Digital Samba
Data Processing Agreement

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

Last modified: 30 April, 2026

Changes: Incorporated clause 4.3 to address professional secrecy obligation.

This Data Processing Agreement ("**DPA**") supplements the Digital Samba Customer Agreement (the "**Agreement**"). Capitalised terms not defined in this DPA have the meanings given in the Agreement. Terms such as Data Controller, Data Processor, personal data, and processing have the meanings given in the GDPR.

This DPA only applies to the extent that the Customer instructs Digital Samba to process personal data on Customer's behalf in relation to the Services.

This Data Processing Agreement is between:

COMPANY NAME

REGISTRATION NUMBER

ADDRESS

POSTCODE, CITY

COUNTRY

(the "**Customer**")

and

COMPANY NAME	**DIGITAL SAMBA, S.L.**
REGISTRATION NUMBER	B63229629
ADDRESS	TRAVESSERA DE GRÀCIA, 98 BIS, 6/2
POSTCODE, CITY	08012 BARCELONA
COUNTRY	SPAIN

("**Digital Samba**")

(each a "**Party**"; together the **"Parties**")

1. Preamble

1.1. These contractual clauses (the "**Clauses**") set out the rights and obligations of the Customer and Digital Samba, when processing personal data of persons who use the Services ("**User**" or "**Users**") on behalf of the Customer.

1.2. The Clauses have been designed to ensure the Parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

1.3. In the context of the provision of the Services, Digital Samba will process Users' personal data on behalf of the Customer in accordance with the Clauses.

1.4. In the event of any conflict relating to the processing of personal data, the following order of precedence applies (highest first):

(a) any Standard Contractual Clauses that the Parties have expressly executed or expressly incorporated by reference (including in electronic form);

(b) these Clauses (including their appendices);

(c) the Agreement (including any Orders and referenced policies).

For all other matters, the Agreement governs. Documented instructions may not reduce the protections in these Clauses or any executed Standard Contractual Clauses.

1.5. From their Effective Date, these Clauses replace any prior data processing terms between the Parties, and any later data-processing addendum referencing the Agreement supersedes these Clauses from its Effective Date to the extent of conflict.

1.6. Four appendices are attached to the Clauses and form an integral part of the Clauses.

1.7. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

1.8. Appendix B includes the current list of subprocessors authorised by the Customer. Appendix B may be updated by Digital Samba in accordance with clause 6.

1.9. Appendix C contains the Customer's instructions with regards to the processing of personal data.

1.10. Appendix D contains provisions for other activities which are not covered by the Clauses.

1.11. The Clauses along with appendices shall be retained in writing, including electronically, by both Parties.

1.12. The Clauses shall not exempt Digital Samba from obligations to which Digital Samba is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

1.13. The Customer may use the Services either (a) as a controller, or (b) as a processor acting on behalf of its own customers or end clients. Where the Customer acts as a processor, Digital Samba acts as a sub-processor within the meaning of Article 28(4) GDPR. The Customer warrants that it has all necessary authority to enter into this DPA, issue processing instructions to Digital Samba, and authorise sub-processors, whether in its own capacity as controller or on behalf of the relevant controller.

2. The rights and obligations of the Data Controller

2.1. The Data Controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

2.2. The Data Controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

2.3. The Data Controller shall be responsible, among others, for ensuring that the processing of personal data, which Digital Samba is instructed to perform, has a legal basis.

2.4. Where the Customer is not the Data Controller, the Customer warrants that (a) it acts with the authority of, and on behalf of, the relevant Data Controller; (b) it has communicated the Data Controller's instructions to Digital Samba; and (c) it will ensure that all instructions given to Digital Samba are consistent with the Customer's own obligations to the Data Controller.

3. Digital Samba acts according to instructions

3.1. Digital Samba shall process personal data only on documented instructions from the Customer, unless required to do so by Union or Member State law to which Digital Samba is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the Customer throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

3.2. Digital Samba shall immediately inform the Customer if instructions given by the Customer, in the opinion of Digital Samba, contravene the GDPR or the applicable EU or Member State data protection provisions.

4. Confidentiality

4.1. Digital Samba shall only grant access to the personal data being processed on behalf of the Customer to persons under Digital Samba's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

4.2. Digital Samba shall at the request of the Customer demonstrate that the concerned persons under Digital Samba's authority are subject to the abovementioned confidentiality.

4.3. Digital Samba shall act as a subprocessor in support of activities carried out by professionals who are subject to statutory obligations of professional secrecy. Digital Samba, and in particular its employees, shall, being aware of the criminal consequences of any breach, preserve the confidentiality of all third-party secrets and confidential information to which they are granted access in the course of the performance of the Clauses.

Where Digital Samba engages subprocessors in accordance with clause 6, Digital Samba shall ensure that such subprocessors are bound in text form to confidentiality obligations. Digital Samba shall further ensure, by appropriate contractual or organisational measures, that any persons acting for such subprocessors who may gain access to confidential information or third-party secrets are informed of the confidential nature of such information and of the legal consequences of any breach, including, where applicable, criminal consequences under Sections 203 and 204 of the German Criminal Code.

The obligation of confidentiality under this clause 4.3 shall survive termination of the Clauses and shall continue for an unlimited period.

The foregoing confidentiality obligations shall not apply to the extent that Digital Samba is required to disclose confidential information of the Customer pursuant to a binding order or decision of a competent authority or court. To the extent legally permissible and practicable in the individual case, Digital Samba shall inform the Customer in advance of any such obligation to disclose.

Digital Samba shall ensure that all processing activities are carried out exclusively by personnel who are duly bound by confidentiality obligations.

5. Security of processing

5.1. Article 32 GDPR stipulates that - taking into account the state of the art - the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Customer and Digital Samba shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The Customer shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

5.1.1. Pseudonymisation and encryption of personal data;

5.1.2. The ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

5.1.3. Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

5.1.4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

5.2. According to Article 32 GDPR, Digital Samba shall also – independently from the Customer – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the Customer shall provide Digital Samba with all information necessary to identify and evaluate such risks.

5.3. Furthermore, Digital Samba shall assist the Customer in ensuring compliance with the Customer's obligations pursuant to Articles 32 GDPR, by inter alia providing the Customer with information concerning the technical and organisational measures already implemented by Digital Samba pursuant to Article 32 GDPR along with all other information necessary for the Customer to comply with the Customer's obligations under Article 32 GDPR.

If subsequently- in the assessment of the Customer- mitigation of the identified risks requires further measures to be implemented by Digital Samba, than those already implemented by Digital Samba pursuant to Article 32 GDPR, the Customer shall specify these additional measures to be implemented in Appendix C.

6. Use of subprocessors

6.1. General authorisation. The Customer grants a general written authorisation for Digital Samba to engage subprocessors. Digital Samba shall maintain a current list of authorised subprocessors in Appendix B.

6.2. Engagement & change management. Digital Samba shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a subprocessor).

6.2.1. Notice of change. Digital Samba shall notify the Customer in writing at least thirty (30) days before any intended addition or replacement of a subprocessor becomes effective. This notification of a change in the subprocessor list ("**Change Notice**") shall be sent to the Customer and shall identify, at a minimum, the subprocessor's name, role/services, country(ies) of processing, the effective date of the change, and (if applicable) the transfer mechanism for restricted transfers.

6.2.2. Right to object. Upon receiving a Change Notice, if the Customer has specific, reasonable grounds that engagement of the proposed subprocessor would: (i) cause the Customer to breach applicable data-protection law; (ii) result in a material reduction in the level of security or compliance applicable to the processing of personal data under these Clauses; (iii) involve a Restricted Transfer without a valid transfer mechanism and appropriate supplementary measures; or (iv) conflict with a binding order or instruction of a competent supervisory authority applicable to the Customer, then the Customer may submit a written objection ("**Objection**") to Digital Samba within fifteen (15) days of receipt of the Change Notice ("**Objection Period**"). The Objection must set out the legal basis relied upon, the facts giving rise to the concern, and the processing at issue. Objections based solely on commercial considerations, vendor preference, or speculative harms do not constitute reasonable grounds. If Digital Samba does not receive an Objection within the Objection Period, the proposed addition or replacement of the subprocessor described in the Change Notice shall be deemed accepted by the Customer and may take effect on the effective date specified therein.

6.2.3. Good-faith resolution. Upon receipt of an Objection within the Objection Period, the Parties shall discuss in good faith to address the Customer's concerns. Without limitation, Digital Samba may (a) provide additional information or independent attestations, (b) implement additional appropriate technical and organisational measures, or (c) isolate, re-route or otherwise re-configure the processing for the Customer to avoid use of the disputed subprocessor where reasonably feasible.

6.2.4. No unreasonable withholding. The Customer shall not submit an Objection unreasonably, or unreasonably withhold, condition, or delay acceptance of the Change Notice, where the proposed subprocessor affords at least a materially equivalent level of protection as required under these Clauses and applicable Data Protection Laws (including, if applicable, a valid transfer mechanism and any necessary supplementary measures for any Restricted Transfer). The Customer must specify in writing any residual, concrete non-compliance or material risk, with reference to specific facts and applicable law.

6.2.5. No resolution. If, after the Parties' good-faith discussions under Clause 6.2.3, an Objection is not resolved within fifteen (15) days of Digital Samba's receipt (the "**Resolution Period**"), either Party may, by written notice, terminate the Agreement in accordance with Clause 13.5.

6.2.6. Emergency replacement. Where Digital Samba reasonably determines that an immediate subprocessor change is necessary to maintain confidentiality, integrity or availability of the services (including to address a security incident, service disruption or legal requirement), it may replace or add a subprocessor without prior notice, provided it issues a Change Notice without undue delay (and where legally restricted, as soon as permitted). The Customer may object under clause 6.2.2, and clauses 6.2.3–6.2.5 shall apply.

6.2.7. Clarification. For clarity, a change of subprocessor in accordance with this Section 6 does not, by itself, constitute a breach of the Agreement or these Clauses.

6.3. Imposed obligations. Where Digital Samba engages a subprocessor for carrying out specific processing activities on behalf of the Customer, the same data protection obligations as set out in the Clauses shall be imposed on that subprocessor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR. Digital Samba shall therefore be responsible for requiring that the subprocessor at least complies with the obligations to which Digital Samba is subject pursuant to the Clauses and the GDPR.

6.4. Liability. If the subprocessor does not fulfil its data protection obligations, Digital Samba shall remain fully liable to the Customer as regards the fulfilment of the obligations of the subprocessor. This does not affect the rights of the data subjects under the GDPR – in particular, those foreseen in Articles 79 and 82 GDPR – against the Data Controller and the Data Processor, including the subprocessor.

6.5. Third-country transfers. Where a subprocessor is located outside the EEA (or otherwise engages in a restricted transfer), Digital Samba shall ensure a valid transfer mechanism and implement supplementary measures as required by GDPR and applicable laws.

6.6. Transparency. Upon reasonable request, Digital Samba shall provide information reasonably necessary to demonstrate the subprocessor's compliance with this Section 6, subject to confidentiality.

7. Transfer of data to third countries or international organisations

7.1. Any transfer of personal data to third countries or international organisations by Digital Samba shall only occur on the basis of documented instructions from the Customer and shall always take place in compliance with Chapter V GDPR.

7.2. In case transfers to third countries or international organisations, which Digital Samba has not been instructed to perform by the Customer, is required under EU or Member State law to which Digital Samba is subject, Digital Samba shall inform the Customer of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

7.3. Without documented instructions from the Customer, Digital Samba therefore cannot within the framework of the Clauses:

> **7.3.1** Transfer personal data to a Data Controller or a Data Processor in a third country or in an international organisation
>
> **7.3.2** Transfer the processing of personal data to a subprocessor in a third country
>
> **7.3.3** Have the personal data processed by Digital Samba in a third country

7.4. The Customer's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

7.5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the Parties as a transfer tool under Chapter V GDPR.

8. Assistance to the Customer

8.1. Taking into account the nature of the processing, Digital Samba shall assist the Customer by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the Customer's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that Digital Samba shall, insofar as this is possible, assist the Customer in compliance with:

> **8.1.1.** The right to be informed when collecting personal data from the data subject
>
> **8.1.2.** The right to be informed when personal data have not been obtained from the data subject

8.1.3. The right of access by the data subject

8.1.4. The right to rectification

8.1.5 The right to erasure ("the right to be forgotten")

8.1.6. The right to restriction of processing

8.1.7. Notification obligation regarding rectification or erasure of personal data or restriction of processing

8.1.8 The right to data portability

8.1.9. The right to object

8.1.10. The right not to be subject to a decision based solely on automated processing, including profiling

8.2. In addition to Digital Samba's obligation to assist the Customer pursuant to Clause 5.3, Digital Samba shall furthermore, taking into account the nature of the processing and the information available to Digital Samba, assist the Customer in ensuring compliance with:

8.2.1. The obligation to notify the personal data breach to the competent supervisory authority without undue delay and, where feasible, not later than 48 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

8.2.2. The obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

8.2.3. The obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

8.2.4. The obligation to consult the competent supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Customer to mitigate the risk.

8.3. The Parties shall define in Appendix C the appropriate technical and organisational measures by which Digital Samba is required to assist the Customer as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 8.1. and 8.2.

9. Notification of personal data breach

9.1. In case of any personal data breach, Digital Samba shall, without undue delay after having become aware of it, notify the Customer of the personal data breach.

9.2. Digital Samba's notification to the Customer shall, if possible, take place within 24 hours after Digital Samba has become aware of the personal data breach to enable the Customer to comply with its notification obligations.

9.3. In accordance with Clause 8(2)(a), Digital Samba shall assist the Customer in notifying the personal data breach, meaning that Digital Samba is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the notification to the competent supervisory authority:

9.3.1. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

9.3.2. The likely consequences of the personal data breach;

9.3.3. The measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

9.4. The Parties shall define in Appendix C all the elements to be provided by Digital Samba when assisting the Customer in the notification of a personal data breach to the competent supervisory authority.

10. Erasure and return of data

10.1. On termination of the provision of personal data processing services, Digital Samba shall be under obligation to delete all personal data processed on behalf of the Customer and certify to the Customer that it has done so unless Union or Member State law requires storage of the personal data.

11. Audit and inspection

11.1. Digital Samba shall make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, by the Customer or another auditor mandated by the Customer.

11.2. Procedures applicable to the Customer's audits, including inspections, are specified in Appendix C.7.

11.3. Digital Samba shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Customer's and Digital Samba's facilities, or representatives acting on behalf of such supervisory authorities, with access to Digital Samba's physical facilities on presentation of appropriate identification.

12. The Parties' agreement on other terms

12.1. The Parties may agree to other clauses concerning the provision of the personal data processing services specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

13. Commencement and termination

13.1. The Clauses shall become effective on the date of both Parties' signature.

13.2. Both Parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

13.3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the Parties.

13.4. Upon expiry or termination of the Agreement, or earlier if the processing of Personal Data under the Agreement ends, and once Digital Samba has returned or deleted Personal Data in accordance with Clause 10.1 and Appendix C.4, these Clauses automatically terminate, without further notice, to the extent they relate to such processing. Provisions that by their nature survive (including confidentiality and return/deletion obligations) continue in force.

13.5. Notwithstanding clause 13.3, where the Customer has submitted an Objection within the Objection Period that meets the requirements of Clause 6.2.2 and the Parties have not resolved the Objection within the Resolution Period, either Party may terminate the Agreement (and, as a consequence, these Clauses) by written notice. This termination is no-fault and without penalty: (a) no refunds or credits are due, (b) no early-termination fees or further charges accrue after the termination effective date, and (c) except for fees accrued and payable up to the termination effective date, neither Party shall have any further liability to the other arising out of or in connection with the unresolved Objection, the subprocessor change, or the termination under this clause; provided that nothing in this clause limits a Party's liability for amounts due and owing, fraud, wilful misconduct, or breaches occurring before the termination effective date. The Parties shall promptly cease the affected processing, and Digital Samba shall return or delete Personal Data in accordance with Clause 10.1 and Appendix C.4. Termination under this Clause is the Parties' sole and exclusive remedy for an unresolved Objection.

14. Contact points and notices

14.1. Designated contacts. The Parties designate the contact points below for communications under these Clauses. Notices under Clause 6 (including Change Notices and Objections) must be sent to the “Notice Email” listed below. Email notice is sufficient.

14.2. Deemed receipt. An email notice is deemed received when sent, provided the sender does not receive an automatic non-delivery message. If sent outside the recipient’s business hours at its principal place of business, it is deemed received at the start of the next business day.

14.3. Updates. Each Party shall keep its contact details up to date and may update them by emailing the other Party. Notices sent to the last notified contact details are valid until an update takes effect.

Customer contact details

FULL NAME

POSITION

TELEPHONE

NOTICE EMAIL

Digital Samba contact details

FULL NAME	ROBERT STROBL
POSITION	CEO, DIGITAL SAMBA
TELEPHONE	+34 937 370 415
NOTICE EMAIL	dpo@digitalsamba.com

15. Execution and signatures

15.1. These Clauses shall become effective on the date of the last signature executed below (the "**Effective Date**"). The Parties agree that electronic signatures shall have the same legal force and effect as original handwritten signatures.

15.2. Each signatory represents that they are duly authorised to bind the Party they represent.

Signed for and on behalf of the Customer

COMPANY NAME

FULL NAME

POSITION

DATE

SIGNATURE

Signed for and on behalf of Digital Samba

COMPANY NAME	DIGITAL SAMBA, S.L.
FULL NAME	ROBERT STROBL
POSITION	CEO, DIGITAL SAMBA
DATE	
SIGNATURE	

Appendix A:
Information about the processing

1. The nature and purpose of the processing

Personal data is processed for the purpose of providing the Services to Users. The specific purposes are as follows:

1.1. To provide and operate the Services. We process personal data to deliver the Services, including authenticating Users, enabling participation in sessions, storing and delivering session content, and maintaining the operational functionality of the Services.

1.2. To provide analytics and reporting. We process usage and session data to provide the Customer with analytics, statistics, and reporting features within the Services.

1.3. To provide customer support. If the Customer chooses to engage us for supporting their Users, we process User information to resolve technical issues, respond to requests for assistance, and diagnose service problems.

1.4. To deliver data to the Customer. We process personal data to transmit session events, participant activity, and other data to the Customer's systems via webhooks and the API, as configured by the Customer.

2. The types of personal data processed

Personal data is processed as a consequence of using the Services, inputting data into the Services, providing data via the API, or providing data to us outside the Services. The types of personal data processed depend on the capacity in which the User interacts with the Services, as described below.

2.1. Account registration and management data. When Users create accounts to access the Services, we collect and process registration information including email address and password credentials. To complete their account profile, Users may provide their name, phone number, company name, job title, industry, and country. Country may be derived from the User's IP address at the time of registration; the IP address itself is not stored as part of this process. Where Users enable two-factor authentication, we process the associated authentication secret. Where Users generate API credentials, we process and store the associated keys. We also process team membership data, including roles and invitation status, where multiple Users manage a single account.

2.2. Participant identification data. When Users join a session, identification data is collected to enable participation. This includes a display name and, optionally, initials. The Customer may also provide a participant identifier via the API (external ID) to correlate session participants with users in the Customer's own systems. A randomly generated browser identifier is stored to support session continuity and moderation features such as participant bans. This identifier is not derived from the User's device or browser characteristics.

2.3. Content created during sessions. Users may create content during sessions, including chat messages, questions and answers, poll and quiz responses, shared notes, and files or documents uploaded for presentation. Where recording is enabled, audio and video recordings of the session are created and stored. Where captioning is enabled, speech-to-text transcripts are generated and stored. Where session summaries are enabled, an AI-generated summary is derived from the transcript and stored.

2.4. Data generated automatically during sessions. The Services automatically collect technical and usage data during sessions. This includes per-connection data such as device and browser metadata (browser name and version, operating system, and device type) and session participation records (join time, leave time, and duration), as well as aggregate usage statistics (such as total minutes of video, audio, and screen sharing). Per-connection records are stored alongside the participant identification data described in Section 2.2.

2.5. Telephony data. Where telephony dial-in is enabled, the phone number and caller identification of Users who connect via the public telephone network are processed as part of call handling. This data is recorded in call detail record log files and is not stored at the application level.

2.6. Data returned to the Customer. Where the Customer configures webhooks or uses the API to retrieve session data, personal data - including participant names, identifiers, and session activity - is transmitted to the Customer's own systems. The Services do not retain a separate copy of data transmitted via webhooks; the source data resides in the records described in Sections 2.2 through 2.4.

2.7. Information provided through support channels. If the Customer chooses to engage us for supporting their Users, Users may choose to submit information regarding a question or problem they are experiencing with the Services. Whether the User designates themselves as a technical contact, opens a support ticket, speaks to one of our representatives directly or otherwise engages with our support team, the User will be asked to provide contact information, a summary of the problem they are experiencing, and any other documentation, screenshots or information that would be helpful in resolving the issue.

2.8. Server-side technical data. The Services generate and process server access logs for connection handling, security monitoring, and troubleshooting. The only personal data contained in these logs is the User's IP address. No other personally identifiable information is recorded in server access logs. This data is not stored at the application level and is processed by Digital Samba as an independent controller (see Appendix A, Section 5).

3. The categories of data subjects being processed.

3.1. Users. Persons who use the Services, including account holders and participants in sessions hosted through the Services. The types of personal data processed depend on the capacity in which a User interacts with the Services, as described in Section 2.

4. The duration of the processing

How long personal data is retained depends on the type of data, as described below. When personal data is deleted - whether by User action, Customer action, or upon termination of the Agreement - it is removed from the application immediately. Residual copies in backup archives and server logs are purged within ninety (90) days through standard rotation. During this period, backup and log data is securely stored and isolated from any further use.

4.1. Account registration and management data. Account data (Section 2.1) is retained for as long as the account remains active. When a User deletes their account, all associated personal data is removed from the application immediately.

4.2. Participant identification data. Participant identification data (Section 2.2) is retained as part of the session record. The Customer may delete session records at any time through the Services or the API, at which point all participant personal data within the deleted records is removed from the application immediately. Where a participant has been banned from a session, the browser identifier and associated data are retained until the ban expires or is revoked by the Customer.

4.3. Content created during sessions. Session content (Section 2.3) is retained until the Customer deletes it. The Customer may delete session content and recordings at any time through the Services or the API, at which point the personal data within the deleted content is removed from the application immediately.

4.4. Data generated automatically during sessions. When session records are deleted (see Section 4.2), participant identification data (Section 2.2) is removed from the per-connection records. The remaining non-identifying statistical data (Section 2.4) is retained to support the Customer's analytics and reporting needs.

4.5. Telephony data. Call detail record log files containing telephony data (Section 2.5) are retained for a maximum of ninety (90) days and then automatically purged through log rotation.

4.6. Data returned to the Customer. Once personal data has been transmitted to the Customer via webhooks or the API (Section 2.6), the transmitted copy is under the Customer's control. As no separate copy is retained by the Services, the retention of the underlying source data is governed by the applicable provisions in Sections 4.2 through 4.4.

4.7. Information provided through support channels. Support data (Section 2.7) is retained in our support ticketing system for the duration of the business relationship with the Customer. Upon termination of the Agreement, support tickets and associated personal data are removed within ninety (90) days. Certain support data may be retained beyond this period where required to comply with legal obligations or to resolve outstanding disputes.

4.8. Server-side technical data. Server access logs (Section 2.8) are retained for a maximum of ninety (90) days and then automatically purged through log rotation. This data is processed by Digital Samba as an independent controller, as described in Section 5.

4.9. Termination. Upon termination or expiry of the Agreement, Digital Samba will remove all personal data processed on behalf of the Customer from the application. Residual copies in backup archives and server logs are purged within ninety (90) days, unless retention is required by applicable law.

5. Digital Samba as an independent controller

For certain limited operational purposes, Digital Samba processes personal data as an independent controller. These purposes include: (a) security monitoring and abuse prevention, including the processing of IP addresses in server access logs (retained for a maximum of 90 days, legal basis: Article 6(1)(f) GDPR); (b) service improvement through Digital Samba's own aggregated, de-identified usage analytics; (c) compliance with legal obligations; and (d) account administration and billing. This processing arises from Digital Samba's own legal and operational obligations and is not subject to the Customer's instructions under these Clauses.

Appendix B: Authorised subprocessors

1. Approved subprocessors

On commencement of the Clauses, the Customer authorises the engagement of the following subprocessors:

Name	Registration Number	Address	Description of processing
LEASEWEB DEUTSCHLAND GMBH	HRB 89607	LEASEWEB DEUTSCHLAND GMBH KLEYERSTRASSE 75-87 60326 FRANKFURT AM MAIN	German hosting partner with data centres located in Germany.
LEASEWEB NETHERLANDS B.V.	30141839	LEASEWEB NETHERLANDS B.V. HESSENBERGWEG 95 1101 CX AMSTERDAM NETHERLANDS	Dutch hosting partner with data centres located in the Netherlands.
SCALEWAY SAS	FR35433115904	SCALEWAY SAS 8 RUE DE LA VILLE L'EVÊQUE 75008 PARIS FRANCE	French hosting partner with data centres located in Europe.
AKENES SA ("Exoscale")	CHE-423.524.322	AKENES SA BOULEVARD DE GRANCY 19A 1006 – LAUSANNE SWITZERLAND	Swiss hosting partner for on-demand infrastructure scaling in Europe.
GreenPT B.V.	97084360	GREENPT B.V. PLOMPETORENGRACHT 4 3512CC UTRECHT NETHERLANDS	Dutch provider of AI speech-to-text (transcriptions, captions) and LLM services (translations, summaries, prompts).
HUBSPOT, INC.	000955519	HUBSPOT, INC. 25 FIRST STREET CAMBRIDGE, MA 02141 USA	**OPTIONAL** COMPONENT In certain cases, you may ask us to provide direct support to Users of the Services. Data entered into support tickets is processed and stored in Hubspot. As part of the Services, we may also redirect Users to experience feedback forms. Data entered in those forms is processed and stored in Hubspot. This feature can be disabled.

Appendix C:

Instructions on the use of personal data

1. The subject of/instruction for the processing

Digital Samba's processing of personal data on behalf of the Customer shall be carried out by Digital Samba performing the following:

- Personal data of Users is processed for the purpose of providing the Services to Users.

2. Security of processing

The level of security that shall be taken into account: Processing involves a large volume of personal data which is why a "high" level of security should be established.

Digital Samba shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

Digital Samba shall, however– in any event, and at a minimum– implement the following measures that have been agreed with the Customer:

2.1. Information security policies. A set of policies for information security is defined, approved by management, published, and communicated to employees and relevant external parties.

2.2. Organisation of information security. Information security responsibilities are defined and allocated.

2.3. Human resource security. Background verification checks are carried out in accordance with relevant laws and regulations and contractual agreements state the responsibilities for information security. All team members receive appropriate awareness education and regular updates in organisational policies.

2.4. Asset management. An inventory of information assets and processing facilities is maintained and rules for acceptable use are documented and implemented. Information is classified and procedures for the handling of assets in accordance with the classification scheme are implemented.

2.5. Access control. An access control policy is established, documented, and reviewed and access to information and applications is restricted accordingly. Processes for user registration and deregistration as well as access provisioning are implemented. Access rights are reviewed at regular intervals.

2.6. Cryptography. A policy on the use of cryptographic controls for the protection of information is implemented.

2.7. Physical security. Systems are exclusively hosted in data centres providing adequate standards for information security.

2.8. Operations security. Operating procedures are documented and changes to information processing facilities are controlled. Development, testing, and operational environments are separated to reduce the risk of unauthorised changes to the operational environment. Controls to protect against malware are implemented and backups of information are taken and tested regularly. Event logs recording system administrator activities and security events are produced and regularly reviewed. Information about technical vulnerabilities of information systems is obtained in a timely fashion and appropriate measures to address the associated risk are taken.

2.9. Communications security. Networks are managed and controlled to protect information and groups of information services are segregated on networks. Communication with applications utilised cryptographic controls such as TLS to protect the information in transit over public networks. Stateful firewalls, web application firewalls, and DDoS protection are used to prevent attacks.

2.10. System acquisition, development, and maintenance. Information security requirements are taken into consideration for new information systems or enhancements to existing information systems. Rules for the secure development of software and systems are established and applied and testing of security functionality is carried out at regular intervals.

2.11. Incident management. Incident management responsibilities and procedures are established to ensure a quick, effective and orderly response to security incidents.

3. Assistance to the Customer

Digital Samba shall insofar as this is possible assist the Customer by implementing the following technical and organisational measures:

3.1. Measures for ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services

3.2. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

3.3. Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures to ensure the security of the processing

3.4. Measures for User identification and authorisation

3.5. Measures for the protection of data during transmission

3.6. Measures for the protection of data during storage

3.7. Measures for ensuring the physical security of locations at which personal data are processed

3.8. Measures for ensuring events logging

3.9. Measures for internal IT and IT security governance and management

3.10. Measures for certification/assurance of processes and products

3.11. Measures for ensuring data minimisation

3.12. Measures for ensuring data quality

3.13. Measures for ensuring limited data retention

3.14. Measures for ensuring accountability

3.15. Measures for allowing data portability and ensuring erasure

4. Storage period/erasure procedures

Personal data is stored for the time of providing the Services to Users after which the personal data is automatically erased by Digital Samba.

Upon termination of the provision of personal data processing services, Digital Samba shall either delete or return the personal data in accordance with Clause 10.1., unless the Customer - after the signature of the contract – has modified the Customer’s original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the Customer’s prior written authorisation:

- Europe
- United States (OPTIONAL)

European B2B customers can choose a configuration (by excluding the optional components listed in Appendix B) where all personal data processing is performed exclusively in European locations.

6. Instruction on the transfer of personal data to third countries

As recommended by the European Data Protection Board (EDPB), when personal data is transferred to third countries, appropriate transfer tools are verified in accordance with Chapter V GDPR (the transfer tools listed under Articles 46 GDPR). Additionally, the law or practice of the third country is assessed, and supplementary measures are identified and adopted to bring the level of protection of the data transferred up to the EU standard of essential equivalence. The level of protection is reevaluated at appropriate intervals.

If the Customer does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, Digital Samba shall not be entitled within the framework of the Clauses to perform such transfer.

7. Procedures for the Customer's audits, including inspections, of the processing of personal data being performed by Digital Samba

As required pursuant to article 28(3)(h) GDPR, Digital Samba will allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer required pursuant to article 28(3)(h) GDPR. The Customer shall give Digital Samba reasonable notice of any audit or inspection to be conducted and shall make (and ensure that each of its mandated auditors makes) reasonable effort to avoid any damage, injury or disruption to Digital Samba, its premises, equipment, personnel and business. Under all circumstances, all costs concerning an audit are borne by the Customer.

Appendix D:

Terms of agreements on other subjects

There are no additional terms.