SumizAI .com Your Second Brain, Powered by Intelligence.

https://sumizai.com/legal/dpa.html

LEGAL

Data Processing Agreement

This agreement covers the one case where we actually process personal data on your behalf: the frozen legacy web application at `app.sumizai.com`. **The desktop application sends us nothing** — no account, no note, no question, no key — so there is no processing for a DPA to govern there. Read the first section before you ask us to sign anything.

Last updated: 2026-08-14 **Version:** 1.0 **Operator:** 10UP Jan Śliwa, Kminkowa 26, 72-003 Bezrzecze, Poland

01 When this DPA applies (and when it does not)

Three different things are called SumizAI. Only one of them puts us in the role of a processor. This matters more than anything else in this document, so it comes first.

The desktop application — this DPA does not apply

> The desktop application has no accounts, no login and no server of ours. The database lives at `~/Library/Application Support/app.sumizai.desktop/sumizai.db`, the notes are `.md` files in a folder you choose, and your AI provider key sits in the operating-system keychain. Calls to the AI provider go straight from your device to the provider you picked; they do not pass through any SumizAI server. There is no telemetry, no analytics, no crash reporting and no auto-updater. We therefore receive no personal data of yours and process none. Signing a data processing agreement for the desktop product would describe a relationship that does not exist.

The website `sumizai.com` — this DPA does not apply

> On the marketing website we run Google Analytics 4 and Microsoft Clarity, and only after you consent. There we are the *controller*, not your processor, so the relationship is governed by the Privacy Policy and the Cookie policy, not by this agreement.

The legacy web application `app.sumizai.com` — this DPA applies

> The older web application keeps accounts in a database and note files in object storage on a server we operate, and it calls the AI provider on your behalf using the key you supplied. That is

> processing of personal data on your instruction. Everything below is about that application and nothing else.

The web application is frozen: it is not the product we develop. This document does not assert that the instance is currently deployed and open to users — if you have no account there, this agreement has no subject matter, and you do not need it.

02 Definitions and precedence

- **GDPR** — Regulation (EU) 2016/679.
- **Operator**, **we** — 10UP Jan Śliwa, Kminkowa 26, 72-003 Bezrzecze, Poland, NIP 8521091009, contact contact@sumizai.com.
- **Customer**, **you** — the person or organisation holding an account in the web application and instructing us through its use.
- **The web application** — the software served at `app.sumizai.com`.
- **Customer content** — the notes, source questions and answers, conversations and vault structure you create in the web application, plus whatever personal data you choose to write inside them.
- **Sub-processor** — a third party we engage to process personal data covered by this agreement *on our behalf*. The first table of Annex 3 lists them; the second table of that annex lists third parties that are expressly not sub-processors.

This DPA forms part of the Terms of Service. Where the two disagree on a data-protection question, this DPA wins. Where this DPA and the GDPR appear to disagree, the GDPR wins and the conflicting sentence here is to be read as void, not as an excuse.

03 Roles of the parties

You are the controller of the account data and customer content in the web application. You decide what goes into a note. **We are the processor** and act on your instructions.

If you are yourself a processor for someone else, you are engaging us as a sub-processor and this agreement applies with the words *controller* and *processor* read one step along the chain. You confirm in that case that you have the authority to do so.

What you are responsible for

As controller you decide why and how the data is processed, and that part stays with you. In particular you are responsible for having a lawful basis for the personal data you put into the web application, for the accuracy and relevance of that data, for informing the data subjects and answering them, and for any notification to a supervisory authority or to data subjects after a breach. Because the security measures in Annex 2 are not designed for it, you should not enter

special categories of personal data (Article 9 GDPR) or data on criminal convictions (Article 10) into the application. You also choose the AI provider, and by choosing it you decide that your content may be sent to it.

We act as an **independent controller**, not as your processor, for a narrow set of our own purposes: correspondence you send to contact@sumizai.com and records we must keep under Polish accounting and tax law. That mailbox is our own: it runs on our own server in Germany (Postfix and Dovecot), so no e-mail provider holds what you write to us. Server logs are kept both as part of running the service for you and for our own security, so we treat them under this agreement and handle them in the way the Privacy Policy describes.

The AI provider is your relationship, not ours. The application has no AI access of its own — you choose one of the supported providers and supply your own key. When the web application sends your content to that provider, it does so because you configured it to. Whether the provider trains on that content is governed by the terms of the account whose key you pasted. We are not a party to that agreement and cannot change it.

04 Subject matter, duration and instructions

Subject matter. Hosting and operating the web application: storing your account record and your vaults, indexing them, and passing your content to the AI provider you selected so that the application can draft notes, place them in the table of contents and check for duplicates.

Duration. For as long as you hold an account and we hold your data, and afterwards only for the short period needed to complete a deletion or an export you asked for, or for as long as a law obliges us to keep a particular record.

Instructions. Your documented instructions are: this agreement, the Terms of Service, the settings you configure in the application (including which AI provider you select), and anything else you send us in writing to contact@sumizai.com. We process personal data only on those instructions, including on transfers, unless EU or Polish law requires otherwise — in which case we tell you before processing, unless that same law forbids the notice.

If we consider an instruction to infringe the GDPR or Polish data-protection law, we say so and may suspend that instruction until it is resolved.

Annex 1 sets out the categories of data subjects and personal data in full.

05 Our obligations as processor

Confidentiality

Every person authorised to process personal data under this agreement is bound to confidentiality, either by contract or by a statutory duty. We are a sole proprietorship, so the circle of people with access is small by construction, and access is limited to what operating and

supporting the service requires.

Security

We apply the technical and organisational measures listed in **Annex 2**. That annex lists what actually exists in the code, and it also states plainly what does not — most importantly that **no automated backups exist**. Please read it before deciding what to store in the web application.

Assistance with data-subject requests

We help you answer requests under Articles 15 to 22 GDPR, taking into account the nature of the processing. In practice:

- **Access and portability** — the application exports a vault as a ZIP, and also as PDF and PowerPoint. Account fields we supply on request.
- **Erasure — the web application has no self-service account-deletion endpoint.** The database schema cascades correctly, but only a manual operation triggers it. Write to contact@sumizai.com and we perform the deletion and confirm in writing.
- **Rectification and restriction** — likewise handled manually on a written request.
- The product sends no e-mail of any kind: there is no mail sending anywhere in it, no verification mail and no password reset. Everything of this sort travels through contact@sumizai.com, from a person.

Assistance with Articles 32 to 36

We assist you, taking into account the nature of processing and the information available to us, with security of processing, breach notification and communication to data subjects, data protection impact assessments and prior consultation with the supervisory authority. Concretely that means answering your questions in writing and supplying the facts in Annex 1 and Annex 2. We do not hold an audit report or a certification to hand you instead.

Records

We maintain a record of the categories of processing carried out on your behalf, as required by Article 30(2) GDPR, and make it available to you or to a supervisory authority on request.

Deletion or return

At the end of the processing you choose deletion or return; see the term and termination section below.

06 Sub-processors

You give a **general written authorisation** for us to engage the sub-processors listed in the first table of **Annex 3**, on the conditions in this section.

Read that annex carefully, because it also names third parties that are **not** our sub-processors: Sign in with Google, Sign in with Apple and the AI provider you selected. We do not engage them on your behalf — the sign-in providers act on their own account when a user chooses that route, and the AI provider is a relationship between you and that provider, opened with the key you supplied. The commitments in this section, including our full liability for a sub-processor, apply to the sub-processors we engage; we cannot honestly extend them to parties whose terms we neither set nor sign.

- Any sub-processor is bound by data-protection obligations no weaker than those in this agreement.
- We remain **fully liable to you** for a sub-processor's performance of those obligations.
- Before we add or replace a sub-processor we give you **at least 30 days' notice**. Notice is sent by a person from contact@sumizai.com to the e-mail address on your account, and Annex 3 is updated with a new version number and date on this page. The product itself sends no e-mail, so do not wait for an automated message.
- Within those 30 days you may **object on reasonable data-protection grounds**. We will try to resolve the objection; if we cannot, you may stop using the affected part of the service and terminate it, and we will delete or return your data as described below.

Annex 3 is short. It names **Hetzner Online GmbH**, in Falkenstein, Germany, as the provider of the machines we operate on, and it says just as plainly what it does not settle: whether the legacy web application is deployed on that machine. The hosting of that instance therefore keeps a row of its own, still without a company name; we confirm it in writing on request, rather than print here something we have not verified. There is no mail provider on the list either — the mailbox is on our own machine.

07 International transfers

The infrastructure we run ourselves includes a Hetzner Cloud machine: **Hetzner Online GmbH**, Industriestrasse 25, 91710 Gunzenhausen, Germany, in Hetzner's **Falkenstein (FSN1)** location in Germany. The `sumizai.com` website and the `contact@sumizai.com` mailbox are served from that machine. Germany is in the EU and therefore in the European Economic Area, so that hosting is not a transfer to a third country and needs no Chapter V mechanism for it.

What we do not assert here is that the legacy web application runs on it. Whether that instance is deployed at all, and on which server, is not something this document states. Ask us in writing at contact@sumizai.com and you get the provider, the country and the transfer basis for that instance, before you rely on it.

We undertake that we will not transfer personal data covered by this agreement outside the European Economic Area, or engage a sub-processor that does, unless the transfer is covered by a mechanism in Chapter V GDPR — an adequacy decision, or the Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914) with any supplementary measures a transfer impact assessment shows to be necessary.

Two transfers are not ours to arrange, and we do not restate someone else's terms as if they were our commitments:

- **Sign in with Google and Sign in with Apple** — used only if a user chooses that route on the sign-in screen, and only when the corresponding client id is configured. The applicable terms and transfer mechanism are the provider's own.
- **The AI provider you selected** — you chose it and supplied its key, so the transfer to it happens under the terms of your account with that provider. If you run a local Ollama at `127.0.0.1`, there is no transfer at all: the content never leaves the machine.

08 Audits and information

On written request we give you the information needed to demonstrate compliance with Article 28 GDPR. Ask at contact@sumizai.com.

We hold **no ISO 27001, SOC 2 or comparable certification** and we claim none. There is no third-party audit report to send you instead of answering. If a certification is a requirement for you, say so before you rely on the web application.

You, or an auditor you mandate who is not our competitor and who is bound to confidentiality, may audit the processing:

- on at least 30 days' written notice;
- during ordinary working hours, in a way that does not disrupt the service;
- once in any 12-month period, and additionally after a personal data breach affecting you or where a supervisory authority requires it;
- without access to other customers' data, to our confidential internal information, or to anything a duty of confidentiality prevents us from showing.

You bear the cost of an audit, unless it reveals a material failure by us to meet this agreement, in which case we bear our own costs of remedying it.

09 Personal data breaches

If we become aware of a personal data breach affecting personal data we process for you, we notify you **without undue delay and in any event within 72 hours** of becoming aware. The notice comes from a person at contact@sumizai.com, sent to the e-mail address on your account.

The notice describes, as far as we know it at the time:

- the nature of the breach, including the categories and approximate number of data subjects and records concerned;
- the likely consequences;
- the measures taken or proposed to address it and to mitigate its effects;
- a contact point for further information.

If we cannot give all of that at once, we send what we have and follow up in stages, without further undue delay.

Notifying the supervisory authority under Article 33 and the data subjects under Article 34 is your duty as controller, not ours. We assist you with it and supply the facts we hold.

One honest limitation: server logs carry a request and trace identifier and mask secrets, but **the log retention period is not yet fixed**. How far back an incident can be reconstructed therefore depends on what is still in the logs. We will state the retention period here once it is set, and you may ask for the current position at any time.

10 Liability

This agreement does not change how liability is allocated in the Terms of Service; it sits inside them.

Article 82 GDPR applies as written: each party answers for the damage it causes by its own infringement, a processor answers where it acted outside or against lawful instructions, and a party that has paid full compensation may claim back the share attributable to the other. Nothing in this document limits or excludes that.

Nothing here limits liability for damage caused intentionally, for personal injury, or in any other case where Polish law forbids a limitation. **Consumers, and sole traders who conclude a contract not of a professional character for them (przedsiębiorcy na prawach konsumenta), keep every right the law gives them**; no sentence in this agreement is to be read as taking such a right away.

This document states what we do. It is not legal advice about your own obligations as controller.

11 Term, termination, deletion or return

This DPA takes effect when you start using the web application under the Terms of Service and lasts as long as we process personal data on your behalf. Provisions that by their nature should survive — confidentiality, liability, and the deletion obligations below — survive its end.

At the end of the processing you choose:

1. **Return** — export your vaults from the application as a ZIP, PDF or PowerPoint file before your account is deleted; or
2. **Deletion** — we delete the data. Because there is no self-service deletion endpoint, this is a manual operation: write to contact@sumizai.com, we perform it and confirm in writing when it is done.

Two details you should know, because they change what "deleted" means:

- Note files sit in an object-storage bucket with **versioning enabled**. Deleting an object leaves earlier versions behind until those versions are purged, so deletion on request includes purging the versions of the deleted objects.
- Where Polish law requires us to keep a specific record — accounting and tax documents, for example — we keep only that record, only for the period the law requires, and only for that purpose.

12 Governing law, contact and changes

This agreement is governed by Polish law and by directly applicable EU law, in particular the GDPR. Statutory consumer protections that apply regardless of a choice of law are unaffected. The Polish supervisory authority is the President of the Personal Data Protection Office (Prezes Urzędu Ochrony Danych Osobowych), and you may lodge a complaint with it or with the authority in your own country.

Operator and point of contact

- 10UP Jan Śliwa, sole proprietorship registered in Poland (CEIDG)
- Kminkowa 26, 72-003 Bezrzecze, Poland
- NIP 8521091009
- contact@sumizai.com — all data-protection matters, sub-processor objections, deletion requests, audit requests and breach questions

We have **not appointed a data protection officer** and are not required to. There is no separate DPO address to write to: the address above reaches the person who answers. We have no establishment outside the European Union, so no Article 27 representative is required either.

Accepting the Terms of Service accepts this DPA for the web application. If you need it as a separate signed document, write to us and we will provide one with the same wording.

We change this document by publishing a new version with a new version number and date at the top of this page. Changes that reduce your protection or add a sub-processor are announced in advance as described in the sub-processor section.

13 Annex 1 — Description of the processing

This annex describes the processing in the web application at `app.sumizai.com`. It does not describe the desktop application, where we process nothing.

ITEM	DESCRIPTION
Subject matter	Operating the web application: accounts, storage of vaults and notes, and calls to the AI provider the customer selected.
Nature and purpose	Storage, indexing, retrieval, display, export, and transmission to the customer's chosen AI provider so that a note can be drafted, placed in the table of contents and checked against existing notes for duplication.
Duration	For the life of the account, then until a requested deletion is carried out; longer only where a law requires a specific record to be kept.
Categories of data subjects	The customer's account holders and end users, and any person the customer writes about inside a note, a question or a conversation.
Categories of personal data — account	Identifier, e-mail address, password hash (null for accounts created through Google or Apple), creation and update timestamps, interface language, and for OAuth accounts the provider name and the provider's subject id. There is no name, avatar or phone column in the schema.
Categories of personal data — content	Note files in object storage, the database index of them, the source question-and-answer text, conversations and messages, vault and table-of-contents structure, and whatever personal data the customer chooses to put inside that content.
Credentials	The customer's AI provider API key, stored encrypted and decrypted per request on the server. It is never returned to the browser in full.
Technical data	Session and CSRF cookies; server logs carrying a request or trace identifier, with secrets masked. Log retention period: not yet fixed — see the breach section.
Special categories	None are requested by the application and none are needed for it to work. The customer controls what goes into a note; the measures in Annex 2 are not designed for special-category data, so the customer should not enter it.
Frequency	Continuous, for as long as the customer uses the application.
Recipients	The parties listed in Annex 3 — our sub-processors, and the third parties the customer's own choices bring in — and nobody else.

ITEM	DESCRIPTION
What is sent to the AI provider	Not only the typed question. The system prompt is assembled from the vault: the table of contents plus the full text of at most five most relevant notes, within a 24 000-character budget. The application shows which notes it used. The full question-and-answer text is sent again to draft the note, to place it in the table of contents, and to judge whether it duplicates an existing note.

14 Annex 2 — Technical and organisational measures

These are the measures that exist in the web application, described as they are implemented. Nothing is listed here as aspiration.

MEASURE	WHAT IT ACTUALLY IS
Password storage	Passwords are hashed with BCrypt, minimum length eight characters. Accounts created through Google or Apple have no password at all.
Provider key at rest	The customer's AI provider key is encrypted with **AES-256-GCM** and decrypted per request on the server. It never returns to the browser in full.
Session cookie	`SUMIZAI_SESSION` is `httpOnly` and `SameSite=Lax`, so page scripts cannot read it and it is not sent on cross-site navigations.
CSRF protection	A separate `XSRF-TOKEN` cookie carries the cross-site-request-forgery token; it is readable by scripts by design, because the front end must echo it back on state-changing requests.
Login throttling	Five failed sign-in attempts pause the account for fifteen minutes.
Federated sign-in	Google and Apple sign-in run over OIDC, and their scripts load on the sign-in screen only, and only when the corresponding client id is configured.
Logging	Server logs carry a request and trace identifier and **mask secrets**, so keys and tokens are not written in clear text.
Object storage	Note files live under `<user-id>/<vault-id>/notes/*.md` in a bucket with **versioning enabled**, which protects against an accidental overwrite or delete until the versions are purged.
Segregation	Storage paths and database rows are keyed by user and vault, so one account's content is addressed separately from another's.
Deployment	The application runs as containers behind a reverse proxy (Caddy).

What is not in place — stated plainly

- **There are no automated backups.** Bucket versioning is not a backup: it protects an object from being overwritten, not the system from being lost. Treat the web application as a place your data lives, not as the only place it lives, and keep your own export.
- There is no e-mail verification and no password reset, because the product sends no e-mail of any kind.
- There is no self-service account deletion; deletion is a manual operation on written request.
- The **log retention period is not fixed** and no backup retention period exists to state.
- We hold **no security certification** — no ISO 27001, no SOC 2, no equivalent — and no conformity assessment of any kind.

15 Annex 3 — Sub-processors

The list is deliberately short, and it separates two things that are often mixed up: the parties *we* engage to process data for you, and the parties *your own choices* bring into the picture. Only the first table is a sub-processor list.

Sub-processors we engage

SUB-PROCESSOR	WHAT IT DOES	WHEN IT IS INVOLVED	LOCATION AND TRANSFER BASIS
Hetzner Online GmbH — our infrastructure host	Provides the machines we operate on. Industriestrasse 25, 91710 Gunzenhausen, Germany. The `sumizai.com` website and the `contact@sumizai.com` mailbox are served from a Hetzner Cloud machine that we administer ourselves.	Continuously, for whatever of ours runs on that machine.	Hetzner's **Falkenstein (FSN1)** location, Germany — the EU, and therefore the EEA. No transfer outside the EEA arises from this hosting, so no Chapter V mechanism is needed for it. We claim no certification on Hetzner's behalf.
Hosting provider of the legacy web application	Runs the servers and the object storage on which that application and the notes sit, wherever that instance is deployed.	Continuously, whenever that application is running.	**Not named in this document.** We give the provider, the country and the transfer basis in writing on request to contact@sumizai.com. We would rather leave this row open than print a company we have not confirmed.

Why the second row is still open. The first row does not say that the legacy web application runs on the Hetzner machine. Whether that instance is deployed at all, and on which server, is not settled in this document, so its hosting keeps a row of its own and we keep the honest answer:

write to contact@sumizai.com and we name the provider, the country and the transfer basis for that instance before you rely on it. What is settled either way is the undertaking in the transfers section: no personal data covered by this agreement leaves the EEA without a Chapter V mechanism.

That is the whole list. **There is no mail provider**: `contact@sumizai.com` is a mailbox we run ourselves (Postfix, Dovecot and OpenDKIM) on that same Hetzner machine, so mail you send us sits on our own EU infrastructure and reaches no processor other than Hetzner as the host. The product itself still sends no e-mail of any kind. There is no analytics or crash reporting in the application, no payment processor in the code, and no backup service, because no automated backups of the web application exist.

Third parties that are not our sub-processors

These receive data because of a choice made on your side, not because we engaged them for you. We do not promise their terms, and the sub-processor commitments above do not extend to them.

PARTY	WHAT IT DOES	WHEN IT IS INVOLVED	WHOSE RELATIONSHIP IT IS
Google	Sign in with Google (OIDC): authenticates a user and returns a provider subject id.	Only if the user chooses that route on the sign-in screen, and only when a Google client id is configured. The script loads on the sign-in screen only.	Google acts on its own account as the identity provider. Its own terms and its own transfer mechanism apply; we do not restate them here and we do not warrant them.
Apple	Sign in with Apple (OIDC): authenticates a user and returns a provider subject id.	Only if the user chooses that route on the sign-in screen, and only when an Apple client id is configured. The script loads on the sign-in screen only.	Apple acts on its own account as the identity provider. Its own terms and its own transfer mechanism apply; we do not restate them here and we do not warrant them.
The AI provider the customer selects	Generates the answer, the note text, the placement in the table of contents and the duplicate check, from the content described in Annex 1.	Whenever the customer starts a conversation. The customer chooses the provider from those the application supports and supplies that provider's key; the application has no AI access of its own. A local Ollama at `127.0.0.1` means nothing leaves the machine.	Yours. The key is from your account with that provider, so the terms of that account govern the transfer and govern whether the provider trains on the content. We are not a party to it.

Nothing outside these two tables receives personal data from the web application. The website `sumizai.com` loads Google Analytics 4 and Microsoft Clarity after consent, but that is the website and our own controller role, not processing on your behalf — see the Cookie policy. The desktop application has no sub-processors at all, because it has no server.