ZeeDo Data Processing Addendum (Article 28 GDPR)

ZeeDo

Version 3 · Zuletzt aktualisiert am 3. November 2026 · Fingerabdruck d4a2ca2d9c05

Rechtstexte werden auf Englisch veröffentlicht; maßgeblich ist der englische Text. Diese Version bleibt unverändert erhalten. Alle Versionen, jeweils mit PDF: https://zeedo.cloud/de/legal/versions/dpa

1. Parties and roles

1.1 This addendum is between the Customer (**controller)** and ZeeDo GmbH, c/o Ramzy J A Abushaaban, Elsa-Neumann-Straße 53, 13629 Berlin, Germany, registered in the commercial register of the Amtsgericht Charlottenburg under HRB 292967 B and represented by its managing director, Ramzy J A Abushaaban (**processor, "ZeeDo").** It forms part of the ZeeDo Terms of Service (the "**Terms")** and is concluded in electronic form when the Customer accepts the Terms (Article 28 (9) GDPR). The email in which ZeeDo will confirm the contract will name the version of this addendum in force, give the address at which that version is kept and attach it as a PDF.

1.2 ZeeDo processes Customer Personal Data only as the Customer's processor. For its own account, billing, security and abuse data, ZeeDo is a controller; the Privacy Policy describes that processing.

1.3 "**Customer Personal Data"** means personal data in Customer Content that ZeeDo processes on the Customer's behalf. Other capitalised terms have the meaning the Terms give them.

2. Instructions

2.1 ZeeDo processes Customer Personal Data only on the Customer's documented instructions, unless EU or member-state law requires otherwise. In that case, ZeeDo tells the Customer first, unless the law forbids it.

2.2 **The Customer's instructions** are:

- the Terms and this addendum;
- the configuration of the Customer's organisation, workspaces and bots, including goals, briefs, constraints, connections, credentials, policies, approvals, standing approvals and memory-retention settings; and
- actions Members take in the product or through the API.

2.3 **Bots.** Under the agency model (Terms, section 3), a bot acts on the Customer's instructions. What a bot does within the authority the Customer configured, including an action induced by third-party content within the scope of the tools, connections, credentials and standing approvals the Customer granted that no enforced control was documented to stop (Terms, sections 3.4 and 3.5), is processing on the Customer's instructions. This does not limit ZeeDo's obligations under sections 4 and 9 and Annex 2.

2.4 ZeeDo tells the Customer immediately if, in ZeeDo's opinion, an instruction infringes data-protection law, and may hold off following that instruction until the Customer confirms or changes it. This does not oblige ZeeDo to check the lawfulness of the Customer's processing.

2.5 **The Customer's responsibilities as controller.** The Customer decides why and how its bots process personal data and is responsible for the lawfulness of that processing. In particular, the Customer:

- gives only instructions that comply with the law;
- has a lawful basis for what its bots process, including any special categories of personal data (Article 9 GDPR) and data about criminal convictions and offences (Article 10 GDPR), and gives data subjects the information that Articles 13 and 14 GDPR require;
- decides whether a data-protection impact assessment is needed and carries it out (ZeeDo assists under section 8);
- answers data-subject requests, using the tools in section 7; and
- does not direct its bots to process personal data that it has no right to process.

3. Confidentiality

ZeeDo ensures that everyone it authorises to process Customer Personal Data is bound to confidentiality, by contract or by law. Access to ZeeDo's production systems is limited to the persons ZeeDo authorises for operating the service. ZeeDo will introduce staff access to production systems that is time-limited, approved by a second person and recorded in the Customer's audit log.

4. Security

4.1 ZeeDo implements the technical and organisational measures in Annex 2. A measure that section 3 or Annex 2 describes in the future tense is one ZeeDo does not take yet, and the Customer cannot require it before ZeeDo introduces it.

4.2 ZeeDo may update Annex 2 as technology develops. An update will not reduce the overall level of protection that Annex 2 describes; a reduction would be a change of this addendum under section 23 of the Terms.

4.3 The Customer is responsible for the security of what it controls: its Members' accounts and sign-in methods, the roles it assigns, its API keys, the credentials, connections and standing approvals it grants, and its own systems.

5. Sub-processors

5.1 The Customer gives ZeeDo general written authorisation to engage the sub-processors listed in Annex 3, and to add or replace sub-processors under 5.3.

5.2 ZeeDo publishes the list at https://zeedo.cloud/legal/subprocessors, with each sub-processor's location, and names its hosting sites, not only its vendors.

5.3 **Changes.** ZeeDo gives at least 30 days' notice, by email to the Owners and on the published list, before adding or replacing a sub-processor, including a model provider named on the list. The Customer may object on reasonable data-protection grounds before the change takes effect. If ZeeDo cannot resolve the objection, the Customer may end the affected service with effect from the change date, and ZeeDo refunds the fees paid in advance for the time after it. Where ZeeDo must replace a sub-processor at shorter notice to keep the service secure or available, it gives the notice as soon as it can and before the new sub-processor processes Customer Personal Data, and the Customer's rights under this section run from that notice. Changing the model that ZeeDo's model uses at a provider already on the list is not a change of sub-processor; section 13.3 of the Terms applies to it. Removing a sub-processor needs no notice.

5.4 ZeeDo engages each sub-processor under a written contract that imposes data-protection obligations equivalent to those in this addendum, and remains responsible to the Customer for their performance.

5.5 **Model providers.** Where the Customer uses its own model-provider key (BYOK), the provider is the Customer's own processor, engaged by the Customer, and not ZeeDo's sub-processor. ZeeDo's model is the default for every workspace on every plan, Free included, unless a bot or its workspace uses the Customer's own key (BYOK) or an Owner or Admin has switched ZeeDo's model off for the workspace. Its requests go to OpenRouter and to the model provider named for each model on the sub-processor list: each model is served by one named provider. Every request is restricted to providers that keep no copy of prompts or responses (zero data retention) and do not train on them, and ZeeDo sets this restriction on each request itself. For an organisation of ZeeDo's EU region, requests go only through OpenRouter's EU endpoint and are processed in the EU; a request that cannot be served there fails and is not sent elsewhere. For an organisation of another region, requests go through the endpoint ZeeDo names for that region. OpenRouter and those providers are ZeeDo's sub-processors. Two uses are served from the United States, by a decision model run by Perplexity and reached through OpenRouter; the same restriction applies to both, so the provider keeps no copy and does not train on what it receives. (a) Reading rules: when a person types a message that sets or changes a rule for a bot (with words such as "never", "always" or "from now on"), the typed text of that message and the words of the rules it concerns are sent, to tell whether it is a standing rule; so is the start of a request to a bot whose rules do not all fit in front of it. For this reading, what a person pastes, and anything a bot read, are not sent. (b) Checking a press: before a bot presses a button or another control that ZeeDo's own signals show could pay, order, sign, file, send, publish, delete or change an account, ZeeDo sends the control's labels to tell what pressing it would do, so that it can stop the press or ask a person first: the control's label, the labels of its form's fields and of a dialog it answers, the currencies shown, the site's domain and the pattern of the form's address (its path, without the query: a part written only in lower-case letters a to z, hyphens and underscores is kept as written, so it can be a name, such as a user name or a page's name, and every other part is replaced by a placeholder). Field values, the page's text and its links are never sent. Inside a label, every number written in digits (a house number, a postcode, an amount, a date or a reference alike), email addresses, phone numbers, account and card numbers and web addresses written with their scheme (such as https://) or starting with www.

are replaced by a placeholder first; the other words of a label are sent as written and may name third parties, streets or places, and an amount written out in words is sent as written. Pages of the banking, tax, health and government websites the site registry marks as sensitive, of a site a workspace has marked as sensitive, and of webmail are never sent to the United States: for an organisation of ZeeDo's EU region they are checked in the EU by ZeeDo's model, or not by a model at all. ZeeDo keeps only the answer and the site's full host name, never the labels, for at most 30 days in the organisation's region. Neither use is made for a workspace on the Customer's own key. For an organisation of ZeeDo's EU region, neither goes to the United States once an Owner or Admin turns on **Keep every model check in the EU** in Settings: rules are then read by ZeeDo's model in the EU, and presses are checked by ZeeDo's model or, until that check is available, only by ZeeDo's own word lists and the signals in the page. With the setting on, ZeeDo's model makes these two checks also for a workspace on the Customer's own key, as ZeeDo's processing through its sub-processors in the EU, and never sends them to that key's provider; the Customer chooses the setting and may turn it off.

5.6 **Embeddings.** To make bot memory searchable by meaning, ZeeDo turns text into vectors (text embeddings): each episode summary and each procedure document it stores (a bot's brief is one), each line kept from a bot's chat, and each memory search. It does this for every workspace and on every plan with ZeeDo's own embedding model, which runs on ZeeDo's servers in the Customer's region (Annex 3.1 and 3.5), whatever key the Customer's bots use: no third party receives the text, and the model keeps no copy of it; the vector is stored with the item and deleted with it. To order what a memory search finds, ZeeDo's own reranking model on the same servers reads the search's words beside the texts found, and keeps no copy either. Tool search: the names and descriptions of the tools a workspace has connected (which may be the vendor's own text) and the words a bot searches its tools with are turned into vectors by ZeeDo's own embedding model, the one that embeds memory text by default, on ZeeDo's servers; the vectors are kept with the workspace's tool registry and deleted with it. The text embedded can contain personal data, including data tagged personal. An Owner or Admin may instead choose, in the workspace's Models settings, an embedding model of the Customer's own OpenAI account: from then on that workspace's memory text and searches are sent to OpenAI under the Customer's own key and terms, OpenAI is the Customer's own processor for them, as under BYOK (5.5), and not ZeeDo's sub-processor, and ZeeDo re-embeds the workspace's memory with that model. Adding a model-provider key for the Customer's bots never changes the embedding model.

6. Location and transfers

6.1 **Location.** Customer data is stored and processed in the EU (France, Germany and Ireland):

- bot machines, ZeeDo's own embedding and reranking models, the control-plane server and the primary file storage run at Scaleway in its Paris region (fr-par), France;
- a copy of the file storage is kept at OVH in Limburg, Germany;
- the database (Neon), the workflow service (Temporal Cloud), key management (AWS KMS) and transactional email (Amazon SES) run in Amazon Web Services' Frankfurt region (eu-central-1), Germany;

- the web application's functions run on Vercel in Frankfurt (fra1), Germany; and
- traces are kept by Langfuse in its EU region, in Ireland.

Annex 3 lists every sub-processor with its location.

The exceptions are those in Annex 3: requests on ZeeDo's model of an organisation outside ZeeDo's EU region; the decision model that reads the rules people set for a bot and checks the labels of a control a bot is about to press, which may be served from the United States unless an organisation of ZeeDo's EU region keeps every model check in the EU (5.5); WorkOS, which processes Members' sign-in data in the United States; the delivery of the web application's pages and responses through Vercel's global edge network, which passes them through the edge location nearest the user; and access from the United States, namely support by Langfuse's group and possible access by the companies named in 6.4. Memory text, memory searches and the descriptions of a workspace's tools are embedded and reranked on ZeeDo's own servers (5.6); where an Owner or Admin chose an embedding model of the Customer's own OpenAI account, that workspace's memory text is processed where that account processes it.

6.2 The region is set when the Customer's first workspace is created and cannot be changed by the Customer. A region move is an export and re-import carried out by support on a signed request, where a second region is offered by contract.

6.3 ZeeDo places a workspace's Machine only on a server in the organisation's region, and a server of another region refuses it.

6.4 **Transfers.** The Customer instructs ZeeDo to make the transfers that Annex 3 describes. Where a sub-processor is in a country outside the EEA, or may access Customer Personal Data from one, the transfer is made under the Standard Contractual Clauses adopted by the European Commission (Implementing Decision (EU) 2021/914), as that sub-processor's data processing terms incorporate them (for Microsoft and Perplexity, OpenRouter's data processing terms). This applies to OpenRouter, Perplexity and WorkOS, which are in the United States, and to the sub-processors that process Customer Personal Data in the EU but are, or belong to, companies in the United States that may access it from there: Amazon Web Services, Neon (part of Databricks), Temporal, Vercel, Microsoft and Grafana Labs, and Langfuse's group for its support. Where Annex 3 says that a recipient states its certification under the EU–US Data Privacy Framework, ZeeDo relies on that certification in addition. ZeeDo has assessed these transfers and the measures that support them. The Customer may ask privacy@zeedo.cloud for a copy of the safeguards.

7. Assistance with data-subject requests

7.1 ZeeDo gives the Customer tools to answer data-subject requests:

- **Erasure.** At the Customer's request, ZeeDo erases a data subject's personal data. An erasure request runs one job across the stores that hold the text of bot memory, chats, runs, cards and approvals, automations, standing approvals and connections, traces, recordings, checkpoints and the files people hand bots. Within 72 hours it permanently deletes what the identifiers given find: in bot memory the matching raw episodes, notes, facts and relations,

and the summaries that name the person; the chat lines that name them, each replaced by a marker that a line was erased; the text of the runs, cards and approvals that name them, and those runs' checkpoints and screen recordings; trace bodies; the files handed in those messages and runs; and the text of automations, standing approvals' conditions and connection account names. It then produces a report. Data the identifiers cannot find, such as a face or a name visible only in a screen recording or in a checkpoint of a run whose text never names the person, is deleted when its own period ends (14 days for recordings, 30 days for checkpoints). Deleted data leaves backups within 30 days. Audit and consent records are kept and listed in the report as retained with a reason. The job does not search the files bots made or anything else on a Machine's disk, what people wrote to set up a workspace (such as a bot's name and goal), the operational logs of the servers that run Machines, or the history of finished workflows. The report lists the files bots made in the runs concerned, for the Customer to delete. What is on a Machine's disk, and that setup text, stays until a person deletes it or the workspace is deleted; the logs and the workflow history are deleted when their periods end (Annex 4). An export archive made before the request is deleted seven days after it was written. Where a workspace keeps screen recordings longer than 14 days, the recordings the identifiers cannot find are deleted when that longer period ends. The full text of each raw memory episode is stored sealed and cannot be searched for a name, so the job deletes the full texts of all raw episodes in every workspace of the organisation; the summaries that do not name the person stay.

- **Export.** While an organisation is active, and while it is read-only until day 60 of the end-of-service clock, an Owner or Admin can export its data as one archive signed by ZeeDo. The archive is produced within 24 hours and can be downloaded for seven days. Section 18 of the Terms lists what the archive contains.
- **Access and rectification.** Through the dashboard and, on paid plans, the API. An ordinary correction to a fact in memory supersedes it and keeps the earlier fact as invalid history; a request to erase it deletes it.
- **Memory retention.** The Customer controls memory retention. Raw episodes are kept at most 90 days; summaries, facts and relations, procedures and notes people write are kept until the Customer deletes them or the workspace is deleted.

7.2 Assistance through these tools is included in the price. Other assistance with data-subject requests is provided at reasonable cost, unless the request arises from ZeeDo's breach.

7.3 If a data subject asks ZeeDo directly about Customer Personal Data, ZeeDo refers them to the Customer and passes the request on to the Customer. ZeeDo does not answer the request itself unless the Customer instructs it to.

8. Assistance with other obligations

ZeeDo provides reasonable assistance with the Customer's obligations on the security of processing, on personal-data breaches, on data-protection impact assessments and on prior consultations (Articles 32 to 36 GDPR), taking into account the nature of the processing and the information available to ZeeDo. It does so primarily through its documentation and this addendum. ZeeDo publishes information for the Customer's data-protection impact assessment

at https://zeedo.cloud/legal/dpia. Assistance beyond that is provided at reasonable cost.

9. Personal-data breaches

9.1 ZeeDo notifies the Customer of a personal-data breach affecting Customer Personal Data without undue delay, and where feasible within 48 hours of confirming it, unless an Enterprise order form sets a different period. ZeeDo sends the notice by email to the Owners.

9.2 The notice describes the breach, the data and data subjects concerned, the likely consequences and the measures taken or proposed, as far as that information is available. ZeeDo provides further information as it becomes available.

9.3 The Customer decides whether to notify its supervisory authority and the data subjects (Articles 33 and 34 GDPR). ZeeDo's notice is not an acknowledgement of fault or liability.

9.4 ZeeDo notifies a security incident that does not affect personal data only where an Enterprise order form provides for it.

10. Deletion, return and switching

10.1 **Export.** While an organisation is active, and while it is read-only until day 60 of the end-of-service clock, an Owner or Admin can export its data as one archive signed by ZeeDo, as 7.1 describes.

10.2 **End of service.** End of service is the day that section 18 of the Terms sets, for example the end of the paid period after a cancellation, or the day the subscription ends for non-payment under section 17 of the Terms. Day 0 is end of service. Days 0 to 60: the organisation is read-only; bots are paused and no new runs start; reads, exports and downloads work, and the Customer may reactivate by subscribing again. Day 60: access and export end, and ZeeDo sends a deletion notice to the Owners. Days 60 to 90: the data is held but not accessible; the Customer may still reactivate by writing to support@zeedo.cloud. Day 90: ZeeDo deletes the organisation's data from its live systems. Within 30 days after deletion: it is purged from backups.

10.3 **Switching.** The Customer may at any time ask, in text form to support@zeedo.cloud, to switch to another provider or to its own systems, or to have its data erased. Section 18 of the Terms sets how such a request proceeds: a notice period, a transitional period in which the service continues, the retrieval period of days 0 to 60 in 10.2, and erasure.

10.4 If the Customer deletes a workspace or its organisation itself, deletion starts at once and backups are purged within 30 days.

10.5 After deletion, ZeeDo keeps only data that EU or member-state law requires it to keep, such as invoices, and the audit and consent records in Annex 4, section 2. The Customer instructs ZeeDo to keep those records for their full period, also after the end of service, as the record of what its bots did and who authorised it; ZeeDo deletes them when that period ends.

10.6 **Return or deletion.** The Customer receives its data back through the export in 10.1 and, for

the files bots made, by downloading them, as section 18 of the Terms describes. ZeeDo does not return data in any other way. When the retrieval period ends, ZeeDo deletes the data as 10.2 states: by not exporting before day 60, the Customer chooses deletion over return (Article 28 (3) (g) GDPR).

11. Audits and information

11.1 ZeeDo makes available the information needed to demonstrate compliance with Article 28 GDPR, primarily this addendum, its Annexes and the published sub-processor list.

11.2 **Current evidence.** ZeeDo holds no third-party certification or attestation report. ZeeDo tests its own security as Annex 2 describes under Testing.

11.3 **Audits.** Where the Customer reasonably considers that the information in 11.1 and 11.2 is not enough to demonstrate compliance, the Customer may audit ZeeDo's compliance with this addendum itself, or appoint an independent auditor who is bound to confidentiality and is not a competitor of ZeeDo. An audit may take place once a year, with 30 days' notice in text form, during ZeeDo's business hours (Monday to Friday, 9:00 to 17:00 Berlin time, except public holidays in Berlin), and at the Customer's cost. An audit must not give access to other customers' data and must not disturb ZeeDo's operations more than necessary. ZeeDo may charge its reasonable costs for the time its staff spend on the audit, unless the audit finds a material breach of this addendum by ZeeDo. The limit of once a year does not apply to an audit that a supervisory authority requires, or to an audit after a personal-data breach at ZeeDo that affected Customer Personal Data. The sites of ZeeDo's sub-processors are audited only as their own terms allow; ZeeDo passes on, where those terms allow, the audit reports and certifications they make available to it.

12. Liability and precedence

12.1 Liability under this addendum is governed by section 20 of the Terms, including recourse between the parties under Article 82 (5) GDPR. Nothing in this addendum or the Terms limits either party's liability to a data subject under Article 82 GDPR. Except in the cases of section 20.1 of the Terms, each party bears any fine imposed on it.

12.2 If this addendum conflicts with the Terms on data protection, this addendum prevails. An Enterprise order form prevails over this addendum only where it says so expressly.

12.3 ZeeDo changes this addendum only as section 23 of the Terms provides.

Annex 1 — Details of processing (Article 28 (3) GDPR)

Item	Description
Subject matter	Providing the ZeeDo service: hosting and running the Customer's AI bots on isolated machines, and storing their data, memory, recordings and records

Item	Description
Duration	As long as the Terms apply, plus the periods in section 10 and Annex 4
Nature of processing	Collection by bots through connectors and a browser; storage; structuring into memory; computing text embeddings of memory and of the workspace's connected tools for search, and ordering search results, on ZeeDo's own models (5.6); retrieval; transmission to model providers; checking the labels of a control a bot is about to press, to tell what pressing it would do (5.5); transmission to third parties the Customer's bots contact; screen recording; logging; erasure
Purpose	To perform the tasks the Customer assigns to its bots, and to give the Customer control over and a record of what its bots did
Categories of data subjects	The Customer's Members; the Customer's employees, customers, suppliers and contacts; any person whose data appears in systems or websites the Customer connects its bots to, including third parties named in the labels of a page a bot works on; recipients of bot messages
Categories of personal data	Determined by the Customer. May include names, contact details, correspondence, documents, account data at third-party services, and any data visible on screens a bot works on, among it the labels of the buttons, form fields and dialogs of a page a bot is about to press on, which may name people
Special categories	The Customer decides whether its bots process special categories of personal data or data about criminal convictions and offences, for example in health or payroll systems, and needs its own legal basis and assessment for that. Traces of pages on websites that the site registry marks as sensitive keep the page's address, the step and its outcome, not the page's content; the run's checkpoints and screen recordings keep what the bot saw for their own periods. ZeeDo offers no HIPAA business associate agreement
Credentials	Stored encrypted in the vault. Bots use them without reading them

Annex 2 — Technical and organisational measures

These are the technical and organisational measures ZeeDo takes under Article 32 GDPR. This Annex also serves customers that must assess the security of their suppliers, for example under the NIS2 Directive. A measure described in the future tense is one ZeeDo does not take yet, and the Customer cannot require it before ZeeDo introduces it.

Organisation

- Everyone ZeeDo authorises to process Customer Personal Data is bound to confidentiality, and access to production systems is limited to the persons ZeeDo authorises for operating the service (section 3).

Isolation

- Each workspace runs in its own Firecracker microVM, its Machine, with its own guest kernel.
- Inside a Machine, each bot works as its own Linux user, with its own cgroup (limits on CPU, memory and processes) and its own seccomp profile.

- A weekly job checks published security advisories for the components that isolate Machines, among them Firecracker, the host and guest kernels and the browsers, and raises an advisory of the escape class at the highest priority.
- ZeeDo will introduce a 14-day patch cycle for host kernels and the rotation of each host every 30 days.

Tenant separation in the database

- PostgreSQL row-level security is enabled and forced on every table that holds customer data, with a policy that limits a transaction to one organisation's rows. The application's database roles cannot bypass it. An automated test checks every table for this policy, and tests check that a transaction for one organisation cannot read or change another organisation's rows.

Access control

- Members sign in through ZeeDo's sign-in provider, for example with a passkey, a password, or Google or Microsoft, or, for organisations with the SSO add-on, through their own SAML or OIDC single sign-on.
- People in the Owner, Admin, Manager and Member roles must sign in with a passkey, a password with a one-time code from an authenticator app, the organisation's own single sign-on, or their own Google or Microsoft account. For a Google or Microsoft account, ZeeDo relies on that account's own security, including its 2-step verification, which the account holder controls and ZeeDo cannot see. A person who holds an authenticator app is asked by ZeeDo's sign-in provider for its one-time code at that sign-in as well; a person who has used a passkey in the organisation and holds no authenticator app is asked for the passkey instead of their Google or Microsoft account.
- Sessions use HTTP-only cookies, end after 12 hours without activity and last at most 30 days.
- Sensitive acts need a fresh re-authentication within the previous 5 minutes: by a passkey, by a password with a one-time code from an authenticator app, or by a fresh sign-in through the person's own Google or Microsoft account, at which a person who holds an authenticator app is asked for its code as well; a person who has used a passkey in the organisation and holds no authenticator app confirms with the passkey. ZeeDo asks for the fresh sign-in; whether Google or Microsoft asks for the account's password or 2-step verification again is decided by that provider and the account's settings, and a browser still signed in to the account may not be asked. They include deleting a workspace or the organisation, creating or rotating API keys, changing single sign-on or billing details, saving or revealing a vault credential, saving a provider key, granting a standing approval and releasing an action class from approval. An API key can never satisfy the re-authentication.
- Access rights follow six roles (Owner, Admin, Manager, Member, Viewer and Billing) and grants on single resources, decided by one permission function that ZeeDo's tests cover.

Credentials and keys

- Vault credentials are encrypted in the Member's browser, to a key held in AWS KMS in

Frankfurt (eu-central-1), before they reach ZeeDo, and only ZeeDo's gateway services can open them. A bot uses a credential without reading it: ZeeDo places it into the request or types it into the page that asks for it, and no operation returns it to a model. A Member with the right role may reveal a credential after re-authenticating, and each reveal is recorded in the audit log.

- Provider keys for BYOK are encrypted in the browser in the same way and opened only in ZeeDo's model gateway, which keeps an opened key in memory for at most 5 minutes.
- Provider keys do not enter a bot's Machine. A vault credential reaches a Machine only when it is typed into the page that asks for it, and the bot cannot act on the screen while it is typed.

Network

- Each Machine has its own network namespace with no route out. Its outbound traffic leaves only through ZeeDo's egress broker on its server, which applies the workspace's egress policy, and a kernel-level (eBPF) filter drops any other traffic.
- The broker refuses private, loopback, link-local and cloud-metadata addresses and ZeeDo's own internal addresses; enforces the workspace's egress policy; removes secret patterns, such as API keys and private keys, from responses and refuses a request that carries one to a host that is not that secret's own origin; obeys robots.txt for the pages a bot chooses to open; limits the rate of requests per site; and refuses sites that the site registry marks as prohibited.

Actions

- Each tool call a bot makes is checked against the workspace's policy before it runs, and is allowed, sent to a person for approval, or refused. Actions in the six action classes, external messages among them, need approval by default.
- Paying, entering a payment instrument, submitting a regulated filing and defeating a human-verification challenge are always refused, and no setting changes that.
- An approval covers the exact arguments shown, and a call that differs from them is refused. An approval request that nobody answers expires after 72 hours.

Recording and logging

- Screen recordings are still images taken while a bot works. In the bot's browser, the password fields, payment fields and fields the vault types into that the browser finds on the page are masked when the image is captured, before it is encoded, and a frame is masked whole when the browser has not reported those fields in time. A field the browser cannot find on a page, and fields in other programs on a Machine's screen, are not masked. No keystrokes or clipboard content are recorded.
- The audit log is append-only: ZeeDo's application cannot change or delete its rows. An hourly copy of it is written to object storage locked against change and deletion for 400 days, at both storage sites.
- Trace attributes are limited, for each kind of span, to a closed list of identifiers, enumerations and numbers, and the trace store refuses any other attribute. Content is kept only in trace bodies, which are deleted after 30 days.

Encryption

- Objects derived from Customer Content that ZeeDo keeps in object storage, such as snapshots, screen recordings, files, memory texts and the audit log's copy, are encrypted by ZeeDo with AES-256-GCM under a data key per workspace or organisation before they are written. Export archives, which the Customer downloads, are not encrypted by ZeeDo in this way. The data keys are stored only in encrypted form, under a key held in AWS KMS.
- The data directories of the servers that run Machines, which hold the Machines' volumes, snapshots and memory images, are encrypted (LUKS2), and a production server refuses to start on an unencrypted one.
- The database is encrypted at rest by its provider, Neon.
- ZeeDo uses TLS for connections between its services over a network, to its providers and to users' browsers. In production, ZeeDo's services refuse a database or cache connection to another server that is not encrypted with a verified certificate, and an object store reached over a network without TLS.

Availability

- ZeeDo keeps a copy of its object storage at a second provider, OVH in Limburg, Germany.

Memory erasure

- When an episode, note, fact or relation is written to memory, ZeeDo marks it if it recognises personal data in it, such as an email address, a telephone number or a person's name. An erasure request does not depend on that mark: the erasure job in section 7.1 finds a person's data by the identifiers given and deletes it within 72 hours.

Testing

- ZeeDo tests its own security. It builds a release of its software only from a version for which its automated tests, its scans of dependencies, secrets, code and container images, and its red-team suite against prompt injection, played against ZeeDo's policy engine and vault, have passed.
- ZeeDo has carried out an OWASP ASVS level 2 self-assessment of its service.
- ZeeDo will also play its red-team suite every night against the live model, run microVM escape tests on its production hardware and run automated attack scans of a staging environment.

Incident response

- ZeeDo runs an incident process with severity levels and notifies personal-data breaches as section 9 states.

Annex 3 — Sub-processors

These are the sub-processors ZeeDo engages for the ZeeDo service, with the sites where they process data. ZeeDo gives at least 30 days' notice, by email to the Owners and on this list, before adding or replacing a sub-processor, as section 5.3 of the Data Processing Addendum

provides.

In the tables, "SCCs" means the Standard Contractual Clauses adopted by the European Commission (Implementing Decision (EU) 2021/914), as the recipient's data processing terms incorporate them. "DPF" means the EU–US Data Privacy Framework (the Commission's adequacy decision of 10 July 2023); it is named only where the recipient states that it is certified under it, and then in addition to the SCCs. "None needed (EEA)" means that the data stays with a company in the European Economic Area.

3.1 Hosting sites

Vendor	Function	Data	Location	Transfer mechanism
Scaleway SAS (Elastic Metal dedicated servers; Scaleway Object Storage)	Bot machines and their snapshots and recordings, the control-plane server, ZeeDo's own embedding and reranking models and the self-hosted software in 3.5; the primary object-storage buckets	Customer Content	Paris region (fr-par), France	None needed (EEA)
OVH (OVH Object Storage)	The replica of the object-storage buckets only	Customer Content, encrypted by ZeeDo before it is stored	Limburg, Germany	None needed (EEA)
Amazon Web Services	The region that hosts Neon, Temporal Cloud, AWS KMS and Amazon SES	The data of those services, as 3.2 and 3.3 describe	Frankfurt region (eu-central-1), Germany	SCCs in Amazon Web Services' data processing terms, and the DPF, under which Amazon Web Services states it is certified

3.2 Vendors that may touch Customer Content

Vendor	Function	Data	Location	Transfer mechanism
Neon (Databricks, Inc. and its subsidiary Neon, LLC)	Managed PostgreSQL database with pgvector	All database rows: bots, runs, checkpoints, memory, the audit log, cost records	Amazon Web Services' Frankfurt region (eu-central-1), Germany	SCCs in Neon's data processing terms, and the DPF, under which Neon states it is certified

Vendor	Function	Data	Location	Transfer mechanism
Temporal Technologies (Temporal Cloud)	Workflow orchestration for bot runs	Workflow history and payloads	Amazon Web Services' Frankfurt region (eu-central-1), Germany	SCCs in Temporal's data processing terms
Amazon Web Services (AWS KMS)	Key management: the keys that protect vault credentials, provider keys, stored objects and signing keys	Key material and wrapped data keys; no Customer Content in readable form	Frankfurt region (eu-central-1), Germany	SCCs in Amazon Web Services' data processing terms, and the DPF, under which Amazon Web Services states it is certified
Vercel (Vercel Inc.)	Hosting of the web application and its API routes	Data served to the dashboard and the API	Functions in Frankfurt (fra1), Germany; content delivery through Vercel's global edge network	SCCs in Vercel's data processing terms, and the DPF, under which Vercel states it is certified
Langfuse GmbH, part of the ClickHouse group (Langfuse Cloud)	Trace store: the record of each run's steps and model calls	Traces: their metadata (identifiers, timings, counts), kept 13 months, and their bodies (prompts, responses and tool results), kept 30 days	Langfuse's EU region on Amazon Web Services in Ireland (eu-west-1); support from the United States under its terms	None needed (EEA) for the EU region; SCCs in Langfuse's data processing terms for support from the United States
Grafana Labs (Raintank, Inc.; Grafana Cloud)	Logs, metrics, service traces and alerts of ZeeDo's systems	Identifiers and network addresses; the logs of the servers that run bot machines also hold the commands a bot ran, with their arguments, the paths of the files it wrote (not their contents) and the hosts it reached	An EU region of Grafana Cloud in Germany	SCCs in Grafana Labs' data processing terms, and the DPF, under which Grafana Labs states it is certified

Vendor	Function	Data	Location	Transfer mechanism
OpenRouter (OpenRouter, Inc.)	ZeeDo's model: the default model access of every workspace on every plan, unless the Customer uses BYOK or switches it off; it passes each request to the provider named for the model	Prompts and model responses of workspaces on ZeeDo's model, restricted to providers that keep no copy of them (zero data retention) and do not train on them	OpenRouter, Inc. is in the United States. For an organisation of ZeeDo's EU region, requests are processed in the EU through OpenRouter's EU endpoint, and a request is refused rather than sent elsewhere; for other regions, through the endpoint named for the region. The decision model is reached from the United States for every region, unless an organisation keeps every model check in the EU	SCCs in OpenRouter's data processing terms
Microsoft (Azure), as OpenRouter's sub-processor	Serves ZeeDo's default model	Prompts and model responses on ZeeDo's default model	Azure's EU endpoint; processed in the EU	SCCs in OpenRouter's data processing terms, and the DPF, under which Microsoft states it is certified

Vendor	Function	Data	Location	Transfer mechanism
Perplexity, as OpenRouter's sub-processor	Serves the decision model that reads the rules people set for a bot, and that checks what a control a bot is about to press would do	For the rules: the typed text of a message that sets or changes a rule for a bot, and the words of the rules it concerns; also the start of a request to a bot whose rules do not all fit in front of it; what a person pastes, and anything a bot read, are not sent. For a press: the labels of the control, of its form's fields and of a dialog it answers, the currencies shown, the site's domain and the pattern of the form's address, whose parts written only in lower-case letters are kept as written and may be a name; field values, page text and links are never sent; inside a label, numbers written in digits, email addresses, phone numbers, account and card numbers and web addresses are replaced by placeholders, and its other words are sent as written and may name third parties, streets or places; pages of sensitive sites and of webmail are never sent	United States, for every region, unless an organisation of ZeeDo's EU region keeps every model check in the EU	SCCs in OpenRouter's data processing terms
Scaleway SAS (Scaleway Object Storage), with a replica at OVH	Regional object storage: snapshots, home volumes, recordings, files, the full text of memory episodes, the audit log's hourly copy, and export archives, which are kept at Paris only	Customer Content, encrypted by ZeeDo before it is stored, except export archives	Paris (fr-par), France; replica in Limburg, Germany	None needed (EEA)

3.3 Vendors that process account, identity, billing or notification data

ZeeDo is the controller for much of this data (the Privacy Policy describes it). These vendors are listed here so that the list is complete.

Vendor	Function	Data	Location	Transfer mechanism
WorkOS (WorkOS, Inc.)	Sign-in (AuthKit), single sign-on and directory sync (SCIM)	Members' identity and sign-in data	United States	SCCs in WorkOS's data processing terms
Stripe (Stripe Payments Europe, Limited)	Checkout, subscriptions, invoices and tax. Stripe is an independent controller for payment processing and fraud prevention; for its billing services it is ZeeDo's processor	Billing contacts, the legal entity's name and address, VAT ID, invoices; payment details, which Stripe collects and ZeeDo never receives	Ireland; Stripe's group also processes data in the United States	SCCs in Stripe's data processing terms, and the DPF, under which Stripe states it is certified
Amazon Web Services (Amazon SES)	Transactional email: alerts, notices and approval mirrors	Recipient address, message content	Frankfurt region (eu-central-1), Germany	SCCs in Amazon Web Services' data processing terms, and the DPF, under which Amazon Web Services states it is certified
Better Stack	Uptime probes and the public status page, with subscriptions by email	Probe results; status-page subscribers' email addresses	The United States and other countries where Better Stack and its sub-processors operate, as its data processing terms state	The DPF, under which Better Stack's data processing terms state it is certified; the SCCs in those terms apply where the DPF does not

Browser push notifications use standard Web Push (VAPID) and are sent from ZeeDo's own servers, with no push vendor. Each message is encrypted end to end and relayed by the push service of the recipient's browser maker, which cannot read it and sees only an endpoint and the time; these relays are transmission services, not sub-processors. If ZeeDo releases native mobile apps, their notifications will go through Apple's and Google's push services, and ZeeDo will add those services to this list, with notice, before the apps are released.

3.4 Operational services (no Customer Content)

Vendor	Function	Data	Location	Transfer mechanism
Functional Software (Sentry)	Error reports of the application	Error reports built only from the error's type, the place in ZeeDo's code where it arose and a closed list of labels; never text a person or a bot wrote, and no personal data	Sentry's EU region, Germany	SCCs in Sentry's data processing terms, and the DPF, under which Sentry states it is certified

Alerts to ZeeDo's on-call staff carry only an alert's name, its severity, a fixed summary and the address of its runbook, with no Customer Content and no personal data. A service that only delivers them to the staff is therefore not a sub-processor. If a provider in this section is to receive Customer Personal Data, it is added to 3.2 with the notice section 5.3 of the Data Processing Addendum requires.

3.5 Not sub-processors (self-hosted software on ZeeDo's own servers)

These run on ZeeDo's servers at Scaleway above (3.1), so the site is the sub-processor, not the software's author: **Nango (**integrations gateway); **coturn (**the relay for live screen viewing); **Valkey (**budget ledger and caches); the Web Push sender; and ZeeDo's own embedding model (**BAAI/bge-m3,** an open model under the MIT licence) and reranking model (**bge-reranker),** served by Hugging Face's open-source Text Embeddings Inference beside ZeeDo's model gateway. Memory text, memory searches and the descriptions of a workspace's tools are embedded there, and memory search results ordered there, for every workspace; no embeddings vendor is used.

3.6 Chosen by the Customer (not ZeeDo sub-processors)

- **Model providers under BYOK (**for example Anthropic, OpenAI, Google, xAI, Mistral, DeepSeek, AWS Bedrock, Azure OpenAI, Vertex AI, Groq, Together, Fireworks, OpenRouter on the Customer's own key, and custom endpoints). The Customer contracts with the provider directly; the provider is the Customer's own processor. Embeddings follow the workspace's embedding model, not the bots' keys: ZeeDo's own model (3.5) whatever key the Customer's bots use, or an OpenAI embedding model of the Customer's own account where an Owner or Admin chose one, in which case OpenAI is the Customer's own processor for that workspace's memory text.
- **Connectors and MCP servers** the Customer connects.
- **Websites** a bot visits.

Annex 4 — Retention annex

1. Retention of Customer Content

Data	Retention
Run history (the step record, not files)	Per plan: Free 7 days, Starter 30, Pro 90, Business 365, Enterprise as agreed. A paid add-on extends it in 90-day steps
Conversations with bots	On every plan, until the bot or the workspace is deleted. An erasure of a person deletes the lines that name them
Tasks on the board that are done or cancelled	The run-history period of the plan. A task still open stays
Decisions and standing instructions on the board	Until a person deletes them or the workspace is deleted
Screen recordings	14 days on every plan. Business may extend this to 90 days and Enterprise to 400, never shorten it
Model context: run checkpoints and trace bodies	30 days, on every plan
Trace metadata (identifiers, timings, counts; no content)	13 months
Workflow history of finished jobs	At most 30 days after the job ends
Operational logs of the servers that run Machines (commands run, paths of files written, hosts reached)	At most 30 days
Memory: raw episodes	At most 90 days
Memory: summaries, facts and relations, procedures, notes people write	Until the Customer deletes them or the workspace is deleted
Memory: notes bots write	30 days by default
Files bots made	Until a person deletes them or the workspace is deleted; files that are screen recordings follow the recordings' 14 days
Files a person hands a bot	A file that was never sent with a message or card is deleted at the first nightly pass at least a day after it was stored, so within two days. A file that was sent is kept as long as the message or card it was sent with, and deleted with it
Vault credentials and browser sessions	Until the Customer revokes or deletes them; then deleted at once
Workspace machine snapshots	For the life of the workspace
Export archives	7 days after they are written
Failed webhook deliveries	Retried for 24 hours, then kept 7 days for replay

Data	Retention
Audit log and consent records, including approval decisions and standing approvals	400 days on every plan, and at most a month longer, because the log is deleted one calendar month at a time. The plan limits how far back the log can be searched, not how long rows are kept
The audit log's hourly write-once copy	400 days
An organisation after end of service	The clock in Terms 18: read-only with export days 0 to 60, deleted on day 90, purged from backups within 30 days after
Backups	Rolling, at most 30 days

Long-lived memory. Episode summaries, facts and relations, procedures and notes people write have no fixed maximum life. The Customer controls them: they are kept until the Customer deletes them or the workspace is deleted (section 10), and an erasure request permanently deletes matching entries within 72 hours (7.1).

2. Audit and consent retention exemption

- Audit rows, including consents, approval decisions and standing approvals, are kept 400 **days on every plan,** and at most a month longer, because the log is deleted one calendar month at a time.
- The Customer instructs ZeeDo to keep them and not to erase them on a data subject's request: they are the record of what its bots did and who authorised it, which either party may need to establish, exercise or defend legal claims (Article 17 (3) (e) GDPR). The rows hold identifiers (a member's pseudonymous id and, for some requests, the network address and browser they came from), the action and the time, not what was said.
- The erasure report lists them as **retained with reason,** not silently skipped.
- The actor in an audit row is a **pseudonymous member id.** The display name is resolved at read time from the member record. Erasing a person therefore removes their name from every view without altering the append-only audit table.
- The plan controls how far back the audit log can be searched. It does not control how long rows are kept.

3. Deletion

- End of service: read-only with export on days 0 to 60, deletion on day 90, and purge from backups within 30 days after deletion (section 10).
- Files: as the rows for files bots made and files a person hands a bot in section 1 state.
- A removed Member's data: deleted 30 days after removal, except the pseudonymous member id in audit rows.