Data Processing Agreement (DPA)

according to art. 28 GDPR

Date of publication for the current version: August 6, 2026

Data controller

For data processing responsible client

(hereinafter referred to as the client)

Data processor
fonio GmbH
Neustiftgasse 73-75/3/7
1070 Wien
Wien
Austria
(hereinafter referred to as the contractor)

Unless otherwise agreed between the Client and the Contractor, this Data Processing Agreement forms an integral part of the Contractor’s General Terms and Conditions, which are available at https://www.fonio.ai/agbs. This Data Processing Agreement applies between the Client and the Contractor whenever the Contractor processes personal data on behalf of the Client in connection with the provision of its services.

1. BACKGROUND AND SPECIFICATION OF DATA PROCESSING

1.1 The contractor is a company that offers the following services:

- Configuration, Management, and Deployment of an AI Telephony Assistant via the B2B fonio.ai Web App

1.2 The client is a company that plans to use the contractor's services in the areas specified.

1.3 This Data Processing Agreement specifies the conditions for the processing of personal data by the contractor with the client's approval in accordance with the General Data Protection Regulation (GDPR). The contractor acts as a processor within the GDPR's definition.

2. NATURE, PURPOSE, OBJECT, AND LEGAL BASIS OF DATA PROCESSING

2.1 The Contractor’s services are described in the Contractor’s General Terms and Conditions (GTC), which can be accessed at https://www.fonio.ai/agbs.

2.2 In the course of providing services, the client shall provide the contractor with the personal data required for the provision of services in the appropriate manner in each case, for example, by electronic or physical means, via discussions and analyses, the performance of other contractually regulated activities, verbally, or via software tools.

2.3 Personal data may be processed, in particular, by organizing, arranging, storing, and, if necessary, adapting or modifying, querying, linking, restricting, deleting, combining, copying, hiding, connecting, analyzing, reading, receiving, sending, and updating, insofar as this is necessary for the provision of the agreed services.

2.4 The purpose of the processing is the contractually agreed provision of services to the client.

2.5 The Contractor is not obliged to verify the lawfulness of the client's underlying data processing.

3. CATEGORIES OF PERSONAL DATA AND DATA SUBJECTS CONCERNED

3.1 As part of the agreed services, several categories of personal data may be processed. In particular, this can be the following categories:

- Log data
- Communications Data
- Information that you send us by e-mail
- Contact data
- Telephony metadata
- Configuration data
- Technical Information
- Appointment data
- AI prompts and other AI-related information
- Telephone numbers
- Cookies and similar technologies
- Payment data
- Personal preferences
- IP Address
- Identifying Data
- Audio Voice Data
- Browser information
- Data on user behavior and interactions
- Invoice data
- Error-related technical data
- Device Information
- Phone-conversation data
- All data that conversation participants themselves introduce in the course of the conversation with the AI
- User behavior relevant for error analysis
- Technical authentication data (e.g., API keys)
- Transaction data
- Information you provide as free text
- Authentication data
- Data related to service quality
- Subscription related data

3.2 In general, the processing covers all special categories of personal data (Art. 9 GDPR) necessary for the provision of the agreed services. In particular, the following special categories of

personal data may be processed in connection with the provision of the agreed services (for example, for healthcare providers):

- Health data

3.3 In general, all categories of data subjects necessary for the provision of the agreed services are covered by the processing. In particular, this includes the following categories of data subjects:

- Customers
- Third parties under contract with the Client
- Employees of the Client
- Customers of the Client's customers
- Partners of the Client
- Suppliers of the Client

3.4 Given the nature of the agreed services, the client acknowledges that the contractor cannot review or maintain the list of categories of data subjects. Therefore, the client shall inform the contractor of any necessary changes to the list of categories of data subjects.

3.5 The contractor shall process the client's personal data regarding all data subjects listed above in accordance with the agreed services. If, due to changes to the list of categories of data subjects, changes to the agreed processing operations become necessary, the client shall issue additional instructions to the contractor accordingly.

3.6 No Voice Identification or Voice Verification

(a) The contractor does not perform voice identification or voice verification in connection with the agreed services. In particular, it does not create, store, or compare voice profiles ("voiceprints", voice templates) and does not deploy technical methods aimed at the unique identification of, or cross-conversation recognition of, a natural person on the basis of their voice. Audio voice data is processed exclusively for voice input and output as well as for transcription (speech-to-text/text-to-speech). A technically necessitated distinction between conversational contributions within a single conversation (e.g., separating caller and assistant) does not serve identification and does not enable recognition beyond the respective conversation.

(b) According to the contractor's own understanding, the audio voice data processed therefore does not constitute biometric data for the purpose of uniquely identifying a natural person within the meaning of Art. 4 No. 14, Art. 9 para. 1 GDPR. Point 3.6(a) contains a statement of fact, point (b) a legal opinion of the contractor; no warranty or representation in the legal sense is associated with it. The data-protection classification, in the individual case, of the processing operations initiated by the client is the responsibility of the client as controller; Point 2.5 remains unaffected.

(c) This is without prejudice to the fact that the processing may, for other reasons, comprise special categories of personal data within the meaning of Art. 9 GDPR, in particular health data (Point 3.2), and that the content of conversations may allow inferences to be drawn as to such data.

4. TERMS AND CONDITIONS OF DATA PROCESSING

4.1 The contractor shall comply with all requirements of the GDPR during the entire provision of services.

4.2 The contractor shall only process personal data based on written instructions in the form of a contract with the client. Deviations from these instructions require the client's prior written consent.

4.3 The contractor processes the personal data in accordance with the principle of data minimization pursuant to Art. 5 para. 1 lit c GDPR and therefore only to the extent necessary to provide the agreed services.

4.4 Access to the client's personal data is only granted to individuals who require this access due to contractual or legal obligations.

4.5 All individuals on the contractor's side who have access to the client's personal data shall be obliged to maintain confidentiality. In particular, the duty of confidentiality of the individuals entrusted with data processing shall remain even after termination of their activity with the contractor.

If the client is subject to a statutory professional duty of confidentiality, the Undertaking of Confidentiality and Data Protection referred to in Appendix 4, in the version provided for the client's state of domicile, shall additionally apply; it is retrievable, version-accurate, at the reference source indicated in Appendix 4. It shall be deemed agreed upon conclusion of the contract, without the need for a separate agreement or signature; a countersignature is provided at the client's request but is not required for its validity. For clients domiciled in Switzerland, the Addendum for Clients Domiciled in Switzerland shall apply in this respect.

4.6 The contractor shall implement and maintain all suitable, appropriate, and state-of-the-art technical and organizational measures to ensure the availability, confidentiality, and integrity of personal data. A list of the agreed technical and organizational measures is attached to this data processing agreement in Appendix 1.

4.7 The contractor shall support the client in complying with its obligations under the GDPR, in particular with regard to the rights of data subjects.

4.8 Unless otherwise required by law, the contractor shall inform the client immediately if it receives information or notification from a data subject, the data protection supervisory authority, or another authority or a third party, and this information or notification is directly or indirectly related to the processing of personal data under this Data Processing Agreement.

4.9 In the context of the contracted data processing, the contractor shall support the client—to the extent required by law—in the creation and updating of the record of processing activities, in the performance of the data protection impact assessment, and, if required, in prior consultations with the data protection supervisory authority within the meaning of Art. 36 GDPR. The contractor shall provide all necessary details and information for this purpose. In addition, the contractor shall maintain its own record of processing activities and, if required, carry out data protection impact assessments and appoint a data protection officer.

4.10 The contractor shall inform the client immediately, but at the latest within 24 hours, if the personal data provided to the contractor has been used unlawfully and/or the data subjects are at risk of harm. The contractor shall provide the client with all necessary information so that the Client can fulfill its reporting obligations to the data subjects in accordance with data protection laws.

4.11 Any transfer of personal data by the contractor to a third country or international organization shall be in accordance with Union or national law and must, in particular, comply with the provisions of the GDPR.

4.12 The parties may agree in Appendix 2 on other clauses concerning the provision of the personal data processing service, as long as they do not contradict directly or indirectly this data processing agreement or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

4.13 The contractor shall immediately inform the client if it believes that an instruction from the client violates data protection regulations of the Union or the Member States.

5. SUB-PROCESSORS

5.1 Depending on the contractually agreed service provision, a dedicated approved list of subprocessors is involved in the data processing.

5.2 The use of subprocessors may result in data being transferred to third countries. The contractor shall ensure that the requirements of Articles 44–49 GDPR are complied with when transferring personal data to third countries and shall inform the client of the guarantees used in each case (e.g., standard contractual clauses, adequacy decision).

5.3 A list of sub-processors approved by the client upon conclusion of the agreement is included in Appendix 3.

5.4 A contract shall be concluded between the Contractor and the subprocessors in accordance with Art. 28 (4) GDPR. The subcontract shall take into account the data protection requirements to the same extent as those agreed between the client and the contractor in this agreement, and data processing may only be carried out for the purpose specified in the separately contracted service.

5.5 The contractor shall regularly check that subprocessors comply with the data protection obligations applicable under this data processing agreement. If, in the course of this check, the contractor becomes aware that the subprocessor is not fulfilling, or is not sufficiently fulfilling, the data protection obligations incumbent upon it under this data processing agreement, it shall immediately inform the client without being asked to do so.

5.6 The outsourcing to subprocessors or / the change of the existing subprocessors is permissible insofar as:

- the contractor announces such subcontracting to subprocessors at least two weeks in advance in writing or in text form, and
- the client does not raise any objections to the planned outsourcing in writing or in text form within two weeks of receipt of the announcement, or, in the case of the first-ever transfer of data to the contractor, at the latest by that point in time. In the event of an objection to the planned involvement of a subprocessor, the latter may not be used until an agreement has been reached. A change within the meaning of this point also includes the expansion of the scope of use of a subprocessor already named, in particular the addition of a further processing location in a third country.

6. AUDIT AND COMPLIANCE

6.1 The contractor shall permit the client or its designated representatives to conduct audits and inspections to verify compliance with the terms of this Data Processing Agreement. Such audits shall be conducted with reasonable advance notice and shall not unreasonably interfere with the contractor's operations. The client is aware that any inspections of sub-processors must be coordinated directly with these sub-processors, and that the contractor has no influence on the conditions applied.

The client shall bear the costs of conducting the audit, unless the audit reveals a serious breach of this Data Protection Agreement by the contractor.

6.2 Any third-party auditors shall be subject to confidentiality agreements.

6.3 The contractor shall provide the client with all necessary information and work with the client to demonstrate compliance with the GDPR.

7. DURATION AND TERMINATION OF CONTRACT

7.1 This Data Processing Agreement shall remain in force for the duration of the data processing activities and shall terminate upon completion of the provision of the services or as otherwise agreed by the parties.

7.2 Upon termination of the Data Processing Agreement (or at any time prior thereto at the client's request), the contractor shall, at the client's discretion, either destroy the processed personal data (including any copies) itself or hand them over to the client in their entirety, provided that this does not conflict with any statutory obligation to retain them. The contractor shall continue to guarantee compliance with these clauses until the data is deleted or returned. If the client does not comment on the procedure, the contractor shall destroy the data 30 days after termination of the agreement, subject to statutory obligations to retain the data.

7.3 The contractor shall arrange the destruction or handover of data by any sub-processors.

8. FINAL CLAUSES

8.1 Amendments and supplements to this data processing agreement and all its components require a written agreement, which may also be in an electronic format (text form), and the express indication that it is an amendment or supplement to this data processing agreement. This also applies to the waiver of this formal requirement.

Clause 2.3 of the Terms and Conditions (amendment by fictitious consent) does not apply to this Agreement and its Appendices.

8.2 This Data Processing Agreement shall be governed by and construed in accordance with applicable law in Austria. The place of jurisdiction is Wien.

8.3 In case individual provisions of this Data Processing Agreement become invalid or unenforceable, the remainder of the Data Processing Agreement shall remain unaffected. These provisions shall be deemed to be replaced by valid and enforceable provisions that best achieve the economic purpose intended by the contracting parties.

Appendix

Appendix 1: Technical and Organisational Measures(TOMs)

Technical Measures

- Service operation in an ISO 27001-Certified Data Center: The fonio app is operated in an ISO 27001-certified data center.
  Third-party security certifications, such as ISO 27001, provide evidence that an organization has met a specific standard of information security management. They are an important element in building trust with customers and partners.
- Physical Security / Access Control to Office Premises: Office premises are adequately protected against unauthorized entry, are closed outside business hours, and visitors may enter only with constant escort/accompaniment.

Protecting office premises from unauthorized access and ensuring that external persons are constantly accompanied helps protect personal data within office spaces.

- Strict Separation of Production and Test Environments: Production and testing environments are strictly segregated at both the logical and infrastructural levels. The processing of actual production data (live personal data) within staging environments is strictly prohibited. If data is required for testing purposes, it must be completely anonymized or synthetic data must be used.
  The strict separation of environments ensures that software development and testing activities do not impact the stability or security of live systems. Prohibiting the use of production data in non-production environments prevents accidental data leaks, since development environments typically lack the stringent security controls found in production systems.
- Firewalls: Firewalls monitor and control inbound and outbound network traffic, allowing only necessary, explicitly authorized connections.
  Firewalls are network security systems that monitor and control incoming and outgoing network traffic based on predefined security rules. They establish a barrier between trusted internal network segments and untrusted external networks, such as the internet.
- State-of-the-Art Network Protocols and Configurations: Secure, state-of-the-art network protocols and configurations are deployed as hardening measures to protect data during transmission.
  Secure network protocols, such as correctly configured, TLS-based HTTPS, provide security controls—including encryption during data transmission—and help safeguard data in transit.
- Network Monitoring: Network activities are continuously monitored to detect and respond to security threats.
  Network monitoring is a critical IT process in which all network components, such as routers, switches, firewalls, servers, and VMs, are continuously monitored and evaluated for faults, security incidents, and performance issues to maintain and optimize their availability. Early detection of issues or security incidents can prevent unexpected downtime.
- System Hardening: Hardening measures are applied to all relevant systems through secure configuration based on CIS Benchmarks and/or the provider's recommendations.
  A secure system configuration means setting up systems and software to reduce the risk of exploitation by malicious actors. This includes measures such as disabling unnecessary services, establishing appropriate user permissions, and keeping systems up to date.
- Malware Protection: Anti-malware measures have been implemented to protect systems and data from malicious software. This includes installing and operating malware detection software on relevant systems, as well as monitoring and handling alerts triggered by potentially detected threats.
  Anti-malware measures involve deploying software tools to detect and remove malicious software that could compromise system security and data integrity.
- Patch Management Process: All software and hardware components are regularly updated through a dedicated patch management process to protect against known vulnerabilities. Patches are applied at varying intervals depending on the system type, at least once per quarter, and immediately if a patch addresses a critical vulnerability.
  Regular updates to software and hardware ensure protection against known vulnerabilities. Updates often include patches for security flaws discovered since the last version of the software or hardware.
- Identity & Access Management (IAM) and Lifecycle Processes: A centralized Identity and Access Management (IAM) system is implemented alongside a structured "Joiner-Mover-Leaver" (JML) process.
  An integrated IAM and JML process ensures that user identities, access rights, and permissions are managed systematically throughout the entire employment lifecycle—from onboarding (Joiner), to internal role changes (Mover), to offboarding (Leaver). Upon

termination of employment or contract, all access privileges to personal data and internal systems are revoked automatically and immediately. It effectively mitigates the risk of "privilege creep" and prevents unauthorized access by former employees or external contractors.

- Authorization Concept: Strict access controls have been implemented based on the "Need-to-Know" and "Least Privilege" principles regarding personal data. Where feasible and appropriate, multi-factor authentication (MFA) is implemented, and the mandatory use of password managers and randomly generated passwords with a minimum length of 20 characters is required. Administrative privileges are granted in accordance with the dual-control principle and may only be used for legitimate purposes. The use of administrative privileges is monitored.
  Access controls are measures that define who is permitted to access specific resources, such as personal data. They are crucial for preventing unauthorized access and ensuring that only authorized individuals can access data.
- Limitation of Administrative Activities to Qualified Personnel: Only specifically trained, qualified, and authorized personnel may perform administrative tasks on infrastructure components. Authorization is granted strictly based on verified technical competence, and administrative users are required to complete regular, documented security-related training for administrative activities.
  Restricting administrative access to verified experts ensures that critical system modifications are only executed by competent individuals. This minimizes the risk of security vulnerabilities, misconfigurations, or accidental data loss caused by human error or a lack of technical expertise.
- Session Management and Automatic Timeout: User and administrator sessions within the application and internal administrative systems are automatically terminated after a predefined period of inactivity.
  Automatic session timeouts mitigate the risk of unauthorized data access if a workstation or mobile device is left unattended in an unsecure environment.
- Handling of Credentials and Other Sensitive Information: To secure access to personal data, two-factor authentication (2FA) is utilized. Credentials and other sensitive information are stored in a password manager. All access points to the password manager are encrypted.
  Two-factor authentication adds an extra layer of security by requiring users to provide two forms of identification before accessing data. This makes it significantly harder for unauthorized individuals to gain access.
- Password Management Tools: Password management tools are used to create, store, and manage secure passwords for systems and applications in accordance with internal password policies.
  Password management tools help users generate, store, and manage unique, complex passwords for different accounts, thereby reducing the risk of password reuse and improving overall password security.
- Data Encryption: Stored data (Data at Rest) and data in transit (Data in Transit) are encrypted in compliance with industry best practices to protect them from unauthorized access.
  Data encryption ensures that sensitive data is stored and transmitted in encrypted form on the storage medium, protecting it from unauthorized access, particularly in the event of theft or loss of the medium.
- Data Pseudonymization: Data pseudonymization techniques are used to reduce the risk of data breaches.
  Pseudonymization is a de-identification procedure in which personal identification fields within a dataset are replaced by one or more artificial identifiers or pseudonyms to protect data privacy.

- Audit Logs: Audit logs are maintained to record who accessed which personal data and when. Further, security-relevant logs are stored immutably.
  Audit logs record when users access systems and data. This can be crucial in the event of a security incident, as it helps trace actions and identify potential perpetrators.
- Regular Backups: Data is regularly backed up where necessary and appropriate to prevent data loss.
  Regular data backups are crucial to prevent data loss during incidents such as data breaches or technical failures. They ensure that even in the worst-case scenario, the organization can restore data and maintain business continuity.
- Automated Vulnerability Scanning: Automated internal and external vulnerability scans are performed regularly across all infrastructure components, applications, and network segments.
  Automated scanning complements periodic penetration testing by providing real-time detection of newly discovered security vulnerabilities and misconfigurations, allowing for swift patch remediation.
- Penetration Testing: Penetration tests are conducted regularly to identify potential vulnerabilities in systems.
  Penetration tests, also known as pen tests, are simulated cyberattacks on information systems and IT environments to identify vulnerabilities that can be exploited. The process includes gathering information about the target prior to the test, identifying potential entry points, attempting to breach them, and reporting back the findings.

Organizational Measures

- Information Security Policies: Information security policies are established and are regularly reviewed and updated.
  Information security policies set the framework for what is expected from employees and systems regarding information security. Regularly reviewing and updating these policies ensures they remain effective and relevant in light of the evolving security landscape.
- Data Protection Officer (DPO): A Data Protection Officer (DPO) has been appointed to monitor compliance with the GDPR.
  A Data Protection Officer (DPO) is responsible for overseeing a company's data protection strategy and its implementation to ensure compliance with GDPR requirements. The DPO serves as the point of contact for the company, data subjects, and supervisory authorities.
- Privacy by Design and Privacy by Default: The principles of Privacy by Design and Privacy by Default are adhered to.
  Privacy by Design and Privacy by Default refer to integrating data protection into processing activities and business practices, from the design phase throughout the entire lifecycle. This helps ensure that data protection is not an afterthought but is embedded into the design and architecture of IT systems and business practices.
- Data Minimization Principle: The principle of data minimization is respected; only the personal data required to provide the service is collected.
  Data minimization is a key principle of the GDPR. It means that an organization should collect and process only the personal data it needs for its specific purpose.
- Records of Processing Activities (RoPA): We maintain a GDPR-compliant Record of Processing Activities that documents all relevant processing operations, associated data flows, involved third parties, and the respective legal basis for processing.
  A Record of Processing Activities (RoPA) establishes transparency regarding data flows and helps identify potential risks in processing. It further ensures that every processing activity and transfer of personal data is based on a valid legal ground.
- Data Protection Impact Assessments (DPIA) & Transfer Impact Assessments (TIA): Regular Data Protection Impact Assessments as well as Transfer Impact Assessments are conducted

to identify and mitigate risks both during processing and when transferring personal data across corporate and national borders.
Data Protection Impact Assessments (DPIAs) and Transfer Impact Assessments (TIAs) identify, evaluate, and mitigate or minimize data protection risks in data processing. DPIAs are important because they help organizations identify and fix problems early, reducing the associated costs and potential reputational damage that might otherwise occur.

- Vendor Risk Management / Data Processing Agreements: Information security assessments of data processors are conducted, and Data Processing Agreements (DPAs) are concluded to ensure and contractually secure compliance with security standards.
  Information security assessments of data processors are crucial to verify whether third-party service providers or vendors adhere to the same data protection and security standards as the organization. This helps minimize the risk of data breaches or data leaks caused by third parties. According to the GDPR, this must be formalized through a Data Processing Agreement (DPA).
- Data Subject Rights Handling Procedure: A standardized workflow is established to ensure that requests from data subjects—such as the right to access, rectification, or data portability—are verified, processed, and fulfilled within the statutory timelines.
  Establishing a clear internal procedure for data subject rights ensures compliance with GDPR transparency obligations and prevents legal escalations or regulatory complaints.
- Employee Training: Employees receive regular training on data protection and GDPR compliance.
  Regular training ensures that employees are informed about data protection principles and their responsibilities under the GDPR. This can help prevent data breaches caused by human error and ensure that issues are correctly reported and resolved.
- Information Security Awareness Campaigns: Regular campaigns (awareness training) to sensitize users to information security are conducted to educate employees about potential cyber threats.
  Information security awareness campaigns (awareness training) are crucial for educating employees about cyber threats such as phishing, social engineering, and malware, and for promoting data protection best practices.
- Secure Coding Training for Developers: Software developers are regularly offered security training to ensure secure programming practices.
  Regular security training for developers is essential to raise awareness of the latest security threats and best practices for writing secure code, thereby reducing the likelihood of introducing vulnerabilities into the software.
- Deletion Procedures (Data Retention and Erasure): Based on a data deletion concept, personal data is automatically deleted—insofar as legally permissible—once the purpose of the service provision has been fulfilled or if the data subject explicitly requests it (Right to Erasure / Right to be Forgotten).
  The regular deletion of data that no longer serves a purpose is an important component of data management and GDPR compliance. It helps reduce the risk of data breaches and ensures that the organization does not retain personal data longer than necessary.
- Incident Response Plan: A detailed response plan has been established to handle potential data breaches or cybersecurity incidents affecting personal data.
  An incident response plan is a set of instructions that helps identify, respond to, and recover from security incidents. A robust plan is crucial to minimizing the impact of a data breach and enabling rapid recovery.
- Data Breach Notification Procedure: A data breach notification procedure is in place to inform affected data subjects, supervisory authorities, or other relevant parties.
  In the event of a data breach, the GDPR requires organizations to notify affected data subjects and competent supervisory authorities. This procedure enables timely notification and can help mitigate the consequences of a data breach.

- Regular Review of Data Protection Practices: Data protection management practices are reviewed at regular intervals to ensure up-to-dateness and proper implementation, and any deviations are evaluated and addressed.
  Regular reviews of data protection practices ensure that changes in processing or gaps in measures are identified and appropriately addressed, to avoid or, if necessary, detect and remediate deviations from GDPR requirements at an early stage.

Appendix 2: Additional clauses

Version date of this appendix: October 28, 2026

- Neither the contractor nor its subprocessors will use personal data for the training, improvement, or evaluation of AI models.
- The following default retention periods apply:
  - Audio recordings: 30 days from the end of the call
  - Transcripts and summaries of the conversation: 90 days from the end of the call
  - Webchats: 90 days for each message from message creation
  - Webchat-Traces: 14 days
  - Dialog logs and technical logs: 30 days from the end of the call
  - Telephony metadata: 6 months from the end of the call
  - Accounting-related documents: 7-year statutory retention period from the date of issuance
  - Backups: 90 days
  - For any other categories of data, Section 7.2 of this Data Protection Agreement applies
- Provisions Regarding Reseller Partners
  - If this Data Processing Agreement is entered into with a reseller partner, fonio will act as a sub-processor for that partner.
  - If the client obtains the services through a reseller partner and the contract between the client and the reseller partner refers to this Data Processing Agreement for processing by the contractor, this Agreement applies directly between the client and the contractor; the preceding provision does not apply in this respect.
  - If the reseller partner provides its own services to the client that involve access to personal data in the client’s account (in particular, support and implementation), it acts directly on behalf of the client in this regard. The client shall enter into the necessary agreement pursuant to Article 28 of the GDPR with the reseller partner.

Appendix 3: Sub-processors

Version date of this appendix: October 28, 2026

Clarification for clients domiciled in Switzerland: The guarantees indicated in this Appendix for transfers to the United States refer to the EU-US Data Privacy Framework and the EU Standard Contractual Clauses. For clients domiciled in Switzerland, the corresponding Swiss transfer instruments apply in addition to, or in place of, these, namely the Swiss-U.S. Data Privacy Framework (for correspondingly certified recipients; the U.S. was added to Annex 1 of the Swiss Data Protection Ordinance by the Federal Council on 14 August 2024) and, for non-certified recipients and other third countries, the standard contractual clauses recognized by the FDPIC (EU SCCs in the version dated 4 June 2021, including the so-called "Swiss Finish"). Details are governed by the Addendum for Clients Domiciled in Switzerland.

Main Providers for Service Provision

The following providers are always used. In the event that a fallback provider has been selected as the primary provider at the customer’s express request, it is also possible—again at the customer’s express request—to exclude the previous provider from the list of primary providers below.

- Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany
  - Description of the service: System Hosting
  - Legal basis for any transfer to a third country: n/a
  - Server location: Data centers in Nuremberg, Falkenstein, and Helsinki are used. Further information:https://docs.hetzner.com/cloud/general/locations/
  - BSI C5:2020 Type 2 attestation dated 02.03.2026: https://files.hetzner.com/docs/BSIC52020Typ2_Testat_2026.pdf
- OVH GmbH, Christophstraße 19, 50670 Cologne, Germany (a company of the OVHcloud Group; parent company: OVH SAS, 2 rue Kellermann, 59100 Roubaix, France)
  - Service description: System hosting
  - Legal basis for any transfer to a third country: N/A
  - Server location: Data centers in Germany and France are used.
  - Information on certifications for OVH services (including BSI:C5 testat and ISO 27001): https://www.ovhcloud.com/de/compliance/
- Twilio Ireland Limited, 25-28 North Wall Quay D01 H104 Dublin, Ireland
  - Description of the service: Telephony
  - Legal basis for any transfer to a third country:
    - EU-US Data Privacy Framework — https://www.dataprivacyframework.gov/list
    - Swiss-U.S. Data Privacy Framework — https://www.dataprivacyframework.gov/list
    - Binding Corporate Rules are agreed upon as a secondary contractual safeguard (fallback) for international data transfers: https://www.twilio.com/en-us/legal/bcr/processor
    - Standard contractual clauses (Module 3), including the "Swiss Finish", are additionally agreed upon to ensure comprehensive protection of personal data during international data transfers.
  - Server location: EU — Ireland region. Further information: https://www.twilio.com/docs/global-infrastructure/edge-locations
  - Information on data retention: No audio data is stored (Zero-Data-Retention).
- Voxbone SA, Avenue Louise 489, 1050 Brussels, Belgium (a company of the Bandwidth Group; parent company: Bandwidth Inc., 900 Main Campus Drive, Raleigh, NC 27606, USA)
  - Service description: Telephony / PBX telephony
  - Legal basis for any transfer to a third country:
    - The data processing agreement is concluded with Voxbone SA (Belgium); this company provides services to clients in the EEA.
    - EU-US Data Privacy Framework - https://www.dataprivacyframework.gov/list
    - StandardContractual Clauses (Module 3), including the “Swiss Finish,” are additionally contractually agreed upon to ensure comprehensive protection of personal data during international data transfers.
  - Information on data retention: No audio data is stored (Zero Data Retention).
  - Server location: Germany, Belgium, Ireland
- LiveKit Inc., 4285 Payne Avenue, Suite 9154, CA 95157 San Jose, California, United States
  - Description of the service: Virtual meeting rooms
  - Legal basis for any transfer to a third country:
    - EU-US Data Privacy Framework https://livekit.com/legal/privacy-policy.

        - Standard contractual clauses (Module 3), including the “Swiss Finish,” are agreed upon as a secondary contractual safeguard (fallback) for international data transfers.
    - Server location: With Region Pinning enabled, data does not leave the European region, according to the provider. Further information: https://docs.livekit.io/deploy/admin/regions/region-pinning/
    - Information on data retention: No persistent storage of audio data occurs (real-time streaming / ZDR).
- Soniox, Inc. 1045 Helm Ln Foster City, CA 94404 United States
    - Description of the service: Speech-To-Text
    - Legal basis for any transfer to a third country:
        - EU Standard Contractual Clauses (SCC), contractually specified in the DPA with Soniox.
    - Server location: Processing exclusively in Europe under the Enterprise Agreement. Further information:https://soniox.com/europe.
    - Additional information: "Zero Data Retention" is applied.
- OpenAI Ireland Ltd. 1st Floor, The Liffey Trust Centre 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland
    - Description of the service: LLM
    - Legal basis for any transfer to a third country:
        - EU Standard Contractual Clauses (SCC - Module 3), including the "Swiss Finish", contractually specified in the DPA with OpenAI.
    - Server location: Processing within Europe under an Enterprise Agreement. Further information: https://openai.com/index/introducing-data-residency-in-europe/
    - Additional information: "Zero Data Retention" is applied.
- Theai, Inc. dba Inworld AI, 1975 W El Camino Real #300, Mountain View, CA 94040, USA (Replaces Eleven Labs Inc. as of August 6, 2026)
    - Description of the service: Text-to-Speech
    - Legal Basis for any transfer to a third country:
        - Standard Contractual Clauses (Module 3), including the "Swiss Finish", have been agreed upon for international data transfers.
    - Server Location: EU data residency agreed upon via an enterprise contract
    - Data Retention: No audio data is stored (zero-data retention). Further Information: https://docs.inworld.ai/portal/zero-data-retention
    - Additional Information on Security and Certifications: https://trust.inworld.ai/
- Sinch AB (Mailgun), Lindhagensgatan 112, 112 51 Stockholm Sweden
    - Description of the service: E-Mail delivery
    - Legal basis for any transfer to a third country:
        - The DPA was concluded with Sinch AB in Stockholm, which is the parent company of the US entity Mailgun Technologies, Inc., 112 E Pecan St #113 San Antonio, TX 78205, United States. Mailgun Technologies, Inc. is part of the EU-US Data Privacy Framework https://sinch.com/legal/terms-and-conditions/other-sinch-terms-conditions/data-processing-agreement/.
        - Standard contractual clauses (Module 3), are agreed upon as a secondary contractual safeguard (fallback) for international data transfers.
    - Server location: "EU" region. Further information:https://www.mailgun.com/about/regions/
- New Relic, Inc., 188 Spear Street, Suite 1200, CA94105 San Francisco, California, United States
    - Description of the service: Logging and Monitoring
    - Legal basis for any transfer to a third country:
        - EU-US Data Privacy Framework — https://www.dataprivacyframework.gov/list

        - Swiss-U.S. Data Privacy Framework — https://www.dataprivacyframework.gov/list
        - Standard contractual clauses (Module 3), including the "Swiss Finish", are agreed upon as a secondary contractual safeguard (fallback) for international data transfers.
    - Server location: Fonio uses the European location. Further information:https://docs.newrelic.com/docs/accounts/accounts-billing/account-setup/choose-your-data-center/

Fallback Providers to Increase Availability

The following providers serve as a fallback in the event that a main provider fails or is unable to deliver the required service quality. This serves to increase the availability and quality of the Service. The use of fallback providers is deactivated by default for holders of a professional duty of confidentiality and can be activated at the customer's request. For all other customers, who are not subject to a professional duty of confidentiality, fallback providers are activated by default but can be deactivated at the customer's request. It is also possible to use the providers mentioned as the primary provider upon the customer's express request.

- Deepgram, Inc., 548 Market St, Suite 25104, CA 94104-5401 San Francisco, California, United States
    - Description of the service: Speech-to-Text
    - Legal basis for any transfer to a third country:
        - EU Standard Contractual Clauses (SCC - Module 3), contractually specified in the DPA with Deepgram.
    - Server location: Processing strictly within Europe via its own EU endpoint under an Enterprise Agreement.
    - Additional information: "Zero Data Retention" is applied.
- Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, D04 E5W5, Irland
    - Description of the service: LLM
    - Legal basis for any transfer to a third country:
        - EU-U.S. Data Privacy Framework - https://www.dataprivacyframework.gov/list
        - Swiss-U.S. Data Privacy Framework - https://www.dataprivacyframework.gov/list
        - Standard contractual clauses (Module 3), including the “Swiss Finish,” have been agreed upon as a secondary contractual safeguard (fallback) for international data transfers.
    - Server location: Europe region
    - Additional information: "Zero Data Retention" is applied.
- Eleven Labs Inc., 169 Madison Ave #2484, NY 10016 New York, New York, United States
    - Description of the service: Text-to-Speech
    - Legal basis for any transfer to a third country:
        - EU-US Data Privacy Framework https://elevenlabs.io/privacy-policy
        - Standard contractual clauses (Module 3) are agreed upon as a secondary contractual safeguard (fallback) for international data transfers.
    - Server location: Under an Enterprise contract, all data remains exclusively within Europe. Further information: https://elevenlabs.io/docs/overview/administration/data-residency
    - Additional information: "Zero Data Retention" is applied.

Optional Providers

The following providers are used only optionally and solely at the customer's express request.

- Nylas, Inc., 2100 Geng Rd. #2100, Palo Alto, CA 94303
  - Description of the service: Calendar integration for connecting calendar accounts (Google Calendar, Microsoft Outlook) via OAuth for availability checks, appointment booking, and bidirectional synchronization of calendar events.
  - Legal basis for any transfer to a third country:
    - EU-US Data Privacy Framework — https://www.dataprivacyframework.gov/list
    - Swiss-U.S. Data Privacy Framework — https://www.dataprivacyframework.gov/list
    - Standard contractual clauses (Module 3) are agreed upon as a secondary contractual safeguard (fallback) for international data transfers.
  - Server location: The data residency region is Europe (Ireland). Further information:https://developer.nylas.com/docs/dev-guide/platform/data-residency/.
- Meta Platforms Ireland Ltd., Merrion Road, Dublin 4, D04 X2K5, Ireland
  - Description of the service: WhatsApp-Integration
  - Legal basis for any transfer to a third country:
    - EU-US Data Privacy Framework — https://www.dataprivacyframework.gov/list
    - Swiss-U.S. Data Privacy Framework — https://www.dataprivacyframework.gov/list
    - Standard contractual clauses (Module 3) are agreed upon as a secondary contractual safeguard (fallback) for international data transfers.
  - Additional information: The services of Meta Platforms Ireland Ltd. are optional and are only used at the customer's request.
- SideGuide Technologies, Inc. (Firecrawl), 2261 Market Street STE 85367, CA 94114 San Francisco, United States
  - Description of the service: Search-Engine
  - Legal basis for any transfer to a third country:
    - Standard contractual clauses (Module 3), including the "Swiss Finish".
- LangChain, Inc., 501 2nd Street, Suite 120, CA 94107 San Francisco, United States
  - Description of the service: Web-chat-Integration and tracing
  - Legal basis for any transfer to a third country:
    - Standard contractual clauses (Module 3)
  - Server location: The LangChain EU endpoint is configured
- Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, D04 E5W5, Ireland
  - Description of the service: Delivery of push notifications to Android devices via Firebase Cloud Messaging (FCM)
  - Used only if the fonio phone app is used and push notifications are enabled
  - Legal basis for any transfer to a third country:
    - EU-U.S. Data Privacy Framework – https://www.dataprivacyframework.gov/list
    - Swiss-U.S. Data Privacy Framework – https://www.dataprivacyframework.gov/list
    - Standard contractual clauses (Module 3), including the “Swiss Finish,” have been agreed upon as a secondary contractual safeguard (fallback) for international data transfers.
  - Server location: No European data residency is available for Firebase Cloud Messaging; delivery is handled via Google’s global infrastructure, including locations in the United States.
  - Additional Information:
    - When using push notifications in the fonio app, the following additional data is processed: FCM registration token or Firebase Installation ID, delivery metadata, and the end device’s technical connection data (specifically the IP address). The notifications may also include phone numbers, call summaries, or names.

        - Information on data retention: Push notifications are retained only for the period necessary for delivery.
        - Further information: https://firebase.google.com/support/privacy
    - Addendum regarding push notifications for iOS devices:
        - For iOS devices, delivery is handled via the Apple Push Notification Service. In our view, Apple acts as a separate data controller; this does not constitute data processing on behalf of another party, which is why Apple is not listed as a subprocessor in this appendix.
- T-Systems International GmbH, Hahnstraße 43d, 60528 Frankfurt am Main, Germany
    - Service description: System hosting on the “T Cloud Public”
    - Note: This provider is offered exclusively to customers of Deutsche Telekom AG and its subsidiaries as an alternative hosting service to Hetzner and OVH.
    - Legal basis for any transfer to a third country: n/a
    - Server location: Netherlands
    - Information on T Cloud Public certifications (including ISO/IEC 27001, BSI C5 Type II Certificate, SOC 2...): https://www.t-cloud-public.com/de/produkte-services/core-services/zertifikate

Additions Regarding Failover Mechanisms

To ensure the availability of our service and its service quality, we deploy a US failover (temporary rerouting of the affected provider's data flow to US server locations) for the following providers in the event of unavailability or insufficient availability of the EU locations — and only in that event:

- Soniox, Inc
- OpenAI Ireland Ltd.
- Theai, Inc. dba Inworld AI

Failover mechanisms are used only for the minimum time necessary. Deactivation of the US failover is possible at any time at the customer's request.

For holders of a professional duty of confidentiality, a US failover is deactivated by default.

Appendix 4: Undertaking of Confidentiality and Data Protection

The following Undertakings of Confidentiality are attached to this Agreement as Appendix 4. The client may rely on the version applicable to it, without any substantive modification:

- Undertaking of Confidentiality and Data Protection — Germany (§§ 203, 204 of the German Criminal Code (StGB), § 62a of the German Tax Advisory Act (StBerG), § 43e of the German Federal Lawyers' Act (BRAO));
- Undertaking of Confidentiality and Data Protection — Austria (§ 121 of the Austrian Criminal Code (StGB), § 54 of the Austrian Physicians Act (ÄrzteG), § 9 of the Austrian Lawyers' Act (RAO), § 80 of the Austrian Professional Code for Tax Advisors and Auditors (WTBG 2017), § 6 of the Austrian Data Protection Act (DSG)).

For clients domiciled in Switzerland, no separate declaration is maintained; the corresponding provision (Art. 321 of the Swiss Criminal Code (chStGB)) is contained in Point 4 of the Addendum for Clients Domiciled in Switzerland.

This Data Processing Agreement was created using the Metasoul DPA-Generator.