Contents

Data Processing Agreement

1. Parties and scope
2. Subject matter, duration and kind of processing
3. Instructions
4. Confidentiality
5. Security
6. Sub-processors
7. International transfers
8. Helping with people's requests
9. Personal data breach
10. Other help (Articles 32 to 36)
11. Return and deletion
12. Proof and audits
13. Liability and governing law
14. Versions and acceptance
15. Annex 1. Sub-processors
16. Annex 2. Security measures

Data Processing Agreement

Version 2026-11-03

This agreement applies when Respiresoft LLC (nerix.ai, "nerix") processes personal data for a customer who uses nerix.ai. It meets Article 28 of the GDPR and the same rules in the UK GDPR and the Swiss data protection act. It forms part of the Terms.

1. Parties and scope

The customer is the organisation that owns the workspace, the controller of the personal data it puts into nerix.ai (a processor of it, where it acts for its own customers). Respiresoft LLC, 32 N Gould St, Sheridan, WY 82801, United States, is the processor.

This agreement covers personal data in the customer's workspace: documents, conversations, Sheets, work records, meetings and recordings, library embeddings, members' names and email addresses, and the audit trail. It does not cover personal data for which nerix decides the purposes itself, such as the sign-in account of a person or billing records. Those are described in the privacy policy.

If this agreement and the Terms disagree about personal data, this agreement prevails.

2. Subject matter, duration and kind of processing

Item	Detail
Subject matter	Providing the nerix.ai service: storing, reading, searching and answering from the customer's documents, writing documents, running work and meetings.
Duration	From the day the customer accepts this agreement until the workspace is deleted and the retrieval period in section 9 has ended.
Nature of processing	Storage, indexing for search, transmission to AI model providers to answer a request, display, export and deletion.
Purpose	Only to provide the service the customer asked for, and to keep it secure.
Types of personal data	Whatever the customer puts into the workspace. Names, contact details, job roles, financial and employment details, and other content in documents and conversations. Special categories only if the customer puts them there.
People concerned	The customer's staff, clients, suppliers, applicants and any other people named in the customer's documents and conversations.

3. Instructions

nerix processes personal data only on the customer's documented instructions. The Terms, this agreement, the settings the customer chooses in the product (for example the AI region, the providers, the retention periods and hiding names from the AI) and what its members ask the product to do are the instructions. That includes transfers to a third country: they happen only as these instructions and the sub-processor list allow.

nerix tells the customer at once if it believes an instruction breaks data protection law. If the law requires nerix to process otherwise, it tells the customer first unless the law forbids that.

4. Confidentiality

Everyone at nerix who can reach customer personal data is bound by a written duty of confidentiality, gets access only when the work needs it, and every look by staff into a customer's conversation is recorded in the customer's own audit trail.

5. Security

nerix takes the measures of Article 32 GDPR. Annex 2 lists the ones that exist today. nerix may change them if the level of protection does not go down.

6. Sub-processors

The customer gives general written authorisation for the sub-processors in Annex 1. nerix binds each of them to the same data protection duties by contract, and stays fully liable to the customer for them.

nerix tells the owner of each workspace at least 30 days before it adds or replaces a sub-processor, in the product and by email, and updates the public list at nerix.ai/legal/subprocessors. The customer may object on reasonable data protection grounds within those 30 days. nerix then tries to offer the service without that sub-processor, for example by keeping the workspace on EU only providers. If that is not possible, the customer may end the contract and gets a refund of prepaid fees for the time not used.

A customer chooses the AI region and the providers for its own workspace. A provider the customer switches on itself in Settings is the customer's own choice and not a change by nerix.

7. International transfers

Customer data is stored in the European Union (France, with encrypted files and backups in the Netherlands). nerix is established in the United States. Where personal data is transferred to or accessed from a country without an adequacy decision, the parties agree the Standard Contractual Clauses of the European Commission (Decision (EU) 2021/914) as follows. Module Two (controller to processor) applies when the customer is a controller, and Module Three (processor to processor) when the customer is itself a processor. They are part of this agreement by reference.

- Clause 7 (docking clause): included.
- Clause 9(a): option 2, general authorisation, with the 30 days notice in section 6.
- Clause 11(a): the optional independent dispute resolution body does not apply.
- Clause 17: the law of the Republic of Ireland. Clause 18(b): the courts of Ireland.
- Annex I.A parties are in section 1; Annex I.B is section 2; the competent supervisory authority is the one of the customer's establishment (or, if none, the Irish Data Protection Commission). Annex II is Annex 2 below. Annex III is Annex 1 below.

For personal data under the UK GDPR the parties also agree the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner (version B1.0, in force 21 March 2022). Its tables are filled from this section and the annexes, and either party may end it as its section 19 says.

For personal data under the Swiss data protection act the SCCs apply with these changes: the Swiss Federal Data Protection and Information Commissioner is the competent authority; references to the GDPR include the Swiss act; the place of jurisdiction for claims by people in Switzerland is Switzerland; and "member state" does not stop a person in Switzerland suing at their habitual residence.

If nerix is certified under the EU-US Data Privacy Framework for the transfer, that certification is the main safeguard and the SCCs apply as a fallback if the framework stops being valid. A government access request is handled as the SCCs say: nerix challenges requests that are unlawful, shares the least it can, and tells the customer unless the law forbids it.

8. Helping with people's requests

If a person asks nerix about data it holds for the customer, nerix does not answer on the merits and passes the request to the customer without undue delay (within five working days). nerix gives the customer tools to help: export of a workspace and of one person's own account data, deletion, correction and the audit trail. Beyond those, nerix helps with reasonable effort and at no charge when it is a small task.

9. Personal data breach

nerix tells the owner of each affected workspace without undue delay and at the latest 24 hours after it becomes aware of a personal data breach that affects the customer's data, in the product and by email. The notice says what is known: what happened, which data and roughly how many people, the likely effects, what nerix has done and what it advises the customer to do. Further facts follow as they are found. nerix keeps a register of breaches and gives the customer what it needs for its own notice to the authority (Article 33) and to the people (Article 34).

10. Other help (Articles 32 to 36)

nerix helps the customer with security, breach notice, data protection impact assessments and prior consultation, taking into account what it can see. nerix provides a summary of its data protection impact assessment of the AI features on request.

11. Return and deletion

The customer can export the whole workspace at any time, free of charge, from Settings (documents in their original files, conversations, Sheets, records, audit trail), and can delete data and the workspace itself. When the contract ends, nerix keeps the workspace for a retrieval period of at least 30 days so that the customer can export it, then deletes the personal data, backups included within 30 further days, unless the law requires nerix to keep it. nerix confirms the deletion on request.

12. Proof and audits

nerix gives the customer the information needed to show that Article 28 is met, and lets the customer or an auditor it appoints inspect it, with 30 days notice, in business hours, under confidentiality, not more than once a year unless a breach or an authority requires more, and at the customer's cost. nerix may meet this first with current independent reports and its answers to the customer's security questionnaire.

13. Liability and governing law

Liability under this agreement follows the Terms, except that nothing limits liability that cannot be limited by law and the SCCs, where they apply, prevail over everything else. This agreement is governed by the law of the Republic of Ireland for the SCCs, and otherwise by the Terms.

14. Versions and acceptance

The customer accepts this agreement in the product: the owner of the workspace confirms it, and nerix records the date, the version and who accepted. A new version is shown to the owner with what changed, and applies once accepted; the version accepted stays visible in Settings. Enterprise customers can ask for a copy with signature lines. Questions: info@nerix.ai.

15. Annex 1. Sub-processors

The public list at nerix.ai/legal/subprocessors is the current one. On the date of this version:

Sub-processor	What it does	Where	When
OVHcloud (servers in Gravelines, France)	Runs the service and stores its databases	France, EU	Always
Mistral AI SAS	Language models that write answers	France, EU	Always; the only AI provider while a workspace is EU only
OpenAI	Language models	Set by the provider; may be outside the EU	Only if the customer switches it on
Anthropic	Language models	Set by the provider; may be outside the EU	Only if the customer switches it on
Google	Language models	Set by the provider; may be outside the EU	Only if the customer switches it on
DeepSeek	Language models	People's Republic of China	Only if the customer switches it on, with a caution shown. Personal data should not be sent there without an assessment by the customer.
Soniox	Speech to text	Set by the provider	Only when speech is used
Stripe	Card payments	EU and US	For paid plans: billing contact and payment data only, not workspace content
Email delivery provider	Sends the product's emails	See the public list	When the product sends an email
Backblaze (storage in Amsterdam, the Netherlands)	Stores encrypted files and backups	Netherlands, EU	Always

16. Annex 2. Security measures

These measures exist in the product today.

- Separation of customers: every record carries its workspace, and every query in the code must name the workspace or it fails; files are stored per workspace.
- Encryption: connections use TLS. Provider keys and customers' stored credentials are encrypted with envelope encryption, the master key is held outside the database in a file only the service can read.
- Access: sign-in with a password, passkeys or Google or GitHub; two step sign-in; roles for owner, admin, member and viewer; sessions can be listed and ended; API keys can be revoked at once.

- Staff access: separate staff identity with its own sign-in and second step; staff see a customer's conversation only with a recorded reason and each look is written to the customer's audit trail; impersonation is shown to the customer in the audit trail.
- Audit trail: append only record of who did what in the workspace, with exports; kept for the retention period the owner sets.
- AI safety: names of people and clients and personal details such as email addresses and phone and account numbers can be replaced with codes before text reaches a model and put back in the answer; owners can lock this setting; a model provider is never allowed to train on customer data; the AI region can be limited to EU only or to models on our own servers.
- Retention and deletion: the owner can set how long documents and conversations are kept, they are then deleted by the service; deletion removes files from disk, not only rows; a workspace deletion runs after a 30 day grace period.
- Backups: kept in the EU; deleted data leaves backups within 30 days.
- Resilience: separate processes for the web, the background work and the AI hub, health checks and restarts without dropping jobs; changes are tested before release.
- Breach process: a written runbook, a register, notice to affected owners within 24 hours, and a Security notice in the product.
- People: a confidentiality duty and access only when the work needs it.