DATA PROCESSING ADDENDUM

1. This Data Processing Addendum (“**Addendum**”) forms part of the Terms of Services (“**Principal Agreement**”) between: (i) Stonly **(“Vendor”)** acting on its own behalf and as agent for each Vendor affiliate; and (ii)

   (“**Company**”) acting on its own behalf and as agent for each Company Affiliate.

2. In consideration of the mutual obligations set out herein, the Parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Principal Agreement. Except where the context requires otherwise, references in this Addendum to the Principal Agreement are to the Principal Agreement as amended by, and including, this Addendum.

3. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect. Nothing in this Addendum shall derogate from Vendor's obligations under the Principal Agreement in relation to the protection of Personal Data or entitles Vendor to process (or permit the processing of) Personal Data in a manner which is prohibited by the Principal Agreement.

4. The Parties state that under the Principal Agreement and this Addendum, for the purposes of the GDPR, the Company is the Controller and Vendor is the Processor, and for the purposes of the CCPA, the Company is a business and the Vendor is a service provider.

5. Under the Principal Agreement the nature and purposes of processing Personal Data by the Vendor as data processor shall be limited to those set forth in Schedule 1.

6. In the event of inconsistencies between the provisions of this Addendum and the Principal Agreement, the provisions of this Addendum shall prevail. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, if applicable, the Standard Contractual Clauses shall prevail.

7. Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (a) amended as necessary to ensure its validity and enforceability, while preserving the parties’ intentions as closely as possible or, if this is not possible, (b) construed in a manner as if the invalid or unenforceable part had never been contained therein.

8. **Definitions**

8.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 “**Applicable Laws**” means (a) European Union or Member State laws with respect to any Company Personal Data in respect of which any Company Group Member is subject to EU Data Protection Laws; (b) the California Consumer Privacy Act of 2018 (“**CCPA**”) with respect to any Company Personal Data in respect of which any Company Group Member is subject to the CCPA, and (c) any other applicable law with respect to any Company Personal Data in respect of which any Company Group Member is subject to any other Data Protection Laws;

1.1.2 "**Adequacy Recognition**" means the recognition of a territory by the European Commission as providing adequate protection to Personal Data;

1.1.3 "**Company Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.4 "**Company Group Member**" means Company or any Company Affiliate;

1.1.5 "**Company Personal Data**" means any Personal Data Processed by Vendor on behalf of a Company Group Member pursuant to or in connection with the Principal Agreement;

1.1.6 **"Data Privacy Framework"** means the adequacy decision issued by the European Commission on July 17, 2023 about the EU-U.S. Data Privacy Framework;

1.1.7 "**Data Protection Laws**" means EU Data Protection Laws, the CCPA, The Israeli Privacy Protection Law, 1981 and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.8 "**EEA**" means the European Economic Area;

1.1.9 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.10 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.11 "**Restricted Transfer**" means:

1.1.11.1 a transfer of Company Personal Data from any Company Group Member to Vendor; or

1.1.11.2 an onward transfer of Company Personal Data from Vendor to a Sub-processor, or between two establishments of Vendor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under Section 14.1 below;

1.1.12 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Vendor for Company Group Members pursuant to the Principal Agreement;

1.1.13 "**Standard Contractual Clauses**" means the contractual clauses set out in Schedule 2, amended as indicated (in square brackets and italics) in that Schedule and under Section 15.3.1;

1.1.14 "**Sub-processor**" means any person (including any third party and any Vendor affiliate, but excluding an employee of Vendor or any of its sub-contractors) appointed by or on behalf of Vendor to Process Personal Data on behalf of any Company Group Member in connection with the Principal Agreement; and

1.1.15 "**Vendor**" means Vendor and any entity that owns or controls, is owned or controlled by or is or under common control or ownership with Vendor, where control is defined as the possession, directly or indirectly, of the power to direct or

cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.1.16 "**Party**"/"**Parties**" means the Company Group Members and the Vendor separately, or jointly, as the case may be;

1.1.17 "**Purpose**" means as described in Schedule 1; and

1.1.18 "**Supervisory Authority**" means any court, regulatory agency or authority which, according to Applicable Laws and/or regulations, supervises privacy issues and/or the processing of personal data.

1.2 The terms, "**commission**", "**controller**", "**service provider**", "**business**", "**customer**", "**business purpose**", "**data subject**", "**member state**", "**personal data**" or "**personal information**", "**personal data breach**", "**processing**", "**processor**" and "**supervisory authority**" "**sale**" shall have the same meaning as in the GDPR or in the CCPA, as applicable, and their cognate terms shall be construed accordingly. In addition, each of the terms defined in this section 8.2 shall have the meaning of its equivalent in the GDPR or in the CCPA, as applicable.

2. Special Undertakings of the Parties

2.1 Roles, ownership of personal data, processing and purpose

2.1.1 The Company and each Company Affiliate shall be considered, in the context of the CCPA as the business, and in the context of the GDPR as the controller of the personal data processed on its behalf and in accordance with its instructions, which concerns its respective data subjects, or customer, as applicable. However, for the avoidance of doubt, the Company and the Company Affiliates shall not be regarded as joint controllers in relation to the personal data concerning each other's data subjects. The Vendor shall be considered, in the context of the CCPA as the service provider and in the context of the GDPR, as a processor of the personal data processed on behalf of the Company Group Member.

2.1.2 The Company pays Vendor service fees in consideration for the Services to be provided by Vendor pursuant to the Principal Agreement. Vendor does not receive from the Company and the Company does not pay Vendor any monetary or other valuable consideration for Vendor's Collection of the Company Personal Data on behalf of the Company.

2.1.3 The Vendor may only process the Company Group Member's personal data for the Purpose and to the extent it is necessary for the fulfilment of the Vendor's obligations under this Addendum or the Principal Agreement. It is hereby clarified that the Company has the right and the obligation to make decisions about the Purposes and means of the processing of the personal data.

2.1.4 Vendor is prohibited from: (i) Selling Company personal data; and (ii) retaining, using, or disclosing Company personal data outside of the direct business relationship between Vendor and Company. Vendor understands the above restrictions and will comply with them.

2.1.5 Without prejudice to processing of personal data that is carried out in accordance with this Addendum, in the event that the Vendor infringes the Applicable Laws by determining the purposes and means of processing (e.g. by processing the personal data in violation of the Purpose), in the context of the GDPR, the processor will be regarded as the controller in respect of that processing. It should be noted that the Vendor, under the aforementioned circumstances, will be fully liable as the controller for such processing under the Applicable Laws including in relation to any sanctions under the said provisions.

2.1.6 The Vendor acknowledges that, between the Parties, all rights, title and interest in the personal data processed as a result of this Addendum is vested solely in the Company or the relevant Company Affiliate, irrespective of whether and to what extent the Vendor is considered to be a controller of the personal data.

2.2 **Special undertakings of the Company Group Members**

2.2.1 The Company and each Company Affiliate, each in respect of itself, undertakes to:

(a) Ensure that there is a legal ground for processing the personal data covered by this Addendum;

(b) Inform the Vendor about any erroneous, rectified, updated or deleted personal data subject to the Vendor's processing;

(c) Provide the Vendor with documented instructions regarding the Vendor's processing of the personal data, as may be required from time to time; and

2.3 **Special undertakings of the Vendor**

2.3.1 **The Vendor undertakes to:**

(a) Only process personal data in accordance with Applicable Laws and the Company Group Member documented instructions, including with regard to transfers of personal data to a third country outside of the EEA or an international organisation (such documented instructions shall indicate, among others, which transfer tools need to be used by Vendor), unless required to do so by Applicable Laws; in such a case, the Vendor shall inform the Company Group Member of that legal requirement before processing the personal data, unless such information is prohibited by the Applicable Laws on important grounds of public interest;

(b) Ensure that only such employees (of the Vendor or its subcontractors) which must have access to the personal data in order to meet the Vendor's obligations under this Addendum shall have access to the personal data processed on behalf of the Company Group Member, and that such employees have received appropriate training and instructions regarding processing of personal data as well as committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) Taking into account the nature of the processing, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (and as a minimum the security measures further described in Schedule 3) and assist the Company Group Member by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the obligations of the controller or the business, as applicable, to respond to requests for exercising the data subject or customer, as applicable, rights laid down in the Data Protection Laws. Unless prohibited by law, Vendor shall without undue delay notify Company of any material changes impacting the technical and organisational security measures implemented by Vendor which cause such measures to fall short of Vendor's data security obligations under this Addendum.

(d) Assist the Company Group Member in ensuring compliance with the obligations pursuant to GDPR, Articles 33 to 36 (e.g. assisting the controller in case of data breach, when conducting data protection impact

assessments and prior consultations) taking into account the nature of the processing and the information available to the Vendor;

(e) Make available to the Company Group Member all information necessary to demonstrate compliance with the obligations laid down in this Addendum and allow for and contribute to audits, including inspections, conducted by the Company or another auditor mandated by it, in accordance with Clause 5; and

(f) Otherwise comply with the Applicable Laws in its daily business.

2.3.2 The Vendor shall immediately inform the Company Group Member, if, in its opinion, an instruction infringes the Applicable Laws.

3. Authority

Vendor warrants and represents that, before Vendor processes any Company Personal Data on behalf of any Company Group Member, Vendor's entry into this Addendum as agent for and on behalf of any Vendor affiliate will have been duly and effectively authorised (or subsequently ratified) by that Vendor affiliate.

4. Processing of Company Personal Data

4.1 Vendor shall:

4.1.1 immediately inform Company Group Member if it is at the opinion that it has been given an instruction that does not comply with the Applicable Laws;

4.1.2 comply with all applicable Data Protection Laws in the processing of Company Personal Data;

4.1.3 not Process Company Personal Data other than on the relevant Company Group Member's documented instructions as it will provide from time to time, unless processing is required by Applicable Laws to which the relevant Vendor is subject, in which case Vendor shall to the extent permitted by Applicable Laws inform the relevant Company Group Member of that legal requirement before the relevant processing of that Personal Data;

4.1.4 agrees that from the effective date of this Addendum, and continuing as long as the Vendor possesses, stores, transmits or processes Personal Data on behalf of Company Group Member, the Vendor shall not do or omit to do anything which may cause Company Group Member to be in breach of any Applicable Laws - especially not to process the Personal Data for any other purpose save for the Purposes agreed hereunder; and

4.1.5 undertakes to comply with the requirements of the GDPR and when applicable the CCPA, and to take all appropriate technical and organisational measures required under the GDPR or the CCPA when applicable, including appointing a data protection officer and representative in the EEA.

4.1.6 If it collects Personal Data for or on behalf of Company, or provides, or otherwise makes available Personal Data to Company, then the following will apply:

4.1.6.1 At Company's request, Vendor will provide supporting evidence, to demonstrate that: (i) Vendor collects, obtains and processes Personal Data lawfully, without violating any third parties' rights, contractual obligations or Data Protection Laws; (ii) Vendor has all rights, consents, authorization and title to grant the rights and permissions

to use the Personal Data under the terms of the Agreement; (iv) Processing and use of the Personal Data by Company and modification thereof by Company's clients under the terms of the Principal Agreement will not violate the Data Subjects or customers, as applicable, rights and other third parties, including without limitation privacy, data protection, good-will, good name, publicity, confidentiality and intellectual property rights.

4.1.6.2 Without limiting the aforesaid, Vendor confirms, and at Company's request will demonstrate that all Data Subjects or customer, as applicable, received appropriate disclosures and notifications, as required under Data Protection Laws, including for the use, distribution and trans-border transfer of Personal Data, which encompasses the use of the Personal Data under the terms of the Principal Agreement. Where a third party provided the notices to the Data Subjects or customer, as applicable, and received their consent, Vendor will bear sole responsibility to verify and will be able to demonstrate that the notices and consents were sufficient for the purposes of use under the terms of the Agreement and adequate pursuant to Privacy Laws and Regulations.

4.2 Each Company Group Member:

4.2.1 instructs Vendor (and authorises Vendor to instruct each Sub-processor) to:

4.2.1.1 process Company Personal Data; and

4.2.1.2 in particular, transfer Company Personal Data to any country or territory,

1.1. as reasonably necessary for the provision of the Services and consistent with the Principal Agreement; and

4.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in Section 4.2.1.1 on behalf of each relevant Company Group Member.

4.3 Schedule 1 to this Addendum sets out certain information regarding the Vendor's processing of the Company Personal Data as required by article 28(3) of the GDPR. Company may make reasonable amendments to Schedule 1 by written notice to Vendor from time to time as Company reasonably considers necessary to meet those requirements. Nothing in Schedule 1 (including as amended pursuant to this Section 4.3) confers any right or imposes any obligation on any party to this Addendum.

5. Confidentiality

1.2. Vendor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of Vendor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the Purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Vendor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality. The list of the persons authorised to access Company Personal Data needs to be reviewed periodically by Vendor. On the basis of the said review, access to personal data can be withdrawn and in this case, personal data cannot be accessible anymore to those persons.

6. Data Security

6.1 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 for the rights and freedoms of natural persons, Vendor shall in relation to the Company Personal Data implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in any Data Protection Law, and at least those measures indicated in Schedule 3.

6.2 In assessing the appropriate level of security, Vendor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

6.3 Vendor will regularly monitor compliance with these safeguards. Vendor will not materially decrease the overall security of the Services during the term of the Principal Agreement.

7. Sub-processing

7.1 Each Company Group Member authorises Vendor to appoint (and permit each Sub-processor appointed in accordance with this Section 7 to appoint) Sub-processors in accordance with this Section 7 and any restrictions in the Principal Agreement.

7.2 Vendor may continue to use those Sub-processors already engaged by Vendor as of the date of this Addendum and which are listed in Schedule 2 attached hereto, subject to Vendor meeting the obligations set out in Section 7.4.

7.3 Vendor shall give Company prior written notice of the appointment of any new Sub-processor, including full details of the processing to be undertaken by the Sub-processor. If, within 30 days of receipt of that notice, Company notifies Vendor in writing of any objections (on reasonable grounds) to the proposed appointment:

7.3.1 Vendor shall work with Company in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Sub-processor; and

7.3.2 where such a change cannot be made within 30 days from Vendor's receipt of Company's notice, notwithstanding anything in the Principal Agreement, Company may by written notice to Vendor with immediate effect terminate the Principal Agreement to the extent that it relates to the Services which require the use of the proposed Sub-processor.

7.4 With respect to each Sub-processor, Vendor shall:

7.4.1 before the Sub-processor first processes Company Personal Data, carry out adequate due diligence to ensure that the Sub-processor is capable of providing the level of protection for Company Personal Data required by the Principal Agreement;

7.4.2 ensure that the arrangement between the Vendor, and the Sub-processor, is governed by a written contract including terms which offer at least the same level of protection for Company Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR (the "**Sub-processor Agreement**");

7.4.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one Vendor and the Sub-processor;

7.4.4 provide to each Company Group Member for review such copies of the agreements with Sub-processors (which may be redacted to remove confidential

commercial information not relevant to the requirements of this Addendum) as any Company Group Member may request from time to time; and

7.4.5 ensure that the Company is deemed as a third-party beneficiary in the agreement between the Vendor and its Sub-processor, such that any Sub-processor should be directly liable to Company and Company may be entitled to request directly from any Sub-processor to return any personal data.

7.5 Vendor shall ensure that each Sub-processor performs the obligations under this Addendum, as they apply to processing of Company Personal Data carried out by that Sub-processor, as if it were party to this Addendum in place of Vendor.

7.6 Vendor shall update Schedule 2 attached hereto promptly upon the engagement with a new Sub-processor for the processing of the Company Personal Data.

7.7 Notwithstanding the foregoing in section 7.4.5, the Vendor shall remain responsible for all obligations performed and any omission to perform or comply with the provisions under this Addendum by Sub-processor to the same extent as if such obligations were performed or omitted by the Vendor. The Vendor shall also remain the Company Group's sole point of contact. For the avoidance of doubt, the fact that the Company Group Member pursuant to this section may enter into data processing agreements and Standard Contractual Clauses directly with a Sub-processor will not affect the Vendor's responsibility for such Sub-processor acting under such agreement.

8. Data subject rights

8.1 Taking into account the nature of the Processing, Vendor shall assist each Company Group Member by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company Group Members' obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights or customer's rights, as applicable, under the Data Protection Laws.

8.2 Vendor shall:

8.2.1 promptly notify Company Group Member if Vendor receives a request from a data subject or a customer, as applicable, under any Data Protection Law in respect of Company Personal Data; and

8.2.2 ensure that the Vendor does not respond to that request except on the documented instructions of Company or the relevant Company Affiliate or as required by Applicable Laws to which the Vendor is subject, in which case Vendor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Vendor responds to the request.

8.2.3 endeavour to help Company Group Member to enable Data Subjects or customers, as applicable, to exercise their rights under Data Protection Laws, such as access requests and requests for the rectification, erasure or portability of personal data as well as making objections to the data processing and any other request that the Data Subjects or customers, as applicable, might be entitled to file to Company Group Member.

8.3 Where Company is required to delete Personal Data about a Data Subject, or customer, as applicable, it will direct Vendor accordingly and Vendor will immediately delete the such Personal Data from its records.

9. Personal Data Breach

9.1 Vendor shall notify Company without any delay but no later than within 24 hours in writing upon Vendor or any Sub-processor becoming aware or has reasons to believe of any Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow each Company Group Member to meet any obligations to report or inform Data Subjects or customers, as applicable, of the Personal Data Breach under the Data Protection Laws.

9.2 The notice shall include the following information:

9.2.1 the nature of the unauthorised disclosure or use;

9.2.2 the relevant data accessed, disclosed or used;

9.2.3 the identity of the person(s) or entity(ies) who received the unauthorised disclosure or made the unauthorised access or use;

9.2.4 what corrective action the Vendor took or shall take to prevent further unauthorised disclosures or uses;

9.2.5 what the Vendor did or will do to mitigate any deleterious effect of such unauthorised disclosure or use; and

9.2.6 any other information as the Supervisory Authority may reasonably request.

9.3 Vendor shall use its best efforts to immediately remedy any security incident and Personal Data Breach and prevent any further consequences at its own expense in accordance with Applicable Laws, regulations and standards.

9.4 Immediately following Vendor's notification to Company of a Personal Data Breach, the Parties shall coordinate with each other to investigate the breach. Vendor agrees to fully cooperate with Company and each Company Group Member in Company's handling of the matter, including, without limitation:

9.4.1 enabling Company to make the notification required under the Data Protection Laws within 72 hours from the detection of the Personal Data Breach

9.4.2 assisting with any investigation;

9.4.3 providing Company and its respective designees with unconditional access to the facilities and operations affected and all pertinent records to conduct a review of Vendor's compliance with the data security requirements;

9.4.4 facilitating interviews with Vendor's employees and others involved in the matter; and

9.4.5 making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards or as otherwise reasonably required by Company.

9.5 In the event of any security event, Vendor shall:

9.5.1 conduct a reasonable investigation of the reasons for and circumstances of such security event;

9.5.2 use reasonable endeavours to take all necessary actions to prevent, contain, and mitigate the impact of, such security event;

9.5.3 promptly (and in any event within one business day after Vendor discovered such security event) provide notice to Company in writing, if there is a risk of Personal Data Breach;

9.5.4 as soon as practicable after Vendor discovers a security event, provide a written summary to Company providing relevant details concerning such security event, if there is a risk of Personal Data Breach;

9.5.5 collect and preserve all evidence concerning the discovery, cause, vulnerability, remedial actions and impact related to such security event;

9.5.6 document the incident response and remedial actions taken; and

9.5.7 if requested by Company, provide notice to individuals whose Personal Data was or may have reasonably been exposed in a manner and format reasonably specified by Company.

9.6 Vendor agrees to assist Company in advising the Supervisory Authority and data subjects or customer, as applicable, about Personal Data Breach. It shall not, however, inform any third party of any Personal Data Breach without first obtaining Company's prior written consent, other than to inform a complainant (if any) that the matter has been forwarded to Company. Further, Vendor agrees that Company shall have the sole right to determine:

9.6.1 whether notice of the Personal Data Breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law or regulation, or otherwise in Company's discretion; and

9.6.2 the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation.

9.7 Vendor shall reimburse Company for actual reasonable costs incurred by Company in responding to, and mitigating damages caused by any security incident or Personal Data Breach, including all costs of notice and/or remediation.

9.8 Vendor hereby authorizes Company when it is required to do so in accordance with applicable requirements at Company's discretion, to provide notice to third parties of, and information and documents concerning, any Personal Data Breach, including without limitation individuals or entities that may have been impacted by the breach.

10. Data Protection Impact Assessment and Prior Consultation

10.1 Vendor shall provide reasonable assistance to each Company Group Member with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required of any Company Group Member by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Vendor.

11. Cooperation and Coordination

11.1 Vendor agrees to reasonably cooperate and coordinate with Company concerning: (a) Company's investigation, enforcement, monitoring, document preparation, notification requirements and reporting concerning Personal Data Breach and Vendor's and Company's compliance with Data Protection Laws; and (b) and any other activities or duties set forth under the Principal Agreement for which cooperation between Company and Vendor may be reasonably required by Company.

11.2 Upon reasonable request by Company, Vendor shall as promptly and as reasonably practicable provide Company with a written report containing information reasonably requested by Company relating to: (a) any security event and Personal Data Breach; or (b) actual or reasonably suspected non-compliance with this Addendum. In addition, Vendor shall provide Company with any documents requested by Company related to the foregoing, including without limitation, any information security assessment and security control audit reports.

12. Deletion or return of Company Personal Data

12.1 Subject to Sections 12.2 and 12.3, within twenty-four (24) months of the date of termination or expiration of any Services involving the Processing of Company Personal Data (the "**End Date**"), Vendor shall delete all copies of those Company Personal Data.

12.2 Subject to Section 12.3, Company may in its absolute discretion by written notice to Vendor require Vendor to (a) return a complete copy of all Company Personal Data to Company by secure file transfer in such format as is reasonably notified by Company to Vendor; and (b) delete and procure the deletion of all other copies of Company Personal Data Processed by Vendor. Vendor shall comply with any such written request within thirty (30) days of the request date.

12.3 Vendor may retain Company Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Vendor shall ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

13. Audit rights

13.1 At least once per year, Vendor shall conduct site audits of the information technology and information security controls for all facilities used in complying with its obligations under this Addendum, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognized third-party audit firm based on the recognized industry best practices. Company shall treat such audit reports as Vendor's confidential information.

13.2 Company shall have the right to perform, no more than once per year, an audit of the Vendor's processing of the Company Group Member's personal data (including such processing as may be carried out by the Vendor's Sub-processors, if any) in order to verify the Vendor's, and any Sub-processor's, compliance with this Addendum.

13.3 Upon the provision of reasonable notice to the Vendor during the term of the Principal Agreement, Company (or any third party reasonably selected by Company) may undertake an assessment and audit of information security and data protection. Such assessment may include:

13.3.1 access rooms in the presence of an authorised employee of Vendor;

13.3.2 demand explanations in writing;

13.3.3 take the necessary steps in case of any actual or threatening infringement of data protection and privacy rules.

13.4 Therefore, Vendor shall make available to each Company Group Member on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by any Company Group Member or an auditor mandated by any Company Group Member in relation to the Processing of the Company Personal Data by the Vendor.

13.5 Any Company Group Member undertaking an audit shall give Vendor reasonable notice of any audit or inspection to be conducted under Section 13.2 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Vendor's premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection.

13.6 If any Supervisory Authority: (i) contacts the Vendor with respect to its systems or any processing of personal data carried out by the Vendor, (ii) conducts, or gives notice of its intent to conduct, an inspection of the Vendor with respect to the processing of personal data, or (iii) takes, or gives notice of its intent to take, any other regulatory action alleging improper or inadequate practices with respect to any processing of personal data carried out by the Vendor, then the Vendor shall immediately notify any Company Group Member and shall subsequently supply any Company Group Member with all information pertinent thereto to the extent permissible by law. Notwithstanding the aforesaid, any Supervisory Authority shall always have direct and unrestricted access to the Vendor's premises, data processing equipment and documentation in order to investigate that the Vendor's processing of the personal data is performed in accordance with the Applicable Laws.

13.7 The Vendor shall at all times keep a comprehensive and up to date record of where the IT system(s) used to process personal data on behalf of any Company Group Member is/are located. For the avoidance of doubt, this shall include the locations of any IT systems belonging to any Sub-processor(s). Upon request, the Vendor shall promptly provide any Company Group Member with a copy of the record.

13.8 Each Party shall bear its own costs for audits set out herein except where the audit reveals non-compliance with this Addendum or the Applicable Laws, in which case the Vendor shall bear all costs of the audit.

14. Transfer of Personal Data

14.1 Where the processing of Personal Data by Vendor or any of its Sub-processor (both as "data importer") (1) relates to data subjects located in the European Union, EEA, United Kingdom or Switzerland or is otherwise subject to the GDPR and (2) takes place in a country outside the EEA, the parties agree to comply with the terms of the Standard Contractual Clauses. For this purpose, the following additional provisions shall apply to this Addendum or, as applicable, be included in the Sub-processor Agreement:

14.1.1 The Standard Contractual Clauses shall be incorporated into this Addendum or the Sub-processor Agreement, as applicable, and shall be considered duly executed between the parties;

14.1.2 If so required by the laws or regulatory procedures of any jurisdiction, any Company Group Member (as "data exporter") and Vendor (as "data importer"), or Vendor (as "data exporter") and Sub-processor (as "data importer"), as applicable, will execute or re-execute the Standard Contractual Clauses in a separate document setting out the proposed transfers of Personal Data in such a manner as may be required. In the event that the Standard Contractual Clauses are (i) amended, replaced or repealed by the European Commission, (ii) declared invalid by a court of competence, or (iii) otherwise terminated, annulled, replaced or repealed under any data privacy legislation, the data exporter and the data importer shall work together in good faith to enter into any updated version of the Standard Contractual Clauses or other appropriate successor transfer mechanism or negotiate in good faith any other solution to enable the transfer of the Personal Data to data importer.

14.1.3 The data importer will assess whether the laws applicable to it provide adequate protection under EU Data Protection Law. If and to the extent that the data

importer has reasons to believe that any such laws are likely to have a substantial adverse effect on the level of data protection mandated by the Standard Contractual Clauses and required under EU Data Protection Laws, it will inform the data exporter about the relevant laws and its effect on the protection of the Personal Data received under the Standard Contractual Clauses ("**SCC Personal Data**") and, to the extent necessary, it will agree in good faith with the data exporter on any supplementary measures to mitigate this effect to the extent required under EU Data Protection Laws.

14.1.4 The data importer undertakes to implement appropriate safeguards to protect SCC Personal Data in accordance with the requirements of the EU Data Protection Laws, including by implementing appropriate technical and organisational safeguards.

14.1.5 In the event that the data importer receives a legally binding request for access to the SCC Personal Data by a public authority of a non-EEA country ("**Disclosure Request**"), it will promptly notify the data exporter of such request to enable the data exporter to intervene and seek relief from such disclosure, unless the data importer is otherwise prohibited from providing such notice by applicable laws. The data importer will, to the extent permitted by applicable law, put the Disclosure Request on hold until the supervisory authority competent for the data exporter has been informed by the data exporter and/or data importer about the Disclosure Request. If the data importer is prohibited from notification and/or suspension of the request, then:

14.1.5.1 It will use its reasonable best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible.

14.1.5.2 In the event that, despite having used its reasonable best efforts, the data importer is not permitted to notify the data exporter, it will make available on an annual basis general information on the requests it received to the data exporter and/or the competent supervisory authority of the data exporter.

14.1.5.3 Oppose any such Disclosure Request and contest its legal validity to the extent legally permitted under applicable law.

14.1.6 In any event, the data importer will:

14.1.6.1 Not make any disclosures of SCC Personal Data to any public authority in response to a Disclosure Request in a manner that it would go beyond what is strictly required and proportionate to comply with the Disclosure Request; and

14.1.6.2 Upon request from the data exporter, provide it with general information on the number and type of Disclosure Requests the data importer received in the preceding 12 months period, to the fullest extent permitted by applicable law.

14.2 Vendor or its Sub-processor, as applicable, shall not transfer or remove Personal Data across international or jurisdictional boundaries, to the extent such transfers are subject to restrictions under applicable data privacy legislation, unless:

14.2.1 Any Company Group Member, and where legally required the data subject, have consented to such transfer in writing and such transfer complies and continues to comply with the requirements for international data transfers under applicable data privacy legislation; or

14.2.2 Such transfer is required by applicable data privacy legislation to which Vendor or its Sub-processor, as applicable, are subject. In such a case, Vendor or its Sub-processor, as applicable, shall inform Company Group Member of that legal requirement before carrying out the required processing, unless that law prohibits such information on important public interest grounds.

15. General Terms

Governing law and jurisdiction

15.1 Without prejudice to Mediation and Jurisdiction and Governing Law sections of the Standard Contractual Clauses:

15.1.1 the Parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

15.1.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

Assignation of rights or obligations

15.2 Neither Party may assign its rights or obligations under this Addendum without the prior written consent of the other Party.

Changes in Data Protection Laws, etc.

15.3 Each Company Group Member may:

15.3.1 if: (i) the Data Privacy Framework is invalidated; (ii) Vendor or any of its agents are no longer able to continue complying with the principles of the Data Privacy Framework; (iii) the Adequacy Recognition is invalidated or otherwise terminated; (iv) the Standard Contractual Clauses are invalidated or no longer in effect; or (v) any other Personal Data transfer safeguard is no longer in effect for any reason, then Vendor will take such alternative lawful measures, as may be available and applicable, to continue facilitating the lawful transfer of Company Personal Data by Vendor, and by Vendor's agents, other processors, or equivalents thereof; and

15.3.2 Propose any other variations to this Addendum which Company reasonably considers to be necessary to address the requirements of any Data Protection Law.

15.4 If Vendor is unable to provide an alternative measure to continue transferring Company Personal Data in accordance with Data Protection Laws, then Company, may terminate the Addendum and the Principal Agreement, or those portions of the Services, which cannot be provided without the transfer of the Company Personal Data, upon a written notice with immediate effect, and Company will receive a pro-rated refund of applicable pre-paid fees or a pro rata reduction of future fees.

15.5 Vendor shall not require any additional consent or approval of to amend this Addendum pursuant to this section 15.3 or otherwise.

Notices

15.6 All notices to a Party under this Addendum shall be in writing and sent to its address as set forth at the beginning of this Addendum, or to such other address as such Party has provided the other in writing for such purpose. Notices may be sent by post, courier, fax or email.

15.7 Notices shall be deemed to have been duly given (i) on the day of delivery when delivered in person or by courier, (ii) three (3) business days after the day when the notice was sent when sent by post, and (iii) on the day when the receiver has manually confirmed that it is received when sent per fax or email.

Remuneration

15.8 The remuneration for the Vendor's undertakings under this Addendum shall be included in the remuneration paid by the Company Group Member under the Principal Agreement. Vendor shall not be entitled to additional remuneration based on this Addendum.

Term and Termination

15.9 This Addendum shall enter into force on the date hereof. Unless terminated earlier (i) due to a material breach of the terms of this Addendum, in which case this Addendum shall be terminated with immediate effect if the other Party fails to cure such breach in a satisfactory manner within fifteen (15) days after the other Party's written demand thereof, or (ii) in accordance with Section 15.10, this Addendum shall remain in force until the termination or expiration of the Principal Agreement, whereupon it shall terminate automatically without further notice. The termination or expiration of this Addendum shall immediately terminate any processing agreement entered into between Vendor and any Sub-processor.

15.10 The Company may terminate this Addendum in relation to itself or in relation to any Company Affiliate by giving the Vendor thirty (30) days written notice. A Company Affiliate may terminate this Addendum in relation to itself by giving the Vendor thirty (30) days written notice. For the avoidance of doubt, a termination in relation to a particular Company Affiliate in accordance with this Section 15.10 shall not affect the validity of this Addendum as regards between the Company, any remaining Company Affiliates, and the Vendor. In the event that this Addendum is terminated due to the Vendor's failure to fulfil its obligations hereunder or under the Principal Agreement, this Addendum shall terminate in relation to the Company as well as all Company Affiliates, unless otherwise agreed between the Parties in writing. It is hereby clarified that Vendor shall cease all processing activities of Company or Personal Data, upon termination of this Addendum, provided that such Addendum is not replaced by a similar agreement conforming to Data Protection Laws.

Liability and Indemnification

15.11 Each Party shall indemnify and hold the other Party harmless from and against all losses due to claims from third parties including government/authority fines and penalties resulting from, arising out of or relating to any breach by such first-mentioned Party of this Addendum and in the applicable Data Protection Laws.

15.12 Any loss suffered by a Party resulting from, arising out of or relating to a breach of this Addendum by the other Party that is not due to claims from third parties under Section 15.11 shall be governed by the provisions regarding liability and limitation of liability in the Principal Agreement.

15.13 Vendor acknowledges and agrees that any unauthorised access to, use or disclosure of Personal Data would cause immediate and irreparable harm for which money damages would not constitute an adequate remedy and that in the event of any unauthorised use or disclosure of Personal Data, any Company Group Member shall be entitled to immediate injunctive relief.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above.

Signed by Company	**Signed by Stonly**
_____	_____
Full name:	Full name:
Title:	Title:
Date:	Date:

Schedule 1
Description of the processing of personal data

1. The project

Stonly will provide crafted and personalised in-app experiences and guidance based on client properties and events

2. Data subjects

The personal data processed concern the following categories of data subjects:

- Company's employees – those with Stonly logins or licences
- Company's end-users - those viewing the Stonly guides (they can be Company's employees or customers, depending on how Stonly is used)

3. Categories of personal data

The personal data processed concern the following categories of personal data:

Company's employees:

- Name and email
- [Only if using the Stonly extension] Page views on all domains whitelisted by Company

Company's end-users:

- User, browser and session identifiers
- Stonly content browsing activity and inputs (including contact form submissions)
- [Only if using Targeting] Targeting events and properties sent by Company to Stonly

4. Purpose of the personal data processing

- Access management to the Stonly platform
- Personalise Stonly content shown to Company's customers and employees
- Provide analytics and reporting to Customer in the Insights section of the Stonly platform, or as exports

5. Processing operations

The personal data processed will be subject to the following basic processing activities:

Access, analytics, collection, transmission, retrieval, storage

6. Duration of processing

Duration of the agreement + 2 years, unless the Company requests otherwise

7. Security measures

The security measures are described in Schedule 3

stonly

Schedule 2
Sub-Processors

Service	Location	Process customer data	Process customers' customer data	Type of data	Purpose	Contact	Links
AWS	France	yes	yes	Email, Name, IP Address, Online identifiers, Client identifiers, Usage Data	Cloud hosting	aws-EU-privacy@amazon.com	Privacy Notice
imgix	France (in our VPC)	yes	no	User uploaded images	Image Processing	privacy@imgix.com	Privacy Policy
Brevo (formerly Sendinblue)	France	yes	yes	Email, Name, request content	Customer Communication (transactional emails, contact forms)	dpo@sendinblue.com	Privacy Policy
Zendesk	France	yes	no	Email, Name, request content	Customer Support (email)	privacy@zendesk.com	Privacy and Data Protection
Altinity	France (in our VPC)	yes	yes	Guide browsing and inputs	Cloud Management	privacy@altinity.com	Privacy Policy
Microsoft Azure	France (in our VPC)	yes	no	Stonly content	[Only for Stonly AI customers] AI Answers feature	Privacy Contact Form	Privacy Policy
Hex Technology	United States	yes	yes	Email, Name, IP Address, Online identifiers, Client identifiers, Usage Data	[Only for customers with custom dashboards] Analytics	privacy@hex.tech	Privacy Policy

stonly

Schedule 3
Technical and Organisational Measures

Organisational Measures

Policies

Stonly has policies in place to ensure the security of the personal data that we process. They are regularly reviewed both internally and externally to make sure they remain effective.

Policy	Purpose
Access Control Policy	To limit access to information and information processing systems, networks, and facilities to authorised parties in accordance with business objectives.
Asset Management Policy	To identify organisational assets and define appropriate protection responsibilities.
Business Continuity & Disaster Recovery Plan	To prepare Stonly in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame.
Cryptography Policy	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
Data Management Policy	To ensure that information is classified and protected in accordance with its importance to the organization.
Human Resources Policy	To ensure that employees and contractors meet security requirements, understand their responsibilities, and are suitable for their roles.
Incident Response Plan	Policy and procedures for suspected or confirmed information security incidents.
Information Security Policy	Communicate our information security policies and outline the acceptable use and protection of Stonly's information and assets
Operations Security Policy	To ensure the correct and secure operation of information processing systems and facilities.
Physical Security Policy	To prevent unauthorised physical access or damage to the organization's information and information processing facilities.
Risk Management Policy	To define the process for assessing and managing Stonly's information security risks in order to achieve the company's business and information security objectives.

Policy	Purpose
Secure Development Policy	To ensure that information security is designed and implemented within the development lifecycle for applications and information systems.
Third-Party Management Policy	To ensure protection of the organization's data and assets that are shared with, accessible to, or managed by suppliers, including external parties or third-party organizations such as service providers, vendors, and customers, and to maintain an agreed level of information security and service delivery in line with supplier agreements.
Workstation Security Policy	To establish the procedures and protocols for the use and security of end-user workstations (e.g. laptops, desktops, etc.) and their connection to the network to ensure they are properly secured to protect the confidentiality, integrity, and availability of Sensitive Data.

DPO

Stonly has appointed a DPO: Jean Roman

The DPO can be reached at dpo@stonly.com

Security Certifications

Stonly is SOC 2 type 2 certified and HIPAA compliant as of March 2023.

Third Party audits

On top of the annual SOC 2 review by our auditors, Dansa d'Arata Soucia, we have other third parties reviewing the security of our application and infrastructure:

- Bug-bounty program, always accepting reports
- Quarterly penetration tests

Both programs are run by the platform Yogosha, and we are committed to resolving all vulnerabilities with an SLA associated to their level of criticality.

Technical Measures

Measures on data

- Pseudonymisation and anonymisation when possible
- Encryption both at rest and in transit
- Frequent data back-ups, with recovery tests
- RPO of 30 minutes
- Access control: access on a "need to know" basis

Measures on software and applications

- Access control: multi-factor authentication on all sensitive systems, and force usage of a password manager

- Formal inventory of production system assets
- Use of static application security tests in our CI/CD
- Segregation of test, staging and production environments
- Automated functional and security tests before each code deployment in production
- Control of software installation
- Regular software update
- Use and regular update of anti-virus software and security patches
- Intrusion detection and prevention systems
- RTO of 150 minutes
- Logging system and audit logs

Measures on the communication networks

- Secure exchange via SSL/HTTPs
- DDoS protection
- Intrusion detection or prevention systems
- Firewalls
- Web-Application Firewalls (WAFs)
- VPN
- Proxy servers

Measures on paper records

- Access control: access on a “need to know” basis
- Locked office and cupboard
- A clean desk policy
- Secured destruction of paper record

Measures on hardware and facilities

All our information processing related to Stonly’s business activities are located in Stonly’s Virtual Private Cloud (VPC), managed by AWS, and no Stonly office contains any physical device processing user data.

Measures to protect hardware and data processing facilities are therefore delegated to AWS.

Measures on workstations

- Automatic desktop lock
- Encryption of hard drives
- Anti-Virus software

Schedule 4
Standard Contractual Clauses

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex

II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to

address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(a) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(b) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(c) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(d) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three: , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(f) The Parties agree that those shall be the courts of the EU Member State in which the data exporter is established.

(g) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(h) The Parties agree to submit themselves to the jurisdiction of such courts.

stonly

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses:

Signature and date:

Role: Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: Stonly SAS

Address: 43, rue du Président Wilson, 92300 Levallois-Perret, France

Contact person's name, position and contact details: Jean Roman, DPO, jean@stonly.com

Activities relevant to the data transferred under these Clauses: Stonly will provide crafted and personalised in-app experiences and guidance based on end-user properties and events

Signature and date:

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- *Company's employees – those with Stonly logins or licences*
- *Company's end-users - those viewing the Stonly guides (they can be Company's employees or customers)*

Categories of personal data transferred

Company's employees:

- Name and email
- [Only if using the Stonly extension] Page views on all domains whitelisted by Company

Company's end-users:

- User, browser and session identifiers
- Stonly content browsing activity and inputs (including contact form submissions)
- [Only if using Targeting] Targeting events and properties sent by Company to Stonly

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 only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Not applicable

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

continuous

Nature of the processing

Access, analytics, collection, transmission, retrieval, storage

Purpose(s) of the data transfer and further processing

- Access management to the Stonly platform
- Personalise content shown to Company's customers and employees
- Provide analytics and reporting to Customer in the Insights section of the Stonly platform, or as exports

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Duration of the agreement + 2 years, unless the Company requests otherwise

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

See Schedule 2

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

CNIL (French data regulator)

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

See Schedule 3

ANNEX III – LIST OF SUB-PROCESSORS

See Schedule 2