# Digital Samba Embedded
# Data Processing Agreement

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

Last modified: 17 September, 2025

Changes: Added GreenPT subprocessor. Clarified subprocessor conditions.

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 controller, processor, personal data, and processing have the meanings given in the GDPR.

This DPA only applies to the extent that Customer (as Data Controller) instructs Digital Samba (as Data Processor) 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 "**Data Controller**")

and

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

(the "**Data Processor**")

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

# 1. Preamble

**1.1.** These contractual clauses (the "**Clauses**") set out the rights and obligations of the Data Controller and the Data Processor, when processing personal data of the Data Controller's End Users ("**User**" or "**Users**") on behalf of the Data Controller.

**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, the Data Processor will process Users' personal data on behalf of the Data Controller 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 Data Controller. Appendix B may be updated by the Data Processor in accordance with clause 6.

**1.9.** Appendix C contains the Data Controller'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 the Data Processor from obligations to which the Data Processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

## 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 the Data Processor is instructed to perform, has a legal basis.

## 3. The Data Processor acts according to instructions

**3.1.** The Data Processor shall process personal data only on documented instructions from the Data Controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the Data Controller 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.** The Data Processor shall immediately inform the Data Controller if instructions given by the Data Controller, in the opinion of the Data Processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

## 4. Confidentiality

**4.1.** The Data Processor shall only grant access to the personal data being processed on behalf of the Data Controller to persons under the Data Processor'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 access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

**4.2.** The Data Processor shall at the request of the Data Controller demonstrate that the concerned persons under the Data Processor's authority are subject to the abovementioned confidentiality.

## 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 Data Controller and Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

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

The Data Controller 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, the Data Processor shall also – independently from the Data Controller – 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 Data Controller shall provide the Data Processor with all information necessary to identify and evaluate such risks.

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

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

## 6. Use of subprocessors

**6.1. General authorisation.** The Data Controller grants a general written authorisation for the Data Processor to engage subprocessors. The Data Processor shall maintain a current list of authorised subprocessors in Appendix B.

**6.2. Engagement & change management.** The Data Processor 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.** The Data Processor shall notify the Data Controller 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 Data Controller 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 Data Controller has specific, reasonable grounds that engagement of the proposed subprocessor would: (i) cause the Data

Controller 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 Data Controller, then the Data Controller may submit a written objection ("**Objection**") to the Data Processor 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 the Data Processor 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 Data Controller 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 Data Controller's concerns. Without limitation, the Data Processor 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 Data Controller to avoid use of the disputed subprocessor where reasonably feasible.

**6.2.4. No unreasonable withholding.** The Data Controller 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 Data Controller 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 the Data Processor'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 the Data Processor 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 Data Controller 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 the Data Processor engages a subprocessor for carrying out specific processing activities on behalf of the Data Controller, 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. The Data Processor shall therefore be responsible

for requiring that the subprocessor at least complies with the obligations to which the Data Processor is subject pursuant to the Clauses and the GDPR.

**6.4. Liability.** If the subprocessor does not fulfil its data protection obligations, the Data Processor shall remain fully liable to the Data Controller 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), the Data Processor shall ensure a valid transfer mechanism and implement supplementary measures as required by GDPR and applicable laws.

**6.6. Transparency.** Upon reasonable request, the Data Processor 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 the Data Processor shall only occur on the basis of documented instructions from the Data Controller and shall always take place in compliance with Chapter V GDPR.

**7.2.** In case transfers to third countries or international organisations, which the Data Processor has not been instructed to perform by the Data Controller, is required under EU or Member State law to which the Data Processor is subject, the Data Processor shall inform the Data Controller 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 Data Controller, the Data Processor 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 the Data Processor in a third country

**7.4.** The Data Controller'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 Data Controller

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

This entails that the Data Processor shall, insofar as this is possible, assist the Data Controller in the Data Controller's 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 the Data Processor's obligation to assist the Data Controller pursuant to Clause 5.3, the Data Processor shall furthermore, taking into account the nature of the processing and the information available to the Data Processor, assist the Data Controller in ensuring compliance with:

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

**8.2.2.** The Data Controller's 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 Data Controller's 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 Data Controller's 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 Data Controller to mitigate the risk.

**8.3.** The Parties shall define in Appendix C the appropriate technical and organisational measures by which the Data Processor is required to assist the Data Controller 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, the Data Processor shall, without undue delay after having become aware of it, notify the Data Controller of the personal data breach.

**9.2.** The Data Processor's notification to the Data Controller shall, if possible, take place within 24 hours after the Data Processor has become aware of the personal data breach to enable the Data Controller to comply with the Data Controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

**9.3.** In accordance with Clause 8(2)(a), the Data Processor shall assist the Data Controller in notifying the personal data breach to the competent supervisory authority, meaning that the Data Processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the Data Controller's 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 the Data Processor when assisting the Data Controller 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, the Data Processor shall be under obligation to delete all personal data processed on behalf of the Data Controller and certify to the Data Controller that it has done so unless Union or Member State law requires storage of the personal data.

## 11. Audit and inspection

**11.1.** The Data Processor shall make available to the Data Controller 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, conducted by the Data Controller or another auditor mandated by the Data Controller.

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

**11.3.** The Data Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Data Controller's and Data Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the Data Processor'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 the Data Processor 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 Data Controller 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 the Data Processor 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.

**Data Controller contact details**

| | |
|---|---|
| NAME | |
| POSITION | |
| TELEPHONE | |
| NOTICE EMAIL | |

**Data Processor contact details**

| | |
|---|---|
| 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 Data Controller**

COMPANY NAME

NAME

POSITION

DATE

SIGNATURE

**Signed for and on behalf of the Data Processor**

| | |
|---|---|
| COMPANY NAME | DIGITAL SAMBA, S.L. |
| 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.

How we use the information we collect depends in part on which features of the Services are used, how they are used and any preferences communicated to us. Below are the specific purposes for which we use the information we collect.

**1.1. To provide the Services and personalise the User's experience.** We use information about Users to provide the Services to them, including to process transactions, authenticate Users when logging in, providing customer support and operating and maintaining the Services. For example, we use the name and picture provided by Users to identify them to other Users of the Services. The Services also include tailored features that personalise the User's experience, enhance productivity, and improve the ability to collaborate effectively with other Users.

**1.2. For research and development.** We are always looking for ways to make the Services smarter, faster, more secure, integrated and useful. We use collective learnings about how Users use the Services and feedback provided directly to us to troubleshoot and to identify trends, usage, activity patterns and areas for integration and improvement of the Services. In some cases, we apply these learnings across the Services to improve and develop similar features or to better integrate the Services used. We also test and analyse certain new features with some Users before rolling the feature out to all Users.

**1.3. To provide customer support.** If the Data Controller chooses to engage us for supporting their Users, we use User information to resolve technical issues encountered, to respond to requests for assistance, to analyse crash information, and to repair and improve the Services.

**1.4. For safety and security.** We use information about Users and the Services to monitor suspicious or fraudulent activity and to identify violations of applicable policies of the Services.

**1.5. To protect our legitimate business interests and legal rights.** Where required by law or where we believe it is necessary to protect our legal rights, interests and the interests of others, we use information about Users in connection with legal claims, compliance, regulatory, and audit functions, and disclosures in connection with the acquisition, merger or sale of a business.

**1.6. With the User's consent.** We use information about Users where they have given us consent to do so for a specific purpose not listed above.

## 2. The types of personal data processed

User data is processed as a consequence of using the Services, inputting data directly into the Services or providing the data directly to us outside the Services. The processing of each of these data types is explained below.

**2.1. Profile information provided by Users.** When interacting with the Services, Users may choose to provide a screen name, profile photo, job title and other similar profile information to be displayed to other Users in the Services.

**2.2. Content provided by Users.** When interacting with the Services, Users may choose to provide content, including the name and details of a meeting, input messages (for example, chat messages, notes or Q&A messages) screen sharing, video and audio transmission, and User feedback. Content also includes files and links uploaded to the Services, as well as recordings made while using the Services.

**2.3. Data generated while using the Services.** The Services generate, process and store analytical and statistical usage data. This includes data on how Users interact with certain features of the Services.

**2.4. Information provided through support channels.** If the Data Controller 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.

## 3. The categories of data subjects being processed.

**3.1. Customer.** Person who uses the Services.

## 4. The duration of the processing.

How long we keep information we collect about Users depends on the type of information, as described in further detail below. After such time, we will either delete or anonymise personal information or, if this is not possible (for example, because the information has been stored in backup archives), then we will securely store the information and isolate it from any further use until deletion is possible.

**4.1. User profile information.** If the User does not interact with the Services, other than providing profile information, then the profile data is generally not stored and is processed only to display the User's profile information to other Users while the video conference is live. There are exceptions, such as when another User chooses to record the video conference. Recordings are part of User content, which is covered in the next section.

**4.2. User content.** When a User provides content to the Services during a video conference, this content forms part of the collective video conference experience and cannot be purged without

affecting the experience of other Users. We must therefore retain User content for the duration of the business relationship with the Data Controller and a reasonable time thereafter to allow for reactivation.

**4.3. User usage data.** We retain User usage data for the duration of the business relationship with the Data Controller and a reasonable time thereafter to allow for reactivation. Certain User usage data is retained for the duration necessary to comply with our legal obligations, to resolve disputes, to enforce our agreements, to support business operations and to continue to develop and improve the Services. Where we retain information for improvement and development of the Services, we take steps to eliminate information that directly identifies Users, and we only use the information to uncover collective insights about the use of the Services, not to specifically analyse any personal characteristics.

**4.4. Customer support data.** If the Data Controller chooses to engage us for supporting their Users, then User support data will be stored and processed in our support ticketing system. We retain User support data for the duration of the business relationship with the Data Controller and a reasonable time thereafter to allow for reactivation. In the absence of a clear relationship between the User and the Data Controller, in which case we cannot link the two entities, the User support data is retained until the User makes a deletion request or until a period of inactivity has passed, as defined in our data retention policies. In either case, certain User support data is retained for the duration necessary to comply with our legal obligations, to resolve disputes, to enforce our agreements, to support business operations and to continue to develop and improve the Services. Where we retain information for improvement and development of the Services, we take steps to eliminate information that directly identifies Users, and we only use the information to uncover collective insights about the use of the Services, not to specifically analyse any personal characteristics.

# Appendix B: Authorised subprocessors

## 1. Approved subprocessors

On commencement of the Clauses, the Data Controller authorises the engagement of the following subprocessors:

| Name | Registration Number | Address | Description of processing |
|---|---|---|---|
| LEASEWEB DEUTSCHLAND GMBH | HRB 89607 | LEASEWEB DEUTSCHLAND GMBH<br>KLEYERSTRASSE 75-87<br>60326 FRANKFURT AM MAIN | German hosting partner with data centres located in Germany. |
| LEASEWEB NETHERLANDS B.V. | 30141839 | LEASEWEB NETHERLANDS B.V.<br>HESSENBERGWEG 95<br>1101 CX AMSTERDAM<br>NETHERLANDS | Dutch hosting partner with data centres located in the Netherlands. |
| SCALEWAY SAS | FR35433115904 | SCALEWAY SAS<br>8 RUE DE LA VILLE L'EVÊQUE<br>75008 PARIS<br>FRANCE | French hosting partner used for on-demand scaling of our server infrastructure. |
| AKENES SA<br>("Exoscale") | CHE-423.524.322 | AKENES SA<br>BOULEVARD DE GRANCY 19A<br>1006 – LAUSANNE<br>SWITZERLAND | Swiss hosting partner used for on-demand scaling of our server infrastructure. |
| GreenPT B.V. | 97084360 | GREENPT B.V.<br>PLOMPETORENGRACHT 4<br>3512CC UTRECHT<br>NETHERLANDS | Dutch provider of AI speech-to-text (transcriptions, captions) and LLM services (translations, summaries, prompts). |
| | | | |
| HUBSPOT, INC. | 000955519 | HUBSPOT, INC.<br>25 FIRST STREET<br>CAMBRIDGE, MA 02141<br>USA | **OPTIONAL** COMPONENT<br><br>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.<br><br>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

The Data Processor's processing of personal data on behalf of the Data Controller shall be carried out by the Data Processor 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.

The Data Processor 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.

The Data Processor shall, however– in any event, and at a minimum– implement the following measures that have been agreed with the Data Controller:

**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 Data Controller

The Data Processor shall insofar as this is possible assist the Data Controller 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 the Data Processor.

Upon termination of the provision of personal data processing services, the Data Processor shall either delete or return the personal data in accordance with Clause 10.1., unless the Data Controller - after the signature of the contract – has modified the Data Controller'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 Data Controller'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 Data Controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the Data Processor shall not be entitled within the framework of the Clauses to perform such transfer.

## 7. Procedures for the Data Controller's audits, including inspections, of the processing of personal data being performed by the Data Processor

As required pursuant to article 28(3)(h) GDPR, the Data Processor will allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller required pursuant to article 28(3)(h) GDPR. The Data Controller shall give the Data Processor 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 the Data Processor, its premises, equipment, personnel and business. Under all circumstances, all costs concerning an audit are borne by the Data Controller.

# Appendix D:

# Terms of agreements on other subjects

*There are no additional terms.*