B2B Data Processing Agreement

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

Last modified: 30 November, 2022

Changes: Renamed DPA to B2B and renamed the term OEM to B2B.

This Data Processing Agreement ("**DPA**") applies to **B2B** customers. B2B customers handle invoicing and billing of their own end users and can choose whether they want to activate certain components, which affects whether a certain subprocessor is engaged or not.

This Data Processing Agreement is between:

COMPANY NAME

REGISTRATION NUMBER

ADDRESS

POSTCODE AND CITY

COUNTRY

(the "**Data Controller**")

and

COMPANY NAME	DIGITAL SAMBA, S.L.
REGISTRATION NUMBER	B63229629
ADDRESS	C/ ARIBAU 15, 5/4
POSTCODE AND CITY	08011 BARCELONA
COUNTRY	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 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 video conferencing services (the "**Services**"), the Data Processor will process personal data on behalf of the Data Controller in accordance with the Clauses.

1.4. The Clauses shall take priority over any similar provisions contained in other agreements between the Parties.

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

1.6. 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.

1.7. Appendix B contains the Data Controller's conditions for the Data Processor's use of subprocessors and a list of subprocessors authorised by the Data Controller.

1.8. Appendix C contains the Data Controller's instructions with regards to the processing of personal data.

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

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

1.11. 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.

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

2.3. The Data Controller shall be responsible, among other, 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.

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 require 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. 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. The Data Processor shall therefore not engage another processor (subprocessor) for the fulfilment of the Clauses without the prior general written authorisation of the Data Controller.

6.3. 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. If the subprocessor does not fulfil his 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.

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 in 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 service 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. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the Data Controller pursuant to Clause 10.1. and Appendix C.4., the Clauses may be terminated by written notice by either Party.

13.5. Signed on behalf of the **Data Controller**:

NAME

POSITION

DATE

SIGNATURE

And on behalf of the **Data Processor**:

NAME	ROBERT STROBL
POSITION	CEO, DIGITAL SAMBA
DATE	
SIGNATURE	

14. Data Controller and Data Processor contact points

14.1 The Parties may contact each other using the following contact points:

Data Controller

NAME	
POSITION	
TELEPHONE	
EMAIL	

Data Processor

NAME	ROBERT STROBL
POSITION	CEO, DIGITAL SAMBA
TELEPHONE	+34 93 18 555 10
EMAIL	support@digitalsamba.com

14.2. The Parties shall be under obligation to continuously inform each other of changes to contact points.

Appendix A:

Information about the processing

1. The nature and purpose of the Data Processor's processing of personal data on behalf of the Data Controller

Personal data is processed for the purpose of providing the Services to customers ("**User**" or "**Users**").

How we use the information we collect depends in part on which 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 user 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 the Users in the account to identify them to other Service Users. Our Services also include tailored features that personalise the Users experience, enhance productivity, and improve the ability to collaborate effectively with others. We may use the email domain to infer a User's affiliation with a particular organisation or industry to personalise the content and experience they receive on our websites. Where multiple Services are used, we combine information about Users and their activities to provide an integrated experience, such as to allow Users to find information from one Service while searching from another or to present relevant product information as they travel across our websites.

1.2. For research and development. We are always looking for ways to make our Services smarter, faster, secure, integrated, and useful. We use collective learnings about how people use our 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 our 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 communicate with Users about the Services. We use contact information to send transactional communications via email and within the Services, including confirming purchases, reminding of subscription expirations, responding to comments, questions and requests, providing customer support, and sending technical notices, updates, security alerts, and administrative messages. We send email notifications when Users interact with others on the Services, for example, when a User is invited by another User to their meeting, we send an email invitation with instructions on how to join that meeting. We also send communications as Users onboard to a particular Service to help them become more proficient in using that Service. Some of these communications are part of the Services and in those cases, Users cannot opt out of them. If an opt out is available, Users will find that option within the communication itself.

1.4. To market, promote and drive engagement with the Services. We use contact information and information about how the Services are used to send promotional communications that may be of specific interest to Users, including by email and by displaying our ads on other companies' websites and applications, as well as on platforms like Facebook and Google. These communications are aimed at driving engagement and maximising what Users get out of the Services, including information about new features, survey requests, newsletters, and events we think may be of interest to Users. We also communicate with Users about new product offers, promotions and contests. Users can control whether they receive these communications.

1.5. Customer support. 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.

1.6. For safety and security. We use information about Users and Service use to verify accounts and activity, to monitor suspicious or fraudulent activity and to identify violations of Service policies.

1.7. 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.

1.8. With Users' consent. We use information about Users where they have given us consent to do so for a specific purpose not listed above. For example, we may publish testimonials or featured customer stories to promote the Services, with the User's permission.

2. The processing includes the following types of personal data about data subjects

We collect information about Users when they input it into the Services or otherwise provide it directly to us.

2.1. Account and Profile Information. We collect information about Users when they register for an account, create or modify their profile, set preferences, sign up for or make purchases through the Services. For example, Users provide their contact information and, in some cases, billing information when they register for the Services. They also have the option of adding a user name, profile photo, job title, and other details to their profile information to be displayed in our Services. We keep track of their preferences when they select settings within the Services.

2.2. Content Users provide through our products. The Services include the products used, where we collect and store content that is uploaded, sent, received and shared. This content includes any information about Users that they may choose to include. Examples of content we collect and store include: the name and details of a meeting along with names and emails of people invited to it; the messages exchange with other Users in the Account Centre or via the meeting chat; sharing of Users screen or video and audio to others in a meeting and recording it; and any feedback Users provide to us. Content also includes the files and links uploaded to the Services. If a server version of the Services is used, we do not host, store, transmit, receive or collect information about Users (including User's content), except in limited cases, where permitted by the User or their

organisation: we collect feedback Users provide directly to us through the product and; we collect content using analytics techniques that hash, filter or otherwise scrub the information to exclude information that might identify Users or their organisation; and we collect clickstream data about how Users interact with and use features in the Services. Server administrators can disable our collection of this information from the Services via configuration settings or prevent this information from being shared with us by blocking transmission at the local network level.

2.3. Content provided through our websites. The Services also include our websites owned or operated by us. We collect other content that Users submit to these websites, which include social media or social networking websites operated by us. For example, Users provide content to us when they provide feedback or when they participate in any interactive features, surveys, contests, promotions, sweepstakes, activities or events.

2.4. Information provided through our support channels. The Services also include our customer support, where Users may choose to submit information regarding a question or problem they are experiencing with a Service. Whether the User designates himself as a technical contact, opens a support ticket, speaks to one of our representatives directly or otherwise engage with our support team, the User will be asked to provide contact information, a summary of the problem he is experiencing, and any other documentation, screenshots or information that would be helpful in resolving the issue.

2.5. Payment Information. We collect certain payment and billing information when Users register for certain paid Services. For example, we ask Users to designate a billing representative, including name and contact information, upon registration. Users might also provide payment information, such as payment card details, which we collect via secure payment processing services.

3. Processing includes the following categories of data subjects

3.1. Customers. Users of the video conferencing services.

4. The Data Processor’s processing of personal data on behalf of the Data Controller may be performed when the Clauses commence.

4.1. Processing has the following duration. 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 anonymize 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.

4.2. Account information. We retain Users’ account information for as long as their account is active and a reasonable period thereafter in case they decide to reactivate the Services. We also retain some of the User’s information as 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 our Services. Where we retain information for Service improvement and development,

we take steps to eliminate information that directly identifies Users, and we only use the information to uncover collective insights about the use of our Services, not to specifically analyse any personal characteristics.

4.3. Information you share on the Services. If a user account is deactivated or disabled, some of the information and the content the User has provided will remain in order to allow the Users team members or other Users to make full use of the Services. For example, we continue to display messages Users sent to other Users that received them and continue to display content you provided.

4.4. Managed accounts. If the Services are made available to Users through an organisation (e.g., the employer), we retain User information as long as required by the administrator of the account.

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 ASIA PACIFIC PTE. LTD.	201332642C	LEASEWEB ASIA PACIFIC PTE. LTD. 11 COLLYER QUAY / THE ARCADE #16-02 SINGAPORE 049317	Our Asian hosting partner, which provides us with Asian server infrastructure for **Asian OEM customers**.
LEASEWEB DEUTSCHLAND GMBH	HRB 89607	LEASEWEB DEUTSCHLAND GMBH KLEYERSTRASSE 75-87 60326 FRANKFURT AM MAIN	Our German hosting partner, which provides us with European server infrastructure for **European OEM customers**.
LEASEWEB NETHERLANDS B.V.	30141839	LEASEWEB NETHERLANDS B.V. HESSENBERGWEG 95 1101 CX AMSTERDAM NETHERLANDS	Our Dutch hosting partner, which provides us with European server infrastructure for **European OEM customers**.
LEASEWEB USA, INC.	4863637	LEASEWEB USA, INC. 9301 INNOVATION DRIVE, SUITE 100 MANASSAS, VA 20110 USA	Our North American hosting partner, which provides us with North American server infrastructure for **North American OEM customers**.
HUBSPOT, INC.	000955519	HUBSPOT, INC. 25 FIRST STREET CAMBRIDGE, MA 02141 USA	**OPTIONAL** COMPONENT FOR OEM CUSTOMERS The Service Hub is a customer support platform. In certain cases, we provide **direct support** to the end users of our OEM customers.
CLOUDFLARE, INC.	C3274841	CLOUDFLARE, INC. 101 TOWNSEND ST. SAN FRANCISCO, CA 94107 USA	**OPTIONAL** COMPONENT FOR OEM CUSTOMERS Provides **distributed content caching** to ensure that end users experience a low latency experience when using our products and services.
FUNCTIONAL SOFTWARE, INC.	C3808470	FUNCTIONAL SOFTWARE, INC. 45 FREMONT STREET, 8TH FLOOR SAN FRANCISCO, CA 94105 USA	**OPTIONAL** COMPONENT FOR OEM CUSTOMERS Sentry provides us with a **centralised logging** tool that collects browser data which allows us to monitor, diagnose, fix, and optimise the performance of our products and services.

TWILIO, INC.	C3152782	TWILIO, INC. 375 BEALE STREET SUITE 300 SAN FRANCISCO, CA 94105 USA	**OPTIONAL** COMPONENTS FOR OEM CUSTOMERS The Programmable Voice service provides **phone and web audio integration**. The SendGrid service provides **mail server functionality** for sending emails from our products and services.

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 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 in regular intervals.

2.11. Incident management. Incident management responsibilities and procedures are established to ensure 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 authorization

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 minimization

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

European OEM 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.