Data Protection Agreement (DPA)

Fields in [brackets] are to be filled in per customer.

Between: [Controller legal name], [Address] – the Customer under the Contract ("**Controller**")

and: Ateleris GmbH, Neumarkt 1, 7. OG, 5200 Brugg, Switzerland (UID: CHE-156.417.861) ("**Processor**", "**Ateleris**")

---

1. Purpose and Scope

1.1 This Data Protection Agreement ("**DPA**") supplements the General Terms and Conditions ("**Terms**") and the Customer Contract ("**Contract**") between the Parties (together, the "**Agreement**") and applies whenever Ateleris processes Personal Data on behalf of Controller in connection with the Transcription Service. In case of conflict between these documents, the following order of precedence applies, from highest to lowest: (i) the Contract, for commercial matters; (ii) this DPA, for the Processing of Personal Data; (iii) the Terms; and (iv) the API Documentation.

1.2 This DPA reflects the requirements of the Swiss Federal Act on Data Protection ("**nFADP**", in German the revised DSG) and, to the extent the EU General Data Protection Regulation ("**GDPR**") applies to the relevant Processing, Art. 28 GDPR.

2. Definitions

Terms such as "**Personal Data**," "**Processing**," "**Controller**," "**Processor**," "**Sub-processor**," and "**Data Subject**" have the meaning given in the nFADP and, where applicable, the GDPR. "**Customer Data**" means the audio files submitted by Controller and the transcriptions generated from them as defined in the Terms; where used in this DPA it means that subset of Customer Data which contains Personal Data.

For clarity, and without narrowing the statutory definition, Processing includes the collection, recording, organisation, storage, use, transmission, disclosure, restriction, and deletion of Personal Data, whether or not by automated means.

"**Personnel**" means Ateleris' employees, contractors, freelancers, and other individuals acting under Ateleris' direction, as defined in the Terms.

"**Sub-processor**" means a third party engaged by Ateleris that Processes Customer Data on Ateleris' behalf. A provider that merely transmits Customer Data in transit without access to it in unencrypted form, such as a telecommunications carrier or internet access provider, is not a Sub-processor. A provider that has access to Customer Data in unencrypted form is a Sub-processor and is listed in **Annex 3**, table “Sub-processors (Customer Data, Ateleris as processor)”.

"**Service Data**" has the meaning given in the Terms.

3. Subject Matter and Details of Processing

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

4. Processor Obligations

4.1 **Instructions.** Ateleris will Process Customer Data only on documented instructions from Controller, including as necessary to provide the Service under the Agreement, unless required to do otherwise by law (in which case Ateleris will inform Controller in advance, unless prohibited by law).

4.2 **Confidentiality.** Ateleris ensures that Personnel authorized to Process Customer Data are bound by confidentiality obligations that survive the end of their engagement, and grants access only to those Personnel who need it to perform their duties. Ateleris imposes materially equivalent confidentiality obligations on Sub-processors and their personnel under §4.5.

4.3 **Security.** Ateleris implements the technical and organizational measures described in **Annex 2**, appropriate to the risk. Ateleris may update those measures, provided that it does not materially reduce the level of protection they provide.

4.4 **Location of Processing.** Customer Data is Processed exclusively on infrastructure located in Switzerland, by Ateleris and by the Sub-processors listed in **Annex 3**, table “Sub-processors (Customer Data, Ateleris as processor)”. This commitment applies to all Customer Data as defined in the Terms, whether or not it contains Personal Data. Ateleris will not transfer Customer Data outside Switzerland without Controller's prior written consent, except as required to comply with a legal obligation. Access to Customer Data from outside Switzerland, including remote access by Personnel or by a Sub-processor, counts as a transfer for the purposes of this Section. This Section is subject to §4.9 in respect of Customer Data that Controller chooses to submit by email.

Where a transfer outside Switzerland is agreed or legally required, and the destination does not benefit from an adequacy decision, the Parties will apply the European Commission’s Standard Contractual Clauses together with the amendments and interpretations issued by the Swiss Federal Data Protection and Information Commissioner, which are deemed incorporated into this DPA for that transfer, in the module applicable to a controller-to-processor relationship.

4.5 **Sub-processors.** Controller authorizes Ateleris to engage the Sub-processors listed in **Annex 3**, table “Sub-processors (Customer Data, Ateleris as processor)”. The providers listed in the second table of Annex 3 process Service Data for which Ateleris acts as Controller, and are not Sub-processors for the purposes of this Section. Ateleris will impose data protection obligations on Sub-processors that are materially equivalent to those in this DPA, including the confidentiality obligation in §4.2 in respect of their own personnel, and remains fully liable to Controller for their performance. Ateleris will notify Controller of any intended change to Sub-processors at least 30 days in advance, and Controller may object on reasonable data protection grounds within that period, in which case the parties will discuss a resolution in good faith. Where no resolution is found within a further 30 days, Controller may terminate the Agreement in respect of the affected Processing, without charge and without regard to any minimum term.

4.6 **Assistance.** Taking into account the nature of Processing, Ateleris will provide reasonable assistance to Controller in responding to Data Subject requests (e.g. access, erasure) and, where applicable, in relation to data protection impact assessments or consultations with a supervisory authority, to the extent Controller cannot reasonably fulfil these itself.

4.7 **Personal Data breach notification.** Ateleris will notify Controller without undue delay, and as a target within 48 hours, after becoming aware of a Personal Data breach affecting Customer Data, and will provide available information reasonably necessary for Controller to meet its own notification obligations. Notification is sent to the email address Controller specifies in the Contract; Controller is responsible for keeping that address current.

4.8 **Retention and deletion.**

- Audio submitted for transcription is deleted after transcription is complete or failed.
- The resulting transcription is deleted once it has been retrieved by Controller via the API.
- On termination of the Agreement, Ateleris will delete any remaining Customer Data still held, unless retention is required by law. Ateleris confirms deletion in writing on Controller’s request.
- This Section does not apply to invoices, usage records, and other business records that Ateleris is required to retain under Art. 958f OR or other applicable law, which contain no audio and no transcription content and are retained for the statutory period.

4.9 **Support cases.** Where Controller submits a support request that refers to specific Customer Data, or asks Ateleris to investigate a specific transcription, this constitutes an instruction under §4.1 to access and Process that Customer Data to the extent necessary to investigate and resolve the case. Such access is logged. Customer Data retained for the purposes of a support case is deleted when the case is closed, and in any event within 30 days.

Ateleris' email environment is operated by Microsoft within the EU and EFTA. Customer Data that Controller submits by email therefore leaves Switzerland, to states recognised by the Federal Council as providing adequate data protection. It is Controller’s responsibility to provide access to Customer Data in a way that makes sure the data stays in Switzerland, e.g. through a Swiss file transfer service.

4.10 **No use for model training.** Ateleris does not use Customer Data to train or improve its models, except where Controller has separately and explicitly agreed in writing to provide data for a dedicated model-training engagement, which is treated as a separate Processing activity subject to its own terms.

4.11 **Records and evidence of compliance.** Upon reasonable written request, Ateleris will provide Controller with information reasonably necessary to demonstrate compliance with this DPA (e.g. a summary of technical and organizational measures, relevant certifications if available). Where that information is not sufficient for Controller to meet a legal obligation, Controller may audit Ateleris' Processing of Customer Data once in any 12-month period, on at least 30 days' written notice, during business hours, subject to a confidentiality undertaking, at Controller's cost, and without access to the data or systems of other customers of Ateleris. Ateleris may satisfy an audit request by providing an audit report or certification issued by a qualified independent third party, where that report covers the matters Controller wishes to audit. Additional audits may be conducted following a Personal Data breach affecting Customer Data, or where required by a supervisory authority.

4.12 **Service Data.** Ateleris generates and Processes Service Data in order to operate, secure, and support the Service, to prevent abuse, to plan capacity, to troubleshoot faults, and to calculate fees. What Service Data includes and what it does not include is defined in the Terms. Ateleris retains Service Data for a maximum of 6 months in its production systems, plus the backup retention described in **Annex 2**, except where a longer period is required to investigate a security incident or to comply with a legal obligation, and except for the aggregated usage totals required for invoicing and for the statutory retention of business records. In respect of Service Data that constitutes Personal Data, Ateleris acts as Controller for these purposes, and Ateleris does not use Service Data to reconstruct the content of Customer Data. Information on Ateleris' Processing of Service Data in that capacity, including the rights of the individuals concerned, is set out in Ateleris' Privacy Notice, which is attached. That notice is provided for information only and does not form part of this DPA.

5. Controller Obligations

5.1 Controller is responsible for the lawfulness of the Personal Data it submits for Processing, including having any necessary legal basis, consents, or notices in place.

5.2 In particular, where Customer Data includes recordings of identifiable individuals, Controller is responsible for ensuring such individuals are informed, before recording, of what data is collected, why, how long it is kept, who can access it, and their rights, and for honoring any Data Subject rights requests it receives. Ateleris' Privacy Notice does not cover these individuals, and Controller cannot discharge its obligation under this Section by referring to it.

5.3 Controller will not issue instructions that would cause Ateleris to violate applicable data protection law.

5.4 Controller’s obligations regarding the lawfulness of recordings, including under Art. 179bis and 179ter of the Swiss Criminal Code, are set out in §4.4 of the Terms and apply in addition to this Section.

6. Liability

Liability under this DPA is subject to the limitation of liability set out in the General Terms and Conditions. This does not affect the direct liability of either Party towards a Data Subject or a supervisory authority under applicable data protection law, which cannot be limited by agreement.

7. Term

This DPA applies for as long as Ateleris Processes Personal Data on behalf of Controller under the Agreement. Sections 4.7 (breach notification), 4.8 (deletion), and 4.11 (records and audit) survive termination to the extent necessary to complete outstanding obligations.

8. Governing Law and Jurisdiction

This DPA is governed by the same governing law and jurisdiction as the General Terms and Conditions, that is, Swiss law, with the exclusive place of jurisdiction in Brugg, Canton of Aargau, Switzerland.

Annex 1 – Details of Processing

Subject matter	Automated speech-to-text transcription of audio submitted by Controller via Ateleris' API
Duration	For the term of the Agreement, subject to §4.8 (deletion)
Nature and purpose	Conversion of audio recordings into text using automated speech recognition, for Controller's use in its own product/service
Types of personal data	Voice recordings (audio) and the resulting text (transcriptions), which may include content such as names, contact details, or other personal information spoken by data subjects
Categories of data subjects	End users / customers of Controller whose voice recordings are submitted for transcription; Controller's own personnel, where they appear in recordings or submit support requests
Retention	Audio: deleted right after job completion or failure. Transcriptions: on retrieval. Support-case Customer Data: on case closure, at the latest after 30 days.

Annex 2 – Technical and Organizational Measures

- **Access control:** role-based access to production systems, limited to personnel who need access to perform their duties; unique credentials per user; access revoked promptly upon role change or departure; multi-factor authentication for administrative access.
- **Encryption:** Customer Data is encrypted in transit using current TLS versions and cipher suites, and encrypted at rest using AES-256 on the storage used by the Service. Cryptographic keys are held separately from the encrypted data and access to them is restricted to the Personnel who require it.
- **Data minimization / deletion:** automated deletion of audio after transcription and of transcriptions after retrieval, as described in §4.8, with the time limits stated there enforced automatically rather than manually.
- **Logging and monitoring:** logging of access to production systems sufficient to support incident investigation; logs are protected against unauthorized modification and retained as described in §4.12.
- **Network security:** segmentation and firewalling of production environments; restricted administrative access.
- **Physical security:** Ateleris operates no data center of its own. Customer Data is hosted exclusively in data centers located in Switzerland, operated by the Sub-processor listed in **Annex 3**, table "Sub-processors (Customer Data, Ateleris as processor)". Service Data is additionally held in Switzerland by the processor listed in **Annex 3**, table "Processors engaged by Ateleris for Service Data (Ateleris as controller)". Each provider operates its own physical and environmental security controls for its facilities, including controlled access, monitoring, fire detection and suppression, and redundant power and cooling.
- **Vulnerability and patch management:** monitoring of security advisories for the components used by the Service, and application of security updates within a period appropriate to the severity of the vulnerability.
- **Personnel:** Personnel with access to Customer Data are bound by confidentiality obligations and receive data protection and security instruction appropriate to their role.
- **Availability and backup:**
    - No backups of Customer Data are taken.
    - Service Data except logs is backed up continuously, daily, weekly, and monthly. Continuous backups are kept for 30 days, daily backups for a week, weekly backups for a month, and monthly backups for 6 months.
    - Logs are backed up daily, weekly, and monthly. Daily backups are kept for a week, weekly backups for a month, and monthly backups for 3 months.
    - Backups are done on the infrastructure of the providers listed in **Annex 3,** in the table applicable to the data concerned, and held in the locations documented there.

Annex 3 – Sub-processors

Sub-processors (Customer Data, Ateleris as processor)

Sub-processor	Service	Location
Infomaniak Network SA	Cloud hosting infrastructure	Switzerland

Providers that only transmit Customer Data in transit without access to it in unencrypted form are not Sub-processors and are not listed, in accordance with §2.

Processors engaged by Ateleris for Service Data (Ateleris as controller)

Processor	Purpose	Location
Microsoft Azure	Storage, processing, visualization of Service Data	Switzerland North region