Standard Data Processing Agreement

DPA / Auftragsverarbeitungsvertrag (AVV)

Version 1.6 · effective 25 August 2026

Processor	Ömer Dertlioglu, operating under the business name SonicR1, Kurfürstendamm 96, 10709 Berlin, Germany (“SonicR1”)
Customer	The legal person or entity identified as the customer in the Main Agreement (“Customer”)
Effective Date	The effective date of the Main Agreement, or the date on which Customer first uses Services involving processing of Customer Personal Data, whichever occurs first
Privacy contact	legal@sonicr1.com (postal: address above). No telephone contact is designated; e-mail is the binding channel.

This Data Processing Agreement (the “DPA”) forms part of the Terms of Service, Subscription Agreement, Order Form, or other agreement governing Customer's use of the SonicR1 services (the “Main Agreement”). It applies whenever SonicR1 processes Personal Data on Customer's behalf. If there is a conflict concerning the processing of Personal Data, this DPA prevails over the Main Agreement to the extent of that conflict.

1. Scope and roles

1.1 Customer is the controller and SonicR1 is the processor with respect to Customer Personal Data, except where Customer acts as a processor for another controller, in which case SonicR1 acts as Customer's subprocessor. Customer represents that it is authorised to appoint SonicR1 in that capacity.

1.2 The subject matter, duration, nature and purpose of the processing, the types of Personal Data, and the categories of Data Subjects are described in Annex 1.

1.3 This DPA applies only to processing carried out by SonicR1 on Customer's behalf. It does not govern data for which SonicR1 independently determines the purposes and means of processing. That data is limited to account administration, billing, fraud prevention and platform security, statutory record-keeping, the retention of call metadata tombstones after a content purge or after deletion under Section 13.2, the retention of consent-attestation and erasure records as evidence for the establishment, exercise or defence of legal claims, and correspondence with Customer's account contacts about the contractual relationship, and is governed by the SonicR1 Privacy Policy. SonicR1 does not process call audio, transcripts, knowledge-base content, CRM or calendar content, or AI outputs derived from them for any purpose of its own.

1.4 Where Customer acts as a processor for another controller: (a) Customer warrants that its documented instructions are consistent with the instructions it has received from that controller; (b) Customer exercises the rights under Sections 8, 12 and 13 on that controller's behalf and passes on to it the information SonicR1 makes available under Sections 9.2, 10.2 and 11; (c) Customer warrants that this DPA meets the requirements its own agreement with that controller imposes on subprocessors; and (d) SonicR1 owes the obligations in this DPA to Customer alone and is not required to deal directly with that controller.

2. Definitions

2.1 “Customer Personal Data” means Personal Data processed by SonicR1 on behalf of Customer in connection with the Services.

2.2 “Data Protection Laws” means the GDPR, the German Federal Data Protection Act (BDSG), and other applicable laws governing the processing of Personal Data under the Main Agreement.

2.3 “EEA” means the European Economic Area. “GDPR” means Regulation (EU) 2016/679. “Personal Data”, “processing”, “controller”, “processor”, “Data Subject”, “Personal Data Breach”, and “supervisory authority” have the meanings given in the GDPR.

2.4 “Subprocessor” means a third party engaged by SonicR1 to process Customer Personal Data on behalf of Customer.

2.5 “Approved Global Processing” means a workspace setting or other documented instruction by which Customer authorises specifically approved AI processing outside the EEA. It is a processing permission, not a storage location, and does not change the EU storage location of SonicR1-hosted customer records. As of this version, no Customer Personal Data is routed to a non-EEA AI inference endpoint and no non-EEA language-model processing option is enabled (see Section 11.4 and Annex 2); the setting has no effect until Annex 2 is updated in accordance with Section 10.

2.6 “Services” means the SonicR1 services made available to Customer under the Main Agreement.

3. Documented instructions

3.1 SonicR1 shall process Customer Personal Data only on Customer's documented instructions, unless processing is required by Union or Member State law. The Main Agreement, this DPA, Customer's configuration and use of the Services, and written support or implementation requests constitute documented instructions. Configuration and use of the Services constitute instructions only within the functionality the Services present. Mere use of the Services is not an instruction under Section 6.4 or Section 11.2; an instruction under Section 6.4, and an instruction under Section 11.2 to transfer Customer Personal Data to a recipient that is neither an authorised Subprocessor listed in Annex 2 nor a third-party system Customer has itself connected under Annex 1, Part E, each require a separate express instruction in writing. Customer's enabling of Approved Global Processing under Section 3.4, and Customer's connection and configuration of its own third-party systems under Annex 1, Part E, are documented instructions for the purposes of Section 11.2.

3.2 If applicable law requires SonicR1 to process Customer Personal Data other than on Customer's instructions, SonicR1 shall inform Customer of that legal requirement before processing, unless the law prohibits such notice on important grounds of public interest.

3.3 SonicR1 shall immediately inform Customer if, in SonicR1's opinion, an instruction infringes Data Protection Laws. SonicR1 may suspend the affected processing until the parties agree on a lawful instruction.

3.4 Should a non-EEA AI provider be approved in the future, Customer's enabling of Approved Global Processing would constitute a documented instruction to use the provider(s) then identified in Annex 2 for the capabilities covered by that setting. SonicR1 shall not infer or enable that permission based on IP address, locale, billing address, or similar signals.

4. Customer responsibilities

4.1 Customer is responsible for the lawfulness, fairness, transparency, accuracy, and scope of Customer Personal Data and Customer's instructions. Customer shall provide all required notices and establish an appropriate legal basis for processing, including for employees, sales representatives, prospects, customers, and other call participants.

4.2 Customer is responsible for complying with applicable telecommunications, call-recording, workplace, employment, co-determination, and consent requirements. SonicR1 provides technical consent and disclosure features but does not determine whether a particular call may lawfully be recorded or analysed.

4.3 Customer shall not intentionally submit special categories of Personal Data under Article 9 GDPR, criminal-conviction data under Article 10 GDPR, or highly regulated data unless the parties have expressly agreed appropriate instructions and safeguards in writing. The parties acknowledge that free-form speech and text may incidentally contain such data.

4.4 Customer shall configure user access appropriately, protect credentials, review AI-generated outputs before relying on them, and ensure that Customer's use of coaching scores or analytics complies with applicable employment and AI-governance requirements.

5. Confidentiality and personnel

5.1 SonicR1 shall ensure that persons authorised to process Customer Personal Data are bound by confidentiality obligations or an appropriate statutory duty of confidentiality.

5.2 SonicR1 shall limit access to persons who require it to provide, secure, support, or maintain the Services and shall provide appropriate privacy and security guidance for those persons.

6. Security of processing

6.1 SonicR1 shall implement and maintain appropriate technical and organisational measures to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Personal Data. The current measures are described in Annex 3.

6.2 SonicR1 may update the measures to reflect technical progress, changes in the Services, or evolving risks, provided that the overall level of protection is not materially reduced during the term.

6.3 Customer acknowledges that security is a shared responsibility and shall use the security and access-control features made available by SonicR1, including role assignments, approved integrations, consent controls, retention settings, and data-region settings.

6.4 SonicR1 shall not itself use Customer Personal Data to train a shared or general-purpose model without Customer's documented instruction. SonicR1 shall use the provider account controls and contractual terms available to it to restrict Subprocessor use of Customer Personal Data for shared-model improvement; specifically, SonicR1's speech-to-text account (AssemblyAI) is enrolled in the provider's model-improvement opt-out and an account-level time-to-live of one (1) day for provider-side audio and transcripts is configured (see Annex 2).

6.5 SonicR1 maintains a process for regularly testing, assessing and evaluating the effectiveness of the measures in Annex 3, as required by Article 32(1)(d) GDPR. Automated tests enforcing the regional egress and access-control boundaries run on every change to the code base, and SonicR1 reviews and documents the measures at least once every twelve (12) months and after any material change to the Services, the architecture, or the Subprocessors. The date of the most recent review is available to Customer on request via legal@sonicr1.com.

7. Personal Data Breach

7.1 SonicR1 shall notify Customer without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Personal Data Breach affecting Customer Personal Data. Notice shall be given by e-mail to Customer's account owner and to any administrator or privacy contact designated by Customer.

7.2 Taking into account the nature of the processing and the information available to SonicR1, the notice shall include, to the extent known: the nature of the breach; the categories and approximate number of affected Data Subjects and records; likely consequences; measures taken or proposed; and a contact point for further information. Information may be provided in phases where it is not available at the same time.

7.3 SonicR1 shall take reasonable steps to contain, investigate, mitigate, and remediate the breach and shall reasonably cooperate with Customer's obligations under Articles 33 and 34 GDPR. Notification is not an admission of fault or liability.

8. Data Subject requests

8.1 Taking into account the nature of the processing, SonicR1 shall assist Customer by appropriate technical and organisational measures, insofar as possible, to fulfil Customer's obligations to respond to requests under Articles 12 to 23 GDPR.

8.2 If SonicR1 receives a request directly from a Data Subject concerning Customer Personal Data, SonicR1 shall not respond on Customer's behalf unless authorised or legally required, and shall forward or direct the request to Customer where reasonably possible.

8.3 Customer may request access to Customer Personal Data and its export, correction, and deletion by contacting the SonicR1 privacy contact identified in Annex 4; SonicR1 assists with such requests in accordance with Section 8.1. Where SonicR1 makes self-service functions for these requests available in the Services, Customer shall use them before requesting manual assistance. SonicR1 may charge reasonable costs for exceptional, repetitive, or technically bespoke assistance not included in the Services, where permitted by the

Main Agreement and applicable law, subject to the cost-estimate procedure in Section 9.3.

9. Assistance with compliance

9.1 Taking into account the nature of processing and information available to SonicR1, SonicR1 shall reasonably assist Customer with its obligations under Articles 32 to 36 GDPR, including security assessments, breach obligations, data protection impact assessments, and prior consultation with supervisory authorities.

9.2 SonicR1 shall make available the information reasonably necessary to demonstrate compliance with Article 28 GDPR, including this DPA, relevant security documentation, and information concerning Subprocessors and international transfers.

9.3 Assistance under Sections 8 and 9 is provided taking into account the nature of the processing and the information available to SonicR1. Where Customer requests assistance that is repetitive, materially exceeds Annex 3 and SonicR1's standard security documentation, or requires bespoke technical work, SonicR1 may charge its reasonable documented costs, provided SonicR1 notifies Customer of the estimated cost in text form and Customer agrees to it before the work begins.

10. Subprocessors

10.1 Customer grants SonicR1 general authorisation to engage the Subprocessors listed in Annex 2 and to add or replace Subprocessors in accordance with this Section.

10.2 SonicR1 shall provide at least thirty (30) days' prior notice of an intended addition or replacement of a Subprocessor by e-mail to Customer's account owner or administrator contact; SonicR1 may additionally use in-product notice. SonicR1 shall keep the Subprocessor information in Annex 2 (including provider identity, country, purpose, data categories, location and transfer mechanism, with links to the legal pages on which each provider publishes its data-processing terms or, where the terms were concluded by signature, a note to that effect, and, where the provider maintains one, a link to its own subprocessor list) current, and shall provide it to Customer at any time via legal@sonicr1.com. Where a Subprocessor must be added or replaced at shorter notice to preserve the security or continuity of the Services — for example because a provider ceases to supply the service, becomes insolvent, or is replaced following a security incident — SonicR1 shall give notice as soon as reasonably possible together with the reason. Customer may object under Section 10.3 within thirty (30) days of that notice; neither prohibition in Section 10.3 on engaging the Subprocessor applies to such a replacement, and if the objection is not resolved the remedies in Section 10.3 apply.

10.3 Customer may object during the notice period on reasonable and documented data-protection grounds. SonicR1 shall not engage the proposed Subprocessor for Customer Personal Data during the notice period or while a timely objection remains unresolved. The parties shall work in good faith to resolve the objection. If no commercially reasonable resolution is available, SonicR1 may discontinue the affected feature or Customer may terminate the affected Services; in either case Customer receives a pro-rata refund of prepaid fees covering the unused period following discontinuation or termination.

10.4 SonicR1 shall impose data-protection obligations on each Subprocessor that provide at least the level of protection required by Article 28(4) GDPR — through the provider's data-processing terms and, where a provider requires separate execution, through a countersigned provider DPA — and shall remain responsible to Customer for the Subprocessor's performance of those obligations. The “Transfer safeguards” column of Annex 2 names the instrument for each Subprocessor and states the date of execution where the terms were separately executed; where no date is stated, the provider's terms are incorporated on acceptance of its online terms. SonicR1 shall not disclose Customer Personal Data to a Subprocessor before those written terms are in force. Annex 2 records the instrument for each Subprocessor and, where the terms were concluded by separate execution, the date of execution. Where a provider's terms are incorporated on acceptance of its online terms, they were in force before any Customer Personal Data was disclosed to that provider.

11. International transfers

11.1 SonicR1 stores the customer records it hosts — account and workspace data, retained call audio, transcripts, AI outputs, and knowledge-base content — in the EU, and routes all AI inference through EU endpoints. Hosting, logging and control-plane data, background-orchestration step state (which may contain

conversation-derived text), and transactional e-mail content and metadata, are processed in part outside the EU as set out in Section 11.5 and Annex 2. The detailed current processing topology is described in Annexes 1 to 3.

11.2 SonicR1 shall not transfer Customer Personal Data to a third country or international organisation except on Customer's documented instructions or as necessary to provide the Services using an authorised Subprocessor, and only where a valid transfer mechanism and any required supplementary measures are in place. As at the effective date of this version, written data-protection terms and, where applicable, a transfer mechanism are in force with every Subprocessor listed in Annex 2. SonicR1 shall report their current status to Customer on request via legal@sonicr1.com.

11.3 Where applicable, transfer mechanisms may include an adequacy decision, participation in the EU-U.S. Data Privacy Framework by an eligible recipient, or the European Commission Standard Contractual Clauses adopted by Implementing Decision (EU) 2021/914 — Module 3 (processor to processor) where SonicR1 transfers Customer Personal Data to a Subprocessor — together with supplementary measures where required.

11.4 As of this version, no Customer Personal Data is routed to a non-EEA AI inference endpoint and no non-EEA language-model processing option is enabled; all AI inference runs on EU endpoints. For clarity: some providers of EU-endpoint processing (for example AssemblyAI, Inc. for speech-to-text) are established in the United States — their legal establishment is distinct from the processing endpoint, and Annex 2 identifies both. The Approved Global Processing mechanism (Sections 2.5 and 3.4) exists in the product but has no effect until a provider is added to Annex 2 with notice under Section 10.

11.5 Regional deployment labels do not necessarily determine the location of a provider's account data, control plane, support access, logs, or metadata. Annex 2 identifies known limitations, including Resend's storage of account data, message content and e-mail metadata in the United States regardless of the selected sending region, and Inngest's US-hosted data stores, which receive job identifiers, execution metadata and the return values of workflow steps — including pseudonymised transcript text and, for CRM write jobs, the generated write payload with tokens resolved back to their original values, together with derived call metrics — and, for transactional-e-mail jobs, the recipient's e-mail address and the variables required to render the message, which may include the name or e-mail address of another workspace member named in the notice.

11.6 SonicR1 shall conclude, in its own name as data exporter, the Standard Contractual Clauses adopted by Implementing Decision (EU) 2021/914, Module 3 (processor to processor), with each Subprocessor that processes Customer Personal Data in a third country, including by accepting them through that provider's data-processing terms. Customer, as controller or on the controller's behalf where Section 1.4 applies, authorises SonicR1 to conclude those clauses and to agree their annexes consistently with Annexes 1 to 4 of this DPA; Customer — or, where Section 1.4 applies, the controller on whose behalf Customer acts — is a third-party beneficiary of them. Annex 2 records, for each Subprocessor, the clauses concluded and, where they were concluded by separate execution, the date of execution. Where a Subprocessor requires the controller itself to sign, SonicR1 shall obtain Customer's separate written authority first. SonicR1 shall make the clauses so concluded available to Customer on request via legal@sonicr1.com.

11.7 Where Customer is established outside the EEA and SonicR1 makes Customer Personal Data available to Customer, the Standard Contractual Clauses adopted by Implementing Decision (EU) 2021/914, Module 4 (processor to controller), are incorporated into this DPA by reference, with SonicR1 as data exporter and Customer as data importer; Annexes 1 to 3 of this DPA populate the annexes to those clauses, and the contacts in Annex 4 are the parties' contact points. For those clauses the parties agree that the optional docking clause in Clause 7 applies, that the optional language in Clause 11(a) does not apply, that the governing law under Clause 17 is the law of Germany, and that the courts of Berlin, Germany are designated under Clause 18(b). For transfers subject to United Kingdom law, the UK International Data Transfer Addendum applies to those clauses; for transfers subject to Swiss law, they apply with the amendments published by the Swiss Federal Data Protection and Information Commissioner. Where such a transfer is made to a Subprocessor, SonicR1 shall conclude the corresponding addendum or amendments with that Subprocessor, and Annex 2 records where it has done so.

12. Audits and inspections

12.1 SonicR1 shall allow for and contribute to audits, including inspections, by Customer or an independent auditor mandated by Customer, as required by Article 28(3)(h) GDPR.

12.2 Audits shall ordinarily begin with a review of this DPA, Annex 3, and SonicR1's written responses to Customer's security questionnaire, together with any certification or independent assurance report SonicR1 holds at the time. SonicR1 holds no SOC 2 or ISO/IEC 27001 certification of its own and operates no data centre; hosting is provided by the Subprocessors listed in Annex 2, whose own assurance reports are available from those providers. On-site or intrusive technical audits are limited to systems and records under SonicR1's control; SonicR1 shall permit such an audit where the foregoing information is insufficient to address a reasonable, specific compliance concern, and may offer supervised remote access instead where that addresses the concern.

12.3 Unless a Personal Data Breach, supervisory-authority request, or reasonable evidence of material non-compliance justifies otherwise, Customer may conduct one audit in any twelve-month period, with at least thirty (30) days' notice, during normal business hours, subject to confidentiality, security, and non-disruption requirements.

12.4 Customer shall bear its audit costs and SonicR1's reasonable documented costs of exceptional assistance, subject to the cost-estimate procedure in Section 9.3, unless the audit identifies material non-compliance by SonicR1, in which case SonicR1 shall bear its own costs of assistance and of remediation and shall not charge them to Customer. SonicR1 may object to a proposed auditor only on the basis of a documented conflict of interest, confidentiality risk, or security risk, in which case Customer selects another suitably qualified independent auditor; the final choice of auditor remains with Customer. The auditor shall protect other customers' information and SonicR1's confidential information.

13. Return and deletion

13.1 During the term, Customer may use available export and deletion functions and may configure retention or ephemeral modes where offered by the Services. Annex 1, Part D sets out the retention periods and plan caps applied to stored call content, the cases in which no automatic purge runs, and the deletion rules applied to derived data.

13.2 Upon termination of the Services involving processing, SonicR1 shall, at Customer's choice, return or delete Customer Personal Data. A return comprises all Customer Personal Data then held by SonicR1, other than the AI-generated evaluations dealt with below, provided as a machine-readable export through the Services' export functions where those cover the data and by another reasonable means agreed between the parties where they do not, in each case within fourteen (14) days of Customer's request and without additional charge for one export per termination. As a technical and organisational measure under Section 6.1 and Annex 3, AI-generated evaluations of an individual user are disclosed only to that user and are therefore not part of a standard return to Customer, but SonicR1 shall provide them to Customer where Customer requires them to respond to a request under Articles 15 to 22 GDPR or to meet another legal obligation. Customer may request an export within thirty (30) days following termination; after that period (or earlier on Customer's instruction), SonicR1 shall delete active Customer Personal Data within a further thirty (30) days, unless Union or Member State law requires retention. Deletion following termination is carried out against a documented deletion specification that classifies every table carrying a workspace, project, organisation or call identifier; tables holding data only as children of such a table are covered where the parent is deleted. Execution is automated: the workspace is queued for deletion, remains retrievable for the period stated above, and is then purged by a scheduled job without operator intervention. An operator-run tool applies the same specification where a deletion has to be started or completed by hand. Simulation and role-play practice conversations are bound to the individual user rather than to the workspace: on deletion under this Section the workspace link is removed and the record remains bound to the user who created it, unless Customer instructs SonicR1 to delete them, in which case SonicR1 shall do so. SonicR1 shall confirm completion of deletion upon request.

13.3 Data in backups shall be deleted through the hosting provider's ordinary backup lifecycle. The production database currently uses a rolling seven (7)-day daily-backup window (provider setting, verified 22 July 2026); in any event, backup copies expire no later than thirty-five (35) days after deletion of the active data and remain protected and unavailable for ordinary use until deletion. If restoration of a backup reintroduces deleted

Customer Personal Data, SonicR1 shall reapply the relevant deletion where reasonably possible.

13.4 SonicR1 shall retain Customer Personal Data in its capacity as processor beyond the periods set out in this Section and in Annex 1, Part D only where Union or Member State law requires storage, save for the two suspensions disclosed in Annex 1, Part D. Where SonicR1 retains consent-attestation and erasure records as evidence for the establishment, exercise or defence of legal claims, it does so as a controller for that purpose alone (Section 1.3); those records contain no conversation content and are isolated and access-restricted. Where SonicR1 retains metadata tombstones after a content purge or after deletion under Section 13.2 — a call row reduced to identifiers, timestamps, duration, status and the purge marker, containing no conversation content — it does so as a controller for billing and usage integrity and abuse prevention alone (Section 1.3), and deletes them when the workspace is closed. The operational retention periods for active systems, temporary artefacts, exports, logs, and consent-attestation evidence are documented in Annex 1, Part D.

14. Government and law-enforcement requests

14.1 Unless prohibited by law, SonicR1 shall notify Customer of a legally binding request by a public authority for Customer Personal Data. SonicR1 shall review the request for validity, challenge unlawful or disproportionate requests where there are reasonable grounds to do so, and disclose only the minimum data legally required.

15. Liability

15.1 Liability between the parties arising from this DPA is subject to the limitations and exclusions in the Main Agreement, to the extent permitted by Data Protection Laws.

15.2 Nothing in this DPA limits any rights of Data Subjects or powers of supervisory authorities, or allocates responsibility in a manner that conflicts with Articles 82 or 83 GDPR.

15.3 Where one party has paid compensation under Article 82 GDPR for damage caused in whole or in part by the other party's breach of this DPA or of the obligations Data Protection Laws impose on that other party, the paying party may claim back from the other party the share of the compensation corresponding to the other party's part of the responsibility, in accordance with Article 82(5) GDPR; Section 15.1 does not limit that statutory claim. Where a party has paid an administrative fine under Article 83 GDPR that was caused in whole or in part by the other party's breach of this DPA, it may claim compensation from that other party to the extent applicable law permits; claims under this sentence are subject to Section 15.1.

16. Term, precedence, and changes

16.1 This DPA remains in effect for as long as SonicR1 processes Customer Personal Data.

16.2 If this DPA conflicts with the Main Agreement concerning Personal Data processing, this DPA prevails. The European Commission Standard Contractual Clauses, where applicable, prevail over inconsistent terms of this DPA.

16.3 SonicR1 may amend this DPA only (i) to reflect a change in Data Protection Laws or a binding decision of a supervisory authority or court, (ii) to reflect a change to the Services or to the Subprocessors made in accordance with Section 10, (iii) to reflect an update to the technical and organisational measures permitted by Section 6.2, or a re-verification of the factual statements in Annexes 1 to 3, provided the overall level of protection is not reduced, or (iv) to increase the level of protection of Customer Personal Data. SonicR1 shall give at least thirty (30) days' prior notice of a material amendment by e-mail to Customer's account owner or administrator contact, except where the amendment reflects a Subprocessor addition or replacement for which Section 10.2 permits shorter notice, in which case the notice period and reason requirement in Section 10.2 apply; and Customer may object during that period on reasonable and documented data-protection grounds, in which case the procedure and remedies in Section 10.3 apply. No amendment shall, during a current subscription term, materially reduce the level of protection of Customer Personal Data or expand the purposes of processing; a materially different international-transfer risk may be introduced only through a Subprocessor change made in accordance with Section 10, to which Customer's objection right and the remedies in Section 10.3 apply.

17. General

17.1 This DPA is governed by German law, without prejudice to the mandatory application of Data Protection Laws and the governing-law provisions of any applicable Standard Contractual Clauses. The courts of Berlin, Germany have jurisdiction to the extent permitted by law and the Main Agreement.

17.2 Notices under this DPA shall be sent using the notice mechanisms in the Main Agreement. Data-protection communications to SonicR1 shall be sent to legal@sonicr1.com.

17.3 If any provision is invalid or unenforceable, the remaining provisions remain effective. The parties shall replace the affected provision with a lawful provision that most closely reflects its purpose.

17.4 This DPA is concluded in English. Any translation, including the German reading version published by SonicR1, is provided for convenience only; in the event of a discrepancy, the English version governs.

Acceptance and optional signature

This DPA is binding when incorporated into or accepted with the Main Agreement. If the parties choose to sign a separate copy, the signature blocks in the PDF version may be used; an electronic signature and counterparts are permitted. Download the PDF via the link at the top of this page and return the countersigned copy to legal@sonicr1.com.

Annex 1 — Details of processing

Subject matter	Provision of the SonicR1 AI-assisted sales intelligence, live coaching, call analysis, training, knowledge-base, calendar, CRM integration, reporting, collaboration, support, security, and related SaaS functions.
Duration	For the term of the Main Agreement and thereafter until Customer Personal Data has been returned or deleted in accordance with Section 13 and the retention rules in Part D.
Frequency	Continuous, recurring, or on-demand depending on Customer's use and configuration of the Services.
Nature of processing	Collection, receipt, capture, recording where enabled, transmission, transcription, organisation, structuring, storage, retrieval, consultation, redaction, pseudonymisation/tokenisation, analysis, AI inference, generation, scoring, summarisation, display, integration, export, restriction, support access, and deletion.
Purposes	To provide and secure the Services; transcribe and analyse sales conversations; generate live and post-call coaching; prepare summaries, scorecards, recommended actions and drafts; operate role-play and training; ground outputs in Customer knowledge; synchronise Customer-selected CRMs and calendars; provide team/admin functionality; troubleshoot; prevent abuse; and comply with documented Customer instructions.

A. Categories of Data Subjects

- Customer users, including sales representatives, account executives, managers, administrators, owners, viewers, contractors, and support contacts.
- Prospects, customers, partners, suppliers, and other third parties participating in, mentioned during, or otherwise connected with calls or meetings.
- Contacts, leads, account personnel, opportunity participants, and other individuals contained in Customer-selected CRM and calendar systems.
- Authors, contacts, employees, customers, and other identifiable persons whose information appears in uploaded knowledge-base documents, playbooks, e-mail drafts, meeting descriptions, or free-text fields.
- Invitees and recipients of transactional account, workspace, support, security, and integration e-mails.

B. Categories of Personal Data

Category	Examples
Account and identity data	Names, usernames, profile details, job titles, roles, organisation/workspace membership, user identifiers, authentication and invitation metadata.

Category	Examples
Business contact and CRM data	Business e-mail addresses, telephone numbers, company and account details, lead/contact records, opportunity/deal data, pipeline stage, notes, activities, relationship history, and Customer-selected CRM fields.
Calendar and meeting data	Meeting title, time, participants, contact details, provider, description, join link, agenda and associated preparation information.
Call and audio data	Live or uploaded audio where enabled, speaker/channel information, timing, language, and related capture metadata. SonicR1 does not use voice for biometric identification and does not perform acoustic voice-tone emotion inference.
Transcript and conversation content	Transcripts, words spoken, chat/free text, questions, objections, claims, commitments, product and commercial discussions, and other content supplied during calls or uploads.
AI-generated and inferred data	Live coaching cards, suggested responses, summaries, scorecards, coaching moments, skill and performance analytics, benchmarking, textual sentiment, deal intelligence, next actions, e-mail drafts, CRM previews, classifications, and model-output metadata.
Knowledge-base and uploaded content	Product, competitor, persona, process, playbook, document, URL-import, and other materials uploaded or connected by Customer, including Personal Data contained in them.
Technical, usage and security data	IP address, device/browser and session metadata, timestamps, application events, audit and access logs, consent-attestation metadata, integration identifiers, diagnostic data, error records, rate-limit keys and security events.
Support and implementation data	Support communications, configuration requests, screenshots, diagnostic information, and content Customer chooses to share for troubleshooting.
Transactional e-mail data	Recipient e-mail address, delivery and event metadata, subject and message content required for invitations, authentication, security, support, and service notifications.

C. Special categories and sensitive data

Special categories of Personal Data and criminal-conviction data are not required or intended for ordinary use. Because calls, CRM notes and uploaded documents are free-form, such data may be incidentally included. Customer shall not intentionally direct SonicR1 to process such data unless it has established a lawful basis and the parties have agreed any necessary additional safeguards. Voice/audio data is not processed by SonicR1 for unique biometric identification. Sentiment is derived from transcript text, not from biometric or acoustic affect analysis.

D. Retention and deletion (operational, as implemented)

• Ephemeral live mode (default): call audio, transcript context and rolling coaching state exist only for the live session and are not stored as reusable call content, except limited operational, security and consent-attestation metadata.

• Stored call content — retention window applied by the scheduled purge, by plan: Free 7 days · Solo 3 months · Growth 12 months · Scale 24 months · Enterprise custom/configured. A workspace setting may shorten the window within the plan's cap but never extend it. A scheduled nightly purge job enforces these windows. An anomaly circuit breaker halts the entire scheduled run — for all workspaces, not only the one whose count is abnormal — where the matched-call count exceeds the configured safety limit, so that the run can be reviewed before any deletion; while a run is halted the windows in this Part are not enforced. SonicR1 is alerted automatically, reviews a halted run and completes the deletions without undue delay and in any event within ten (10) days of the halt, so a window may be exceeded by up to ten (10) days. Where a paid subscription lapses, the scheduled purge deliberately does not apply a lower plan's shorter window to content created under the higher plan, and no automatic purge then runs for that workspace unless Customer has configured a retention setting, which continues to be enforced. This is a fail-safe against billing errors, not a retention right of SonicR1's own: the content remains Customer Personal Data processed solely as processor (Section 1.3), Customer may delete it or shorten the window at any time, and Section 13.2 applies in full once the Services terminate. Customer may additionally delete calls at any time using the in-product deletion controls. On expiry, transcripts, AI outputs and derived analyses are deleted and audio objects removed from storage; a metadata tombstone remains.

• Priority rule for derived data: AI outputs derived from a call (debrief modules, scores, summaries) are deleted no later than the underlying call-content deadline — the retention purge removes them together with the call — unless a shorter feature-specific period applies.

• AI debrief outputs (independent ceiling): additionally deleted after 365 days by default (workspace-configurable), even where the call itself is retained longer.

• PII redaction map (re-identification keys): re-identification keys relating to deleted call content are deleted together with that call, in the same purge operation. For calls still retained, the map is additionally deleted at its own TTL (90 days by default, workspace-configurable 7–3650 days); after map deletion, stored content is permanently pseudonymised. The map contains token-to-identifier mappings only, never conversation content.

• Exports: download links for standard exports are signed for 7 days, and a nightly reaper deletes the generated file once the job is older than 7 days. Data-subject and portability requests are fulfilled by SonicR1 on request rather than through a self-service expiring link; the resulting file is deleted once delivered and in any event within 30 days.

• Speech-to-text provider copies: an account-level time-to-live of 1 day is configured at the provider (AssemblyAI); provider-side audio and transcripts are deleted thereafter. Limited provider metadata is retained by the provider for logging and billing under its own terms.

• Consent-attestation and erasure logs: append-only at database level, contain no conversation content, and are retained as evidence for the establishment, exercise or defence of legal claims. They are deliberately excluded from the automated purges and from account deletion; SonicR1 reviews them after the end of the third calendar year following account closure and deletes those no longer required for that purpose.

• Metadata tombstones: after a content purge, the call row retains only identifiers, timestamps, duration, status and the purge marker — kept for billing/usage integrity, abuse prevention and referential consistency (a separate, limited purpose from call content); deleted with the workspace. Where an individual member deletes their own account, the call row belongs to the workspace and remains: only the member's user reference is removed from it.

• Other records retained beyond deletion: acceptance evidence for the Terms and this DPA, including the e-mail address that accepted them; the deletion-request record itself; the workspace offboarding record, which is what allows completion of a deletion to be confirmed under Section 13.2; the address entry on the do-not-send suppression list, retained so that suppression keeps working once the account behind it is gone; and workspace billing data and monthly usage aggregates. None of these records contains conversation content.

• Background-orchestration event payloads carry identifiers rather than call content, and content is retrieved from the authorised workspace data store at execution. Where a workflow step returns content, the orchestration provider persists that return value as step state in order to resume a run (Annex 2); step state is retained under that provider's own terms.

• Backups: rolling 7-day daily database-backup window (provider setting, verified 22 July 2026); contractual ceiling: copies expire no later than 35 days after deletion of active data (Section 13.3).

E. Customer instructions affecting location and recipients

• The default instruction is EU residency and regional-only AI processing. As of this version, no Customer Personal Data is routed to a non-EEA AI inference endpoint and no non-EEA language-model option is enabled, so all AI inference runs on EU endpoints regardless of workspace settings.

• Customer may connect and instruct transfers to its own CRM, calendar, conferencing, or other third-party systems. Those services are selected and contracted by Customer and are not SonicR1 Subprocessors merely because SonicR1 transmits data to them on Customer's instruction.

Annex 2 — Authorised Subprocessors

Provider identity, purpose, data categories and processing location were verified against the production code base and configuration on 25 August 2026; entries that depend on a provider account setting carry the date on which that setting was last checked in the provider's own console. A regional service endpoint does not necessarily localise provider account data, logs, support access, or control-plane data. Provider identity (legal

entity and country), purpose, data categories, location and transfer mechanism are maintained here; each provider's registered-office details and its own downstream subprocessor list are available at the provider legal pages referenced below, and this information is provided to Customer at any time via legal@sonicr1.com. Changes follow Section 10 (30 days' e-mail notice; shorter, with the reason, where Section 10.2 permits a security- or continuity-driven replacement).

Subprocessor	Purpose	Data	Location / processing	Transfer safeguards
Google Cloud EMEA Limited (Dublin, Ireland; Google Cloud Platform)	Vertex AI / Gemini AI text processing; cloud text-to-speech for simulation voices	Transcript and prompt text and model outputs. Call transcript content passes through the redaction layer described in Annex 3 before egress; uploaded knowledge-base documents, imported URL text, briefing and pre-call inputs and knowledge-base questions are sent unredacted, as they carry no call context to tokenise against. TTS receives AI persona text only	Google's EU multi-region AI endpoint (“eu”, requests pinned inside the EU geography) for the current default model, with dedicated EU regions (europe-west1/ west3/west4) for models served there and for failover; the failover chain is restricted to an EU-only location allowlist. TTS via EU endpoint	Google Cloud Data Processing Addendum (auto-incorporated; cloud.google.com/terms/data-processing-addendum); SCCs (2021/914, Module 3 — processor to processor) as incorporated there for any third-country support/ancillary access
AssemblyAI, Inc. (US)	Batch and streaming speech-to-text	Live/uploaded call audio, transcripts, timing/language/speaker metadata	EU API and streaming endpoints (Dublin, Ireland), enforced fail-closed in the application. Account: enrolled in the provider's model-improvement opt-out, with a provider-side time-to-live of 1 day (provider console, checked 22 July 2026)	Provider DPA (assemblyai.com/legal/data-processing-addendum) incl. SCCs (2021/914, Module 3 — processor to processor) for any third-country access; US-established provider, EU processing endpoints
Supabase, Inc. (US)	Database, authentication, object/file storage and related backend services; authentication e-mail	Account/workspace records, call files, transcripts, AI outputs, CRM snapshots, knowledge content, logs	Production project region: Central EU (Frankfurt) (provider console, checked 22 July 2026)	Provider DPA (supabase.com/legal/dpa) incl. SCCs (2021/914, Module 3 — processor to processor) for any third-country support access
Vercel Inc. (US)	Application hosting, serverless compute, deployment, edge delivery and logs	Request content as necessary, IP/device/request metadata, application logs, transient customer content	Application compute pinned to fra1 (Frankfurt); Vercel also operates a global edge/control-plane network — fra1 is not represented as complete account/log residency	Provider DPA (vercel.com/legal/dpa) incl. SCCs (2021/914, Module 3 — processor to processor)

Subprocessor	Purpose	Data	Location / processing	Transfer safeguards
Inngest, Inc. (US)	Background-job and workflow orchestration	Job identifiers (call/run/intent IDs) and execution metadata. Because the provider persists the return value of each workflow step in order to resume a run, its data stores also receive step outputs: these include pseudonymised (tokenised) transcript text used for post-call analysis and, for CRM write jobs, the generated write payload with tokens resolved back to their original values — note subject and body, task titles and descriptions, deal-property values and stage-change reasons. Post-call steps additionally return derived call metrics, including an AI call score and talk ratio. No call audio is sent. Transactional-e-mail jobs additionally carry the recipient's e-mail address and the variables required to render the message, which may include the name or e-mail address of another workspace member named in the notice	Provider states its data stores are hosted in the United States (AWS)	Entity: Inngest Inc, 1039 Iroquois Blvd, Royal Oak, MI 48067, US. Provider DPA executed 4 August 2026 (Common Paper Data Processing Agreement, Standard Terms v1.0), incorporating the Standard Contractual Clauses (2021/914) — Module 3 (processor to processor), SonicR1 acting as Customer's processor and the provider as SonicR1's Subprocessor — together with the UK addendum for transfers subject to United Kingdom law. No call audio is routed through this provider
Upstash, Inc. (US)	Rate limiting and related serverless data functions	Pseudonymous keys/IDs, counters, timestamps and rate-limit metadata; no call content by design	Deployed database region: AWS eu-central-1 (Frankfurt) (provider console, checked 22 July 2026)	Provider DPA (upstash.com/trust/dpa.pdf) incl. SCCs (2021/914, Module 3 — processor to processor)
Fly.io, Inc. (US)	Hosting of simulation call agent and self-hosted speech components	Training/simulation audio or text and transient service metadata, depending on feature use	Configured region fra (Frankfurt) for all workloads	EU-U.S. Data Privacy Framework participant; provider DPA executed 22 July 2026 by both parties, incl. SCCs (2021/914) accepted through the addendum signature; provider retains platform data for 90 days after termination

Subprocessor	Purpose	Data	Location / processing	Transfer safeguards
Plus Five Five, Inc., trading as Resend (US)	Transactional e-mail delivery	Recipient e-mail addresses, message content, delivery events, e-mail metadata, logs and API records	Sending routed through Ireland (EU sending region; provider console, checked 22 July 2026); provider stores account data, message content, metadata, logs and API records in the United States regardless of sending region	Provider DPA auto-incorporated (resend.com/legal/dpa): SCCs (2021/914, Module 3 — processor to processor) and EU-U.S. DPF certification

Approved global AI providers

None. No non-EEA AI inference provider is currently approved or engaged. Before any such provider is engaged (for example for future advanced-analysis capabilities), it will be added to this Annex with notice under Section 10, and the Approved Global Processing setting will remain without effect until then.

Customer-selected external services

CRM, calendar, conferencing and sales systems selected and connected by Customer — for example HubSpot, Salesforce, Pipedrive, Zoho, Monday, Close, Attio, Google Calendar, Microsoft Outlook, Calendly, Google Meet, Microsoft Teams or Zoom — are not automatically SonicR1 Subprocessors. SonicR1 transmits data to those services on Customer's instruction, and Customer is responsible for its contracts, settings and lawful use of those services. If SonicR1 later appoints any such provider for SonicR1's own processing purposes, it must be added to this Annex.

Billing: Stripe processes account-holder billing data for which SonicR1 acts as an independent controller; Stripe does not receive Customer call content and is therefore governed by the SonicR1 Privacy Policy, not this Annex.

Annex 3 — Technical and organisational measures

The measures below describe implemented controls, verified against the production code base on 25 August 2026 and, where a control depends on a provider account setting, against that provider's console on the date given in Annex 2. SonicR1 may replace a measure with an equivalent or stronger control without reducing the overall level of protection.

Control area	Measures
Governance and accountability	Documented data-residency and AI-processing policy; defined provider-routing boundaries; privacy and security responsibilities assigned to the operator; review of material architecture and Subprocessor changes; records supporting compliance and incident response.
EU residency by default	Application compute pinned to Vercel fra1; database/auth/storage in a Frankfurt project; AssemblyAI EU endpoints; Google AI served from EU endpoints only, with the failover chain restricted to an EU-only location allowlist; Fly.io components configured in fra. No Customer Personal Data is routed to a non-EEA AI inference endpoint and no non-EEA language-model option is enabled.
Fail-closed routing controls	Missing or legacy workspace policy defaults to EU/regional-only processing; unsupported explicit policy values fail; regional AI outages do not fall back to a non-EEA provider; STT endpoints are resolved centrally and non-EU overrides require an explicit deployment escape hatch.
Automated bypass prevention	Continuous CI checks reject code that references deleted legacy routing helpers, imports vendor AI/STT SDKs outside approved adapters, accesses STT configuration outside the central adapter, hard-codes non-EU endpoints, or interprets raw data-region values at route level; the checks are self-testing and use exact, justified allowlists.
Data minimisation	Only data needed for the selected features is processed. Background-job event payloads carry identifiers rather than conversation content, although the orchestration provider persists workflow step outputs as described in Annex 2; rate limiting uses keys/IDs rather than call content; e-mail Subprocessor receives recipient addresses and message content only.

Control area	Measures
Pseudonymisation and redaction	A redaction layer detects and tokenises contact and financial identifiers — telephone numbers, e-mail addresses, IBAN/BIC, payment-card numbers, postal codes and URLs — before eligible content is sent to an external language-model provider. On the post-call path, personal names are additionally tokenised by a name list and a machine-learning name recogniser, which is the workspace default; where the recogniser is unavailable the name list still applies. On the latency-critical live path, tokenisation is limited to the identifier types listed above, so personal names in live transcript text are transmitted to the EU model endpoint without tokenisation, over TLS and under the provider terms recorded in Annex 2. Content that carries no call context to tokenise against — uploaded knowledge-base documents, imported URL text, briefing and pre-call inputs, and knowledge-base questions — is sent to the external model unredacted (Annex 2). Production egress to an external model requires a redaction-provenance record — either of applied tokenisation or of the determination that the content carries no call context to tokenise against — and outbound token verification where tokenisation was applied.
Access control and tenant isolation	Authenticated access; role-based workspace permissions; owner/admin-gated privacy and data-region settings; separation of service-role operations from normal routes; project/workspace scoping; database row-level security and application-level project guards. AI-generated evaluations of an individual seller (scores, scorecards, coaching feedback) are disclosed only to that individual: they are not visible to other workspace members or managers, and bulk data exports exclude them.
Authentication and credentials	Managed authentication through Supabase; secrets kept in protected environment configuration; short-lived STT streaming tokens; no API secrets exposed to clients except scoped temporary tokens where required.
Encryption and transmission security	TLS for data in transit; provider-managed encryption at rest for hosted databases, files and supported cloud services; secure WebSocket/HTTPS endpoints for audio and API traffic.
Consent and transparency controls	Recording/AI consent gate with participant disclosure in supported languages before capture where recording/AI analysis is used; append-only consent-attestation metadata without conversation content; Customer remains responsible for lawful basis and call-recording requirements.
Ephemeral processing option	Ephemeral mode is designed not to persist reusable audio, transcripts or summaries after the live session; rolling context exists only for the session, subject to limited security/operational and consent-attestation metadata.
Deletion and retention	Plan-based retention windows enforced by a scheduled nightly purge job with an anomaly circuit breaker (Annex 1, Part D); customer-facing deletion and export controls available at all times; TTL jobs for redaction-map and debrief data; provider-side STT time-to-live; an operator-run termination deletion/return process against a specification that classifies every table carrying a workspace, project, organisation or call identifier; isolated legal retention where required.
Provider model-training restrictions	Speech-to-text account enrolled in the provider's model-improvement opt-out (evidenced at account level); Customer Personal Data is not used by SonicR1 to train shared models without documented instruction.
Logging and auditability	Operational and security logs; external-model egress records identifying provider, purpose and routing reason; operator-gated region-readiness diagnostics that report effective service regions without customer content or secrets.
Availability and resilience	Managed cloud infrastructure, health checks, regional service configuration, error propagation rather than unsafe provider fallback, retry/error handling, and backup/recovery capabilities supplied by relevant infrastructure providers.
Vulnerability and change management	Version-controlled infrastructure and application changes; code review and automated tests; dependency and deployment controls; environment separation; security tests designed to prevent regression of regional egress boundaries.
Incident response	Detection, triage, containment, investigation, remediation, evidence preservation and Customer notification procedures; cooperation with Customer's Articles 33–36 GDPR obligations.
AI-specific controls	SonicR1 makes no automated decision producing legal or similarly significant effects; sentiment is derived from transcript text only; no biometric voice identification and no acoustic emotion inference; AI-generated evaluations of an individual are technically restricted to that individual (see “Access control and tenant isolation”).

Annex 4 — Operational contacts and instructions

Customer privacy contact	The account owner, administrator, or privacy contact identified by Customer in the Main Agreement or Services.
SonicR1 privacy contact	legal@sonicr1.com (e-mail is the designated channel; no telephone contact is designated).
Security incident channel	legal@sonicr1.com and any dedicated incident channel later identified in the Trust/Security documentation or Main Agreement.
Subprocessor notice method	E-mail to the Customer's account owner/administrator contact (binding); in-product notice may be used additionally.
Approved Global Processing instruction	Currently without effect — no non-EEA AI provider is approved (Annex 2). If one is added under Section 10, the Customer owner/admin must explicitly enable the workspace option or give an equivalent written instruction; the safe default remains regional-only.
Return / deletion instruction	Customer submits a request through available account controls or to the privacy contact at any time before account closure, within the thirty (30) days following termination provided for in Section 13.2, or within any longer transition period the parties agree.

The operational verification register (provider agreements, dashboard evidence, dates) is maintained separately by SonicR1 and its current state is available to Customer on request via legal@sonicr1.com.

Signatures

Signing this page is optional: this DPA already applies when it is incorporated into or accepted with the Main Agreement. Where the parties choose to sign, an electronic signature is permitted and the agreement may be signed in counterparts. Return the countersigned copy to legal@sonicr1.com.

Customer	**SonicR1**
Name: _____	Name: _____
Title: _____	Title: _____
Signature: _____	Signature: _____
Date: _____	Date: _____