

Privacy Policy, Unique AI

Unique AI

- **Source:** <https://www.unique.ai/privacy-policy>
- **Date :** 17.09.2026
- **Authors :** Dr. Sina Wulfmeyer, Mathias Reimer, Daylan Araz

Unique AI is a company that offers enterprise AI for finance: a secure platform that gives financial institutions the flexibility to build and buy AI solutions.

This **Privacy Policy** explains how Unique AI ("Unique", "we", "us") collects, uses, discloses, and processes personal data when you visit our website, use our platform, or otherwise interact with our services (the "Services").

This Privacy Policy does not apply to content that we process on behalf of our business customers under their agreements with us — for example, business correspondence, recordings, or other data processed while delivering our Services to a business customer. Our processing of that data is instead governed by the applicable customer agreement and our Data Processing Addendum (DPA); the business customer, not Unique AI, determines how that data is used and is responsible as the data controller.

This Privacy Policy also describes your privacy rights and how to exercise them; see "Data Subject Rights" below for more information.

Legal Basis

The policy operates under *"the Swiss Data Protection Act (S-DPA) of September 25th, 2020"*, as well as the EU GDPR and UK GDPR, which may also apply to companies outside the EU/UK that process data in those territories.

Principles of Data Processing

Processing follows principles including good faith and proportionality, limited purpose usage, destruction of data when no longer necessary, correction of inaccurate data, voluntary consent requirements, and adherence to privacy-by-design and privacy-by-default standards.

Data Collection

Unique AI collects website usage data, device information, customer account details, contact information, and business preferences — either automatically, through user interaction, or via third parties and analytics tools.

Unique AI collects the following categories of personal data, either automatically, through your direct interaction with our Services, or via third parties and analytics tools:

- **Account Information**
Information you provide when creating and managing an account, such as your name, email address, company/organization, and job title.
- **User Content**
Content you submit, upload, or generate through the Services, including chat prompts, uploaded files and attachments, and AI-generated outputs.
- **Communication Information**
Information exchanged when you contact us or use communication features of the Services, including support requests, recorded conversations, transcripts, and, where applicable, video footage.

- **Log Data**
Technical information generated by your use of the Services, such as IP address, browser type, access times, pages viewed, and application usage and error logs.
- **Device Data**
Information about the device used to access the Services, including device type, operating system, unique device identifiers, and application version.
- **Location Data**
General location information (e.g., inferred from IP address) used to provide and secure the Services; we do not collect precise geolocation unless separately disclosed.

Data Uses

Data supports service delivery, legal compliance, and legitimate business interests.

When recording conversations, processing relies on the data subject's freely declared consent according to *"art. 6 para. 6 in conjunction with art. 31 para. 1 S-DPA / art. 6 (1) (a) GDPR"*. The company processes contact information, timestamps, language, voice, transcripts, and potentially video footage in order to analyze conversations and improve the sales process.

Participants may *"withdraw the given consent at any time with effect for the future"* by contacting privacy@unique.ch, though withdrawal might restrict the provision of the service.

Additional purposes include facilitating operations, staff training, user support, understanding usage patterns, optimizing marketing, delivering personalized communications, enhancing security, creating anonymized data, and maintaining legal compliance.

Data Location

Data is maintained *"in Switzerland and other locations, as reasonably necessary"* for service delivery. Unique AI commits to applying its protection standards regardless of local requirements and uses *"Standard Contractual Clauses (SCC)"* for transfers outside the EU/EEA, Switzerland, or the UK.

Data Retention

Customer data is retained as long as necessary for relationship maintenance, legal compliance, and defending potential disputes. Generally, data is kept *"for 10 years after the end of the last transaction"* of the customer relationship, though Unique AI reserves the right to delete or restrict access to data at any time, without obligation or notice, unless legally required otherwise. Details on customer-specific data retention periods is agreed in the contract/ Master Service Agreement.

Data Sharing / Confidentiality

Personal data is treated confidential and is not shared with third parties except as specified in the policy. Unique AI uses contractually bound *sub-processors* in IT services, telecommunications, consulting, and sales/marketing, all of which must comply with applicable data protection laws. A sub-processor list appears in *"Appendix B to the Data Processing Addendum (DPA)"*.

Data is shared with:

- Service providers performing complementary functions
- Business customers, with respect to their own data
- Government authorities or law enforcement, when legally required
- Third-party websites and services (governed by their own terms)
- Others, when necessary to protect rights or safety
- Third-party providers of AI tools (see below)

Data may also be shared among subsidiaries or during ownership changes, or when explicitly approved by the data subject or legally mandated.

We don't "sell" Personal Data or "share" Personal Data for cross-contextual advertising, and we do not process Personal Data for "targeted advertising" purposes. We also don't process sensitive Personal Data for the purposes of inferring characteristics about a consumer.

Use of AI Tools

In order to provide and improve our Services, Unique AI may use third-party AI-based tools and models (for example, large language models and AI-assisted software tools) to process information, including business correspondence and other content shared with us by you or by our business customers. We evaluate and adopt AI tool providers on an ongoing basis, including for testing new models, so the specific providers in use may change from time to time; a current list of the providers used for this purpose is maintained as part of our sub-processor list in Appendix B to our Data Processing Addendum (DPA) and is available upon request.

Where such providers process data outside Switzerland, the EEA, or the UK (for example, in the United States), Unique AI ensures that an appropriate transfer mechanism is in place, as further described under "Data Location" above.

Unless otherwise agreed with a business customer, we do not permit these providers to use your data to train their own models ("**opt-out from model training**"), and each provider is contractually bound to confidentiality and data-protection obligations at least equivalent to those set out in this Privacy Policy.

Cookies, Tracking Technologies and Tools

Unique AI uses cookies and similar technologies on its website. Some of these technologies are necessary to operate the website and provide the requested services. Others, such as analytics and marketing cookies, help us measure website performance, understand how visitors use our website, personalize content, and improve our services. Our cookies are provided by HubSpot and a full list of necessary cookies, its purpose and retention period can be found on their official [Website](#).

Analytics, advertisement, and functionality cookies are only used where you have given your consent through our cookie banner or cookie settings tool. You may manage, refuse, or disable these cookies through your browser settings although, some functionality on our website may be impaired. You may also withdraw or change your consent at any time.

Unique AI's chat service may use browser *localStorage* and *sessionStorage* to store information that is technically necessary for the service to function, maintain the session, and provide the requested service. These technologies are never used for marketing purposes or sold to other companies.

Further information about the cookies and similar technologies we use, including the relevant providers, purposes, categories of data processed, and storage periods, is available in our cookie settings tool and, where applicable, in our list of service providers or sub-processors.

Communications

Service communications inform users about updates, billing, and account changes. Registered users can typically control notification settings, though certain service communications cannot be declined. Promotional communications about features and opportunities may be sent through various channels. Recipients may opt out by emailing privacy@unique.ch, adjusting their profile settings, or following the unsubscribe instructions included in the communication.

Data Security

Unique AI employs "state-of-the-art technical and organizational measures (TOM)", detailed in "Appendix A to the Data Processing Addendum (DPA)". These include technical measures such as "SSL encryption, pseudonymization, logging, access restriction, data backup", and organizational measures such as employee

instructions and confidentiality agreements. However, Unique AI cannot *"guarantee that our Sites or Services will be immune from any wrongdoings, malfunctions, unlawful interceptions or access"*.

Data Subject Rights

Individuals possess the following rights:

- Being informed about the collection of their data
- Requesting information on how their data is processed
- Obtaining rectification and deletion of their data
- Objecting to or restricting processing
- Withdrawing consent
- Data portability
- Being informed about automated decision-making
- Filing complaints with a supervisory authority

Requests should be directed to privacy@unique.ch.

A Note on Accuracy

Services like Unique AI generate responses by reading a user's request and, in response, predicting the words most likely to appear next. In some cases, this output may not be the most factually accurate. For this reason, you should not rely on the factual accuracy of any AI-generated output produced by our Services but cross-check before using the output.

If you notice that an output generated by our Services contains factually inaccurate personal data about you, you may request a correction or removal of that information by contacting privacy@unique.ch. We will consider your request in light of applicable data protection law and the technical capabilities of our models.

Data controller

If you live in the European Economic Area (EEA) or Switzerland, Unique AI AG, with its registered office at Stockerstrasse 34, 8002 Zurich, Switzerland, is the controller and is responsible for the processing of your Personal Data as described in this policy.

If you live anywhere else, our Unique Applications Inc. Office, registered at c/o Industrious | 776A 6th Avenue | 10001 New York | USA, is the controller and is responsible for the processing of your Personal Data as described in this policy.

Processing on Behalf of Business Customers

When processing data on behalf of business customers, Unique AI acts as a service provider (**data processor**), while the customer acts as the **data controller**. The customer bears sole responsibility for determining how the service is used, providing notice to and obtaining consent from affected individuals, ensuring legal compliance, and handling data subject rights requests.

Your Responsibility for Third-Party Personal Data

Where you submit, upload, or otherwise provide content through our Services — including recorded conversations, transcripts, files, or contact information — that includes personal data relating to individuals other than yourself (for example, meeting participants, colleagues, or your own customers or contacts), you are responsible for ensuring that you have the necessary legal basis, rights, permissions, or consents to share that personal data with us and to have it processed as described in this Privacy Policy. This includes, where applicable, informing those individuals that their personal data may be recorded, transcribed, or analyzed, and obtaining their consent where such consent is legally required.

Additional Notices

This policy may be updated by posting an amended version on Unique AI's sites or services. Substantial changes will receive advance notice through available communication channels. The policy applies only to Unique AI's own properties, not to third-party links. The Services are not designed for children under 16, and any detected data belonging to a child will prompt deletion. Unique AI maintains designated EU and UK representatives in accordance with Article 27 GDPR.

Google Integrations

Google Meet™ integration: Recordings created through the standard function (which requires Google Drive™ access) are collected, beginning from the date the integration is connected, together with the connector's email address.

Google Calendar™ integration: Calendar entries are collected to enable automatic recording specification, and the connector's email address is stored.

Calendar conferencing add-on: Unique AI accesses calendar entries to add meeting links that capture recording consent, writing only to those entries, without on-premises storage.

Google Custom Search API: Web search functionality integrates this API, with data processed by Google *"in accordance with your configured settings and Google's Privacy Policy"*. The extent of processing depends on the chosen configuration settings.

Third-Party Integrations

Our Services may allow you to connect third-party applications, tools, or platforms (for example, email, calendar, video-conferencing, or productivity tools) to enhance functionality, including through the Model Context Protocol (MCP), an open standard that allows AI systems to connect to external tools and data sources. Where you choose to enable such an integration, your inputs, outputs, or other content may be sent to, or accessed by, that third-party service, and, for MCP-based integrations, the underlying AI tool or model handling the request (see "Use of AI Tools" above), in order to perform the requested action. Once your data is shared with a connected third party, its handling is also governed by that third party's own privacy policy and terms, which we encourage you to review before enabling the integration. Specific integrations we currently offer, and any related data practices, are described below.

Supervisory Authorities

The Federal Data Protection and Information Commissioner (FDPIC) is the competent authority for matters relating to Switzerland (edoeb.admin.ch). For GDPR or UK GDPR matters, individuals may appeal to the competent data protection supervisory authority; a list is available at edpb.europa.eu.

Amendments to this Privacy Policy

Unique AI may update this policy by sending a revised version to customers or by posting it on the website at unique.ai.

CCPA / CPRA Notice for California Residents

This section describes the California privacy rights that apply to residents of California (including rights created or expanded by the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA)). It supplements the other sections of this Privacy Policy and, where applicable, governs how **Unique Applications Inc.** ("Unique AI", "we", "us", or "our") collects, uses, discloses, and protects personal information of California residents.

Categories of Personal Information We Collect and Disclose

Category	Examples
Identifiers	Name; email; phone number; account ID
Commercial information	Purchase history; subscription plan; billing records
Internet or network activity	IP address; device identifiers; browser and usage logs
Content you provide	Chat prompts; uploaded files; attachments; messages
Professional or employment information	Employer name; job title (when provided)
Payment information	Payment card token; billing address (we do not store full card numbers)
Inferences and profiling	Preferences; model personalization signals

Your California Privacy Rights

California residents have the following rights under CCPA/CPRA. We describe how to exercise each right and how we verify requests.

- **Right to Know / Access** — Request the categories and specific pieces of personal information we collected about you, the sources, the business or commercial purpose for collection, and the categories of third parties with whom we shared or disclosed the information.
- **Right to Delete** — Request deletion of personal information we maintain about you, subject to certain exceptions (e.g., to complete a transaction, comply with legal obligations, or for security and fraud prevention).
- **Right to Correct** — Request correction of inaccurate personal information we maintain about you.
- **Right to Data Portability** — Request a copy of your personal information in a portable, commonly used, machine-readable format.
- **Right to Opt-Out of Sharing for Targeted Advertising** — Opt out is default. We never share or sell personal information for cross-context behavioral advertising.
- **Right to Limit Use of Sensitive Personal Information** — Request limits on our use and disclosure of sensitive personal information for purposes beyond those necessary to provide the service.
- **Right to Non-Discrimination** — You have the right not to receive discriminatory treatment for exercising your CCPA/CPRA rights.

How to Exercise Your Rights

You may submit requests using any of the following methods:

- **Email:** privacy@unique.ch
- **Authorized Agent:** You may designate an authorized agent to submit requests on your behalf. We require written authorization from you and verification of the agent's identity.

Verification: To protect your privacy and security, we will verify your identity before fulfilling requests. Verification may require matching information you previously provided (e.g., account email, recent transaction details) or other reasonable steps. For requests to access or delete information about an account, we will verify using the account credentials or the email address associated with the account. We will not provide personal information to an agent unless we have received signed permission from you and verified the agent's identity.

We will respond to verifiable requests within the timeframes required by law and will notify you if we need additional time or information.

Categories of Sources and Purposes of Use

Sources: We collect personal information directly from you (e.g., when you create an account, submit prompts, upload files, or contact support), from your device and browser, from service providers (e.g., payment processors, analytics providers), and from publicly available sources.

Purposes: We use personal information to provide and improve our services, process payments, communicate with you, personalize your experience, detect and prevent fraud, comply with legal obligations, and for other business purposes described in this Privacy Policy.

Disclosures to Third Parties

We disclose personal information to service providers and vendors who perform services on our behalf (e.g., hosting, analytics, payment processing), to comply with legal obligations, to respond to lawful requests, and in connection with business transactions (e.g., mergers, asset sales). When we engage service providers, we require contractual protections limiting their use of personal information.

Sale and Sharing

- **Sale:** We do not sell personal information.
- **Service Providers:** We may disclose personal information to service providers for business purposes; such disclosures are not “sales” under the CCPA/CPRA when the service provider acts on our behalf under contract.

Retention and Security

We retain personal information for as long as necessary to provide services, fulfill the purposes described in this policy, comply with legal obligations, resolve disputes, and enforce agreements. We implement reasonable administrative, technical, and physical safeguards to protect personal information.

Sensitive Personal Information and Children

We minimize collection of sensitive personal information. Where we collect or process sensitive personal information, we will do so only for limited purposes (e.g., to provide a requested feature) and will provide the right to limit use and disclosure as required by CPRA.

We do not knowingly sell or share personal information of minors under 16 without affirmative authorization. If you are under 16, please obtain parental or guardian consent before using our services.

Contact, Complaints, and Enforcement

If you have questions, want to exercise your rights, or wish to file a complaint, contact us at:

- **Email:** privacy@unique.ch
- **Mail:** Unique Applications Inc. c/o Industrious | 776A 6th Avenue | 10001 New York | USA

You may also submit a complaint to the California Privacy Protection Agency.