Acceptable Use Policy

Applicable to Sion AI

Entity: IdeaSynesthesia B.V. (the "Company")
Effective date: 3 May 2026

This Acceptable Use Policy ("AUP") explains what is and is not allowed when using Sion AI and related services, modules, interfaces, APIs, and integrations (the "Service").

This AUP is designed for global users and is interpreted in line with applicable laws, including Dutch law, GDPR/UAVG data-protection principles, and other mandatory laws that apply to your location and use case.

1. Scope and Contract Relationship

1.1 This AUP applies to all users and customers accessing the Sion AI Services in cloud, deployment model.

1.2 This AUP supplements your applicable contract documents, including the relevant Terms and Conditions, the Privacy Policy, and the Cookie Policy.

1.3 This AUP is an operational policy. It does not create additional warranties, service-level commitments, or liability beyond what is required by mandatory law and your governing contract terms.

1.4 If there is any conflict, the following order applies: (a) the applicable B2B Terms and Conditions for baseline commercial/legal terms, (b) the applicable Privacy Policy and (c) the applicable privacy policy.

2. Permitted Use

2.1 You may use the Services only for lawful purposes and only within the scope of your subscription, plan, and documented permissions.

2.2 You are responsible for all activity performed through your account(s), API credentials, and connected tools by your authorized users or agents acting on your behalf.

3. Prohibited Conduct

You must not use the Services to do, attempt, or assist any of the following:

3.1 Illegal activity, including violations of criminal law, data-protection law, sanctions/export-control law, anti-fraud law, or intellectual-property law.

3.2 Harmful or abusive activity, including harassment, hate, threats, exploitation, unlawful discrimination, or creation/distribution of illegal content.

3.3 Security abuse, including malware distribution, phishing, credential theft, denial-of-service activity, unauthorized scanning, unauthorized penetration attempts, or bypassing authentication, access controls, license controls, safety controls, or usage limits.

3.4 Platform misuse, including use that materially degrades platform stability, reliability, or security for other users.

3.5 Unauthorized surveillance, covert tracking, or unlawful monitoring of individuals.

3.6 Use of the Services to build or operate competing services by unauthorized reverse engineering, extraction, model behavior probing, decompilation, or disassembly, except where non-waivable mandatory law expressly permits limited interoperability actions.

3.7 Submission of content that you do not have rights to use, including copyrighted material, trade secrets, or personal data processed without a valid legal basis.

3.8 Misrepresentation of AI-generated outputs as verified human-reviewed facts when they have not been reviewed.

4. AI-Specific Use Restrictions

4.1 You remain responsible for reviewing, testing, and validating AI outputs before operational, legal, financial, or safety-critical use.

4.2 You must not rely on AI outputs as the sole basis for decisions that may produce legal or similarly significant effects on individuals, unless you implement legally required safeguards, meaningful human oversight, and all required notices/consents.

4.3 You must not use the Services for prohibited high-risk AI deployment without all legally required controls, governance, human oversight, and documentation.

4.4 You must not use the Services to generate deceptive synthetic identities, deepfake fraud, impersonation, or disinformation intended to mislead or cause harm.

5. Data Protection and Privacy Responsibilities

5.1 You are responsible for ensuring a lawful basis for personal-data processing you initiate through the Services and for providing required notices to data subjects.

5.2 If you act as controller for workspace/customer data, you remain responsible for data-subject requests, retention settings, and any required DPIAs or risk assessments under applicable law.

5.3 You should avoid submitting special-category or highly sensitive personal data unless strictly necessary, lawfully supported, and appropriately safeguarded.

5.4 You must not use Service data in ways that conflict with your contractual DPA obligations, privacy commitments, or applicable confidentiality duties.

6. Security, Credentials, and Access

6.1 You must keep credentials, API keys, tokens, and connector secrets confidential and implement appropriate access governance (least privilege, role separation, periodic access review).

6.2 You must promptly notify us of suspected unauthorized access, credential compromise, security incidents, or misuse involving your account or integrations.

6.3 You must not share accounts in a way that defeats auditability or violates your plan or license model.

7. Integrations, Connectors, and Third-Party Services

7.1 You are responsible for ensuring you have rights to connect third-party systems, APIs, and datasets to the Services.

7.2 Third-party services remain subject to their own terms and policies. You are responsible for compliance with those terms when using connected providers.

7.3 You must not configure integrations to extract, transmit, or store data in ways that violate law, contract, or third-party rights.

8. Intellectual Property and Content Integrity

8.1 You retain responsibility for the legality of your inputs and downstream use of outputs generated at your direction.

8.2 You must not use the Services to infringe trademarks, copyrights, database rights, patents, trade secrets, or other proprietary rights.

8.3 You must not remove, alter, or obscure ownership notices, license notices, or attribution information required by law, contract, or open-source license terms.

9. Children and Restricted Uses

9.1 The Services are not directed to children below the minimum digital-consent age required by applicable law.

9.2 You must not use the Services in ways that unlawfully process children's data or target children in violation of applicable law.

10. Export Controls and Sanctions

10.1 You must comply with applicable export-control and sanctions laws when accessing, deploying, or using the Services.

10.2 You must not use the Services from prohibited jurisdictions or for prohibited end uses where such access or use would violate applicable law.

11. Monitoring and Enforcement

11.1 To protect users, infrastructure, and legal compliance, we may implement proportionate safeguards, including abuse monitoring, policy controls, safety filters, rate limits, and risk-based restrictions.

11.2 Where we reasonably determine that use violates this AUP, applicable law, or governing contract terms, we may investigate, require remediation, remove or disable access to affected content/integrations, suspend access, or terminate access as permitted by law and contract.

11.3 We may act immediately where necessary to prevent harm, preserve security, respond to legal requirements, or address urgent compliance risk.

11.4 Enforcement actions are applied in a risk-based manner and do not waive any other legal or contractual rights.

11.5 Safeguards and enforcement under this AUP are risk-based and may not detect, prevent, or remediate every issue in every case. This AUP does not create any promise of uninterrupted service, absolute security, or error-free operation.

12. Reporting and Cooperation

12.1 If you become aware of misuse, security abuse, or policy violations involving the Services, you must promptly report it through official support/privacy/security channels.

12.2 You agree to cooperate in good faith with reasonable incident-response and remediation requests related to your use of the Services.

13. Changes to This AUP

13.1 We may update this AUP to reflect legal, security, product, or operational changes.

13.2 Material changes will be communicated through appropriate channels (for example website notice, in-product notice, account notice, or email) as required by law and applicable contract terms.

14. Governing Law and Global Rights

14.1 This AUP is prepared under Dutch-law compliance principles while honoring mandatory local rights for global users.

14.2 Nothing in this AUP limits mandatory rights or protections that apply under applicable local law.

15. Contact

Policy and Compliance Team – legal@sionai.faith

Primary channel: support@sionai.faith

Alternative channel: privacy@sionai.faith

16. Final Terms

16.1 If any provision of this AUP is held invalid or unenforceable, the remaining provisions remain in effect to the maximum extent permitted by law.

16.2 This AUP applies alongside the governing contract framework and does not limit obligations that are non-waivable under applicable law.