Privacy Policy

Applicable to Sion AI

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

How we collect, use, and protect your personal data

This Privacy Policy explains how IdeaSynesthesia B.V. operating the Sion AI SaaS service ("we", "us", "our"), collect, use, share, and protect personal data when you visit our website, create an account, or use Sion AI, and related services (the "Service").

We are committed to handling personal data carefully, transparently, and in accordance with the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"), the Dutch GDPR Implementation Act (Uitvoeringswet Algemene verordening gegevensbescherming, "UAVG"), the Dutch Telecommunications Act (Telecommunicatiewet) for cookies and electronic communications, the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA/CPRA"), and other applicable privacy and data protection laws, including applicable U.S. state consumer privacy laws.

Our Services are available to users worldwide. If you are located outside the European Economic Area (EEA), or in a jurisdiction with supplemental privacy rights (including certain U.S. states), additional region-specific information may apply to you — please see Section 14.

---

1. Who We Are (Controller)

We are the controller of personal data collected through the Services:

Controllers: IdeaSynesthesia B.V.

Registered Office: Dronryp, Friesland, The Netherlands

Chamber of Commerce (KvK): 42037710

VAT Number: NL869420501B01

Website: www. Sionai.faith and www.app.sionai.faith

We have designated a privacy contact responsible for data protection matters, reachable through privacy@sionai.faith

---

2. Scope of This Privacy Policy

This Privacy Policy applies to personal data processed when you:

- visit our website or landing pages;
- create an account or register for the Services;
- purchase or manage a subscription;
- use platform features, including Artificial Intelligence functionality;
- interact with our AI features (prompts, inputs, outputs);
- contact our support, sales, or customer success teams;
- receive marketing or transactional communications from us;

- participate in demos, webinars, events, beta programs, or user research; or
- apply for a job with us (to the extent described here).

This Privacy Policy does not apply to: (a) third-party websites, services, or applications that we do not control, even if linked from our website; or (b) personal data processed by business customers (Sion AI is a consumer product).

---

3. Categories of Personal Data We Process

Depending on how you interact with the Services, we may process:

3.1 Account and Identity Data

Name, email address, username, password hash, profile photo (if provided), account identifiers, and language/locale preferences.

3.2 Contact Data

Email address, phone number, billing address, and correspondence details.

3.3 Billing and Transaction Data

Subscription plan, invoices, payment status, transaction identifiers, billing history, VAT details, and payment method metadata. Full payment card details are processed by our PCI-DSS compliant payment service providers and are not stored by us (we retain only limited tokens and metadata necessary for billing operations).

3.4 Service Usage Data

Log files, feature usage patterns, session timestamps and duration, pages and screens viewed, click events, diagnostic and performance data, device type, operating system, browser type and version, screen resolution, IP address, approximate geolocation (city/country level derived from IP address), API usage metrics, and referring URL.

3.5 Content and AI Interaction Data

Prompts, files, text, images, configurations, and other content submitted to the platform by you or on your behalf, as well as outputs generated by the Services ("AI Interaction Data"). This may include personal data if you choose to include it in your inputs.

3.6 Communications Data

Support tickets, emails, live chat transcripts, phone call records (if applicable), feedback, and survey responses.

3.7 Marketing and Preference Data

Newsletter subscription status, marketing consent records, campaign interaction data (opens, clicks), communication preferences, and event registration details.

3.8 Security and Compliance Data

Authentication logs, multi-factor authentication metadata, audit trails, consent records, abuse prevention data, and incident records.

3.9 Cookie and Tracking Data

Data collected via cookies, pixels, and similar technologies — see Section 15 for details.

3.10 Job Application Data

If you apply for a role with us: name, contact details, CV/resume, cover letter, interview notes, and assessment results. Recruitment processing details may be provided in a separate notice.

---

4. Purposes and Legal Bases for Processing

We process personal data only where we have a valid legal basis under Article 6 GDPR. Below is a summary of our processing purposes and the legal basis for each.

4.1 Providing and Operating the Services

- Account creation, authentication, and login;
- delivering platform functionality;
- processing AI inputs and generating outputs at your direction;
- customer support and technical assistance;
- transaction processing and subscription management.

Legal basis: performance of a contract with you (Article 6(1)(b) GDPR).

4.2 Improving, Maintaining, and Securing the Services

- Troubleshooting errors and performance issues;
- monitoring system health and uptime;
- fraud, abuse, and threat detection and prevention;
- security incident detection, investigation, and response;
- product analytics to understand how features are used and improve the user experience.

Legal basis: legitimate interests (Article 6(1)(f) GDPR) — our interest in operating a secure, reliable, and continuously improving platform. Where required by law, legal obligation (Article 6(1)(c) GDPR).

4.3 Payments and Financial Obligations

- Processing payments and managing billing;
- issuing invoices and credit notes;
- complying with Dutch and EU tax, accounting, and financial reporting requirements.

Legal basis: performance of a contract (Article 6(1)(b)) and compliance with legal obligations (Article 6(1)(c) GDPR).

4.4 Communications

- Sending service messages, account notifications, and security alerts;
- responding to your support requests and inquiries;
- providing onboarding guidance and product tips.

Legal basis: performance of a contract (Article 6(1)(b)) and legitimate interests (Article 6(1)(f) GDPR).

4.5 Marketing Communications

- Newsletters and product update emails;
- event invitations and webinar announcements;
- promotional offers and feature announcements.

Legal basis: consent (Article 6(1)(a) GDPR) where required by applicable law (including Article 11.7 Dutch Telecommunications Act for electronic marketing). For existing customers, we may send marketing about similar services based on legitimate interests (soft opt-in), with an easy opt-out in every message. You can withdraw consent or opt out at any time.

4.6 Analytics and Product Development

- Aggregated and anonymized usage analytics;
- A/B testing and feature experiments;
- product roadmap prioritization based on usage patterns.

Legal basis: legitimate interests (Article 6(1)(f) GDPR) — our interest in understanding usage and improving the Services. Where data is fully anonymized, GDPR no longer applies.

4.7 Legal Compliance and Rights Enforcement

- Complying with applicable laws, regulations, and court orders;
- responding to lawful requests from authorities;
- establishing, exercising, or defending legal claims.

Legal basis: legal obligation (Article 6(1)(c)) and legitimate interests (Article 6(1)(f) GDPR).

4.8 Consent Records and Withdrawal Right Logging

- Recording checkout consents (immediate access, withdrawal waiver) for consumer compliance;
- maintaining marketing consent and preference records.

Legal basis: legal obligation (Article 6(1)(c) GDPR) and legitimate interests (Article 6(1)(f)).

Where we rely on legitimate interests, we have conducted a balancing assessment to ensure that our interests do not override your fundamental rights and freedoms. You may request details of these assessments by contacting us.

---

5. Artificial Intelligence — Specific Processing

Our Services include AI features powered by machine-learning models. This section explains how personal data is handled in that context.

5.1 How AI Features Process Your Data

When you use AI features, we process the prompts, files, and context you submit ("AI Inputs") to generate outputs ("AI Outputs"). AI Inputs and AI Outputs are processed to perform the service you have requested. By default, this content is handled for service delivery and support purposes and is not used to train our own general-purpose AI models unless you choose an optional opt-in program.

5.2 No Training on Your Personal Data by Default

By default, we do not use personal data in AI Interaction Data to train or fine-tune our general-purpose AI models. We may use limited de-identified or aggregated telemetry to maintain safety, reliability, and performance. If we offer optional data-contribution programs for model improvement, participation is voluntary, clearly disclosed, and based on opt-in consent where required by law. You can withdraw that consent at any time, with effect for future processing.

5.3 Third-Party AI Providers

Certain AI features may involve third-party LLM providers as sub-processors. When this occurs: (a) we apply contractual and technical controls designed to limit processing to requested service delivery; (b) your data is transmitted securely and processed to generate outputs at your request; and (c) your personal data and AI Interaction Data are not made available to those providers for training, retraining, or fine-tuning their general-purpose models. Any exception requires your explicit prior consent and/or applies only where strictly required by mandatory law.

5.4 Automated Decision-Making and Profiling

Our Services may assist with automated processing, but we do not make decisions based solely on automated processing that produce legal effects concerning you or similarly significantly affect you within the meaning of Article 22 GDPR, unless: (a) you have given explicit consent; (b) it is necessary for performance of a contract; or (c) it is authorized by applicable law with appropriate safeguards. If you believe an automated decision has affected you, you may contact us to request human review.

5.5 AI Output Accuracy

AI Outputs are probabilistic and may be inaccurate, incomplete, or unsuitable for your purpose. We recommend reviewing all AI Outputs before relying on them. We are not responsible for decisions you make based on AI Outputs.

---

6. Special Categories of Personal Data

Our Services are not designed for, and we do not request, the routine processing of special categories of personal data as defined in Article 9 GDPR (for example, data revealing racial or ethnic origin, political opinions, religious beliefs, health data, biometric data, or data concerning sex life or sexual orientation).

If you choose to include such data in your inputs to the Services, you do so at your own risk and are responsible for ensuring a valid legal basis and any required safeguards. We strongly advise against submitting sensitive personal data unless necessary and legally permitted.

---

7. Children

Our Services are not directed at children. You must be at least sixteen (16) years old to create an account or use the Services, consistent with the age of digital consent under Article 8 GDPR as implemented by Article 5 UAVG.

If you are under 18, you confirm that you have the consent of a parent or legal guardian.

We do not knowingly collect personal data from children under 16 without valid parental or guardian consent. If we become aware that we have collected personal data from a child under 16 without proper consent, we will take steps to delete it as soon as reasonably practicable and subject to applicable legal retention obligations.

---

8. Sources of Personal Data

We collect personal data from the following sources:

- Directly from you — when you create an account, subscribe, submit content, contact us, or fill in forms;
- Automatically — through your use of the Services (logs, telemetry, cookies, and similar technologies);
- From your organization — if your employer or organization sets up your account as part of a business subscription;
- From service providers and integrations — such as payment processors, identity providers (SSO), and third-party tools you connect to the Services;
- From publicly available sources — such as professional networking profiles, company websites, or public registers, where relevant for sales or business development (on the basis of legitimate interests).

---

9. Recipients and Sharing of Personal Data

We do not sell personal data for monetary consideration. We share personal data only as described below and only to the extent necessary to operate the Services. In some jurisdictions, certain cookie- or advertising-related disclosures may be treated as "sharing" for cross-context behavioral advertising; see Sections 14.2 and 15.

9.1 Service Providers (Processors)

We engage trusted third-party service providers who process personal data on our behalf, under our instructions and subject to data processing agreements. Categories include:

- Cloud hosting and infrastructure providers;
- AI and LLM providers (for AI feature processing — see Section 5.3);

- Payment and billing processors;
- Customer support and ticketing platforms;
- Email delivery and communication services;
- Analytics and product intelligence tools;
- Security monitoring and incident response providers.

An up-to-date list of sub-processors is available on our website privacy pages and through our privacy contact channels.

9.2 Affiliates

We may share personal data with our affiliates for internal administration, shared service delivery, and support, subject to the same protections described in this Privacy Policy.

9.3 Professional Advisers

Legal, accounting, audit, tax, and insurance advisers, where necessary for professional advice or dispute resolution, under professional secrecy obligations.

9.4 Authorities and Courts

Where required by law, regulation, or valid legal process, or where necessary to establish, exercise, or defend legal claims.

9.5 Corporate Transactions

In connection with a merger, acquisition, financing, reorganization, or sale of all or substantially all of our assets, with appropriate confidentiality and data protection safeguards.

---

10. International Data Transfers

Our primary infrastructure is hosted within the European Economic Area (EEA). However, some of our service providers and sub-processors (including AI/LLM providers) may process personal data outside the EEA.

Where personal data is transferred outside the EEA, we ensure appropriate safeguards are in place, including:

- European Commission adequacy decisions (Article 45 GDPR);
- Standard Contractual Clauses (SCCs) approved by the European Commission (Commission Implementing Decision (EU) 2021/914);
- UK International Data Transfer Agreement (UK IDTA) or UK Addendum to the EU SCCs, for transfers subject to UK GDPR;
- Supplementary technical and organizational measures (such as encryption and access controls) where required following a transfer impact assessment.

You may request information about the safeguards in place for specific transfers through the privacy contact channels listed in Section 19.

---

11. Retention Periods

We retain personal data only as long as necessary for the purposes described in this Privacy Policy, taking into account legal, tax, accounting, and dispute-resolution requirements.

Indicative Retention Periods

- Account and identity data: for the duration of your account and up to twelve (12) months after account closure (to handle re-activation, support follow-ups, and residual queries).

- Billing and tax records: seven (7) years after the end of the relevant fiscal year, as required by Dutch tax and accounting law (Algemene wet inzake rijksbelastingen).
- Service usage and analytics data: up to twenty-four (24) months in identifiable form, then anonymized or deleted.
- Support and communications records: up to thirty-six (36) months after resolution, based on operational need and legal risk windows.
- Security and audit logs: up to twenty-four (24) months, unless longer retention is necessary for ongoing investigations or legal proceedings.
- Marketing consent records: for the duration of the consent and a reasonable period thereafter for compliance evidence.
- AI Interaction Data (prompts and outputs): retained only as long as necessary for service delivery and in accordance with your configured retention settings. By default, this data is not used for model training unless you have opted in to a clearly disclosed program.
- Checkout consent records (withdrawal waiver): for the duration of the customer relationship plus two (2) years.
- Cookie data: per the durations specified in our Cookie Notice / Section 15.

When personal data is no longer needed, we securely delete or irreversibly anonymize it. Deletion may be delayed where retention is required or permitted by law, including legal holds, dispute resolution, fraud and security investigations, tax and accounting obligations, backup integrity, or the establishment, exercise, or defense of legal claims. Residual copies may remain in encrypted backups until routine overwrite cycles are completed.

---

12. Your Rights Under GDPR

Under GDPR, you have the following rights in relation to your personal data, subject to applicable legal conditions and exceptions:

Right of Access (Article 15): obtain confirmation of whether we process your personal data and, if so, a copy of your data and information about how it is processed.

Right to Rectification (Article 16): request correction of inaccurate personal data or completion of incomplete data.

Right to Erasure (Article 17): request deletion of your personal data where it is no longer necessary, where you withdraw consent, or where processing is unlawful ("right to be forgotten"), subject to legal exceptions.

Right to Restriction (Article 18): request that we limit how we process your data in certain circumstances.

Right to Data Portability (Article 20): receive your personal data in a structured, commonly used, machine-readable format and transmit it to another controller.

Right to Object (Article 21): object to processing based on legitimate interests (including profiling) or direct marketing. Where you object to direct marketing, we will honor the objection as soon as reasonably practicable and within applicable legal timelines.

Right Not to Be Subject to Automated Decision-Making (Article 22): not to be subject to decisions based solely on automated processing that produce legal effects or similarly significantly affect you, except where permitted by law.

Right to Withdraw Consent: where processing is based on consent, you may withdraw consent at any time. Withdrawal does not affect the lawfulness of processing before withdrawal.

How to Exercise Your Rights

Use the privacy request channels listed in Section 19. We will respond within one (1) month of your request, as required by Article 12 GDPR. If your request is complex or we receive a high volume of requests, we may extend this by up to two (2) additional months, and we will inform you of any extension.

We may ask you to verify your identity before processing your request, to protect your data from unauthorized access.

Exercising your rights is free of charge. In exceptional cases where requests are manifestly unfounded or excessive (particularly if repetitive), we may charge a reasonable fee or refuse to act, as permitted by Article 12(5) GDPR.

Right to Complain

If you believe we are not handling your personal data correctly, you have the right to lodge a complaint with a supervisory authority. In the Netherlands, this is:

Autoriteit Persoonsgegevens

Website: https://autoriteitpersoonsgegevens.nl

Post: Postbus 93374, 2509 AJ Den Haag, the Netherlands

Phone: +31 (0)70 888 8500

If you reside in another EEA country, you may also contact your local supervisory authority.

---

13. Direct Marketing and Opt-Out

13.1 We may send you marketing communications where we have your consent or where we rely on the soft opt-in exemption under Article 11.7(2) of the Dutch Telecommunications Act (i.e., you are an existing customer and we are promoting similar services).

13.2 Every marketing email includes a clear and easy opt-out (unsubscribe) link. You can also update your preferences in your account settings or by contacting us.

13.3 If you opt out, we will stop sending marketing communications as soon as reasonably practicable and, in any event, within applicable legal timelines (typically within ten (10) business days for email suppression updates). Opting out of marketing does not affect transactional or service-related messages (such as billing notifications, security alerts, and account updates).

13.4 We do not engage in unsolicited telephone marketing to consumers without prior consent.

---

14. Additional Information for Users Outside the EEA

Our Services are available globally. Depending on where you are located, you may have additional rights under local privacy laws.

14.1 United Kingdom

If you are located in the United Kingdom, we process your personal data in accordance with the UK GDPR and the Data Protection Act 2018. Your rights under UK GDPR are substantially the same as those described in Section 12. For international transfers, we rely on the UK International Data Transfer Agreement or UK Addendum to EU SCCs. You may lodge a complaint with the Information Commissioner's Office (ICO) at https://ico.org.uk.

14.2 United States State Privacy Rights (including California)

If you are a resident of California or another U.S. state with an applicable consumer privacy law, you may have additional rights in relation to your personal information, subject to verification, permitted exceptions, and limitations under applicable law.

14.2.1 Rights that may apply to you

- know or confirm whether we process your personal information and access it;
- request correction of inaccurate personal information;
- request deletion of personal information, subject to legal exceptions;
- obtain a portable copy of personal information in a usable format where required by law;
- opt out of the sale of personal information, the "sharing" of personal information for cross-context behavioral advertising, targeted advertising, and certain profiling in furtherance of decisions that produce legal or similarly significant effects, where these rights apply; and
- appeal a refusal to take action on your request, where your state law provides an appeal right.

We will verify your identity and, where applicable, your authority to make a request before taking action. We may deny or limit a request where an exemption or exception applies under applicable law.

Please note that the Sion AI SaaS sercied and the data entered in Sion AI during is hosted in Europe, France for all global customers.

14.2.2 California-specific notice

During the preceding 12 months, the categories of personal information we have collected are described in Section 3; the sources of that information are described in Section 8; the purposes for collection, use, and disclosure are described in Sections 4 and 5; and the categories of recipients and disclosures are described in Section 9.

We do not sell personal information for monetary consideration. We may use analytics cookies, pixels, SDKs, or similar technologies that may be considered "sharing" or use for cross-context behavioral advertising under California law. Where required, we provide the right to opt out through cookie settings, Global Privacy Control recognition where legally required, and the request methods described in Section 19.

To the extent we process "sensitive personal information" as defined by California law, we use and disclose it only for the purposes described in this Privacy Policy, for providing and securing the Services, or as otherwise permitted by law, unless we provide a separate notice and obtain any consent required by law.

California residents may use an authorized agent to submit requests on their behalf, subject to verification of the agent's authority and your identity. California residents also have the right not to receive discriminatory treatment for exercising their privacy rights.

14.2.3 Other U.S. state laws

Residents of other U.S. states with applicable privacy laws — including, where applicable, Colorado, Connecticut, Virginia, Utah, Texas, Oregon, Montana, Delaware, Iowa, Nebraska, New Hampshire, New Jersey, Tennessee, Minnesota, Maryland, Indiana, Kentucky, Rhode Island, and other states that adopt similar laws — may have substantially similar rights, although the exact scope, exceptions, and response timelines vary by state.

If we deny a request and your state law grants an appeal right, you may submit an appeal through the privacy contact methods in Section 19. We will review the appeal in accordance with applicable law and explain the outcome.

14.3 Brazil

If you are located in Brazil, you may have rights under the Lei Geral de Protecao de Dados (LGPD), including the right to access, correct, delete, and request portability of your personal data. To exercise your rights, use the privacy channels in Section 19.

14.4 Other Jurisdictions

If you are located in a jurisdiction with specific privacy rights not listed above, we will comply with applicable local requirements. Please contact us if you have questions about your rights.

---

15. Cookies and Similar Technologies

We use cookies and similar technologies (pixels, local storage, fingerprinting techniques) on our website and platform. This section provides an overview; a separate Cookie Notice may provide additional detail.

15.1 What Are Cookies?

Cookies are small text files stored on your device when you visit a website. They help websites function, remember your preferences, and provide analytics.

15.2 Categories of Cookies We Use

Strictly Necessary Cookies: essential for the website and Services to function (authentication, security, load balancing). These cannot be disabled. Legal basis: exempt from consent under Article 11.7a Dutch Telecommunications Act.

Functional Cookies: remember your preferences (language, theme, dashboard layout). Legal basis: legitimate interests or consent, depending on the cookie.

Analytics Cookies: help us understand how visitors use our website so we can improve the user experience. We aim to use privacy-friendly analytics that minimize personal data collection. Legal basis: consent where required; some analytics cookies may qualify for the limited cookie consent exemption under Dutch law if they have minimal privacy impact.

Marketing Cookies: used to measure campaign performance and, where enabled, to support interest-based advertising across third-party sites or services. Depending on jurisdiction, this may be considered "sharing" for cross-context behavioral advertising. We only deploy these cookies when required consent has been obtained and we provide opt-out controls where required by law.

15.3 Managing Cookies

Where required by law, we ask for your consent before placing non-essential cookies through our cookie banner. You can change your cookie preferences at any time through our cookie settings panel or by adjusting your browser settings.

Please note that disabling certain cookies may affect the functionality of the Services.

15.4 Do Not Track / Global Privacy Control

We respect browser-level Do Not Track (DNT) and Global Privacy Control (GPC) signals where technically feasible and legally required. If you enable GPC, we will treat it as a valid opt-out signal for non-essential tracking and, where applicable law requires, for sale/sharing opt-out requests.

---

16. Security Measures

We implement risk-appropriate technical and organizational measures designed to protect personal data against unauthorized access, alteration, disclosure, or destruction, taking into account the nature of the data and the evolving threat landscape. These measures include:

- Role-based access controls and least-privilege principles;
- Encryption in transit and at rest where appropriate;
- Multi-factor authentication for administrative and privileged access where appropriate;
- Security event logging and centralized monitoring;
- Vulnerability scanning, penetration testing, and patch management practices;
- Incident detection, response, and breach notification procedures;
- Staff confidentiality commitments and security awareness training;
- Processor and sub-processor due diligence and contractual safeguards.

Security measures are reviewed and updated over time; however, no method of transmission or storage is completely risk-free, and we cannot guarantee absolute security. If you discover a potential security vulnerability, please report it through the security reporting channel on our website or support portal.

---

17. Data Processing Agreement for Business Customers

Where we process personal data on behalf of business customers (for example, data stored in customer workspaces or processed through Foundry workflows or Synesthesia OS workspace features), we act as a processor under a separate Data Processing Agreement (DPA) in accordance with Article 28 GDPR.

In those cases, the business customer is the controller for their workspace data, and our processing follows the customer's documented instructions, the DPA, and applicable law. End users of business customer accounts should contact their organization for information about how their personal data is handled.

---

18. Changes to This Privacy Policy

18.1 We may update this Privacy Policy from time to time to reflect changes in law, our processing practices, or the Services.

18.2 If changes are material, we will provide notice as early as reasonably practicable, using channels such as email, in-product notice, or a prominent notice on our website. Where applicable law requires a specific notice period or consent mechanism, we will follow those requirements.

18.3 The "Effective Date" and "Last Updated" date at the top of this page always reflect the current version.

18.4 We encourage you to review this Privacy Policy periodically. Where permitted by law, your continued use of the Services after an update constitutes acceptance of the revised Privacy Policy. Where mandatory law requires separate consent or another affirmative step, we will request it.

---

19. Contact and Complaints

For privacy questions, rights requests, or complaints, contact us through one of the channels below:

Privacy Team - Foundry and Synesthesia OS

Primary channel: Use the Privacy Request option in your account settings.

Alternative channel: Use the privacy/contact form on our official website and select "Privacy".

If you require formal legal-notice details, request them through either channel and we will provide the appropriate contact details.

We aim to resolve privacy-related inquiries promptly. If you are not satisfied with our response, you may lodge a complaint with:

Autoriteit Persoonsgegevens (Dutch Data Protection Authority)

Website: https://autoriteitpersoonsgegevens.nl

Post: Postbus 93374, 2509 AJ Den Haag, the Netherlands

Phone: +31 (0)70 888 8500

If you reside outside the Netherlands, you may also contact the supervisory authority in your country of residence.