Terms & Conditions – AI RiskWise BV

Last updated: February 2, 2026

Welcome to AI RiskWise. These Terms & Conditions ("**Terms**") govern your use of our services, including **MeetingWise**. We keep them readable and fair, so you know exactly what we provide, and what we expect from you.

If anything is unclear, please contact us at **legal@airiskwise.com**.

1) Who we are

AI RiskWise BV ("**Provider**", "**we**", "**us**") delivers responsible AI for regulated advisory sectors (insurance, mortgages, pensions, accountancy, notarial).
Address: A. de Bruynkade 38, 3059 SE Rotterdam, The Netherlands • **Chamber of Commerce (KvK):** 98626248 • **Website:** www.airiskwise.com • **Email:** legal@airiskwise.com

Our flagship product **MeetingWise** supports advisers with **transcription, summarisation and IDD-aligned compliance checks**.

2) Scope and precedence

These Terms apply to your use of MeetingWise, our website, and support interactions. If your organisation has a signed **Subscription Agreement** and/or **Data Processing Agreement** (**DPA**), those documents prevail in case of conflict.

3) Nature of the Service (AI support, not advice)

MeetingWise is a **supporting AI tool**. Outputs are **assistive** and **probabilistic**, and depend on audio quality and context. **MeetingWise does not provide legal, compliance or professional advice, and is not a legal stenography service.** Human oversight by a **licensed adviser** is mandatory before any reliance or downstream use.

4) Data protection and roles (GDPR)

- For our **website**, AI RiskWise acts as **data controller**.
- For **MeetingWise**, AI RiskWise acts as **data processor** processing **Customer Personal Data** under the Customer's instructions (controller).
- Processing is **EU-resident**. We do **not** train general-purpose models on Customer Data.
- Details: see our **Privacy Policy** and the **DPA** (both incorporated by reference).

5) Customer account and lawful use

Customer must ensure lawful, legitimate and ethical use of the Services and is responsible for account security and access control. Customer will not upload content Customer is not permitted to process and will comply with all applicable laws, including **GDPR**, **ePrivacy rules** and **IDD**.

Acceptable Use

The Service may not be used to violate the law, infringe rights of others, interfere with the functioning of the Service, or attempt unauthorised access. The Service may not be used to

distribute harmful content, malware or anything that compromises security or trust. Provider may suspend access where necessary to protect the Service or comply with legal obligations.

6) Human oversight and recording transparency (key obligations)

- **Licensed adviser in control:** A duly licensed adviser must **review and approve** any output before reliance, filing or downstream use.
- **Recording notice & legal basis:** Customer is solely responsible for informing meeting participants and obtaining any **consent** or other legal basis required.
- **Not for legal stenography / public or political events:** Customer will not use MeetingWise for official stenography, public or political settings, unlawful surveillance or any purpose that breaches professional standards.

These duties are further detailed in **Annex A** – **Customer Responsibilities** (integral to these Terms).

7) Payment, subscription and termination

Subscriptions are billed in advance. Invoices must be paid within 30 days. If payment is overdue, interest may be charged at 1% per month or the maximum rate permitted by law. If payment remains outstanding after notice, the Service may be suspended. Reactivation after suspension may require a reactivation fee of €150.

Data Return and Deletion

After termination, Customer may export available transcripts and summaries for 30 days. After this period, Provider will remove Customer Data from active systems and schedule deletion from backups according to its retention policy. Provider will confirm deletion on request where reasonably possible.

8) Claims and Notice Period

Any claim relating to the Service must be reported within 30 days after the issue was or reasonably should have been discovered. After that period, the claim is considered waived, unless the law requires otherwise.

9) Intellectual property and data ownership

All IP in MeetingWise (software, models, documentation, brand) remains with AI RiskWise. **Customer owns Customer Data and the outputs** (transcripts, summaries, action points) relating to Customer's meetings, subject to these Terms. No reverse engineering, decompiling or sublicensing of the Service.

10) AI Output Limitations & No-Reliance (critical)

- Outputs are **assistive** and **not authoritative**.
- Customer **must not** present outputs as official, legally binding or error-free.
- **No reliance** without human verification by a licensed adviser.
- Provider **does not** accept responsibility for downstream use in the **Customer**–**client** relationship or for Customer's professional or regulatory decisions.

11) Security Incidents & Notifications

If Provider becomes aware of a personal data breach involving Customer Data, Provider will inform Customer without undue delay and share available details, subject to security considerations. Customer agrees to inform Provider promptly if it suspects misuse of credentials or access. Both parties will cooperate reasonably in managing and resolving incidents.

12) Confidentiality

Both parties will treat all non-public business, technical and security information received from the other party as confidential. Such information may only be used to perform the Agreement and may only be shared with personnel or subprocessors who need the information and are bound by confidentiality obligations. These confidentiality obligations remain in effect for five years after termination, and indefinitely for trade secrets.

13) Service Levels (SLA-light)

We aim to provide a reliable service.

- **Availability target:** 99.5% monthly (excluding planned maintenance and circumstances under Force Majeure).
- **Planned maintenance:** announced in advance; scheduled to minimise impact.
- **Support response targets (business hours):** P1 within 4h; P2 within 8h; P3 within 1 business day.
- **Status & incidents:** material incidents are posted on our status channel and/or communicated to affected Customers.

(For enterprise, a separate SLA can supersede these targets.)

14) Service Changes & Versioning

We continuously improve MeetingWise. We may add, modify or remove features. **Material changes** that reduce core functionality for existing users will be **announced in advance** with reasonable notice. If a change materially impairs agreed use and no workaround exists, Customer may terminate the affected subscription at the end of the current term.

15) Force Majeure

Neither party is liable for delay or non-performance caused by events beyond its reasonable control (including but not exclusively power/network failures, DDoS, acts of government, strikes, pandemics, natural disasters). If a Force Majeure event lasts more than 30 days, either party may terminate the affected services with written notice. Customer remains responsible for fulfilling **consent**, **oversight** and **lawful-use** obligations during and after such events.

16) Disclaimers and allocation of risk

To the maximum extent permitted by law, Provider is **not liable** for:
(a) indirect, incidental, consequential, punitive or exemplary damages;
(b) loss of profit, revenue, goodwill, reputation or business;
(c) **regulatory fines, sanctions or enforcement** against Customer;
(d) claims arising from Customer's failure to obtain consent, provide notices, maintain human

oversight, or comply with law or professional standards;
(e) any **downstream use** of outputs in the Customer–client relationship.

Cap: Provider's aggregate liability in any 12-month period is limited to the **fees paid** by Customer for the Services in that period.
Carve-outs: nothing limits liability for **wilful misconduct or gross negligence**, or any liability that cannot be limited by law.

17) Customer indemnity

Customer will **defend, indemnify and hold harmless** Provider, its affiliates and personnel against regulator or third-party claims, damages, penalties, costs (including reasonable legal fees) arising from:
(i) failure to obtain valid consent or provide required transparency;
(ii) failure to ensure **licensed adviser oversight**;
(iii) breach of law (including **GDPR**, **IDD**) or of these Terms;
(iv) Customer's **downstream use** or representations made to Customer's clients.

18) Suspension and termination for cause

We may suspend or terminate access if Customer breaches these Terms (including consent/oversight obligations), if required by law or regulator, or for security reasons. We will notify Customer where reasonably possible.

19) Changes to these Terms

We may update these Terms (e.g., legal changes, product improvements). We publish the new version on our website and adjust the "Last updated" date. Material changes will be communicated to Customers.

20) General Terms

If any part of these Terms is found unenforceable, the remaining provisions continue to apply. A failure to enforce any provision does not constitute a waiver. These Terms, together with any Subscription Agreement and DPA, form the entire agreement between the parties. The parties act as independent contractors, and no third party has rights under these Terms.

21) Governing law and disputes

These Terms are governed by the laws of the **Netherlands**. The competent Dutch courts have exclusive jurisdiction unless otherwise agreed in writing.

22) Contact

AI RiskWise BV • legal@airiskwise.com • www.airiskwise.com

Annex A – Customer Responsibilities (binding)

At AI RiskWise, we want MeetingWise to help you work more efficiently, safely and confidently. To make this possible, and to ensure that everyone involved is protected, we ask our customers to follow a number of important responsibilities.

These responsibilities are designed to be simple, practical and fully aligned with European law (including GDPR, ePrivacy rules and IDD).
By using MeetingWise, you agree to the following obligations.

1. Be transparent to meeting participants

MeetingWise can only be used when everyone in the meeting knows what is happening.

Please make sure that:

- You **inform all participants** before starting a recording.
- You **explain why** you are recording (for transcription, summarisation and compliance support).
- You **obtain any consent** required under GDPR or national rules.
- You only record meetings when you have a **lawful basis** to do so.

We provide a simple notification text you can use if you wish.

2. Keep a licensed adviser in control

MeetingWise is an AI-assistant, not a decision maker.

This means:

- A **licensed adviser must always review MeetingWise output** before you rely on it.
- You remain responsible for decisions, advice and documents shared with your clients.
- MeetingWise may not be used as a **replacement for professional review**, nor as official or legally binding stenography.

Human oversight is essential, and keeps you safely aligned with IDD and other sector rules.

3. Use MeetingWise only in appropriate settings

MeetingWise works best in professional advisory settings.
To ensure safety and compliance, you may **not** use MeetingWise for:

- legal or official stenography
- political or public events
- unlawful monitoring or surveillance
- any use that goes against professional, ethical or regulatory standards

If you're not sure whether a scenario is allowed, feel free to ask us.

4. Decide how long you keep data

You stay in control of your retention choices.

By default:

- Audio is deleted **immediately after processing**
- Transcript and summary files are kept for **30 days**

You may shorten these periods if your organisation prefers stricter controls.

You are responsible for choosing retention periods that match your own policies, regulatory obligations and risk appetite.

5. Keep your privacy notices and agreements up to date

Because MeetingWise processes personal data on your behalf, it is important that your organisation:

- updates its **privacy notices** to mention the use of MeetingWise
- includes MeetingWise in **client agreements**, where relevant
- performs a **DPIA** or Legitimate Interests Assessment if required
- handles any **data subject requests** you receive from your clients or staff

We provide documentation to help you complete these steps quickly.

6. Protect access to MeetingWise

Security is a shared responsibility.

You agree to:

- keep login details private
- use strong authentication (SSO or MFA where possible)
- immediately report any suspected unauthorised access
- ensure that only authorised users can access meeting content

These measures protect both your clients and your organisation.

7. Represent MeetingWise output responsibly

MeetingWise produces helpful summaries, action points and insights, but:

- they must **never** be presented as official, binding or guaranteed to be error-free
- they are **supporting material**, not professional advice
- you must always verify and interpret the results in the context of your client situation

If you share MeetingWise output with your clients, please ensure it is clearly positioned as supportive.

8. Work with us on (security) incidents

If you suspect that login details have been misused or that data may have been exposed, please contact us as soon as possible so we can help.
We will do the same if we detect an issue on our side.
Cooperation ensures fast resolution and keeps everyone protected.

9. Comply with applicable laws and sector rules

By using MeetingWise, you confirm that your organisation will follow all applicable laws, including:

- **GDPR**
- **ePrivacy rules**
- **IDD** (or equivalent regulatory frameworks in your market)
- any local sector-specific obligations

AI RiskWise provides the tools and transparency to help you stay compliant, but your organisation remains responsible for how MeetingWise is used within your advisory process.

Optional exhibits (on request)

- **Exhibit 1 – Recording Notice Template** (for Customer to share with meeting participants)
- **Exhibit 2 – DPIA Input Pack** (to speed up Customer's privacy assessment)
- **Exhibit 3 – SLA (Enterprise)** (if a bespoke SLA is agreed)