PRIVACY POLICY

Agosec

Last Updated: February 23, 2025

Contents

1 Introduction and Scope

This Privacy Policy (**"Policy"**) describes how Agosec, its affiliates, successors, and assigns (**"we," "us,"** or **"our"**) collect, use, disclose, and protect personal information when you use our mobile application (including the Agosec keyboard extension), our website at agosec.io, and related services (collectively, the **"Service"**).

We are committed to protecting your privacy and being transparent about our data practices. This Policy applies to all users of the Service, regardless of where you are located. By using the Service, you consent to the practices described in this Policy. If you do not agree with this Policy, please do not use the Service.

This Policy should be read together with our Terms and Conditions, which govern your use of the Service.

2 Data Controller and Contact

For purposes of applicable data protection laws, including the General Data Protection Regulation (GDPR), Agosec is the **data controller** responsible for your personal information.

Data Controller:	Agosec
Email:	privacy@agosec.io
Legal/DPO Inquiries:	legal@agosec.io
Website:	https://agosec.io

If you have questions about this Policy or wish to exercise your privacy rights, please contact us using the information above. We will respond to verified requests within the timeframe required by applicable law (typically 30 days for GDPR, 45 days for CCPA).

3 Definitions

- **"Personal Information"** or **"Personal Data"** means any information relating to an identified or identifiable natural person, as defined under applicable privacy laws (e.g., GDPR Article 4(1), CCPA).
- **"Processing"** means any operation performed on personal data (e.g., collection, storage, use, disclosure, deletion).
- **"Sensitive Personal Information"** means categories of data that receive heightened protection, such as precise geolocation, biometric data, health information, or information revealing racial/ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, or data concerning sex life or sexual orientation (as defined under applicable law).
- **"Service"** means the Agosec mobile app, keyboard extension, website, and related features.

4 Information We Collect

We collect information in the following ways:

4.1 Information You Provide Directly

1. **Chat Messages and AI Interactions:** When you use the AI Agent Mode in our keyboard, we process the text you type and the content of your conversations to provide AI-generated responses. This data is transmitted to our backend servers and, for AI processing, to third-party large language model (LLM) providers.

2. **Screenshots and Photo Library Access:** If you choose to import screenshots for AI context, we access selected photos from your device. Screenshots may be processed (including OCR and visual analysis) locally on your device and/or transmitted to our servers and LLM providers to generate contextual assistance. You can decline photo library access; the feature is optional.
3. **Account and Subscription Information:** If you create an account or subscribe, we may collect identifiers such as email address (if provided), and we receive subscription status and transaction identifiers from Apple when you purchase through the App Store.
4. **Website Forms:** If you submit information through forms on our website (e.g., waitlist, contact, or newsletter signup), we collect the information you provide, such as name, email address, company, and any message content.
5. **Communications:** If you contact us (e.g., support, legal inquiries), we collect the content of your communications and contact details you provide.

4.2 Information Collected Automatically

1. **Device Information:** Device type, model, operating system (e.g., iOS version), unique device identifiers, and app version.
2. **Usage Data:** How you interact with the Service, including feature usage, session duration, and error logs, which help us improve the Service and diagnose issues.
3. **Network and Technical Data:** IP address, network type, and connection information when you access our servers.
4. **Apple Transaction Data:** When verifying your subscription, we receive transaction identifiers and subscription status from Apple's App Store Server API. We do not receive your Apple ID, payment card details, or full purchase history from Apple.

4.3 Information from Third Parties

1. **Apple:** Subscription status, transaction IDs, and entitlement information as described above.
2. **LLM Providers:** We use third-party AI/LLM services to process your chat inputs and generate responses. These providers may receive and process the content you submit as part of their service to us. Their processing is governed by our agreements with them and their own privacy policies.

4.4 Information We Do Not Collect

We do not intentionally collect: (a) your precise real-time geolocation for tracking; (b) your contacts or address book; (c) your full typing history outside of explicit AI chat sessions; or (d) payment card details (handled solely by Apple). Granting "Full Access" to the keyboard allows network and inter-app communication; it does not mean we log or store everything you type in other apps.

5 How We Use Your Information

We use personal information for the following purposes:

- **Provide the Service:** To deliver the keyboard, AI agent features, subscription access, and website functionality.
- **Process AI Requests:** To send your messages and optional screenshot content to our backend and LLM providers for response generation.

- **Verify Entitlements:** To confirm your subscription status with Apple and grant or restrict access to premium features.
- **Improve the Service:** To analyze usage patterns, fix bugs, and develop new features.
- **Customer Support:** To respond to your inquiries and provide assistance.
- **Legal and Safety:** To comply with legal obligations, enforce our Terms, protect our rights, and ensure the safety of our users and the Service.
- **Marketing (with consent):** To send promotional communications if you have opted in. You may withdraw consent at any time.

We do not sell your personal information. We do not use your information for profiling or automated decision-making that produces legal or similarly significant effects, except as necessary to provide the Service (e.g., subscription access control).

6 Legal Basis for Processing (GDPR)

If you are located in the European Economic Area (EEA), United Kingdom, or Switzerland, we process your personal data based on the following lawful bases:

- **Contract Performance:** Processing necessary to perform our contract with you (e.g., providing the Service, verifying subscriptions).
- **Legitimate Interests:** Processing for our legitimate interests, such as improving the Service, preventing fraud, and ensuring security, where such interests are not overridden by your rights.
- **Consent:** Where we rely on consent (e.g., optional photo library access, marketing communications), you may withdraw consent at any time.
- **Legal Obligation:** Processing required to comply with applicable law.

You have the right to object to processing based on legitimate interests. We will cease such processing unless we demonstrate compelling legitimate grounds that override your interests, rights, and freedoms, or for the establishment, exercise, or defense of legal claims.

7 How We Share Your Information

We may share personal information in the following circumstances:

7.1 Service Providers

We share data with trusted service providers who assist us in operating the Service, including:

- **AI/LLM Providers:** To process your chat input and generate AI responses.
- **Cloud Infrastructure:** For hosting, storage, and API delivery.
- **Analytics Providers:** For usage analysis and crash reporting (if applicable).

These providers act as processors or subprocessors and are contractually obligated to protect your data and use it only for the purposes we specify.

7.2 Legal Requirements

We may disclose information when required by law, such as in response to subpoenas, court orders, or government requests, or when we believe disclosure is necessary to protect our rights, your safety, or the safety of others.

7.3 Business Transfers

In the event of a merger, acquisition, or sale of assets, your personal information may be transferred as part of that transaction. We will notify you of any such change.

7.4 With Your Consent

We may share information for other purposes with your explicit consent.

8 International Data Transfers

The Service is operated from and our servers and service providers may be located in the United States or other countries outside your country of residence. By using the Service, you consent to the transfer of your personal information to countries that may have different data protection laws.

For transfers from the EEA, UK, or Switzerland to countries not deemed adequate by the European Commission, we implement appropriate safeguards, such as:

- Standard Contractual Clauses (SCCs) approved by the European Commission;
- Binding Corporate Rules (where applicable); or
- Other mechanisms recognized under applicable law.

You may request details of the safeguards we use by contacting us at privacy@agosec.io.

9 Data Retention

We retain personal information only for as long as necessary to fulfill the purposes described in this Policy, unless a longer retention period is required or permitted by law.

- **Chat and AI Data:** Session and message content may be retained temporarily for processing and may be stored in logs for a limited period (e.g., 30–90 days) for debugging and improving the Service, unless you request earlier deletion.
- **Account and Subscription Data:** Retained for the duration of your account and subscription, plus a reasonable period thereafter for legal and accounting purposes.
- **Website Form Submissions:** Retained as long as needed to respond to your inquiry and for legitimate business purposes.
- **Technical and Usage Data:** Aggregated or anonymized data may be retained longer for analytics. Personal identifiers are removed or minimized where feasible.

Upon request, we will delete or anonymize your personal information where required by law or our retention policies, except where we must retain it for legal, regulatory, or legitimate business purposes.

10 Data Security

We implement appropriate technical and organizational measures to protect your personal information against unauthorized access, alteration, disclosure, or destruction, including:

- Encryption of data in transit (TLS/HTTPS) and at rest where feasible;
- Access controls and authentication;
- Regular security assessments and monitoring;

- Contractual safeguards with processors requiring confidentiality and security.

No method of transmission over the Internet or electronic storage is 100% secure. We cannot guarantee absolute security but are committed to maintaining industry-standard practices. You are responsible for maintaining the security of your device and account credentials.

11 Your Privacy Rights

Depending on your location, you may have the following rights:

11.1 Access and Portability

You have the right to request access to the personal information we hold about you and, where technically feasible, to receive a copy in a portable format.

11.2 Correction (Rectification)

You may request correction of inaccurate or incomplete personal information.

11.3 Erasure (Right to Be Forgotten)

You may request deletion of your personal information, subject to certain exceptions (e.g., where we must retain data for legal compliance).

11.4 Restriction of Processing

You may request that we restrict the processing of your data in certain circumstances (e.g., while you contest accuracy).

11.5 Objection

You may object to processing based on legitimate interests or for direct marketing purposes.

11.6 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.

11.7 Complaint

You have the right to lodge a complaint with a supervisory authority in your country of residence. In the EEA, you may find your authority at https://edpb.europa.eu/about-edpb/about-edpb/members_en.

11.8 How to Exercise Your Rights

To exercise any of these rights, contact us at privacy@agosec.io. We will respond within the timeframes required by applicable law (e.g., one month under GDPR, 45 days under CCPA, subject to extension where permitted). We may need to verify your identity before processing your request.

12 California Privacy Rights (CCPA/CPRA)

If you are a California resident, the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) provide you with additional rights:

12.1 Right to Know

You may request disclosure of: (a) the categories of personal information we have collected about you; (b) the categories of sources; (c) the business or commercial purposes for collection; (d) the categories of third parties with whom we share the information; and (e) the specific pieces of personal information we have collected.

12.2 Right to Delete

You may request deletion of your personal information, subject to certain exceptions.

12.3 Right to Correct

You may request correction of inaccurate personal information.

12.4 Right to Opt-Out of Sale or Sharing

We do not sell personal information. We do not share personal information for cross-context behavioral advertising in a manner that constitutes a "sale" or "share" under the CCPA. If our practices change, we will provide an opt-out mechanism.

12.5 Right to Limit Use of Sensitive Personal Information

We do not use or disclose sensitive personal information for purposes beyond those permitted by the CCPA. If our practices change, we will provide a right to limit use.

12.6 Right to Non-Discrimination

We will not discriminate against you for exercising your privacy rights.

12.7 Submitting Requests

California residents may submit requests by emailing privacy@agosec.io or through any in-app or website mechanism we provide. You may designate an authorized agent to submit requests on your behalf. We will verify your identity before fulfilling requests.

13 Other U.S. State Privacy Laws

Residents of other U.S. states with comprehensive privacy laws (e.g., Virginia, Colorado, Connecticut, Utah, Texas) may have similar rights to access, correct, delete, opt out of targeted advertising or sales, and portability. To exercise such rights, contact us at privacy@agosec.io. We will process requests in accordance with the applicable state law.

14 Children's Privacy

The Service is not directed to children under 13 (or the applicable age of digital consent in your jurisdiction). We do not knowingly collect personal information from children under 13. If you are a parent or guardian and believe your child has provided us with personal information

without your consent, please contact us at privacy@agosec.io. We will take steps to delete such information promptly.

For users between 13 and 18, we rely on parental or guardian consent where required by applicable law. Parents or guardians may contact us to review, correct, or delete information provided by their child.

15 Cookies and Similar Technologies

15.1 Our Website

Our website may use cookies and similar technologies (e.g., local storage, pixels) to:

- Remember your preferences and settings;
- Understand how you use our website;
- Improve performance and user experience.

15.2 Third-Party Technologies

Our website loads resources from third parties, such as Google Fonts. These services may set cookies or collect technical data (e.g., IP address) in accordance with their own privacy policies. Google's policy is available at https://policies.google.com/privacy.

15.3 Your Choices

Most browsers allow you to refuse or delete cookies. Doing so may affect website functionality. You may also use browser add-ons or settings to limit tracking.

15.4 Our Mobile App

Our mobile app does not use cookies. It may use similar technologies such as local storage and device identifiers for functionality and, with your consent, for analytics.

16 Do Not Track

Some browsers offer a "Do Not Track" (DNT) signal. There is no universal standard for how websites respond to DNT signals. We do not currently respond to DNT signals in a uniform way. We continue to honor the privacy choices you make through our settings and this Policy.

17 Keyboard-Specific Disclosures

17.1 Full Access (Open Access) Permission

Our keyboard extension may request "Full Access" (Open Access) permission from iOS. This permission is required to:

- Enable network access for AI features (chat and contextual assistance);
- Share entitlement and settings data between the keyboard extension and the main app via App Groups;
- Access the photo library when you explicitly choose to import screenshots for AI context.

Granting Full Access does not mean we collect, log, or transmit everything you type in other applications. We process text and images only when you actively use AI Agent Mode or similar features that require such processing.

17.2 Optional Photo Library Access

Photo library access is optional. If you grant access, we use it solely to let you select screenshots for AI context. You may revoke access at any time in your device Settings. If you choose "Use and Delete" when importing screenshots, we will delete the selected photos from your library after processing, subject to technical limitations.

18 AI and Machine Learning

Our AI features process your input (text and optionally images) to generate responses. This processing involves:

- Transmitting your messages and optional screenshot-derived content to our backend and third-party LLM providers;
- Temporary storage during processing;
- Possible use of aggregated, de-identified data to improve our models and service quality.

We do not use your personal conversations to train third-party LLM providers' general models, except where you have separately agreed to such use (e.g., through an opt-in program). Our contracts with LLM providers require appropriate data handling and confidentiality.

19 Changes to This Policy

We may update this Policy from time to time to reflect changes in our practices, the Service, or legal requirements. We will notify you of material changes by:

- Posting the updated Policy on our website and in the app;
- Updating the "Last Updated" date;
- Providing additional notice (e.g., email or in-app notification) where required by law or for significant changes.

Your continued use of the Service after the effective date of changes constitutes acceptance of the revised Policy. We encourage you to review this Policy periodically.

20 Contact Us

For questions about this Privacy Policy or to exercise your privacy rights:

Privacy Inquiries:	privacy@agosec.io
Legal/DPO Inquiries:	legal@agosec.io
Website:	https://agosec.io

For EU/EEA residents, you may also contact our representative (if designated) or lodge a complaint with your local data protection authority.

— End of Privacy Policy —