Data Processing Agreement (Art. 28 GDPR)

Version: 23 November 2026

> Courtesy translation. In case of discrepancies, the German version prevails.

between

the Ratsch licensee (company, association or other organisation) that uses Ratsch in a professional, association-related or other organisational context

– hereinafter “Controller” –

and

Datafuse SRLs, Rosenheim 21, 39040 Laurein (BZ), Italy · VAT ID: IT03352290211 · Email: info@datafuse.it · Website: https://www.datafuse.it/

– hereinafter “Processor” –

Controller and Processor together also the “Parties”.

1. Subject matter and duration

(1) The subject matter of this agreement is the processing of personal data by the Processor on behalf of the Controller in connection with the use of the “Ratsch” software for recording, transcribing and creating minutes of professional, association-related, organisational or personal meetings, insofar as the Licensee decides on the purposes and essential means of processing and the General Data Protection Regulation applies.

(2) The duration of processing corresponds to the term of the underlying licence agreement. After termination of the licence agreement, return, complete export or deletion takes place in accordance with section 10.

(3) This agreement covers only processing that Datafuse carries out as a processor on behalf of and in accordance with the documented instructions of the Controller. It does not cover independent processing by Datafuse for the general improvement of Ratsch's dialect or speech recognition. For such a purpose of its own, Datafuse is a separate controller; it requires separate information and a separate opt-in by the data subjects. If, on the other hand, processing serves exclusively to improve a function intended only for the respective Licensee or a correction or dialect profile intended only for its users and takes place on its instructions, it may be the subject of this processing relationship.

2. Nature and purpose of processing

(1) The Processor processes personal data only on the documented instructions of the Controller and only for the purposes described in this agreement. It does not determine any purposes of its own for meeting content.

(2) Depending on use, the nature and scope of processing include in particular:

a. receipt, transmission, storage and retrieval of audio recordings, including the import of recordings from Microsoft Teams;
b. conversion of audio into text (transcription) and creation of summaries, minutes, task lists, decisions and, where applicable, translations;
c. management of participant lists, sending of minutes and provision, management and deactivation of read links;
d. storage of attachments to minutes and processing of questions about one's own minutes and the related answers;
e. storage of a user-specific correction memory that assigns corrections exclusively to the respective user or their account and is not used across accounts.

3. Categories of data subjects

Data subjects may in particular be:

a. participants and other data subjects from professional, association-related, organisational or personal meetings, in particular employees, members of governing bodies, members, customers, suppliers and other conversation participants;
b. users of the Controller and account users authorised by it;
c. other recipients of minutes, shared content or read links.

4. Types of personal data

In particular, the following may be processed:

a. contact data, in particular names and email addresses of meeting participants and recipients;
b. communication and content data, in particular audio recordings, transcripts, minutes, summaries, task lists, decisions and, where applicable, translations;
c. metadata on sharing minutes, sending and read links, in particular sending times, recipient addresses and view counts without IP or device data;
d. attachments, in particular documents and photos, and content resulting from or attached to them;
e. questions and answers about one's own minutes, user-specific corrections and technical records of instructions, selections and confirmations, insofar as these are necessary for performing the assignment.

Note: depending on the content of the meeting, special categories of personal data may also be included.

5. Instructions of the Controller

(1) The Controller is solely responsible for the lawfulness of the data processing, including the legal basis, informing the data subjects, safeguarding their rights and defining permissible purposes and retention periods. This also applies where meeting content may contain special categories of personal data.

(2) Instructions are given in particular by electronically accepting this agreement and the underlying licence agreement, by settings in the account, by using and selecting software functions, by written communications or via selection and confirmation processes documented in the software. In each case, the version stored at the time of the instruction, the identity of the accepting or instructing account user and the date and time are decisive, insofar as these details are technically recorded.

(3) The Processor informs the Controller without delay if it considers that an instruction infringes data protection law.

6. Confidentiality

The Processor ensures that the persons authorised to process the data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7. Technical and organisational measures

(1) The Processor takes the technical and organisational measures described in Annex 1.

(2) The Processor is entitled to further develop the measures in line with the state of the art, provided the agreed level of protection is not reduced.

8. Engagement of further processors

(1) The Controller grants the Processor general prior authorisation to engage further processors for the processing described in this agreement. The authorised further processors and the services assigned to them are listed in Annex 2. Services that concern exclusively contract, account, payment or billing data do not constitute processing of meeting content within the meaning of this agreement.

(2) Datafuse informs the Controller of the intended engagement or replacement of a further processor no later than 14 days before the planned start of use. Where available, the information includes the identity and registered office of the further processor, the data categories concerned, the purpose and the place of processing.

(3) Datafuse keeps an up-to-date overview of the further processors used and their services and makes it accessible to the Controller in a suitable manner. The overview in Annex 2 is updated in the event of changes.

(4) Within 14 days of receiving the information, the Controller may object to the engagement or replacement of a further processor for an important and specifically stated data protection reason. The objection must relate to the processing operation concerned.

(5) Datafuse examines the objection and endeavours to find an appropriate solution, in particular by using an equivalent alternative. If the objection cannot be resolved within a reasonable time, the Controller is entitled to terminate the affected service or processing operation with reasonable notice. The other services remain unaffected; any necessary export, return and deletion processes are governed by section 10.

9. Duties to assist

The Processor assists the Controller – where possible and proportionate – in fulfilling its data protection obligations, in particular with:

a. responding to requests from data subjects;
b. ensuring the security of processing;
c. notifying and handling personal data breaches;
d. providing a complete data export and implementing return or deletion instructions;
e. data protection impact assessments and prior consultations.

10. Return and deletion

(1) After the end of the contractual services, the Processor returns or deletes the personal data at the Controller's choice, unless a statutory retention obligation applies. Where technically possible, Datafuse provides the Controller, on request, with a complete export of the meeting content, minutes, attachments, metadata and other assignment-related data stored in its account.

(2) A period of 30 days after termination of the licence agreement or after receipt of the relevant instruction, whichever is later, generally applies to return, complete export and deletion. Within this period, the Controller may request the export, take over data or – where technically possible – request restoration or continuation of the account. After the period expires, Datafuse deletes the data, including any archived data, unless a statutory retention obligation applies; backup copies are overwritten in accordance with the agreed technical and organisational measures. Deviating instructions from the Controller are possible provided they are technically feasible and compatible with legal obligations.

11. Evidence and audits

(1) The Processor provides the Controller with all information necessary to demonstrate compliance with this agreement.

(2) Audits take place after prior notice, during normal business hours and while protecting business and trade secrets; suitable evidence (e.g. reports, certificates, information) should be used primarily.

12. Liability

The liability provisions of the licence agreement apply. Mandatory statutory liability rules remain unaffected.

13. Final provisions

(1) Amendments and additions to this agreement require text form.

(2) Should individual provisions be invalid, the remainder of the agreement remains effective.

(3) Applicable law and place of jurisdiction are governed by the licence agreement.

(4) This agreement can be validly concluded and evidenced by electronic acceptance. Datafuse documents the relevant contract version, the identity of the accepting Licensee or account user

and the date and time of acceptance. Electronic acceptance replaces a signature to the extent permitted by law.

Annex 1 – Technical and organisational measures (TOMs)

1. Access control: role-based permissions, authentication.
2. Transport encryption: encrypted transmission.
3. Storage: encryption of sensitive data.
4. Logging: security and error logs; IP address truncated before storage; automatic rotation and deletion (server logs 7 days, error logs 90 days); access to logs only by authorised administrators.
5. Backup: daily backup (server image) and rolling retention of 7 days; access only for restores and tests by authorised administrators; after a restore, deletions made in the meantime are carried out again.
6. Availability: measures for recoverability.
7. Client separation: logical separation of customer data.
8. Link protection: read links cannot be guessed, are protected by access keys and blocked for search engines; views are counted without IP or device data.
9. Procedures: regular updating and review of the measures.

Annex 2 – Further processors (sub-processors)

The current list is also available online at ratsch.bz/unterauftragsverarbeiter-en.html.

The services listed below are authorised for the purposes stated in each case or are listed to distinguish other Datafuse processing. An authorisation under this agreement exists only insofar as the respective service actually processes meeting content on behalf of the Controller:

1. Hetzner Online GmbH, Germany – hosting, data storage, storage of attachments and backup for meeting content;
2. Microsoft Azure AI Foundry, Sweden Central (EU), where applicable fallback region West Europe (Netherlands) – AI-based transcription, speech processing and creation of minutes; no use of meeting content to train AI models by Microsoft in accordance with the applicable DPA;
3. Hostinger International Ltd. or affiliated Hostinger companies, EU – email and sending service, in particular sending minutes without using a Microsoft account, and processing of the recipient addresses and email content required for this;
4. Fatture in Cloud or TeamSystem S.p.A., Italy/EU – invoicing and processing of contract and billing data; no meeting content;
5. Striptu – transmission of the contract and billing data required for invoicing from Stripe to Fatture in Cloud; no meeting content;
6. Stripe Payments Europe Ltd., Ireland, where applicable affiliated Stripe companies – payment processing and subscription management exclusively for contract, account and payment data. Insofar as Stripe pursues its own purposes for fraud prevention or legal obligations, Stripe acts as an independent controller; meeting content is not the subject of this agreement.

7. Microsoft 365 and Microsoft Graph are not sub-processors of Datafuse within the meaning of this agreement. They are only used when the integration is activated, as a service of the Licensee or its organisation, in particular for sign-in, calendar, OneNote, tasks and sending from the user's own mailbox. The responsible party and the data protection conditions are determined by the Microsoft account or Microsoft 365 contract of the Licensee or its organisation.

Acceptance takes place electronically (checkbox at registration or purchase). Datafuse documents the accepted version, the identity of the account and the date and time; no signature is required.