration, or payout functionality;
- data collection, identity verification, or retention practices; or
- material third-party providers.

The review considers legal and payment-partner requirements, prohibited-content exposure, fraud and chargebacks, account takeover, geographic or sanctions restrictions where applicable, privacy, cybersecurity, intellectual property, and potential harm to users or third parties.

5. CUSTOMER ONBOARDING AND VERIFICATION

Risk-based verification supports account and payment integrity.

MindSyncr follows its separate Customer Onboarding and KYC Policy. Standard controls may include account information, email verification, acceptance of applicable policies, secure authentication, payment authorization, and business verification where appropriate.

Enhanced verification may be requested when risk indicators justify it or when required by a payment provider, regulator, court, or competent authority. MindSyncr seeks to collect only information reasonably necessary for a clear purpose and avoids retaining identity-document copies unless justified and permitted.

6. ACCEPTABLE USE AND PROHIBITED ACTIVITIES

MindSyncr must not be used to facilitate unlawful or prohibited activity.

Prohibited uses include, where applicable:

- fraud, phishing, impersonation, account theft, credential abuse, or deceptive schemes;
- malware, spyware, malicious code, unauthorized access, or instructions intended to compromise systems;
- money laundering, terrorist financing, sanctions evasion, or concealment of unlawful proceeds;
- gambling, wagering, lotteries, unlawful financial trading, or cash-out mechanisms;
- sexual exploitation, child sexual abuse material, or unlawful sexually explicit content;
- illegal drugs, weapons, terrorism, violent extremism, or other unlawful goods or services;
- hateful, threatening, harassing, defamatory, or unlawfully discriminatory content;
- spam, unauthorized solicitation, or abusive automated messaging;
- infringement of privacy, confidentiality, copyright, trademark, or other third-party rights;
- misinformation, material misrepresentation, or deceptive content used to cause harm or obtain an improper benefit; and
- using MindSyncr as a marketplace, payment intermediary, stored-value system, or payout platform without prior written approval.

MindSyncr is a general-purpose productivity tool and does not pre-screen every private user input. CUR-DEV B.V. may investigate reported or reasonably detected misuse and may restrict access where necessary.

7. AI AND CONTENT COMPLIANCE CONTROLS

AI helps users, but does not remove accountability.

- Users remain responsible for the legality and rights associated with content submitted to the service.
- AI output must not be presented as guaranteed legal, medical, financial, or other professional advice.
- High-impact or external actions should use confirmation, approval, and audit mechanisms appropriate to the risk.
- Connectors should be permission-scoped and should not change external systems without applicable authorization or approval.
- Reports of unlawful, infringing, abusive, or dangerous use may be reviewed and acted upon.
- MindSyncr may limit models, features, integrations, or accounts where continued use creates unacceptable risk.

Safeguards will be expanded as hosted AI, connectors, collaboration, or public sharing capabilities are introduced.

---

8. PAYMENT, FRAUD, AND CHARGEBACK CONTROLS

Payments are screened and monitored proportionately.

Payments are processed through approved payment providers. MindSyncr does not intend to store complete payment-card numbers or card security codes.

MindSyncr and its payment partners may use:

- payment authorization and processor fraud screening;
- velocity, device, location, and account-consistency checks;
- review of repeated failures, unusual purchases, trial abuse, or suspected account takeover;
- chargeback and dispute monitoring;
- restriction of suspicious transactions or accounts;
- customer re-verification where risk materially changes; and
- refunds, cancellation, suspension, or account closure where permitted and appropriate.

Sanctions or restricted-party screening is performed where required by applicable law, territory, banking/payment-provider rules, or the risk profile. CUR-DEV B.V. does not claim that every ordinary customer is subject to standalone MindSyncr screening when it is neither required nor proportionate.

9. PRIVACY AND DATA PROTECTION

Personal information is limited to defined purposes.

The compliance process includes:

- data minimization and purpose limitation;
- appropriate notices and policy acceptance;
- access restrictions based on legitimate need;
- reasonable technical and organizational safeguards;
- retention only for as long as reasonably necessary or legally required;
- processes for access, correction, deletion, or objection requests where applicable; and
- review of providers that process personal information for MindSyncr.

Sensitive verification information should receive additional access and retention controls.

10. SECURITY AND INCIDENT ESCALATION

Security incidents are contained, assessed, and documented.

CUR-DEV B.V. may:

1. contain and investigate the event;
2. preserve relevant evidence and logs;
3. restrict accounts, credentials, integrations, or affected functionality;
4. assess customer, legal, payment-partner, and regulatory notification duties;
5. notify affected parties or competent authorities where required; and
6. document corrective and preventive actions.

Public policy documents do not disclose sensitive technical controls that could undermine system security or fraud prevention.

11. MONITORING, REPORTS, AND INVESTIGATIONS

Reviews are triggered by risk indicators and credible reports.

Compliance review may be initiated by:

- customer or third-party complaints;
- payment-provider alerts, disputes, chargebacks, or requests;
- security alerts or suspected account takeover;
- unusual account, transaction, or usage patterns;
- reported prohibited content or intellectual-property infringement;
- internal testing or audit findings; or
- lawful requests from regulators, courts, or competent authorities.

Reviews should be documented proportionately and limited to relevant information. MindSyncr may protect confidential detection methods where disclosure would enable abuse, compromise security, or violate legal obligations.

12. ENFORCEMENT AND REMEDIATION

Actions are proportionate to risk and severity.

CUR-DEV B.V. may:

- issue guidance or a warning;
- remove or restrict content or functionality where appropriate;
- require additional verification or corrective action;
- temporarily limit or suspend an account;
- decline or cancel a transaction or subscription;
- terminate access for material or repeated violations;
- preserve records for disputes, investigations, or legal requirements; and
- report activity where legally required.

Archive, restriction, or suspension may be preferred over permanent deletion where evidence preservation or dispute handling is necessary.

13. COMPLAINTS, APPEALS, AND REPORTING CONCERNS

Customers and third parties can report compliance concerns.

Suspected fraud, prohibited use, privacy concerns, intellectual-property issues, security incidents, or payment disputes may be reported using the contact information published by CUR-DEV B.V. Reports should include enough detail to identify the account, content, transaction, or conduct involved.

Where appropriate, a customer may ask for a compliance decision to be reconsidered. Temporary restrictions may remain in place when needed to protect users, the service, payment partners, or legal interests.

14. THIRD-PARTY AND PROVIDER COMPLIANCE

Material providers are reviewed according to their role and risk.

CUR-DEV B.V. may review a provider's security, privacy, data location, contractual terms, reliability, compliance capabilities, and incident-notification process. This particularly applies to payment processors, AI providers, hosting services, email providers, analytics services, and external connectors.

Providers receive only the access reasonably required for their function. API keys, payment credentials, and other secrets must be protected and should not be exposed after storage.

15. RECORDS AND RETENTION

Compliance decisions and evidence are retained only as needed.

Records may include policy versions and acceptance, account-review notes, verification outcomes, disputes, complaints, incidents, enforcement decisions, provider reviews, and communications with payment partners or authorities.

Records are retained only for as long as reasonably necessary for the relevant purpose and applicable legal, contractual, tax, fraud, dispute, security, or payment-partner requirements. Access is restricted to authorized persons and providers with a legitimate need.

16. SUB-MERCHANTS AND FUTURE HIGHER-RISK FUNCTIONALITY

No sub-merchants or payouts are currently supported.

A marketplace, creator monetization, third-party seller, payout, stored-value, user-to-user payment, or similar capability will not launch until CUR-DEV B.V. has completed a separate legal and payment-partner assessment and implemented appropriate onboarding, KYB/KYC, ownership, sanctions, fraud, content-review, monitoring, contractual, dispute, and reporting controls. Prior payment-provider approval will be obtained where required.

17. TRAINING, TESTING, AND REVIEW

The program evolves with the product and its risks.

Personnel with compliance responsibilities should understand the parts of this policy relevant to their role. Material controls should be tested proportionately before public launch and after significant changes.

This policy will be reviewed at least annually and when there is a material change to the business model, payment flow, supported territories, customer types, product capabilities, legal requirements, risk profile, or payment-provider obligations.

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