**DATA PROCESSING AGREEMENT**

This Data Processing Agreement (“**DPA**”) forms part of the agreement (the “**Agreement**”) between [Company Name] and Textly Inc. d/b/a Linguix (the “**Vendor**”). This DPA shall be effective as of the Effective Date of the Agreement and shall be effective until the earlier of, the termination of the Agreement or until deletion or return of all Personal Data as instructed by [Company Name] under this DPA.

**1. DEFINITIONS**

Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. In the event Data Protection Legislation exists in a jurisdiction the definitions set forth therein will supersede those herein when such Data Protection Legislation contemplates the terminology.

1.1. “**Controller**” means a legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of Processing Personal Data and gives instructions regarding Processing activities.

1.2. “**Data Subject Request**” means any request by a natural person to access, update, revise, correct, object to Processing or delete Personal Data or any similar request, whether or not made pursuant to the applicable Data Protection Legislation.

1.3. “**Data Protection Legislation**” means all applicable law, rule or regulation applicable to the Agreement, the Services, [Company Name] or Vendor, and applicable industry standards concerning privacy, data protection, confidentiality, information security, availability and integrity, or the handling or Processing (including retention and disclosure) of Personal Data, as may be amended, regulated, restated or replaced from time to time.

1.4. “**Personal Data**” or “**Personal Information**” means all data or information obtained by Vendor from or on behalf of [Company Name], in any form or format, that identifies, relates to, describes, is reasonably capable of being associate with, or could reasonably be linked, directly or indirectly, to an identified or identifiable natural person. Personal Data, as defined under the GDPR, submitted or made available by [Company Name] to Vendor for the performance of Vendor’s Services under the Agreement.

1.5. "**Process**” (including “**Processing**” or “**Processed**”) means any operation or set of operations that is performed upon any Personal Information, whether or not by automatic means, including, but not limited to, collection, recording, organization, storage, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, deletion, erasure, or destruction.

1.6. “**Processor**” means the party to this agreement, or under an agreement with the same requirements as this DPA, that processes Personal Data subject to the direction of the Controller and applicable Data Protection Legislation.

1.7. “**Sell**” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Data to a third party for monetary or other valuable consideration.

1.8. “**Services**” means those services that Vendor performs pursuant to the Agreement.

1.9. “**Standard Contractual Clauses**” or “**SCCs**” means (a) where the GDPR applies, the standard contractual clauses annexed to the European Commission’s Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (“**EU SCCs**”); (b) where the UK GDPR applies, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022 (“**UK SCCs**”); and (c) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner (the “**Swiss SCCs**”), each as may be updated from time to time.

1.10. “**Sub-processor**” or “**Service Provider**” means a third-party engaged and supervised by a party to this Agreement, who agrees to receive and process Personal Data under the terms of this DPA, or under an agreement with the same requirements as this DPA, solely for the purposes of processing or delivering Personal Data necessary for the fulfillment of this Agreement.

1.11."**System**” means any system, network, platform, database, computer, or telecommunications or information system owned, controlled or operated by or on behalf of either Party or any of its Affiliates for the purpose of Processing Personal Data pursuant to the Agreement.

**2. ROLES OF THE PARTIES**

2.1. To the extent that [Company Name] Personal Data is processed by Vendor, the parties agree that [Company Name] is the Controller and Vendor is the Processor.

**3. PROCESSING OF PERSONAL DATA**

When providing the Services to [Company Name], Vendor agrees to:

3.1. Process Personal Data solely as necessary to provide the Services to [Company Name], and in accordance with Data Protection Legislation, the Agreement, this DPA including ***Exhibits A*** of this DPA shall serve as Annex I, ***Exhibit B*** shall serve as Annex II, and ***Exhibit C*** shall serve as Annex III, and the written instructions of [Company Name];

3.2. refrain from (i) selling or sharing Personal Data (ii) retaining, using or disclosing the Personal Data for any purpose other than for the purpose specified in the Agreement, (iii) retaining, using or disclosing the Personal Data outside of the direct relationship between [Company Name] and Vendor, and (iv) combining Personal Data from different sources unless necessary for the provision of Services under this Agreement.

3.3. maintain the confidentiality of all Personal Data and ensure that its personnel, including employees, interns, temporary workers, and agency workers, have executed confidentiality agreements that prevent them from unauthorized Processing of Personal Data for the duration of their engagement with Vendor;

3.4. not disclose Personal Data to third parties, including government agencies and Vendor’s Sub-processors without the prior written approval of [Company Name] unless required by Applicable Law, in which case Vendor shall wherever possible (a) notify [Company Name] promptly in writing before complying with any disclosure request, (b) comply with all reasonable directions of [Company Name] with respect to such disclosure, and (c) promptly inform [Company Name] of any Personal Data so disclosed;

3.5. promptly notify [Company Name] of:

3.5.1. any request, inquiry, complaint, notice or communication received from any third party, including a data subject or a supervisory authority, with respect to any Personal Data and comply with instructions of [Company Name] in responding to such request, inquiry, complaint, notice or communication. Without limiting the generality of the foregoing, Vendor shall notify [Company Name] in writing within five (5) business days of receipt of any Data Subject Request relating to Personal Data Processed by Vendor and shall provide [Company Name] its reasonable assistance in responding to any such Data Subject Request (whether or not received directly by Vendor);

3.5.2. any request for the provision of Personal Data to a government body or authority or court, whether through legal means or otherwise, including specific details of the data provided;

3.5.3. any instruction by [Company Name] that Vendor believes to be in violation of Data Protection Legislation prior to engaging in the relevant Processing; and

3.5.4. any substantial changes to the Vendor’s notices, policies or procedures that would impede Vendor’s ability to fulfil the terms of this Addendum regarding protection of Personal Data;

3.6. upon [Company Name]’s request, submit the databases, tools, office space (if applicable), and other similar cloud based or on premises environments or locations used by Vendor to Process Personal Data for audit in accordance with *Section 8. Right to Audit* of the Vendor Agreement and Section 9. Information Requests of the DPA;

3.7. keep records that demonstrate its compliance with its obligations under this Addendum, and make them available to [Company Name] upon reasonable request and/or in connection with any audit referred to in Section 3.6 above and Section 9. Information Requests below;

3.8. reasonably assist and cooperate with [Company Name], including by providing information requested by [Company Name], to allow [Company Name] to comply with its obligations under Data Protection Legislation, including the completion of transfer impact assessments, privacy impact assessments, and data protection impact assessments; and

3.9. retain Personal Data in accordance with *Section 6. Data Retention* of the Vendor Agreement, *Section 8. Deletion or Return of Personal Data* of the DPA, but in no event longer than necessary to perform the Services.

**4. INFORMATION SECURITY MEASURES**

4.1. Administrative, technical, and physical safeguards designed to ensure the security, confidentiality, reliability, and integrity of Personal Data, as well as any Systems, facilities, or software that Vendor accesses or supports in connections with the Agreement. Such safeguards are:

4.1.1. commensurate with the type and amount of Personal Data Processed by Vendor, having regard to the state of the art and industry standards, and should, at minimum, protect Personal Data and Systems against reasonably anticipated threats or hazards, including from unauthorized access, loss, theft, destruction, use, modification, collection, attack, or disclosure;

4.1.2. in accordance with globally recognized security control standards such as ISO, SOC, NIST or similar certification; and

4.1.3. compliant with the any applicable specific industry standards as may apply to the Personal Data being Processed by Vendor

4.2. A written security program and policy that meets or exceeds the requirements imposed under Data Protection Legislation and aligns with established industry practices. Such security program and policy should address, at a minimum, the following:

4.2.1. identification of appropriately defined organizational roles related to information security;

4.2.2. controls with respect to employment of and access given to Personal Data by employees, agent and subcontractors of Vendor including background checks, security clearances that assign specific access privileges to individuals, and training regarding the handling of Personal Data;

4.2.3. an appropriate network security program that includes, without limitation, encryption and network and application partitioning;

4.2.4. . access identification and authentication;

4.2.5. maintenance and media disposal;

4.2.6. audit and accountability;

4.2.7. physical and environmental protections;

4.2.8. system and communication security;

4.2.9. incident response and planning; and

4.2.10. the integrity and reliability of facilities, systems and services, including critical asset identification, configuration and change management for software systems, and contingency planning / redundancy.

4.3. If Personal Data being Processed includes sensitive or biometric data for purposes of uniquely identifying a natural person, or data relating to criminal convictions and offences, Vendor shall apply specific restrictions and/or additional safeguards in compliance with the Data Protection Legislation. [Company Name] agrees that Vendor may implement adequate alternative security measures from time to time, provided the security level of the alternative measures is not materially decreased.

4.4. Vendor shall limit access to Personal Data to those individuals who require access to the Personal Data to meet Vendor’s obligations with respect to the delivery of the Services to [Company Name]. Vendor shall ensure that those individuals are informed in writing of the confidential or sensitive nature of the Personal Data.

**5. DATA SECURITY INCIDENT**

5.1. **Data Security Incident** means (i) the loss or misuse (by any means) of Personal Data; (ii) the inadvertent, unauthorized, and/or unlawful disclosure, access, alteration, corruption, transfer, sale,

rental, destruction, or use of Personal Data; or (iii) any other act or omission that compromises or may compromise the security, confidentiality, or integrity of Personal Data or a System.

5.2. If Vendor suspects or becomes aware of a Data Security Incident:

5.2.1. Vendor will notify [Company Name] without undue delay, and in any case within twenty-four (24) hours, after it becomes aware of any confirmed Data Security Incident;

5.2.2. undertake an investigation of such Data Security Incident and respond to [Company Name]’s reasonable requests for information relating to the Data Security incident as may be necessary;

5.2.3. reasonable assist [Company Name], its regulators and law enforcement agencies, with notification obligations under the applicable Data Protection Legislation. Unless otherwise required in accordance with applicable laws, [Company Name] shall be solely responsible for complying with any Data Protection Legislation data breach notification requirements applicable to [Company Name] and fulfilling any third-party notification obligations related to any Data Security Incident;

5.2.4. not make, and will require that their Sub-processors not make, any public announcements relating to such Data Security Incident without [Company Name]’s prior written approval, which shall not be unreasonably withheld; and

5.2.5. take all reasonable corrective action in a timely manner, at the expense of Vendor, to remediate and prevent a recurrence of such Data Security Incident.

**6. SUB-PROCESSORS**

6.1. [Company Name] hereby grants general written authorization to Vendor to appoint Sub-Processors to perform specific Processing activities on its behalf. A list of Sub-Processors currently engaged by Vendor in connection with the Services (as may be updated by Vendor from time to time in accordance with this DPA) is set forth in Exhibit C hereto.

6.2. Vendor will notify [Company Name], no less than thirty (30) days prior to the use of the change in Sub-processor, of any intended changes concerning the addition or replacement of its Sub-Processors. [Company Name] will have an opportunity to reasonable object to such changes within fourteen (14) days after being notified. If [Company Name] objects, Vendor will use reasonable efforts to find an alternative Sub-Processor to perform the specific Processing activities. If a suitable alternative Sub-Processor or other solution cannot be found, then [Company Name] may terminate the relevant part of the Agreement to which the Sub-Processors services relate.

6.3. Vendor warrants that any Sub-processor engaged by Vendor to Process Personal Data under this Agreement has:

6.3.1. provided appropriate safeguards and maintains adequate level of protection in relation to the processing and transfer of Personal Data;

6.3.2. entered into a written agreement with Vendor, which encompasses substantially similar terms to this Agreement, particularly containing the same data protection obligations as set out in this Agreement, and will provide a copy of such agreement to [Company Name] upon request; and

6.3.3. established the appropriate mechanisms to ensure any Data Subject has enforceable rights and effective legal remedies.

6.4. Vendor acknowledges that as a Processor, it is liable to [Company Name] for Vendor’s Sub-processor’s compliance with its data protection obligations as they may apply to processing of Personal Data Processed under this Agreement.

**7. INTERNATIONAL DATA TRANSFERS**

7.1. **General**. The parties agree that in the event a jurisdiction does not currently have Data Protection Legislation that contemplates data transfers outside of the country, such transfers will be subject to the standards and expectations imposed by the General Data Protection Act (Regulation (EU) 2016/679) and there by subject to the EU Standard Contractual Clauses (“**EU SCCs**”), including transfers between Vendor and its Sub-processors. By signing this DPA, [Company Name] hereby authorizes Vendor to enter into the EU SCCs for and on [Company Name]’s behalf (as exporter) with Vendor’s own affiliates and Sub-Processors, in order to ensure an adequate level of protection to Personal Data as required by Data Protection Legislation. In case of any conflict between this DPA and such EU Standard Contractual Clauses, the EU Standard Contractual Clauses shall prevail to the extent necessary to comply with Data Protection Legislation.

7.2. **Processing in and Data Transfers to Sanctioned Jurisdictions**. In connection with the performance of this DPA and the Agreement, [Company Name] authorizes Vendor to Process and transfer Personal Data from Vendor’s jurisdiction, if necessary, to any jurisdiction in which Vendor or its sub-processors are located, so long as those receiving jurisdictions are not currently sanctioned by the Office of Foreign Assets Control (OFAC) or similar country sanction lists by Canada, United Kingdom, or Australia, and any other country that is recognized by the European Commission as providing an adequate level of protection for Personal Data.

7.3. **Data Transfers from the European Economic Area Subject to the EU Standard Contractual Clauses.** Where the transfer of Personal Data is made subject to the General Data Protection Regulation (Regulation (EU) 2016/679) and there by subject to the EU SCCs, the “data importer” thereunder shall be either the Processor or its Sub-processor, as the case may be and as determined by Processor, and the “data exporter” shall be the Controller of such Personal Data. The Processor shall ensure that the relevant Sub-processor shall (where applicable) comply with the data importer’s obligations, and the Controller shall comply with the data exporter obligations, in each case under the applicable SCCs.

7.3.1. Vendor will be a Processor of Personal Data;

7.3.2. [Company Name] will be a Controller of Personal Data;

7.3.3. Module 2 (Controller to Processor) shall apply;

7.3.4. Clause 7 (Docking Clause) does not apply;

7.3.5. The parties choose Option 2 of Clause 9 and the Vendor shall inform [Company Name] of any sub-processors at least thirty (30) days in advance;.

7.3.6. The option in Clause 11(a) (Redress) does not apply;

7.3.7. The parties choose Option 1 of Clause 17, the law of Ireland shall apply; and

7.3.8. For purposes of the Standard Contractual Clauses, ***Exhibits A*** of this DPA shall serve as Annex I, ***Exhibit B*** shall serve as Annex II, and ***Exhibit C*** shall serve as Annex III

7.4. **Data Transfers from and to countries that offer adequate level of data protections.** Personal Information may be transferred from EU Member States and the EEA member countries (Norway, Liechtenstein, and Iceland) (collectively, “**EEA**”) to countries that offer an adequate level of data protection (including Canada) under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA or the European Commission (“**Adequacy Decisions**”), as relevant and applicable, without any further safeguard being necessary.

7.5. **Data Transfers from Switzerland**. To the extent that the Swiss Supervisory Authority considers the SCCs to provide appropriate safeguards for the purposes of transferring Personal Information and the data of legal entities, the following amendments shall apply in relation to Swiss transfers: (i) the Parties adopt the GDPR standard for all data transfers; (ii) in relation to Clause 13a, the EU Supervisory Authority shall be competent insofar as the data transfer is governed by the GDPR and the Swiss Supervisory Authority (FDPIC) shall conduct parallel supervision as applicable; and (iii) in relation to Clause 18 c, the term ’member state’ shall be interpreted in such a way as to allow data subjects in Switzerland with the possibility of suing for their rights in their place of habitual residence (Switzerland).

7.6. **Data Transfers from the United Kingdom**. To the extent that the UK Supervisory Authority (the Information Commissioner) considers the SCCs to provide appropriate safeguards for the purposes of transferring Personal Information to a third country or an international organisation in reliance on Articles 46 of the UK GDPR and, with respect to data transfers from controllers to processors and/or processors to processors, the following amendments shall apply in relation to UK transfers:

7.6.1. The details of the transfers(s) and in particular the categories of Personal Information that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.

7.6.2. References to “Regulation (EU) 2016/679” or “that Regulation” are replaced by “UK Data Protection Laws” and references to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws. In particular:

7.6.2.1. References to Regulation (EU) 2018/1725 are removed;

7.6.2.2. References to the “Union”, “EU” and “EU Member State” are all replaced with the “UK”;

7.6.2.3. Clause 13(a) is not used and the “competent supervisory authority” is the Information Commissioner;

7.6.2.4. Clause 17 is replaced to state “These SCCs are governed by the laws of England and Wales”;

7.6.2.5. Clause 18 is replaced to state: “Any dispute arising from these SCCs shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

7.6.2.6. The footnotes to the SCCs do not apply to UK transfers.

7.6.2.7. Vendor will be a Processor of Personal Data;

7.6.2.8. [Company Name] will be a Controller of Personal Data;

7.6.2.9. Module 2 (Controller to Processor) shall apply;

7.6.2.10.Clause 7 (Docking Clause) does not apply;

7.6.2.11.The parties choose Option 2 of Clause 9.

7.6.2.12.The option in Clause 11(a) (Redress) does not apply;

7.6.2.13.The parties choose Option 1 of Clause 17, the law of England and Wales shall apply; and

7.6.2.14.For purposes of the UK Addendum, ***Exhibits A*** of this DPA shall serve as Annex I, ***Exhibit B*** shall serve as Annex II, and ***Exhibit C*** shall serve as Annex III

7.7. **Data Transfer from the EEA, UK, or Switzerland to the United States**. Data transfer from the EEA, UK or Switzerland may be deemed adequate when done so under the EU-U.S. Data Privacy Framework or Swiss-U.S. Data Privacy Framework. These frameworks between the United States Department of Commerce, European Commission, UK government, and Swiss Federal Administration solely apply to commercial entities who are actively registered with the U.S. Department of Commerce’s Data Privacy Framework Program, to allow Personal Data to be transferred from the European Union under the European Commission’s adequacy decision. Vendor understands and agrees, that in [Company Name]’s sole discretion, [Company Name] may require Vendor to execute the applicable SCCs in addition to the Vendor’s active status under the aforementioned frameworks.

7.8. **Data Transfer from the Canadian Province of Quebec**. Where the transfer of Personal Data relating to a resident of the Canadian Province of Quebec and thereby made subject to Quebec Law 25, shall conduct a transfer impact assessment in accordance with Law 25 to determine that such transfer to

its Sub-processor, shall have and maintain adequate levels of protection based on the nature and type of the Personal Data, including but not limited to those standards and expectations set forth in this Agreement.

**8. DATA LOCALIZATION**

8.1. **Data Processing Locations.** U.S. Users: Data from users located in the United States is processed and stored on servers located within the United States. This ensures compliance with U.S. data protection regulations and improves data access performance for our U.S. customers.

U.K. and EU Users: Data from users located in the United Kingdom and European Union is processed and stored on servers located within the United Kingdom or European Union, as required by the General Data Protection Regulation (GDPR).

8.2. **Cross-Border Data Transfers.** While we strive to process user data within the regions specified above, there may be instances where data is transferred across borders for operational or compliance reasons. When this occurs, we implement robust security measures to ensure data is protected, including:

Standard Contractual Clauses (SCCs): For data transfers from the U.K. or EU to the U.S. or other non-EU countries, we utilize SCCs to ensure that data transfers comply with GDPR requirements.

Adequate Safeguards: For any other cross-border data transfers, we ensure that adequate legal safeguards are in place to protect the data in accordance with applicable data protection laws.

8.3. **Data Subject Rights.** Users retain the right to request information about where their data is processed, to request the transfer of their data to a different region, or to request that their data be deleted in accordance with applicable laws, including GDPR and CCPA.

**9. RIGHT TO AUDIT OF THE VENDOR AGREEMENT**

9.1. Upon the expiration or earlier termination of the Agreement, Vendor will delete or return, at [Company Name]’s election, all Personal Data in the possession or control of Vendor and Vendor’s Sub-processors, unless the continued retention of such Personal Data is required by applicable law.

9.2. Without limitation to the generality of the foregoing, Vendor and Vendor’s Sub-processors shall, within five (5) business days of an applicable request from [Company Name] , or as a result of a suspension of transfer of Personal Data, provide a copy of the Personal Data in a portable and readily useable format, and thereafter upon receipt of confirmation from [Company Name] as having received a reliable copy of the Personal Data, delete or destroy all copies of Personal Data as directed by [Company Name]..

**10. DELETION OR RETURN OF PERSONAL DATA**

10.1. In accordance with and addition to Section 9. Right to Audit of the Vendor Agreement, Vendor agrees to reasonably cooperate with [Company Name] to provide [Company Name] with such information that is reasonably necessary to enable [Company Name] to demonstrate compliance with the obligations set forth in this DPA and allow for and contribute to audits, including inspections, conducted by [Company Name] or a qualified independent third-party assessor who is reasonably acceptable to Vendor and bound by confidentiality obligations satisfactory to Vendor, to the extent that such information is within Vendor’s control and Vendor is not precluded from disclosing it by applicable law, a duty of confidentiality, a legal privilege or protection, or any other obligation owed to a third party. Audits and inspections shall be conducted no more than once per year, during the term of the Agreement, during regular business hours, unless such audit is (i) in relation to or resulting from a Data Security Incident, or (ii) as a result of a prior failed audit and limited to the audit of the implemented remediation measures.

10.2. Vendor agrees to, taking into account the nature of the processing and the information available to Vendor, reasonably assist [Company Name] in meeting its obligations described in applicable Data Protection Legislation to keep Personal Data secure by maintaining reasonable security standards as set forth in this DPA; reasonably assist [Company Name] in notifying the applicable regulatory or supervisory authority, including the International Commissioner’s Office (“**ICO**”), of Personal Data breaches; reasonably assist in notifying Data Subjects of Personal Data breaches; reasonably assist [Company Name] in carrying out data protection impact assessments (DPIAs) when required, and at [Company Name]’s expense reasonably consult ICO where a DPIA indicates there is a high risk that cannot be mitigated.

**11. NOTICE**

11.1. Notice relating to **Data Security Incidents** must be sent to the following:

To: <>

CC: <>

11.2. Notice relating to **Data Subject Rights Requests** and **Sub-Processor** updates must be sent to the following:

To: <>

11.3. Notices relating to **Government Agencies** or **Regulatory Bodies Disclosure Requests**: To:<>

CC:<>

11.4. All other notices relating to this **Data Processing Addendum** must be sent to the following: To: <>

CC: <>

This DPA and the Agreement are [Company Name]’s complete and final documented instructions at the time of signature of the Agreement to Vendor for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately inwriting.

*[Signature page follows]*

**IN WITNESS WHEREOF**, the parties have caused this DPA to be executed by their respective duly authorized representative as of the Agreement Effective Date.

**EXHIBIT A – APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES**

| **Data Exporter**: [Company Name]  **Address**:  **Contact Person**:  **Activities**: Transferring and accessing the data and any other activities related to the provision of the Services described underthe service agreement with the Controller  **Role**: Processor |
| --- |
| **Data Importer**: Vendor  **Address**: As specified in the Agreement.  **Contact Person**: As specified in the Agreement.  **Activities:** Processing to provide the Services to [Company Name] , as described in the Agreement, including the DPA and its appendices. **Role**: Processor |
| **Data Subjects**  The Personal Data transferred concerning the following categories of data subjects: personal information of employees andother personnel of [Company Name] and its affiliates. |
| **Categories of Data**  The personal data transferred concern the following categories of data:  Client data: business related contact details (email, phone, email address, names, job titles, business address.  Consumer data: Email addresses, names, contact details, job titles, residential or business address; personal;; gender;professional telephone number (including mobile telephone number) and fax number; personal email address; personaltelephone number (including mobile telephone number); IP address; cookie data; login credentials (username and password);traffic data; images and sounds |
| **Special categories of data (if appropriate)**  The personal data transferred concern the following special categories of data (please specify): |
| **Nature of the processing**  Depending on the nature and scope of the Services, collection, storage, use, dissemination (towards Sub-processors in line with the Agreement and this DPA), erasure of Personal Data. |
| **Purpose for which the Personal Data is Processed**  Personal Data that may be collected and used during the provisioning and use of the Services to deliver, support and improve theServices, administer the Agreement and further the business relationship between [Company Name] and Vendor, comply with law, act in accordance with [Company Name]’s written instructions, or otherwise in accordance with this Agreement.  [Company Name] personnel names and contact information may be received in connection with technical support of the Services. |

| **Duration of the Processing.**  Personal Data will be Processed for the duration of the Agreement. |
| --- |
| **COMPETENT SUPERVISORY AUTHORITY**  Where Vendor Processes Personal Data originating from the EEA, the competent supervisory authority shall be determined in accordance with Clause 13 of the Standard Contractual Clauses.  Where Vendor Processes Personal Data originating from the UK, the competent supervisory authority shall be the UK Information Commissioner's Office. |

**EXHIBIT B – APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES/ONWARD DATA TRANSFER AGREEMENT**

[Vendor to supply their data security measures. Example reqs below.]

| [Ex. Soc2]  The Technical and Organizational Measures  Implemented by the Data Importer |
| --- |
| [Ex. AES 256]  Measures of Pseudonymization and Encryption of  Personal Data |
| Measures For Ensuring Ongoing Confidentiality,  Integrity, Availability and Resilience of Processing  Systems and Services |
| Measures For Ensuring the Ability to Restore the  Availability and Access to Personal Data in a Timely  Manner in the Event of a Physical or Technical  Incident  Processes for Regularly Testing, Assessing and  Evaluating the Effectiveness of Technical and  Organizational Measures in Order to Ensure the  Security of the Processing |
| Measures for User Identification and Authorization  Measures for the Protection of Data During  Transmission  Measures for the Protection of Data During Storage |
| Measures for Ensuring Physical Security of Locations  at which Personal Data is Processed |
| Measures for Ensuring Events Logging |
| Measures for Ensuring System Configuration,  Including Default Configuration |

| Measures for Internal IT and IT Security Governance  and Management |
| --- |
| Measures for Certification/assurance of Processes  and Products |
| Measures for Ensuring Data Minimization |
| Measures for Ensuring Data Quality |
| Measures for Ensuring Limited Data Retention |

Measures for Ensuring Accountability

Measures for Allowing Data Portability and Ensuring

Erasure

**EXHIBIT C - VENDOR’S SUB-PROCESSOR LIST**