PREAVA DATA PROCESSING ADDENDUM

Controller (Business) to Processor (Service Provider)

Version 9.1
Last Updated: September 29, 2023

This Preava Data Processing Addendum, including its three exhibits (this "**Addendum**"), is entered into by and between Preava, Inc., a corporation incorporated under the laws of the State of Delaware ("**Preava**") and the customer that has entered into Preava's Master Service Agreement (the "**Agreement**") with Preava (the "**Customer**") (each, a "**Party**" and, collectively, the "**Parties**"). This Addendum is made a part of the Agreement and will become effective when the last Party signs the Agreement (the "**Effective Date**").

Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended or supplemented by, and including, this Addendum.

This Addendum, which may be updated from time to time, forms an integral part of the Agreement. By using Preava's Services in any way, Customer is agreeing to the terms of this Addendum.

RECITALS

WHEREAS, the Parties entered into the Agreement and have retained the power to alter, amend, revoke, or terminate the Agreement as provided in the Agreement;

WHEREAS, in the course of providing its Services pursuant to the Agreement, Preava Processes certain Personal Data; and

WHEREAS, the Parties now wish to amend the Agreement to ensure that such Personal Data is Processed in compliance with applicable data protection principles and legal requirements;

NOW, THEREFORE, in consideration of the mutual agreements set forth in this Addendum, the Parties agree as follows:

1. Definitions

1.1. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified or supplemented below, the definitions of the Agreement shall remain in full force and effect.

1.2. For the purpose of interpreting this Addendum, the following terms (and their applicable cognates) shall have the meanings set out below:

(a) "**Affiliate**" means any entity within a controlled group of companies that directly or indirectly, through one or more intermediaries, is controlling, controlled by, or under common control with one of the Parties.

(b) "**Anonymized Data**" means data that was previously Personal Data which has been irreversibly anonymized by permanently removing and deleting all information that may reasonably be used to identify Data Subjects.

(c) "**Applicable Data Protection Laws**" means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including but not limited to the laws and regulations identified in **Exhibit B** hereto, as may be amended, modified, or supplemented from time to time, as applicable.

(d) "**Contracted Processor**" means any third party appointed by or on behalf of Preava to Process Customer Personal Data on behalf of Customer in connection with the Agreement.

(e) "**Controller**" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

(f) "**Customer Administrative Information**" means any information relating to an identified or identifiable natural person collected by Preava from Customer in connection with the vendor-customer relationship between Preava and Customer (e.g., the names or contact information of individuals authorized by Customer to access the Customer's account).

(g) "**Customer Personal Data**" means any Personal Data Processed by Preava or its Contracted Processors on behalf of Customer pursuant to or in connection with the Agreement.

(h) "**Customer Personal Data Recipient**" means Preava, a Contracted Processor, or both collectively, who receives Customer Personal Data.

(i) "**EU GDPR**" means Regulation (EU) 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," as may be amended from time to time.

(j) "**Personal Data**" means any information relating to an identified or identifiable natural person (a "**Data Subject**"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number,

location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. For clarity, Personal Data includes, but is not limited to, Customer Personal Data.

(k) "**Personal Data Breach**" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data. For the avoidance of doubt, a Personal Data Breach includes breaches of security affecting Customer Personal Data processed by Preava or by any of its Contracted Processors.

(l) "**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

(m) "**Processor**" means a natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of a Controller.

(n) "**Restricted International Transfer**" means any transfer of Customer Personal Data subject to Applicable Data Protection Laws to a Third Country (as defined under **Exhibit B** for each type of Restricted International Transfer) or an international organization in a Third Country (including data storage on foreign servers).

(o) "**Services**" means the services and other activities carried out by or on behalf of Preava for Customer pursuant to the Agreement.

(p) "**Standard Contractual Clauses**" are the model clauses for Restricted International Transfers adopted by the relevant authorities of the jurisdictions indicated in **Exhibit B**, as further defined and specified therein.

2. Term and Applicability

2.1. This Addendum shall take effect on the Effective Date and shall continue concurrently for the duration that Customer Personal Data is Processed by Preava pursuant to the Agreement.

2.2. This Addendum will apply to the Processing of all Customer Personal Data, regardless of country of origin, place of Processing, location of Data Subjects, or any other factor.

3. Processing and Disclosure of Personal Data

3.1. In the context of this Addendum and its exhibits, with regard to the Processing of Customer Personal Data: (1) when Customer acts as a Controller, Preava acts as a Processor; and (2) when Customer acts as a

Processor, Preava acts as a Sub-Processor. For the avoidance of doubt, both situations fall within the scope of and are covered by this Addendum. If Customer has agreed to the use of an anonymized version Customer Personal Data for Preava's training of its machine learning and artificial intelligence systems within the applicable Statement of Work or Order Form, Preava acts as an independent Controller of Customer Personal Data for the purpose of converting it to Anonymized Data. Personal Data being Processed by Preava as an independent Controller in such a situation no longer constitutes Customer Personal Data, and after anonymization, no longer constitutes Personal Data.

3.2. Preava shall:

(a) comply with all Applicable Data Protection Laws in the Processing of Personal Data;

(b) not Process Customer Personal Data other than on Customer's relevant documented instructions (including with regard to any international transfers of Customer Personal Data), unless such Processing is required by applicable laws to which the relevant Customer Personal Data Recipient is subject, in which case Preava shall, to the extent permitted by applicable laws, inform Customer of that legal requirement before the respective act of Processing of that Customer Personal Data;

(c) only conduct Restricted International Transfers of Customer Personal Data in compliance with the Applicable Data Protection Laws and the requirements of **Exhibit B**; and

(d) immediately inform Customer in the event that, in Preava's opinion, a Processing instruction given by Customer may infringe Applicable Data Protection Laws.

3.3. All necessary information relating to the details of the Processing is set out in **Exhibit A**, attached hereto and incorporated by reference. Customer shall be entitled to update **Exhibit A** from time to time by sending updated information to Preava using the contact details set forth in Section 19.1. Preava will be considered to have accepted any such update unless it provides Customer notice of non-acceptance within thirty (30) days following receipt.

3.4. Customer instructs Preava (and authorizes Preava to instruct each Contracted Processor it engages) to Process Customer Personal Data, and, in particular, to transfer Customer Personal Data to any country or territory, only as reasonably necessary for the provision of the Services and consistent with the Agreement and this Addendum.

3.5. Customer represents and warrants that it has all necessary rights to provide Customer Personal Data to Preava for the purpose of Processing such Customer Personal Data within the scope of this Addendum and the Agreement. Within the scope of the Agreement and in its use of the Services, Customer shall be solely responsible for complying with the statutory requirements relating to data protection and privacy, including the Applicable Data Protection Laws, and in particular regarding the disclosure and transfer of Customer Personal Data to Preava and the Processing of Customer Personal Data.

3.6. The parties acknowledge that, with regard to the processing of Customer Administrative Information, Customer is a Controller and Preava is an independent Controller, not a joint Controller with Customer. Preava will process Customer Administrative Information as a Controller to provide, optimize, and maintain the Services, including, without limitation, to: (a) manage the relationship with Customer; (b) carry out Preava's business operations, such as accounting, tax, billing, audit, and compliance purposes; (c) detect, prevent, or investigate security incidents, fraud, and other abuse or misuse of the Services; and (d) comply with Preava's legal or regulatory obligations; or as otherwise permitted under Applicable Data Protection Laws and in accordance with the Agreement, and the applicable Preava privacy notice(s).

3.7. The following is deemed an instruction by Customer to Process Customer Personal Data:

(a) Processing in accordance with the Agreement.

(b) Processing initiated by Data Subjects in their use of the Services.

(c) Processing to comply with other reasonable documented instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

3.8. If Customer has agreed to the use of an anonymized version of Customer Personal Data for Preava's training of its machine learning and artificial intelligence systems within the applicable Statement of Work or Order Form, when Preava Processes Customer Personal Data for conversion to Anonymized Data, Preava agrees to comply with all Applicable Data Protection Laws as they relate to the Processing of such Customer Personal Data as an independent Controller. To the extent Customer acts as an independent Controller for Customer Personal Data, Customer expressly authorizes Preava's Processing of Customer Personal Data for this compatible purpose.

4. Preava Personnel

4.1. Preava shall take reasonable steps to ensure the reliability of any of its employees, agents, or contractors who may have access to Personal Data.

4.2. Preava shall ensure that access to Customer Personal Data is strictly limited to those individuals who need to know or access it, as strictly necessary to fulfil the documented Processing instructions given to Preava by Customer or to comply with Applicable Data Protection Laws.

4.3. Preava shall ensure that all such individuals are subject to formal confidentiality undertakings, professional obligations of confidentiality, or statutory obligations of confidentiality.

5. Security of Processing

5.1. 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 to the rights and freedoms of natural persons, Preava shall, with regard to Personal Data, implement and maintain appropriate technical and organizational security measures to ensure a level of security appropriate to that risk (several of which are described in **Exhibit A**), as well as assist Customer with regard to ensuring Customer's compliance with its

own obligations related to its security measures pursuant to the Applicable Data Protection Laws.

5.2. In assessing the appropriate level of security, Preava shall take account, in particular, of the risks that are presented by the nature of such Processing activities, and particularly those related to Personal Data Breaches.

5.3. Customer is responsible for reviewing the information made available by Preava relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Applicable Data Protection Laws. Customer acknowledges that the security measures are subject to technical progress and development and that Preava may update or modify the security measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by Customer.

5.4. Notwithstanding the above, Customer agrees that, except as provided by this Addendum, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of the Customer Personal Data when in transit to and from the Services, and taking any appropriate steps to securely encrypt or backup any Customer Personal Data uploaded or inputted while utilizing the Services.

6. Subprocessing

6.1. Customer authorizes Preava to appoint (and permit each Contracted Processor appointed in accordance with this Section 6 to appoint) Contracted Processors in accordance with this Section 6 and any possible further restrictions, as set out in the Agreement, as the case may be.

6.2. Preava may continue to use those Contracted Processors already engaged by Preava as of the Effective Date, subject to Preava meeting the obligations set out in Section 6.4. The list of Preava's Contracted Processors has been provided to Customer as an attachment to the applicable Statement of Work or Order Form.

6.3. Customer consents to Preava engaging additional Contracted Processors, provided that Preava provides notifications of any changes to its Contracted Processors to Customer's Legal Notice Email. Preava will provide details of any change in Contracted Processors as soon as reasonably practicable. If, within fourteen (14) days of Preava notifying Customer of a change to its Contracted Processors, Customer notifies Preava in writing of any reasonable objections to the proposed new appointment, Preava shall not appoint, or disclose any Customer Personal Data to, that proposed Contracted Processor until reasonable steps have been taken to address the objections raised by Customer and, in turn, Customer has been provided with a reasonable written explanation of the steps taken to account for any such objections. If Customer, nevertheless, objects to the proposed appointment, it shall be entitled to terminate the Agreement as its sole remedy.

6.4. With respect to each Contracted Processor, Preava shall:

(a) carry out adequate due diligence to ensure that the Contracted Processor is capable of providing the level of protection and security for Customer Personal Data required by this Addendum, the Agreement, and Applicable

Data Protection Laws before the Contracted Processor first Processes Customer Personal Data or, where applicable, in accordance with Section 6.2; and

(b) ensure that the arrangement between Preava and the prospective Contracted Processor is governed by a written contract that includes terms which offer at least the same level of protection for Customer Personal Data as those set out in this Addendum, and that such terms meet the requirements of Applicable Data Protection Laws.

7. Rights of the Data Subjects

7.1. Taking into account the nature of the Processing, Preava shall assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligations in responding to requests to exercise rights of the Data Subjects under Applicable Data Protection Laws.

7.2. With regard to the rights of the Data Subjects within the scope of this Section 7, Preava shall:

(a) promptly notify Customer using the contact details provided in accordance with Section 17.2, or if Customer does not have a Data Protection Officer, then using the contact details provided in accordance with Section 19.2, if any Customer Personal Data Recipient receives a request from a Data Subject under any Applicable Data Protection Laws with respect to Customer Personal Data; and

(b) ensure that the Customer Personal Data Recipient does not respond to that request, except on the documented instructions of Customer or as required by Applicable Data Protection Laws to which the Customer Personal Data Recipient is subject, in which case Preava shall, to the extent permitted by Applicable Data Protection Laws, inform Customer of that legal requirement before the Customer Personal Data Recipient responds to the request.

8. Personal Data Breach

8.1. Preava shall notify Customer without undue delay upon Preava becoming aware of a Personal Data Breach affecting Customer Personal Data under Preava's direct control or upon Preava being notified of a Personal Data Breach affecting Customer Personal Data under the direct control of a Contracted Processor.

8.2. The notification shall provide Customer with sufficient information to allow Customer to meet any applicable obligations pursuant to the Applicable Data Protection Laws, including descriptions of, in as much detail as reasonably possible: (i) the nature of the Personal Data Breach; (ii) where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Customer Personal Data records concerned; (iii) the impact of such Personal Data Breach upon Customer and the affected Data Subjects; and (iv) the measures taken or proposed by Preava to address the Personal Data Breach. Preava shall provide and supplement notifications as and when additional information becomes available.

8.3. Preava shall co-operate with Customer and take all reasonable commercial steps to assist Customer in the investigation, mitigation, and remediation of each such Personal Data Breach, including co-operating with Customer to meet Customer's obligations, if any, to notify supervisory authorities or Data Subjects of the Personal Data Breach.

8.4. Preava's notification of or response to a Personal Data Breach under this Section 8 will not be construed as an acknowledgement by Preava of any fault or liability with respect to the Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

9.1. Preava shall provide Customer with relevant information and documentation with regard to any data protection impact assessments and prior consultations with supervisory authorities when Customer reasonably considers that such data protection impact assessments or prior consultations are required pursuant to Applicable Data Protection Laws (including, without limitation, Article 35 or 36 of the EU GDPR), but in each such case solely with regard to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, the respective Customer Personal Data Recipient. Such reasonable cooperation will be at Customer's expense only if it will require Preava to assign significant resources to that effort.

10. Deletion or Return of Personal Data

10.1. Preava shall provide Customer with the technical means, consistent with the way the Services are provided, to request the deletion of Customer Personal Data upon the request of Customer unless Applicable Data Protection Laws require storage of any such Personal Data.

10.2. Preava shall promptly, and at the latest within thirty (30) days following the date of cessation of Services involving the Processing of Customer Personal Data, at the choice of Customer, delete or return all Customer Personal Data to Customer, as well as delete existing copies, unless Applicable Data Protection Laws require storage of any such Customer Personal Data.

10.3. Preava shall also cause all Contracted Processors that have received Customer Personal Data to delete or return, as applicable, all such Customer Personal Data, with the exception of any Customer Personal Data that may be retained pursuant to applicable laws.

10.4. This Section 10 does not apply to Customer Personal Data that has been archived on back-up systems, which Preava or its Contracted Processors, as applicable, shall securely isolate and protect from any further Processing, except to the extent required by applicable law.

11. Audit Rights

11.1. Where Customer is entitled to and desires to review Preava's compliance with the Applicable Data Protection Laws, Customer may request, and Preava will provide (subject to obligations of confidentiality), relevant documentation or any relevant audit report Preava might have been issued.

11.2. If Customer, after having reviewed such documentation, still reasonably deems that it requires additional information, Preava shall further reasonably assist and make available to Customer, upon a written request and subject to obligations of confidentiality,

all other information (excluding legal advice) and/or documentation necessary to demonstrate compliance with this Addendum and its obligations pursuant to the Applicable Data Protection Laws (Articles 32 to 36 of the EU GDPR in particular).

11.3. Preava shall allow for and contribute to audits, including remote inspections of the Services, by Customer or an auditor selected by Customer (and subject to obligations of confidentiality) with regard to the Processing of Customer Personal Data by Preava, provided that such auditor is not a competitor of Preava. Preava shall provide the assistance described in this Section 11, insofar as in Preava's reasonable opinion, such audits and the specific requests of Customer do not interfere with Preava's business operations or cause Preava to breach any legal or contractual obligation to which it is subject.

11.4. Customer agrees to pay Preava, upon receipt of invoice, a reasonable fee based on the time spent, as well as to account for the materials expended, in relation to Customer exercising its rights under this Section 11 or the Standard Contractual Clauses.

12. Jurisdiction Specific Terms

12.1. To the extent Preava Processes Customer Personal Data originating from, or protected by, Applicable Data Protection Laws in one of the jurisdictions listed in **Exhibit B**, then the terms and definitions specified in **Exhibit B** with respect to the applicable jurisdiction(s) ("**Jurisdiction Specific Terms**") shall apply in addition to the terms of this Addendum.

12.2. Preava may update **Exhibit B** from time to time to reflect changes in or additions to Applicable Data Protection Laws to which Preava is subject. If Preava updates **Exhibit B**, it will provide the updated **Exhibit B** by posting a new version of this DPA with an updated "Last Updated" date, including the updated exhibit, on its website at: https://www.preava.com/legal/dpa. To receive a notification when Preava updates this DPA, including **Exhibit B**, Customer can submit a request at https://www.preava.com/contact. If Customer does not object to the updated **Exhibit B** within fourteen (14) days of its posting, Customer will be deemed to have consented to the updated **Exhibit B**.

12.3. In case of any conflict or ambiguity between the Jurisdiction Specific Terms and any other terms of this Addendum, the applicable Jurisdiction Specific Terms will prevail.

13. International Data Transfers

13.1. International transfers of Customer Personal Data within the scope of this Addendum shall be conducted in accordance with the applicable terms and requirements of **Exhibit B**.

13.2. Where the Standard Contractual Clauses are the applicable data transfer mechanism according to the terms and requirements set out in **Exhibit B**, the applicable module of the Standard Contractual Clauses (if any) will be the module applicable to the role of the Parties as described in **Exhibit B**.

13.3. Preava may update **Exhibits A and B** from time to time to reflect changes in or additions necessary to conclude the Standard Contractual Clauses. Without limiting the generality of the foregoing, if the execution of a new version of the Standard Contractual Clauses adopted by the relevant authorities in the jurisdiction governing the processing of Customer Personal Data is later required in order for the Parties to rely on the Standard

Contractual Clauses as a lawful mechanism for Restricted International Transfers, the Parties are deemed to have agreed to the new version of the Standard Contractual Clauses by entering into this Addendum, and, if necessary, Preava shall be entitled to update **Exhibits A and B** accordingly.

13.4. Preava may update **Exhibit C** from time to time to provide for additional safeguards to Customer Personal Data subject to the requirements of Applicable Data Protections Laws for Restricted International Transfers. If Preava updates **Exhibit C**, it will provide the updated **Exhibit C** by posting a new version of this DPA with an updated "Last Updated" date, including the updated exhibit, on its website at: https://www.preava.com/legal/dpa. To receive a notification when Preava updates this DPA, including **Exhibit C**, Customer can submit a request at https://www.preava.com/contact. If Customer does not object to the updated **Exhibit C** within fourteen (14) days of its posting, Customer will be deemed to have consented to the updated **Exhibit C**.

14. No Selling of Personal Data

14.1. Preava acknowledges and confirms that it does not receive any Customer Personal Data as consideration for any Services or other items that Preava provides to Customer. Customer retains all rights and interests in Customer Personal Data. Customer agrees to refrain from taking any action that would cause any transfers of Customer Personal Data to or from Preava to qualify as selling Customer Personal Data under Applicable Data Protection Laws.

15. Indemnification

15.1. Customer agrees to indemnify and hold harmless Preava and its officers, directors, employees, agents, affiliates, successors, and permitted assigns against any and all losses, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs, or expenses of whatever kind which Preava may sustain as a consequence of the breach by Customer of its obligations pursuant to this Addendum and the Applicable Data Protection Laws.

16. General Terms

16.1. This Addendum supersedes and replaces all prior and contemporaneous proposals, statements, sales materials or presentations, and agreements, oral and written, with regard to the subject matter of this Addendum, including any prior data processing addenda entered into between Preava and Customer in connection with the Agreement.

16.2. All clauses of the Agreement that are not explicitly amended or supplemented by the clauses of this Addendum remain in full force and effect and shall apply, as long as this does not contradict with compulsory requirements of Applicable Data Protection Laws under this Addendum.

16.3. In the event of any conflict between the Agreement (including any annexes, exhibits, and appendices thereto) and this Addendum, the provisions of this Addendum shall prevail. In the event that the Jurisdiction Specific Terms found in **Exhibit B** apply and conflict with the Agreement or the body of this Addendum, the provisions of the applicable Jurisdiction Specific Terms found in **Exhibit B** shall prevail.

16.4. Should any provision of this Addendum be found legally invalid or unenforceable, then the invalid or unenforceable provision will be deemed

superseded by a valid, enforceable provision that most closely matches the intent of the original provision and the remainder of this Addendum will continue in effect.

16.5. If Preava makes a determination that it can no longer meet any of its obligations in accordance with this Addendum (including its exhibits) or the Standard Contractual Clauses (where applicable), it shall: (i) promptly notify Customer of that determination; and (ii) cease the Processing or take other reasonable and appropriate steps to remediate the lack of compliance.

16.6. If you are accepting the terms of this Addendum on behalf of an entity, you represent and warrant to Preava that you have the authority to bind that entity and its affiliates, where applicable, to the terms and conditions of this Addendum.

16.7. Each Party must review this Addendum (including its exhibits) at regular intervals to ensure that this Addendum remains accurate, up to date, and continues to provide appropriate safeguards to the Customer Personal Data. Each Party will carry out these reviews each time there is a change to the Customer Personal Data, the purposes for Processing, the data importer information, or any risk assessments related to the Processing contemplated in this Addendum.

17. Data Protection Officer

17.1. The Data Protection Officer of Preava is:

VeraSafe, LLC
100 M Street S.E., Suite 600
Washington, D.C. 20003
USA
+1 (617) 398-7067
Email: experts@verasafe.com
Web: https://www.verasafe.com/about-verasafe/contact-us/

17.2. Customer shall provide the identity and contact details of Customer's Data Protection Officer to Preava at privacy@preava.com, if applicable.

18. Data Protection Representatives

18.1. The European Union Representative of Preava pursuant to Article 27 of the EU GDPR is:

VeraSafe Ireland Ltd.
Unit 3D North Point House
North Point Business Park
New Mallow Road, Cork T23AT2P
Ireland
Phone: +420 228 881 031

Contact form: https://verasafe.com/public-resources/contact-data-protection-representative

18.2. The United Kingdom ("**UK**") Representative of Preava pursuant to Article 27 of the UK GDPR (as defined in the Jurisdiction Specific Terms) is:

VeraSafe United Kingdom Ltd.
37 Albert Embankment
London SE1 7TL
United Kingdom
Phone: +44 (20) 4532 2003

Contact form: https://verasafe.com/public-resources/contact-data-protection-representative

18.3. Customer shall provide the identity and contact details of Customer's European Union Representative pursuant to Article 27

of the EU GDPR to Preava at privacy@preava.com, if applicable.

18.4. Customer shall provide the identity and contact details of Customer's United Kingdom Representative pursuant to Article 27 of the UK GDPR to Preava at privacy@preava.com, if applicable.

19. Notices Pursuant to this Addendum.

19.1. Notices to Preava shall be sent to privacy@preava.com, unless this Addendum indicates otherwise.

19.2. Notices to Customer shall be sent to the email address listed in the applicable Statement of Work, Order Form, Master Service Agreement, or similar document containing Customer's contact information, unless this Addendum indicates otherwise.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

EXHIBIT A

Details of Processing

A. LIST OF PARTIES:

Preava:

Name:	Preava, Inc. and its relevant Affiliates
Address:	22 Essex Way, #8203 Essex, VT 05451 USA
Contact Person:	Chief Privacy Officer privacy@preava.com
Article 27 EU Representative:	*See* Section 18.1 of this Addendum.
Article 27 UK Representative:	*See* Section 18.2 of this Addendum.
Data Protection Officer:	*See* Section 17.1 of this Addendum.
Activities Relevant to Transferred Data:	Processing activities related to providing the Services, as set forth in the Agreement.
Controllership Role:	*See* Section 3 of this Addendum.
Data Transfer Role:	Data Importer

Customer:

Name, Address, Contact Person:	The identity and contact information of Customer is as listed in the applicable Statement of Work, Order Form, Master Service Agreement, or similar document.
Article 27 EU Representative:	*See* Section 18.3 of this Addendum.
Article 27 UK Representative:	*See* Section 18.4 of this Addendum.
Data Protection Officer:	*See* Section 17.2 of this Addendum.

Activities Relevant to Transferred Data:	Processing activities related to receiving the Services, as set forth in the Agreement.
Controllership Role:	*See* Section 3 of this Addendum.
Data Transfer Role:	Data Exporter

B. DESCRIPTION OF TRANSFER:

Subject Matter of the Processing:	The subject matter of the Processing of Customer Personal Data pertains to the provision of Services, as requested by Customer.
Nature and Purpose of Processing:	The Processing is related to the provision of Services, namely, provision of the Preava Prevent software, to Customer, as further detailed within the Agreement, and Preava and its Contracted Processors (if applicable) will perform such acts of Processing of Customer Personal Data as are necessary to provide those Services according to Customer's instructions, including but not limited to the transmission, storage, and other Processing of Customer Personal Data submitted to the Services.
Further Processing:	Preava shall not carry out any further Processing of Customer Personal Data beyond the provision of the Services under the Agreement. As stated in Section 3.1, If Customer has agreed to the use of an anonymized version of Customer Personal Data for Preava's training of its machine learning and artificial intelligence systems within the applicable Statement of Work or Order Form, Preava acts as an independent Controller of Customer Personal Data for the purpose of converting it to Anonymized Data. Personal Data being Processed by Preava as an independent Controller in such a situation no longer constitutes Customer Personal Data, and after anonymization, no longer constitutes Personal Data.
Retention Criteria (Duration): *(The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to*	The duration of the Processing and retention of Customer Personal Data is generally determined by Customer and is further subject to the terms of this Addendum and the Agreement in the context of the contractual relationship between Preava and Customer.

determine that period.)	
Categories of Data Subjects:	Data Exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the Data Exporter in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of Data Subjects: i. Customer's employees or contractors; ii. Customer's business partners; iii. any additional Data Subjects authorized by Customer; and iv. any Data Subject that is emailed by Customer.
Categories of Personal Data:	Data Exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the Data Exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data: i. biographical information (such as first and last name); ii. professional information (such as role/job title and company name); iii. contact information (such as email address, physical address, phone number); iv. network information and activity (such as IP address, device identifiers, and location information); and v. other information voluntarily provided by the Data Subjects.
Special Categories of Personal Data: *(Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access*	Not applicable, unless submitted by the Customer or Data Subjects.

only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.)	
Frequency of the Transfer: *(e.g. whether Personal Data is transferred on a one-off or continuous basis)*	Continuous during the provision of the Services under the Agreement.
Subject Matter, Nature, and Duration of Contracted Processors:	Any transfer to Contracted Processors will be only as strictly required to perform the Services pursuant to the Agreement. Upon request, Preava will provide to Customer a description of Processing for any Contracted Processor(s), including the subject matter, nature, and duration of Processing.
Technical and Organizational Measures of Contracted Processors:	When Preava engages a Contracted Processor under this Addendum, Preava and the Contracted Processor must enter into an agreement with data protection terms substantially similar to those contained in this Addendum. Preava must ensure that the agreement with each Contracted Processor allows Preava to meet its respective obligations with respect to Customer. In addition to implementing technical and organizational measures to protect Customer Personal Data, Contracted Processors must: i. notify Preava in the event of a Personal Data Breach so that Preava may immediately notify Customer; ii. delete Customer Personal Data when instructed by Preava in accordance with Customer's instructions to Preava; iii. not engage additional Contracted Processors without Preava's authorization; and iv. not process Customer Personal Data in a manner which conflicts with Customer's instructions to Preava.

C. Technical and Organizational Security Measures:

Taking into account the state of the art and the high sensitivity of the Customer Personal Data, Preava implements and maintains appropriate technical and organizational security measures to ensure a level of security appropriate to that risk (including, as appropriate, the measures referred to in Article 32(1) of the EU GDPR).

Type of TOMs	Description of TOMs

Measures for pseudonymization and encryption of Personal Data:	• Secure implementation of the Transport Layer Security (TLS) protocol version 1.2 or higher for Personal Data in transit using 256-bit encryption, and 128-bit encryption when the former is unavailable
	• Encryption of all remote accesses for system maintenance or configuration relating to Personal Data
	• Whole disc encryption, container-level encryption, or file-level encryption in portable workstations and portable mass storage media to secure Personal Data at rest using a minimum of 256-bit encryption
	• Pseudonymization capabilities for Personal Data, such as:
	  o Random number generator (RNG);
	  o Cryptographic hash function;
	  o Encryption

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services:	• Restriction of physical and logical access to IT systems that Process Personal Data to only those individuals who are officially authorized and have an identified need for such access • Firewall protection of external and internal points of connectivity in network architecture • Storage of Personal Data on servers with redundant physical storage and regular back-ups
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:	• Implementation and maintenance of procedures to create and maintain retrievable exact copies of Personal Data that Preava stores or otherwise maintains
Processes for regularly testing, assessing, and evaluating the effectiveness of technical and	• Patch management process for vulnerabilities

Type of TOMs	Description of TOMs
organizational measures to ensure the security of the Processing:	
Measures for user identification and authorization:	• User access is authorized by Google and Microsoft SSO via Auth0, an identification provider. Preava does not store any user passwords or MFA credentials. • Role-based access authorization policy based on least privilege and need to know • Assignment of a uniquely identifiable ID to each user • Configuration of systems and applications to restrict access to only authorized access • Password policies and password management procedures that require strong passwords • Periodic audits of active user accounts and associated access capabilities (at least twice annually and when there is a new user or system change)
Measures for the protection of Personal Data during transmission:	• Encryption of Personal Data during transmission using the Transport Layer Security (TLS) protocol version 1.2 or higher using 256-bit encryption, and 128-bit encryption when the former is unavailable • Secure authentication procedures for executing Personal Data transfers, including access credentials, specific user profiles, biometrics, tokens, etc.
Measures for the protection of Personal Data during storage:	• Encryption of Personal Data during storage (i.e., at rest) using a minimum of AES-256 • Secure configuration for network devices, such as firewalls, routers, and switches • Encryption of Personal Data stored on all mobile devices, including laptops
Measures for ensuring physical security of locations at which Personal Data are Processed:	• Preava processes Customer Personal Data exclusively in AWS data centers. AWS maintains extensive physical security measures at its data centers. Additional information regarding AWS's physical security measures is available at https://aws.amazon.com/compliance/data-center/controls/. • Preava processes all other Personal Data exclusively in Contracted Processor data centers. The respective

Type of TOMs	Description of TOMs
	Contracted Processors maintain appropriate physical security measures at their data centers.
Measures for ensuring events logging:	• Active monitoring and logging of software network and infrastructure security for potential security events at the system and platform levels • Retention of audit logs in accordance with legal requirements
Measures for ensuring system configuration, including default configuration:	• Maintenance of secure images or templates for all systems based on the organization's security baselines • Storage of the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible • Deployment of system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals
Measures for ensuring data minimization:	• Internal processes to remove Personal Data from its systems as soon as that Personal Data is no longer required under the terms of the applicable Agreement
Measures for ensuring data quality:	• Implement and maintain appropriate technical controls to prevent, detect, and correct data integrity violations in IT Systems, including but not limited to checksums, mirroring, ECC memory, redundant storage, and file integrity monitoring tools
Measures for ensuring limited data retention:	• Deleting Personal Data in accordance with all applicable contracts or when it is no longer required • Ensuring secure disposal of devices that store Personal Data
Measures for ensuring accountability:	• Ensuring that personnel responsible for Processing Personal Data are bound to confidentiality obligations (e.g., through a non-disclosure agreement)
Measures for allowing data portability and ensuring erasure:	• Creation of a self-service portal or a ticketed system for Data Subjects to access, export, correct, or delete their Personal Data • Segregation and segmentation of Personal Data in IT systems and databases

EXHIBIT B

Jurisdiction Specific Terms

1. Brazil

1.1. **Definitions**

(a) "**Applicable Data Protection Laws**" (as used in this Addendum) includes "**Brazilian Data Protection Laws**" (as defined below).

(b) "**Brazilian Data Protection Laws**" (as used in this Section) includes the Lei Geral de Proteção de Dados, Law No. 13.709 of 14 August 2018 ("**LGPD**"), as may be amended from time to time.

(c) "**Controller**" (as used in this Addendum) includes "**Controlador**" as defined under the LGPD.

(d) "**Personal Data Breach**" (as used in this Addendum) includes "**Security Incident**" as defined under the LGPD.

(e) "**Processor**" includes "**Operador**" as defined under the LGPD.

2. Canada

2.1. **Definitions**

(a) "**Applicable Data Protection Laws**" (as used in this Addendum) includes Canadian Data Protection Laws.

(b) "**Canadian Data Protection Laws**" includes the Canadian Federal Personal Information Protection and Electronic Documents Act ("**PIPEDA**"), as may be amended from time to time.

(c) "**Personal Data**" (as used in this Addendum) includes "**Personal Information**" as defined under PIPEDA.

(d) **"Contracted Processor**" (as used in this Addendum) includes "**Third Party Organization**" as defined under PIPEDA.

(e) "**Personal Data Breach**" (as used in this Addendum) includes "**Breach of Security Safeguards**" as defined under PIPEDA.

2.2. Customer confirms that it has obtained a valid consent (as defined under PIPEDA) where necessary to Process Personal Data of each Data Subject.

3. European Economic Area

3.1. Definitions

(a) "**Applicable Data Protection Laws**" (as used in this Addendum) includes EEA Data Protection Laws (as defined below).

(b) "**EEA**" (as used in this Section) means the European Economic Area, consisting of the EU Member States, and Iceland, Liechtenstein, and Norway.

(c) "**EEA Data Protection Laws**" means the EU GDPR and all laws and regulations of the EEA, applicable to the Processing of Personal Data, as may be amended from time to time.

(d) "**EU 2021 Standard Contractual Clauses**" (as used in this Section) means the contractual clauses adopted by the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

(e) "**Restricted International Transfer of EEA Personal Data**" (as used in this Section) means any transfer of Personal Data subject to the EU GDPR which is undergoing Processing or is intended for Processing after transfer to a Third Country (as defined below) or an international organization in a Third Country (including data storage on foreign servers).

(f) "**Standard Contractual Clauses**" (as used in this Addendum) includes the EU 2021 Standard Contractual Clauses.

(g) "**Third Country**" (as used in this Section) means a country outside of the EEA.

3.2. With regard to any Restricted International Transfer of EEA Personal Data from Customer to Preava within the scope of this Addendum, one of the following transfer mechanisms shall apply, in the following order of precedence:

(a) A valid adequacy decision adopted by the European Commission on the basis of Article 45 of the EU GDPR that provides that the Third Country, a territory, or one or more specified sectors within that Third Country, or the international organization in question to which EEA Personal Data is to be transferred ensures an adequate level of data protection.

(b) Preava's certification to the EU-U.S. Data Privacy Framework (only to the extent that such self-certification constitutes an "appropriate safeguard" pursuant to EEA Data Protection Laws, as the case may be), provided that the Services are covered by such certification.

(c) The EU 2021 Standard Contractual Clauses (insofar as their use constitutes an "appropriate safeguard" under Article 46 of the EU GDPR).

(d) Any other lawful data transfer mechanism, as laid down in the EEA Data Protection Laws, as the case may be.

3.3. EU 2021 Standard Contractual Clauses:

(a) This Addendum hereby incorporates by reference the EU 2021 Standard Contractual Clauses. The Parties are deemed to have accepted, executed, and signed the Standard Contractual Clauses where necessary in their entirety (including the annexures thereto).

(b) The content of the EU 2021 Annex I and Annex II of the EU 2021 Standard Contractual Clauses is set forth in **Exhibit A** to this Addendum.

(c) The text contained in **Exhibit C** of this Addendum supplements the EU 2021 Standard Contractual Clauses.

(d) The Parties agree to apply the following modules:

i. Module one of the EU 2021 Standard Contractual Clauses when, in accordance with Section 3 of this Addendum, the Data Exporter is Customer and acts as a Controller and the Data Importer is Preava and acts as an independent Controller;

ii. Module two of the EU 2021 Standard Contractual Clauses when, in accordance with Section 3 of this Addendum, the Data Exporter is Customer and acts as a Controller and the Data Importer is Preava and acts as a Processor; and

iii. Module three of the EU 2021 Standard Contractual Clauses when, in accordance with Section 3 of this Addendum, the Data Exporter is Customer and acts as a Processor and the Data Importer is Preava and acts as a Sub-Processor.

(e) For the purposes of Annex I.A:

i. The Parties have provided each other with the identity information and contact details required under Annex I.A.

ii. The Parties' controllership roles are set forth in Section 3 of this Addendum.

iii. The details of the Parties' data protection officers and data protection representatives in the EU are set forth in **Exhibit A** and Sections 17 and 18 of this Addendum.

iv. The activities relevant to the Personal Data transferred under the Standard Contractual Clauses are set forth in **Exhibit A** of this Addendum.

(f) The Parties' Choices under the EU 2021 Standard Contractual Clauses:

i. With respect to Clause 9 of the EU 2021 Standard Contractual Clauses, the parties select "Option 2 General Written Authorization" and the time period set forth in Section 6.3 of this Addendum.

ii. With respect to Clause 13 and Annex I.C of the EU 2021 Standard Contractual Clauses, the competent supervisory authority shall be determined by the location of the data exporter or its data protection representative in the EEA. If the data exporter is not established in an EEA country and the processing activities are subject to the EU GDPR by virtue of application of Article 3(2) EU GDPR, and the data exporter does not have a data protection representative under Article 27 EU GDPR, the Supervisory Authority shall be the Data Protection Commission of Ireland, unless otherwise identified in the applicable Statement of Work or Order Form for the Services, or by providing notice to Preava. Customer is solely responsible for determining whether a different Supervisory Authority should be used and providing appropriate notice to Preava.

iii. With respect to Clause 17 of the EU 2021 Standard Contractual Clauses, the Parties select the law of the Republic of Ireland.

iv. With respect to Clause 18 of the EU 2021 Standard Contractual Clauses, the Parties agree that any dispute arising from the EU 2021 Standard Contractual Clauses shall be resolved by the courts of the Republic of Ireland.

3.4. In cases where the EU 2021 Standard Contractual Clauses apply and there is a conflict between the terms of this Addendum and the terms of the EU 2021 Standard Contractual Clauses, the terms of the EU 2021 Standard Contractual Clauses shall prevail.

4. Switzerland

4.1. Definitions

(a) "**Applicable Data Protection Laws**" (as used in this Addendum) includes Swiss Data Protection Laws (as defined below).

(b) "**Restricted International Transfer of Swiss Personal Data**" (as used in this Section) means any transfer of Personal Data (including data storage in foreign servers) subject to the FADP to a Third Country (as defined below) or an international organization.

(c) "**Standard Contractual Clauses**" (as used in this Addendum) includes the EU 2021 Standard Contractual Clauses (as defined under Section 3 of this Exhibit).

(d) "**Swiss Data Protection Laws**" includes the Federal Act on Data Protection ("**FADP**") and the Ordinance to the Federal Act on Data Protection ("**OFADP**"), as they may be amended from time to time.

(e) "**Third Country**" (as used in this Section) means a country outside of the Swiss Confederation.

4.2. With regard to any Restricted International Transfer of Swiss Personal Data from Customer to Preava within the scope of this Addendum, one of the following transfer mechanisms shall apply, in the following order of precedence:

(a) The inclusion of the Third Country, a territory, or one or more specified sectors within that Third Country, or the international organization in question to which Personal Data is to be transferred in the list published by the Swiss Federal Data Protection and Information Commissioner of states that provide an adequate level of protection for Personal Data within the meaning of the FADP.

(b) Preava's certification to the Swiss-U.S. Data Privacy Framework (only to the extent that such self-certification constitutes an "appropriate safeguard" pursuant to Swiss Data Protection Laws, as the case may be), provided that the Services are covered by the certification.

(c) The EU 2021 Standard Contractual Clauses (as defined under Section 3 of this Exhibit) (insofar as their use constitutes an "appropriate safeguard" under Swiss Data Protection Laws).

(d) Any other lawful transfer mechanism, as laid down in Swiss Data Protection Laws.

4.3. EU 2021 Standard Contractual Clauses:

(a) This Addendum hereby incorporates by reference the EU 2021 Standard Contractual Clauses. The Parties are deemed to have accepted, executed, and signed the Standard Contractual Clauses where necessary in their entirety (including the annexures thereto).

(b) The Parties incorporate and adopt the Standard Contractual Clauses for Restricted International Transfers of Swiss Personal Data in the same manner set forth in Section 3.3 of these Jurisdiction Specific Terms, subject to the following:

(c) Parties' Choices under the EU 2021 Standard Contractual Clauses:

i. For the purpose of Annex I.C and with respect to Clause 13 (when applicable) of the Standard Contractual Clauses, the competent authority shall be the Swiss Federal Data Protection and Information Commissioner, insofar as the data transfer constitutes a Restricted International Transfer of Swiss Personal Data.

ii. With respect to Clause 18 of the EU 2021 Standard Contractual Clauses, the Parties' selection of forum may not be construed as forbidding Data Subjects habitually resident in Switzerland from suing for their rights in Switzerland.

iii. References to "Regulation (EU) 2016/679" and specific articles therein shall be replaced with references to the FADP and the equivalent articles or sections therein, insofar as there any Restricted International Transfers of Swiss Personal Data.

4.4. In cases where the EU 2021 Standard Contractual Clauses apply and there is a conflict between the terms of this Addendum and the terms of the EU 2021 Standard Contractual Clauses, the terms of the EU 2021 Standard Contractual Clauses shall prevail.

5. United Kingdom

5.1. Definitions

(a) "**Applicable Data Protection Laws**" (as used in this Addendum) includes UK Data Protection Laws (as defined below).

(b) "**Restricted International Transfer of UK Personal Data**" (as used in this Section) means any transfer of Personal Data subject to the UK GDPR to a Third Country (as defined below) or an international organization (including data storage on foreign servers).

(c) "**Standard Contractual Clauses**" (as used in this Addendum) includes the EU 2021 Standard Contractual Clauses (as defined under Section 3 of this Exhibit).

(d) "**Third Country**" (as used in this Section) means a country outside of the United Kingdom.

(e) "**UK Data Protection Laws**" (as used in this Section) includes the Data Protection Act 2018 and the UK GDPR (as defined below).

(f) "**UK GDPR**" (as used in this Section) means the United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of Section 3 of the European Union (Withdrawal) Act 2018.

(g) "**UK ICO**" (as used in this Section) means the UK Information Commissioner's Office.

(h) "**UK IDTA**" (as used in this Section) means the International Data Transfer Agreement issued pursuant to Section 119A(1) of the Data Protection Act 2018 and approved by the UK Parliament.

(i) "**UK Transfer Addendum**" (as used in this Section) means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued pursuant to Section 119A(1) of the Data Protection Act 2018 and approved by the UK Parliament.

5.2. With regard to any Restricted International Transfer of UK Personal Data from Customer to Preava within the scope of this Addendum, one of the following transfer mechanisms shall apply, in the following order of precedence:

(a) A valid adequacy decision pursuant to Article 45 of the UK GDPR.

(b) Preava's certification to the UK Extension to the EU-U.S. Data Privacy Framework (only to the extent that such self-certification constitutes an "appropriate safeguard" pursuant to UK Data Protection Laws, as the case may be), provided that the Services are covered by such certification.

(c) The UK IDTA.

(d) The Standard Contractual Clauses (insofar as their use constitutes an "appropriate safeguard" under UK Data Protection Laws, and the Processing activities of the Data Importer are not subject to the UK GDPR by virtue of application of Article 3(2) of the UK GDPR), as they have been adopted for use by the relevant authorities within the United Kingdom, including the UK ICO, using the UK Transfer Addendum.

(e) Any other lawful data transfer mechanism, as laid down in the UK Data Protection Laws, as the case may be.

5.3. EU 2021 Standard Contractual Clauses and UK Transfer Addendum:

(a) This Addendum hereby incorporates by reference any additional modifications and amendments required by the UK Transfer Addendum as they have been adapted for use by the relevant authorities within the United Kingdom to make the EU 2021 Standard Contractual Clauses applicable to Restricted International Transfers of UK Personal Data. The Parties are deemed to have accepted, executed, and signed the adapted EU 2021 Standard Contractual Clauses where necessary in their entirety (including the annexures and any addenda thereto).

(b) For the purposes of the tables to the UK Transfer Addendum:

i. Table 1: The content of Table 1 is set forth in **Part A of Exhibit A**.

ii. Table 2: The content of Table 2 is incorporated and adopted as to Restricted International Transfers of UK Personal Data in exactly the same manner set forth in Section 3.3 of these Jurisdiction Specific Terms.

iii. Table 3: The content of Table 3 (Annexes 1A, 1B, II, and III) is set forth as follows:

(A) *Annex 1(A)*: The content of Annex 1(A) is set forth in **Part A of Exhibit A**, save the details of the Parties' Data Protection Officers and Data Protection Representatives in the UK, which are specified in Sections 19 and 20, respectively, of this Addendum.

(B) *Annex 1(B)*: The content of Annex 1(B) is set forth in **Part B of Exhibit A**.

(C) *Annex II*: The content of Annex II is set forth in **Part C of Exhibit A**.

(D) *Annex III*: Annex III is not applicable as the Parties have elected general authorization under Clause 9 of the EU 2021 Standard Contractual Clauses.

iv. Table 4: The Parties agree that both the Data Importer and the Data Exporter may terminate the UK Transfer Addendum as set out in Section 19 of the UK Transfer Addendum.

(c) The Parties incorporate and adopt the Standard Contractual Clauses as to Restricted International Transfers of UK Personal Data in exactly the same manner set forth in Section 3.3 of these Jurisdiction Specific Terms, with the following distinctions:

i. Clause 13 (Annex I.C): The competent authority shall be UK ICO.

ii. Clause 17: The Standard Contractual Clauses, including the incorporated UK Transfer Addendum, shall be governed by the laws of England and Wales.

iii. Clause 18: The Parties agree that any dispute arising from the Standard Contractual Clauses, or the incorporated UK Transfer Addendum shall be resolved by the courts of England and Wales. A Data Subject may also bring legal proceedings against the Data Exporter and/or Data Importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.

(d) The terms contained in **Exhibit C** to this Addendum supplement the Standard Contractual Clauses.

(e) In cases where the Standard Contractual Clauses, in conjunction with the UK Transfer Addendum, apply and there is a conflict between the terms of this Addendum and the terms of the Standard Contractual Clauses or UK Transfer Addendum, the terms of the UK Transfer Addendum shall prevail with regard to the Restricted International Transfer in question.

5.4. UK IDTA

(a) This Addendum hereby incorporates by reference the UK IDTA. The Parties are deemed to have accepted, executed, and signed the UK IDTA where necessary in its entirety.

(b) For the purposes of the tables to the UK IDTA:

i. Table 1: The information required by Table 1 appears within **Part A of Exhibit A**.

ii. Table 2:

(A) The UK IDTA shall be governed by the laws of England and Wales.

(B) The Parties agree that any dispute arising from the UK IDTA shall be resolved by the courts of England and Wales.

(C) The Parties' controllership and data transfer roles are set out in **Part A of Exhibit A**.

(D) The UK GDPR applies to the Data Importer's Processing of the Personal Data.

(E) This Addendum and the Agreement set out the instructions for Processing Personal Data.

(F) The Data Importer shall Process Personal Data for the time period set out in **Part B of Exhibit A**. The Parties agree that neither Party may terminate the UK IDTA before the end of such time period except as set out in Section 29.2 of the UK IDTA, in which case both the Data Importer and Data Exporter may terminate the UK IDTA.

(G) The Data Importer may only transfer Personal Data to authorized Contracted Processors (if applicable), as set out within Section 6 of this Addendum, or to such third parties that the Data Exporter authorizes in writing or within the Agreement.

(H) Each Party must review this Addendum at regular intervals, to ensure that this Addendum remains accurate and up to date and continues to provide appropriate safeguards to the Personal Data. Each Party will carry out these reviews as frequently as at least once each year or sooner.

iii. Table 3: The content of Table 3 is set forth in **Part B of Exhibit A** and may be updated in accordance with Sections 3.3 and 13.3 of this Addendum.

iv. Table 4: The content of Table 4 is set forth in **Part C of Exhibit A** and may be updated in accordance with Sections 3.3 and 13.3 of this Addendum.

(c) Part 2 (Extra Protection Clauses) and Part 3 (Commercial Clauses) of the UK IDTA are noted throughout this Addendum.

(d) The terms contained in **Exhibit C** to this Addendum supplement the UK IDTA.

(e) In cases where the UK IDTA applies and there is a conflict between the terms of this Addendum and the terms of the UK IDTA, the terms of the UK IDTA shall prevail.

6. United States of America

6.1. **Applicability.** Wherever the Processing pursuant to this Addendum falls within the scope of United States Data Protection Laws (defined below), the provisions of this Addendum and this Section shall apply to such Processing.

6.2. **Definitions**

(a) "**Business Purpose**", "**Commercial Purpose**", "**Sell**", and "**Share**" (as used in this Section) shall have the same meanings as under applicable United States Data Protection Laws, and their cognate and corresponding terms shall be construed accordingly.

(b) "**Controller**" (as used in this Addendum) includes "**Business**" as defined under applicable United States Data Protection Laws.

(c) "**Data Subject**" (as used in this Addendum) includes "**Consumer**" as defined under applicable United States Data Protection Laws.

(d) "**Personal Data**" (as used in this Addendum) includes "**Personal Information**" as defined under applicable United States Data Protection Laws.

(e) "**Personal Data Breach**" (as used in this Addendum) includes "**Breach of Security**" and "**Breach of the Security of the System**" as defined under applicable United States Data Protection Laws.

(f) "**Processor**" (as used in this Addendum) includes "**Service Provider**" as defined under applicable United States Data Protection Laws.

(g) "**United States Data Protection Laws**" include, individually and collectively, enacted state and federal laws, acts, and regulations of the United States of America that apply to the Processing of Personal Data, as may be amended from time to time. Such laws include, without limitation:

i. the California Consumer Privacy Act of 2018, as amended, including as amended by the California Privacy Rights Act of 2020 (Cal. Civ. Code § 1798.100 *et seq.*), and the California Consumer Privacy Act Regulations, together with all implementing regulations;

ii. the Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1301 *et seq.*, together with all implementing regulations;

iii. the Connecticut Act Concerning Data Privacy and Online Monitoring, Pub. Act No. 22015;

iv. the Utah Consumer Privacy Act, Utah Code Ann. S 13-61-101 *et seq.*; and

v. the Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-571 *et seq.*

6.3. Customer discloses Personal Data to Preava solely for: (i) valid Business Purposes; and (ii) to enable Preava to perform the Services under the Agreement.

6.4. Preava shall not: (i) Sell or Share Customer Personal Data; (ii) retain, use, or disclose Customer Personal Data for a Commercial Purpose other than providing the Services specified in the Agreement or as otherwise permitted by United States Data Protection Laws; (iii) retain, use, or disclose Customer Personal Data except where permitted under the Agreement between Customer and Preava; nor (iv) combine Customer Personal Data with other information that Preava Processes on behalf of other persons or that Preava collects directly from the Data Subject, with the exception of Processing for Business Purposes. Preava certifies that it understands these restrictions and will comply with them.

6.5. Customer specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from Sales or other disclosures of Personal Data, to the extent applicable under United States Data Protection Laws.

EXHIBIT C

Supplemental Clauses to the Standard Contractual Clauses

By this **Exhibit C** (this "**Exhibit**"), the Parties provide additional safeguards and redress to the Data Subjects whose Personal Data is transferred to Preava pursuant to Standard Contractual Clauses. This Exhibit supplements and is made part of, but is not in variation or modification of, the Standard Contractual Clauses that may be applicable to the Restricted International Transfer.

1. Definitions

1.1. For the purpose of interpreting this Exhibit, the following terms shall have the meanings set out below:

(a) "**EO 12333**" means U.S. Executive Order 12333.

(b) "**FISA**" means the U.S. Foreign Intelligence Surveillance Act.

(c) "**Schrems II Judgment**" means the judgment of the European Court of Justice in Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems.

2. Applicability of Surveillance Laws to Data Importer

2.1. U.S. Surveillance Laws

(a) Data Importer represents and warrants that, as of the Effective Date, it has not received any national security orders of the type described in Paragraphs 150–202 of the Schrems II Judgment.

(b) Data Importer represents that it reasonably believes that it is not eligible to be required to provide information, facilities, or assistance of any type under FISA Section 702 because:

i. no court has found Data Importer to be an entity eligible to receive process issued under FISA Section 702: (i) an "electronic communication service provider" within the meaning of 50 U.S.C. § 1881(b)(4); or (ii) an entity belonging to any of the categories of entities described within that definition; and

ii. if Data Importer were to be found eligible for process under FISA Section 702, which it believes it is not, it is nevertheless also not the type of provider that is eligible to be subject to UPSTREAM collection pursuant to FISA Section 702, as described in paragraphs 62 and 179 of the Schrems II Judgment.

(c) EO 12333 does not provide the U.S. government the ability to order or demand that Data Importer provide assistance for the bulk collection of information and Data Importer shall take no action pursuant to U.S. Executive Order 12333.

3. Backdoors

3.1. Data Importer certifies that:

(a) it has not purposefully created backdoors or similar programming for governmental agencies that could be used to access Data Importer's systems or Personal Data subject to the Standard Contractual Clauses;

(b) it has not purposefully created or changed its business processes in a manner that facilitates government access to Personal Data or systems; and

(c) national law or government policy does not require Data Importer to create or maintain back doors or to facilitate access to Personal Data or systems.

3.2. Data Exporter will be entitled to terminate the contract on short notice in cases in which Data Importer does not reveal the existence of a back door or similar programming or manipulated business processes or any requirement to implement any of these or fails to promptly inform Data Exporter once their existence comes to its knowledge.

4. Information About Legal Prohibitions

4.1. Data Importer will provide Data Exporter information about the legal prohibitions on Data Importer to provide information under this Exhibit. Data Importer may choose the means to provide this information.

5. Additional Measures to Prevent Authorities from Accessing Personal Data

5.1. Notwithstanding the application of the security measures set forth in this Addendum, Data Importer will implement internal policies establishing that:

(a) Data Importer must require an official, signed document issued pursuant to the applicable laws of the requesting third party before it will consider a request for access to transferred Personal Data;

(b) Data Importer's Data Protection Officer, or if one has not been appointed, the individual responsible for data privacy and protection, shall be notified upon receipt of each request or order for transferred Personal Data;

(c) Data Importer shall scrutinize every request for legal validity and, as part of that procedure, will reject any request Data Importer considers to be invalid;

(d) if Data Importer is legally required to comply with an order, it will respond as narrowly as possible to the specific request; and

(e) if Data Importer receives a request from public authorities to cooperate on a voluntary basis, Personal Data transmitted in plain text may only be provided to public authorities with the express agreement of Data Exporter.

6. Termination

6.1. This Exhibit shall automatically terminate with respect to the Processing of Personal Data transferred in reliance of the Standard Contractual Clauses if the European Commission or a competent regulator approves a different transfer mechanism that would be applicable to the Restricted International Transfers covered by the Standard Contractual Clauses (and, if such mechanism applies only to some of the data transfers, this Exhibit will terminate only with respect to those transfers) and that does not require the additional safeguards set forth in this Exhibit.