

[• LEGAL](#)

Privacy Policy

SumizAI is built so that most of your data never reaches us. The desktop application stores your notes, your conversations and your provider key on your own machine and sends nothing to any server of ours. The website measures traffic, and only after you allow it. The older web application at app.sumizai.com does have accounts and does store notes on a server, so it is described separately and honestly below.

This policy names what exists. Where something is not settled yet, it says so instead of inventing a comfortable answer.

Last updated: 2026-08-16 **Version:** 1.2 **Operator:** 10UP Jan Śliwa, Kminkowa 26, 72-003 Bezrzecze, Poland

01 Who we are

The controller of the personal data described in this policy is:

Operator

10UP Jan Śliwa, a sole proprietorship registered in Poland (CEIDG).

Address

Kminkowa 26, 72-003 Bezrzecze, Poland.

NIP (tax identification number)

8521091009

Contact for anything in this document

contact@sumizai.com

We have not appointed a data protection officer. Write to the address above and a human — the owner of the business — reads it and answers.

Being the controller does not mean we hold everything. For the desktop application we are, in practice, the controller of nothing: your notes never arrive here. Section 04 explains why.

02 What this policy covers

Three different things carry the name SumizAI, and they have opposite data models. Mixing them up is the easiest way to misunderstand this document, so here they are side by side.

SURFACE	WHAT IT IS	WHAT WE CAN SEE
sumizai.com — this website	Static pages: marketing, blog, these documents.	Aggregated traffic measurement, and only after you consent.
The desktop application — the current product	A macOS application. No accounts, no login, no server of ours.	Nothing. It sends us no data of any kind.
app.sumizai.com — the frozen legacy web application	The earlier browser version: accounts, notes stored server-side.	Your account record, your notes and your chats, held on the server.

The desktop application is the product we build today. The web application is legacy and frozen: it receives no new features. Whether that instance is currently deployed and open to users is not something we state here — if it matters to you, ask at contact@sumizai.com and you will get a straight answer.

This policy does not cover the AI provider you choose. That relationship is yours, and it is described in section 06.

03 The website: sumizai.com

The website is static HTML. It has no accounts, no login and no forms that ask for your data. It loads exactly two third-party services, both for measurement, and both only after you have given consent in the banner:

- **Google Analytics 4** (property `G-RKZ7HS09BS`) — which pages were opened, roughly where in the world the visit came from, which site sent you here, which device and browser family was used. It is aggregated traffic measurement; it does not tell us who you are.
- **Microsoft Clarity** (project `y23mz3osxm`) — anonymised session replay: pointer movement, clicks, scrolling and how the page was laid out. It is a reconstruction of a page, not a video of your screen, and we attach no identifier of our own to it. We use it to find out which parts of a page confuse people.

There is nothing else. No advertising pixels, no remarketing tags, no chat widget, no newsletter tracker, no fingerprinting service.

Before you consent: measurement without storage

Both scripts load on every page, including before you answer the banner. Until you accept, they run in what Google calls *Consent Mode advanced* and Microsoft calls *cookieless mode*: they record that a page was opened, and they store **nothing at all on your device** — no cookie, no local storage, no session storage, no identifier that survives the page. Each page view is counted on its own and cannot be joined to your previous or next one. The legal basis for this cookieless measurement is our legitimate interest in knowing which pages are read, Article 6(1)(f) GDPR; because nothing is stored on or read from your device, art. 398 of the Electronic Communications Law does not require consent for it. You can object to it at any time by writing to us.

After you consent

Accepting switches on the cookies listed in the [Cookie policy](#) and starts session replay, on the basis of your consent, Article 6(1)(a) GDPR. Your choice is written to one entry in your browser's local storage — that entry is not a cookie and is the only thing the site stores without asking, because there is no other way to remember that you said no. You can change or withdraw the choice at any time through the *Cookie settings* link in the footer; withdrawal deletes the cookies already set and returns both tools to cookieless mode.

IP addresses

Any request to any web server, including this one, carries your IP address — that is how the internet returns the page to you. In the analytics reports we look at, no IP address is visible to us and we cannot single you out by one. Google and Microsoft handle the address inside their own services under their own privacy terms ([Google](https://policies.google.com/privacy) (<https://policies.google.com/privacy>), [Microsoft](https://privacy.microsoft.com/privacystatement) (<https://privacy.microsoft.com/privacystatement>)). We do not build profiles, we do not enrich this data with anything else, and we do not sell it.

Where the site is hosted

The website runs on our own server at **Hetzner Online GmbH**, Industriestrasse 25, 91710 Gunzenhausen, Germany. The machine sits in Hetzner's Falkenstein (FSN1) location, in Germany, inside the EU. Hetzner is our hosting provider: it runs the machine for us and gets no data for any purpose of its own. Serving this website therefore involves no transfer outside the European Economic Area. We claim no certification for Hetzner, and we state no backup schedule and no log retention period for that machine, because neither is settled.

This covers the website and the mailbox below. It says nothing about where the legacy web application at app.sumizai.com is deployed — that is a separate question, and section 08 answers it as honestly as we can today.

When you write to us

The address contact@sumizai.com is a mailbox we run ourselves — Postfix, Dovecot and OpenDKIM on that same Hetzner machine in Germany. **There is no e-mail provider in between.** Your message, the address it came from and anything you put in it sit on our own server in the EU, and Hetzner as the host of the machine is the only other party involved.

We are the controller of what you write to us. The basis is Article 6(1)(b) GDPR where the message concerns your use of the service, and otherwise Article 6(1)(f) — our legitimate interest in answering people who write to us. How long a message is kept is in section 10. This is a separate matter from the products themselves: **neither application sends any e-mail at all** — no verification message, no password reset.

The individual cookies and storage entries are listed in the [Cookie policy](#).

04 The desktop application: nothing reaches us

This is the important section, and it is short because the truth is short: **the desktop application sends us no data.** There is no account, no login, no sign-up, no sync, no server of ours anywhere in the picture. The local user row inside the application is a fixed placeholder — the identifier `00000000-...-0001` with the address `local@sumizai.app`, which is a stand-in, not a mailbox, and is never sent anywhere.

Where your data lives

The database

A single SQLite file at `~/Library/Application Support/app.sumizai.desktop/sumizai.db`. It holds your vaults, the table of contents, the note bodies, the original question-and-answer text, your conversations and messages, a **mask of your AI key** (enough to show which key is configured — never the key itself), model usage counters and a local change log.

The notes

Plain Markdown `.md` files in a folder you pick yourself, by default `~/SumizAI/<vault-slug>/`. They are ordinary files: open them in any editor, copy them, back them up, put them in your own Git repository.

The provider key

In your operating system's keychain, under the service name `app.sumizai.desktop`. Never in the database, never in the notes folder, never in a configuration file.

What the application does not do

- **No telemetry, no analytics, no crash reporting.** Verified by an exhaustive search of the dependencies and of every outbound URL in the build.

- **No cookies.**
- **No auto-updater.** The application does not call home to check for versions.
- **No synchronisation between devices.** None exists. A laptop and another machine would simply be two separate sets of notes; the local change log talks to no server at all.

The only outbound network destinations in the entire desktop application are the AI provider endpoints listed in section 06 — and those calls go from your machine directly to the provider you chose, never through us. We cannot see that traffic, and we cannot read your notes.

Deleting everything

Remove the application, delete the SQLite file, delete your notes folder and remove the keychain entry. That is all of it. There is nothing on our side to request the deletion of, because there was never anything on our side.

Your content is never training data

We do not use anything you write, ask, paste or import to train any model — ours or anyone else's. There is no training pipeline here to feed. In the desktop application we could not do it even if we wanted to, because your notes and your conversations never reach our servers. What the AI provider whose key you pasted does with what you send it is governed by your agreement with that provider; see [AI providers and what is actually sent](#), and check the setting on your own provider account.

05 The legacy web application: app.sumizai.com

The browser version came first and is now frozen. Where it is used, we do hold your data, so here is precisely what that means.

Your account

An account is an e-mail address and a password, or a sign-in with Google or Apple over OIDC. Stored for each user: the internal id, the e-mail address, the password hash (BCrypt; a password has to be at least eight characters long, and the hash is empty for accounts that only ever signed in with Google or Apple), the creation and update timestamps, the interface language, and — for social sign-in — the provider name and the subject identifier that provider gave you. **There is no column for a name, an avatar or a phone number**, so we do not have those.

Two consequences worth stating plainly, because they are unusual:

- **There is no e-mail verification and no password reset**, because the product sends no e-mail at all — there is no SMTP and no mail provider anywhere in it. (Our own contact mailbox is a different thing; section 03 describes it.) There is therefore no automated way to recover a lost

password; if that happens, write to contact@sumizai.com from the account's own address and we will tell you what can be done.

- Five failed sign-in attempts pause the account for fifteen minutes. That is a brute-force defence, not a punishment.

Your content

Notes are Markdown files in object storage, under the path `<user-id>/<vault-id>/notes/*.md`, with bucket versioning switched on — so an overwritten note leaves an earlier version behind. The database is the index over those files and also stores your chats. You can export a vault as a ZIP, a PDF or a PowerPoint file.

What the server sees

Unlike the desktop application, here the *server* calls the AI provider on your behalf. It decrypts your provider key for each request (the key is stored encrypted with AES-256-GCM and is never returned to the browser in full) and sends the request onward. So in this product the content of the request passes through our infrastructure.

Server logs carry a request and trace identifier and mask secrets. **We have not fixed a retention period for those logs**, and we will not print a number here that we do not actually enforce — see section 10.

Deleting a web-application account

Being blunt: **there is no self-service delete button**. The database schema cascades correctly, but only a manual operation triggers it. Deletion is therefore handled on request — write to contact@sumizai.com from the account's e-mail address and the account, its notes and its chats are removed. Your right under Article 17 GDPR is not weakened by the missing button; it is simply exercised by e-mail.

There are **no automated backups** of this system. Object-storage versioning is the only redundancy that exists. Treat your own export as your backup.

06 AI providers and what is actually sent

SumizAI has no AI capability of its own. You bring your own key, to a provider you choose, and the application talks to that provider on your behalf. In the desktop application the call leaves your device and goes straight to the provider; we are not in the path and cannot see it.

PROVIDER	DEFAULT ENDPOINT	KEY
Anthropic	<code>api.anthropic.com</code>	yours

PROVIDER	DEFAULT ENDPOINT	KEY
OpenAI	api.openai.com/v1	yours
Gemini	generativelanguage.googleapis.com/v1beta/openai	yours
Groq	api.groq.com/openai/v1	yours
OpenRouter	openrouter.ai/api/v1	yours
Ollama	127.0.0.1:11434/v1	none — the model runs on your own machine
Custom	any OpenAI-compatible base URL you enter	whatever that service requires

More than your question leaves the machine

This deserves a clear warning, because it is the one thing people assume wrongly. The prompt is not only what you typed. To answer in the context of your vault, the application assembles a system prompt from the vault itself:

- the **table of contents** of the vault, and
- the **full text of at most five notes** judged most relevant, inside a budget of **24 000 characters**.

The application shows you which notes it used. Afterwards, the full question-and-answer text is sent again — to draft the note, to decide where it belongs in the table of contents, and to judge whether it duplicates a note you already have.

The practical rule: **a note you would not want a third party to read does not belong in a vault you query with a hosted model**. If that is your situation, run a local model through Ollama — then nothing leaves the machine at all.

Whose relationship it is

The provider whose key you pasted is *your* counterparty. Whether it stores your prompts, for how long, and whether it trains on them is governed by the terms of the account that key belongs to — not by us. We are not a party to that contract, we receive nothing from it, and in the desktop product we cannot even observe it. Read your provider's terms; that is the document that decides.

How the model is used inside SumizAI — that an LLM writes the titles, the summaries and the note bodies, places them in the table of contents and judges duplicates — is described in the [EU AI Act notice](#).

07 Legal bases

Every purpose below is matched to its basis under Article 6(1) GDPR. Where we hold nothing, there is no basis to state, and that is written as such.

PURPOSE	DATA	BASIS
Measuring website traffic (Google Analytics 4)	Pages viewed, referrer, approximate region, device and browser family	Article 6(1)(a) — your consent, given in the banner and withdrawable at any time
Understanding how pages are used (Microsoft Clarity)	Anonymised replay of pointer, click and scroll events	Article 6(1)(a) — your consent
Remembering your consent decision	One local-storage entry recording what you chose and when	Article 6(1)(c) with Article 7(1) — we have to be able to show that consent was given
Running an account on the legacy web application	E-mail, password hash or OIDC subject id, language, timestamps, your notes and chats	Article 6(1)(b) — performing the contract you asked for
Keeping that application secure	Sign-in throttling counters, server logs with request and trace ids	Article 6(1)(f) — our legitimate interest in a service that is not trivially broken into
Answering your e-mail	The message and the address it came from	Article 6(1)(b) if it concerns your use of the service, otherwise Article 6(1)(f) — replying to people who write to us
Accounting, where an invoice is issued	The billing details on that invoice	Article 6(1)(c) — Polish tax and accounting law
Using the desktop application	None reaches us	No processing by us, therefore no basis to claim

Where we rely on legitimate interest you may object under Article 21 GDPR, and we will stop unless there is a compelling reason not to. Where we rely on consent you may withdraw it at any time, with no effect on what was lawful before the withdrawal.

Do you have to give us anything?

No statute obliges you to give us any of this. The website works whether or not you accept analytics; declining costs you nothing. For the legacy web application an e-mail address and a password, or a sign-in with Google or Apple, are a *contractual* requirement — an account cannot exist without them — and the only consequence of not providing them is that you cannot use that application. The desktop application asks for nothing at all, because it sends us nothing at all.

08 Who else sees the data

The honest and short list:

- **Google and Microsoft** — as the two analytics services, on this website only and only after your consent. Neither the desktop application nor the legacy web application contains any analytics, so nothing from them is measured. Google can also appear in two unrelated roles, both covered below: as the AI provider, if you choose Gemini, and as a sign-in provider in the legacy web application.
- **The AI provider you chose** — receives the prompt described in section 06. In the desktop application it receives it directly from your device; in the legacy web application our server forwards it. Ollama running on your own machine receives it without any network leaving the machine.
- **Google or Apple** — only if you sign in to the legacy web application with one of them, and only the sign-in exchange itself. Their scripts load on the sign-in screen alone, and only if that option is configured at all.
- **Hetzner Online GmbH** — our hosting provider. This website and the contact@sumizai.com mailbox run on a machine we rent from Hetzner Online GmbH, Industriestrasse 25, 91710 Gunzenhausen, Germany, in its Falkenstein (FSN1) location in Germany. Hetzner runs the machine; it sees what the host of a machine sees and receives nothing for any purpose of its own. There is no separate e-mail provider — the mailbox is on that same server.
- **Hosting of the legacy web application** — where app.sumizai.com is deployed is a different question, and we are not naming a company for it until we can state it accurately. Ask at contact@sumizai.com and we will tell you what is in place; this section will be updated when it is settled.
- **Public authorities** — if a lawful, binding demand requires it.

That is the whole list. There is no advertising network, no data broker, no marketing platform, no e-mail sending service, no CRM. We do not sell personal data and we do not share it for anyone else's advertising.

Where we use a service that processes data on our behalf for the legacy web application, the terms of that processing are described in the [Data Processing Agreement](#).

09 Transfers outside the EEA

We are established in Poland and we do not export data on our own initiative. Transfers happen in two places, and both are worth understanding.

Hosting is not one of them. This website and our contact mailbox run on a machine at Hetzner Online GmbH in Falkenstein, Germany — inside the EU. Serving the site and holding the mail you send us involves no transfer outside the European Economic Area. Where the legacy web application is deployed is not confirmed, so we state nothing about it here; see section 08.

The website analytics. Google and Microsoft operate global infrastructure, and data collected by their services may be processed outside the European Economic Area. That processing runs on the safeguards those companies publish for their own services — we do not have a private arrangement with either of them beyond their standard terms. Those terms are the documents linked in section 03; if you want to see the safeguards that apply to one of these services, ask us and we will point you at the document the provider publishes. If you would rather that this did not happen at all, decline analytics in the consent banner, or withdraw consent later; the scripts then never load.

The AI provider. Most of the providers listed in section 06 operate outside the EEA. In the desktop application the transfer is made *by you*, from your own machine, under the account you hold with that provider: we are not the exporter, we are not a party, and we hold no data to transfer. In the legacy web application our server forwards the request to the provider you configured. A local Ollama at `127.0.0.1` involves no transfer of any kind, because nothing leaves your computer.

If you want zero exposure to non-EEA processing, the combination is: use the desktop application, point it at a local model, and decline analytics on this website.

10 How long anything is kept

- **Desktop application.** For as long as you keep the files. We hold no copy, so we have no period to state. You delete the files and it is over.
- **Consent record on this website.** One entry in your browser's local storage, kept until you clear it or change your choice.
- **Analytics data.** Held inside Google Analytics and Microsoft Clarity under the retention those services apply; we keep no separate copy and we cannot delete a single visitor's history from our side, because we cannot identify one. Withdrawing consent stops any further collection.
- **Legacy web application — account, notes and chats.** Kept while the account exists, and removed when you ask us to delete it, as described in section 05. Object-storage versioning may retain earlier versions of a note file until the whole account is removed.

- **Server logs of the legacy web application. No retention period has been fixed** for these, and we are not going to state one we do not enforce. When it is set, this section changes and the document version changes with it.
- **E-mail you send us.** Held in the mailbox on our own server, for as long as needed to deal with the matter and to show what was agreed, then deleted.
- **Invoices, where issued.** For the period Polish tax and accounting law requires.

11 Your rights

Under the GDPR you have the right to:

- **access** your data and get a copy (Article 15);
- **rectify** anything inaccurate (Article 16);
- **erasure** (Article 17) — for the legacy web application this is done by e-mail, because there is no delete button; see section 05;
- **restriction** of processing (Article 18);
- **portability** of data you gave us, in a machine-readable form (Article 20) — in practice your notes are already portable: Markdown files on the desktop, a ZIP export in the web application;
- **object** to processing based on legitimate interest (Article 21);
- not to be subject to a decision based solely on automated processing that produces legal effects for you (Article 22) — we make no such decisions;
- **withdraw consent** at any time (Article 7(3)) — the *Cookie settings* link in the footer does exactly that.

Write to contact@sumizai.com. We answer without undue delay and in any case within one month; if a request is genuinely complex we will tell you why we need longer. For the legacy web application, please write from the account's own e-mail address — it is the only way we can tell that the request is yours, since we hold no other identifying data.

A note on the desktop application: there is very little for us to do there. We hold no copy of your notes, so a request for access or erasure addressed to us would return nothing. The data is on your machine, under your control. If the question is about what an AI provider stored when it answered you, that request goes to the provider whose key you used.

Complaint to the supervisory authority

If you think we handled your data badly, you can complain to the Polish supervisory authority:

Authority

Prezes Urzędu Ochrony Danych Osobowych (President of the Personal Data Protection Office)

Address

ul. Stawki 2, 00-193 Warszawa, Poland

Website

uodo.gov.pl (<https://uodo.gov.pl>)

You may also complain to the authority of the EU country where you live or work. These rights belong to you as a natural person whether you use SumizAI privately or in a business, and they exist independently of the consumer rights described in the [Terms of Service](#) and the [Refunds policy](#).

12 Security

What is actually implemented, without adjectives:

- **Desktop application** — your provider key is stored in the operating-system keychain under the service `app.sumizai.desktop`, not in the database and not in the notes folder. Only the mask of the key is kept in the database, so the interface can show which key is set. The remaining protection is your own device: disk encryption, a screen lock, and who else can use the machine.
- **Legacy web application** — passwords hashed with BCrypt (minimum eight characters); provider keys encrypted at rest with AES-256-GCM and decrypted only for the duration of a request; the session cookie `SUMIZAI_SESSION` is httpOnly with SameSite=Lax; a separate `XSRF-TOKEN` cookie protects against cross-site request forgery and is readable by scripts by design, because that is how the token is echoed back; five failed sign-ins pause an account for fifteen minutes; secrets are masked in server logs.

We claim no certification. There is no ISO or SOC audit behind this service, and we are not going to imply one. That includes our hosting provider: Hetzner runs the machine the website and our mailbox sit on, and we make no claim about any certification it may or may not hold. There are also **no automated backups** of the legacy web application — object-storage versioning is the only redundancy — which is one more reason to keep your own export.

If you find a security problem, write to contact@sumizai.com with enough detail to reproduce it. You will get a reply.

13 Children

SumizAI is not aimed at children and is not designed for them. We do not knowingly process the data of anyone under 16, and the website asks for no data that would let us know an age in the first place.

If you are a parent or guardian and believe a child's data ended up in the legacy web application, write to contact@sumizai.com and we will delete the account. On the desktop application there is nothing for us to delete: the data is on the device, and removing the application, the database file, the notes folder and the keychain entry removes it entirely.

14 Changes to this policy

This document carries a version number and a date, both shown at the top of the page. When something changes we raise the version and the date; we do not edit history silently.

Several statements here are open on purpose — where the legacy web application is deployed, how long its logs are kept, and whether it is still open to users. When those are settled, the relevant sections get a value instead of an explanation, and the version changes. If a change materially reduces your protection and we hold an address for you, we will tell you before it takes effect.

Continuing to use the website or the applications after a change means the new version applies. If you disagree with it, the desktop application is entirely yours — stop using our website, keep your files.

15 Contact

One address for everything in this document — privacy questions, access and erasure requests, security reports, and corrections to anything here that turns out to be wrong:

E-mail

contact@sumizai.com

Postal address

10UP Jan Śliwa, Kminkowa 26, 72-003 Bezzecze, Poland

NIP

8521091009

We publish no telephone number. Write, and a human answers.