DATA PROCESSING AGREEMENT (DPA)

Between the Customer and AI RiskWise BV
This DPA forms an integral part of both the AI RiskWise Terms & Conditions and the Customer Agreement.

1. Purpose of this Agreement

This Data Processing Agreement explains how AI RiskWise BV processes personal data on behalf of customers who use MeetingWise. It is written in clear and accessible language so customers can understand what we do, why we do it and how we protect it. The DPA exists to provide transparency, trust and compliance with the GDPR and other applicable European rules.
By signing the Customer Agreement or by using the Service, the Customer accepts the terms in this DPA.

2. Roles and responsibilities

The Customer acts as the **Data Controller**, deciding which data is processed and for what purpose. AI RiskWise BV acts as the **Data Processor**, processing personal data only on the Customer's behalf and only for the purposes described here.

AI RiskWise does not determine the purpose of the processing and does not use Customer data for its own purposes. There is no joint controllership.

3. What data we process

MeetingWise processes the information that naturally appears in conversations. This may include the voices of participants, the spoken content of the meeting, names or email addresses mentioned during the conversation, timestamps, and technical metadata such as duration or system logs.

Because MeetingWise supports financial advisers, insurance brokers and mortgage professionals, it may also extract financial information when this is mentioned out loud and relevant to the summary, such as premium amounts, mortgage figures or other advisory details. MeetingWise does not enrich, supplement or obtain financial data from any external source, everything comes from what is said in the meeting.

Audio is deleted immediately after processing. Transcripts and summaries are kept for a limited period, and logs for security purposes. These periods are described later in this DPA.

4. How we process the data

AI RiskWise processes personal data only to deliver MeetingWise. This includes converting speech to text, generating summaries and action points, performing optional IDD-aligned checks, storing the result for a limited time, securing the system, providing customer support, and maintaining the reliability of the service.

MeetingWise does not train general-purpose AI models on Customer data.

We follow the Customer's instructions, which consist of this DPA, the T&C, the Customer Agreement and the actions taken within the MeetingWise interface.

5. Customer responsibilities

The Customer is responsible for informing meeting participants that the conversation is being processed by MeetingWise, and for obtaining consent or another lawful basis when required. The Customer must ensure that its own privacy notice, client terms and internal compliance procedures accurately describe the use of MeetingWise and the lawful basis for processing.

The Customer remains responsible for its own compliance with GDPR, ePrivacy and IDD obligations.

6. Retention periods

AI RiskWise applies strict and predictable retention rules:

- Audio is deleted immediately after it has been processed.
- Transcripts and summaries are stored for up to 60 days, with 30 days as the default unless the Customer requests shorter retention.
- Technical logs used for security and monitoring are stored for up to 365 days.

After a retention period expires, the data is deleted from active systems and later removed from backups according to scheduled secure deletion routines.

On request, AI RiskWise can confirm that personal data has been deleted.

7. Where the data is processed

All data is processed exclusively within the European Union. AI RiskWise does not transfer personal data outside the EEA. No standard contractual clauses or transfer mechanisms are required.

8. Subprocessors

AI RiskWise uses a small number of trusted subprocessors based within the EU:

- Microsoft Azure (EU regions) for secure hosting and infrastructure.
- Mistral AI (EU regions) for AI model inference.

These subprocessors operate under written agreements that provide at least the same level of protection as this DPA.

If AI RiskWise intends to add a new subprocessor, it will inform the Customer in advance. If the Customer has reasonable grounds to object, both parties will work together in good faith to find a suitable way forward. If no solution can be found, the Customer may terminate the part of the service that depends on the new subprocessor at the end of the current term.

9. Security

AI RiskWise maintains strong security practices appropriate for regulated industry use. This includes encryption, strict access control, secure development methods, continuous monitoring,

logging, regular internal reviews and a culture of privacy-by-design. These measures are designed to protect personal data from loss, misuse or unauthorised access.

A more detailed overview of these security measures is available upon request or through our Compliance & Security documentation.

Security is also a shared responsibility. The Customer is expected to protect account access, use strong authentication where available, limit access to authorised users and notify AI RiskWise promptly if access credentials may have been compromised.

10. Data subject rights

AI RiskWise will assist the Customer in responding to data subject rights requests, such as requests for access, correction or deletion. If we receive such a request directly, we will forward it to the Customer, who remains responsible for responding as the Data Controller.

11. Breach notifications

If AI RiskWise becomes aware of a personal data breach involving Customer data, the Customer will be informed within 72 hours. Where possible, the notification will include relevant information to support the Customer in assessing and reporting the breach to regulators.

The Customer must inform AI RiskWise immediately if it suspects that MeetingWise access or credentials have been misused.

12. Audits

AI RiskWise supports documentation-based audits. This means we can provide relevant policies, summaries, reports and certifications to demonstrate compliance.

On-site audits are not part of this Agreement unless required by law or a regulatory authority.

13. Confidentiality

All personnel engaged by AI RiskWise who process Customer data are bound by confidentiality obligations. Confidential information shared by the Customer will not be disclosed to others unless legally required.

14. Data return and deletion at the end of the contract

When the Customer Agreement ends, the Customer may export any remaining transcripts and summaries for a period of 30 days. After that, AI RiskWise will delete the remaining data according to this DPA's retention rules.

Deletion confirmation can be provided on request.

15. Liability

The liability framework described in the AI RiskWise Terms & Conditions applies fully to this DPA. This includes the liability cap and exclusions, as well as the carve-outs for wilful misconduct and

gross negligence. Nothing in this DPA limits rights or obligations that cannot be limited under European law.

16. Relationship to the T&C and Customer Agreement

This DPA is part of, and must always be read together with, both the Terms & Conditions and the Customer Agreement. If there is any conflict between the DPA and those agreements, the DPA governs matters relating to the processing of personal data.

17. Governing law

This DPA is governed by Dutch law. Any disputes will be handled by the competent courts in the Netherlands unless both parties agree otherwise.

18. Contact

For all privacy and data protection matters, the Customer may contact:

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