Data Processing Addendum

Last Updated August 23, 2023

You can see your previous Data Processing Addendum here.

This Data Processing Addendum, including any Schedules (collectively, the "**DPA**") forms part of the Rev.com Terms of Service and the Rev.com Master Services Agreement (as applicable to the type of Services Customer has purchased) (the "**Agreement**") by and between the entity registering an account on Rev to obtain transcription, video caption, translation, and other related document services ("**Customer**") and Rev.com, Inc. ("**Rev**"). Except to the extent otherwise expressly set forth in this DPA, this DPA is governed by the terms and conditions of the Agreement. Any defined terms not otherwise defined herein shall have the meanings set forth in the Agreement. In the event of any inconsistency or conflict between this DPA and the Agreement, the DPA applies.

1. **Definitions**. For the purposes of this DPA, the following definitions apply:
    a. "**Affiliate**" means an entity that controls, is controlled by or is under common control with the applicable party. For purposes of this definition, "control" means ownership of more than fifty (50%) percent of the voting stock or other ownership interest in an entity.
    b. "**Applicable Law**" means all applicable laws (including those arising under common law), statutes, cases, ordinances, constitutions, regulations, treaties, rules, codes, ordinances and other pronouncements having the effect of law of the United States, any foreign country or any domestic or foreign state, county, city or other political subdivision, including those promulgated, interpreted or enforced by any governmental authority. References to "Applicable Law" mean Applicable Law as may be amended or supplemented.
    c. "**European Privacy Laws**" means (i) Regulation (EU) 2016/679 of the European Parliament and of the Council 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) ("**GDPR**"); (ii) the Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; (iii) applicable national implementations of (i) and (ii); (iv) Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance; and (v) in respect of the United Kingdom the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) and any applicable national legislation that replaces or converts in domestic law the GDPR including the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419) ("**UK GDPR**") or any other law relating to data and privacy as a consequence of the UK leaving the European Union (in each case, as may be amended, superseded or replaced).

d. "**EU SCCs**" means the standard contractual clauses for the transfer of personal data to third countries pursuant to GDPR as approved by the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021, as completed, amended, superseded or replaced from time to time in accordance with this DPA and incorporated herein by reference.
e. "**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
f. "**Personal Data Breach**" means any accidental, unlawful or unauthorized access, acquisition, use, modification, disclosure, loss, destruction of or damage to Personal Data or any other unauthorized Processing of Personal Data.
g. "**Privacy Laws**" means all Applicable Laws relating to the privacy, confidentiality, retention or security of Personal Data including, but

not limited to, U.S. State Privacy Laws and/or European Privacy Laws together with any additional implementation, rules, or regulations issued by applicable regulatory bodies.

h. "**Process**" or "**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, alteration, use, access, disclosure, copying, transfer, storage, deletion, alignment or combination, restriction, adaptation, retrieval, consultation, destruction, disposal, or other use of Personal Data.

i. "**Services**" means the services Rev is obligated to provide pursuant to the Agreement.

j. **"Standard Contractual Clauses**" or "**SCCs**" means the EU SCCs and/or the UK SCCs dependent upon the location of the Data Subject (as defined under the GDPR) whose Personal Data is Processed.

k. "**Subprocessor**" means a processor of a Processor.

l. "**Transfer**" means the access by, transfer or delivery to, or disclosure to a person, entity or system of Personal Data where such person, entity or system is located in a country or jurisdiction other than the country or jurisdiction from which the Personal Data originated.

m. "**UK SCCs**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (available as of the Last Updated date of this DPA at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/), completed as set forth in this DPA and as amended, superseded or replaced from time to time in accordance with this DPA, and incorporated herein by reference.

n. "**U.S. Privacy Laws**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, including its regulations and the amendments made by the California Privacy Rights Act of 2020 ("**CCPA**") and any privacy laws passed by other U.S. states, to the extent applicable to Rev's Processing of Personal Data under the Agreement.

o. The terms "**Controller**" (which includes "**Business**" as defined in the CCPA), "**Data Subject**" (which includes "**Consumer**" as defined in U.S. Privacy Laws), "**Processor**" (which includes "**Service Provider**" as defined in the CCPA) are defined as in Privacy Laws.

2. **Scope**. This DPA applies to Rev if Rev Processes any Personal Data as part of or in connection with Rev's performance of the Services for Customer or any of its Affiliates. The scope, classification, purposes and details of the Processing, including its duration and the categories of Data Subjects and Personal Data being Processed, are described in Schedule 1 (Processing Description). Rev will Process the Personal Data at all times in compliance with Privacy Laws.
3. **Roles of Parties.**
    a. To the extent that Customer is the Controller, Rev is its Processor. To the extent that Customer is a Processor of the Personal Data, Rev is its Subprocessor. Each party is responsible for its own compliance with Privacy Laws. Where Customer is a Controller, it warrants and represents that it has taken all legally required measures in order for Rev to receive and Process the Personal Data in compliance with Privacy Laws (including but not limited to, where applicable, providing any required notices and obtaining any required consents). As a Controller, Customer shall not instruct Rev to Process Personal Data in violation of Applicable Law.
    b. Rev hereby certifies that it understands the restrictions and obligations set forth in this DPA and that it will comply with them.
4. **Limitations on Use**.
    a. *Processing in Accordance with Customer's Instructions*. Rev will Process Personal Data on behalf of Customer solely to fulfill its obligations to Customer under the Agreement and this DPA and in compliance with Privacy Laws. Rev shall not: (i) "sell" or "share" any Personal Data, as such terms are defined in U.S. Privacy Laws; (ii) retain, use, or disclose Personal Data outside of the direct business relationship between Rev and Customer; or (iii) otherwise engage in any Processing of the Personal Data that is prohibited for a Processor under Privacy Laws. Rev shall comply with any applicable restrictions under Privacy Laws

on combining Personal Data with personal data that Rev receives from, or on behalf of, another person or persons, or that Rev collects from any interaction between it and any individual.

b. *Conflict with Customer's Instructions*. Rev shall Process Personal Data only in accordance with Customer's instructions, including this DPA. If Applicable Law requires Rev to conduct Processing that is inconsistent with Customer's instructions, then Rev shall notify Customer, unless Applicable Law prohibits such notice. If Rev believes that any instruction from Customer violates or would cause Rev to violate Applicable Law and/or if Rev is unable to comply with the terms of this DPA for any reason, Rev shall notify Customer and cooperate with Customer to reach a reasonable resolution.

c. *Customer's Right of Remediation.* Customer retains the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data, including any use of Personal Data not authorized in this DPA.

5. **Limitations on Disclosure**. Rev will not disclose Personal Data to any third party without first obtaining Customer's written consent, except as provided in Section 6 (Subprocessing), Section 7 (Cooperation to Facilitate Individual Rights Requests) or Section 11 (Cross-Border Transfers). Rev will ensure that all persons it authorizes to Process the Personal Data are adequately trained to Process the Personal Data in compliance with the requirements of this DPA.

6. **Subprocessing**. Rev may subcontract Processing of Personal Data to a Subprocessor only in compliance with this DPA and Applicable Law and any additional conditions for subcontracting set forth in the Agreement. Prior to a Subprocessor's Processing of Personal Data, Rev will impose contractual obligations on any such Subprocessor that are substantially the same and are no less protective of Personal Data as those imposed on Rev under this DPA. Customer agrees that Rev may engage the Subprocessors identified in Schedule 3, and acknowledges that Rev keeps an up-to-date copy of all Subprocessors available upon request to legal@rev.com. Rev remains responsible for its Subprocessors and liable for their compliance with this DPA. This paragraph constitutes Customer's general authorisation to both

Rev's use of the Subprocessors and its sub-processing under the SCCs, as applicable. On at least 30 days' notice to Customer, Rev may engage new Subprocessors subject to requirements of Privacy Laws. If Customer objects to the engagement of any Subprocessor on reasonable grounds relating to the protection of Personal Data, then either (i) Rev will not engage or permit the Subprocessor to process the Personal Data; or (ii) Customer may elect to suspend or terminate the Processing of Personal Data under the Agreement and/or terminate the Agreement without further liability or obligation to Rev. If Customer elects to suspend or terminate the Processing of Personal Data under the Agreement and/or terminate the Agreement as permitted by this Section 6, Customer shall be entitled only to a refund of payments made by Customer to Rev for Services not delivered due to the objection to the engagement of any Subprocessor on reasonable grounds.

7. **Cooperation to Facilitate Individual Rights Requests**. Rev shall, to the extent legally permitted, promptly notify Customer if Rev receives a request from a Data Subject or consumer to exercise the Data Subject's or consumer's rights under Privacy Laws ("**Individual Rights Request**"). To the extent that Customer is unable to fulfill an Individual Rights Request on its own using the features made available to it by Rev, Rev will, upon Customer's written request, render reasonable assistance to Customer in the fulfillment of Customer's obligation to respond to an Individual Rights Request.
8. **Security**. Rev shall maintain (and require its Subprocessors to maintain) reasonable and appropriate technical and organizational measures for the protection of the security, confidentiality, and integrity of Personal Data (including protection against Personal Data Breach). The minimum technical and organizational measures to be implemented by Rev are set forth in Schedule 2 and any changes are part of continuous improvements to the security of Processing. Rev shall ensure that persons authorized to carry out Processing have committed themselves to confidentiality or are under the appropriate statutory obligation of confidentiality.
9. **Personal Data Breach Notification**. Rev shall notify Customer as required under Applicable Law without undue delay where Rev discovers a Personal Data Breach. After providing notice, Rev will investigate the Personal Data

Breach and take all necessary steps to eliminate or contain the exposure of Personal Data.

10. **Data Protection Impact Assessment**. Upon Customer's written request, Rev shall provide Customer with reasonable assistance to fulfill Customer's obligations under the Applicable Law to carry out a data protection impact assessment related to Customer's use of the Services. Rev shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority (as defined under the European Privacy Laws) in the performance of its tasks relating the data protection impact assessment, and to the extent required by Privacy Laws.
11. **Cross-Border Transfers**.
    a. *Standard Contractual Clauses*. Where Rev Processes Personal Data of a European or UK Data Subject in any country, territory or recipient not recognized under the applicable European Privacy Laws as providing an adequate level of protection for the Personal Data, Rev agrees to abide by and comply with the SCCs applicable to the jurisdiction of the Processing which shall be incorporated in full and form an integral part of this DPA.
        i. To the extent that the EU SCCs apply: (i) if Customer is a Controller, both parties shall comply with the Module Two: Controller to Processor Transfers; and (ii) if Customer is a Processor, both parties shall comply with the Module Three: Processor to Processor Transfers. The EU SCCs shall be deemed completed as follows:
            i. Clause 7 (the optional docking clause) is included.
            ii. Under Clause 9 (Use of sub-processors), the parties select Option 2 (General written authorization).
            iii. Under Clause 11 (Redress), the optional requirement that data subjects be permitted to lodge a complaint with an independent dispute resolution body does not apply.
            iv. Under Clause 17 (Governing law), the parties choose Option 1 (the law of an EU Member State that allows for third-party beneficiary rights). The parties select the law of Ireland.

v. Under Clause 18 (Choice of forum and jurisdiction), the parties select the courts of Ireland.
vi. Annexes I-III of the EU SCCs are set forth in Schedules 1-3 of the DPA.
vii. By entering into this DPA, the parties are deemed to be signing the EU SCCs and its applicable annexes.

ii. With respect to Personal Data transferred from Switzerland for which Swiss law (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, references to the GDPR in Clause 4 of the EU SCCs are, to the extent legally required, amended to refer to the Swiss Federal Data Protection Act or its successor ("**FDPA**"), and the concept of supervisory authority shall include the Swiss Federal Data Protection and Information Commissioner. The EU SCCs are deemed to be edited in all other ways necessary to accommodate the application of the FDPA.

iii. With respect to Personal Data transferred from the United Kingdom for which United Kingdom law (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, the UK SCCs form part of this DPA, unless the United Kingdom issues updates to the UK SCCs that, upon notice from Customer, will control. Undefined capitalized terms used in this Section 11(a)(iii) shall mean the definitions in the UK SCCs. For purposes of the UK SCCs, they shall be deemed completed as follows:
    i. Table 1 of the UK SCCs: (1) the Parties' details shall be the parties and their affiliates to the extent any of them is involved in such transfer, including those set forth in Schedule 1; (2) the Key Contact shall be the contacts set forth in Schedule 1;
    ii. Table 2 of the UK SCCs: The Approved EU SCCs referenced in Table 2 shall be the EU SCCs as executed by the parties.
    iii. Table 3 of the UK SCCs: Annex 1A, 1B, II, and III shall be set forth in Schedules 1-3.

iv. Table 4 of the UK SCCs: Either Party may end this DPA as set out in Section 19 of the UK SCCs.
v. By entering into this DPA, the Parties are deemed to be signing the UK SCCs and its applicable Tables and Appendix Information.

iv. Both parties shall take all other actions required to legitimize the Transfer. Rev shall also use reasonable endeavors to procure that any Subprocessors that Process Personal Data transferred under the SCCs enter into the applicable SCCs with Rev. The parties agree that: (1) purely for the purposes of the descriptions in the SCCs, Rev shall be deemed the "data importer" and Customer shall be deemed the "data exporter"; and (2) if and to the extent the SCCs conflict with any provision of the Agreement (including this DPA) the SCCs shall prevail to the extent of such conflict. The parties also agree that if European Privacy Laws require further supplemental measures to be put in place in addition to those set out herein, they shall work together in good faith pursuant to Section 16.

b. *Government Access to Personal Data*. To the extent permitted by Applicable Law, Rev shall take all reasonable actions to prevent disclosure of Personal Data to government authorities and/or in response to a legal demand such as subpoena or similar demand, without Customer's prior express written consent. If and only to the extent that is not legally possible for Rev to comply with this Section 11(b), Rev will notify Customer in advance of any disclosure and provide Customer with the opportunity to object, unless otherwise prohibited by Applicable Law.
c. *Notification Obligations*. Rev shall promptly notify Customer if it makes a determination that it can no longer meet its obligations under this Section 11, and in the event of any such non-compliance, or in the event that a data protection authority and/or Privacy Laws no longer permit the lawful Transfer of Personal Data to Rev pursuant to the terms of this DPA and/or require that the parties adopt an alternative Transfer solution, then without prejudice to any other right or remedy

available to Customer, Rev shall: (i) without undue delay, cease (and require that all its Subprocessors cease) Processing Personal Data if Customer determines in its sole discretion that Rev has not or cannot correct such non-compliance within a reasonable timeframe; and/or (ii) work with Customer and promptly take all reasonable and appropriate steps Customer may deem necessary to ensure such Processing or Transfer is in compliance with Privacy Laws.

d. *Geographic Region*. For certain Rev Services, Customer may select the geographic region in which Personal Data is housed from those available for the Services. Where Customer selects an available geographic region, Rev shall not move the Personal Data without Customer's prior written consent or unless required to comply with Applicable Law. For clarity, Rev may access the Personal Data from other geographic locations, including the United States, where necessary to provide Customer-requested support.

12. **Audit Rights**. Unless otherwise required by Applicable Law, Rev will allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer of its operations and systems, as follows:
    a. If the requested audit scope is addressed in an ISO or similar audit report issued by a third party auditor within the prior twelve (12) months and Rev provides such report to Customer confirming there are no known material changes in the controls audited, Customer agrees to accept the findings presented in the third party audit report in lieu of requesting an audit of the same controls covered by the report.
    b. In the event an audit report is not provided, any audit, whether by Customer or a third party, must be limited to no more than once per twelve (12) month period, and Customer will (i) conduct the audit only on an agreed date during normal business hours (9:00 am – 5:00 pm local time); (ii) limit its audit to only one business day; and (iii) pay Rev's then-current audit fee.
    c. If a third party is to conduct the audit, Customer will provide at least thirty (30) days' advance notice. The third-party auditor must be

reasonably agreed to by the parties (without prejudice to any governmental authority's audit power). Rev will not unreasonably withhold its consent to a third-party auditor requested by Customer, unless such third-party auditor is a competitor or another customer of Rev's. Any third-party auditor must execute a written confidentiality agreement acceptable to Rev.

d. Customer must promptly provide Rev with the results of any audit, including any third-party audit report. All such results and reports, and any other information obtained during the audit (other than Customer's Personal Data) are confidential information of Rev. Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the terms of this DPA.
e. Nothing herein will require Rev to disclose or make available: (i) any data of any other customer of Rev; (ii) Rev's internal accounting or financial information; (iii) any trade secret of Rev; (iv) any information that, in Rev's reasonable opinion, could (1) compromise the security of Rev systems or premises; or (2) cause Rev to breach its obligations under Applicable Law or its security and/or privacy obligations to Customer or any third party; or (v) any information sought for any reason other than the good faith fulfillment of Customer's obligations under the SCCs or Privacy Laws.

13. **Education Records Subject to FERPA**. This Section 13 applies where Customer represents that it is subject to the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g and its implementing regulations) ("FERPA"). Rev is acting as a data processor in providing the Services to Customer.
    a. Certain information that may be provided to Rev by Customer or its student users may be considered an education record as defined under the FERPA regulation 34 CFR § 99.3 ("Education Record"). In such case, the parties agree that Rev is acting as a "school official" with "legitimate educational interests" in such Education Records under FERPA, or if applicable, is acting under another applicable FERPA exception in 34 C.F.R. § 99.31(a)(1), such as the "directory information" exception. Customer acknowledges and agrees that Rev may process

such information for the purpose of providing the Services and related functions, including as described in this DPA and the Agreement. Both parties agree to protect personally identifiable information from Education Records in accordance with FERPA. To the extent permitted by Applicable Law, nothing contained herein shall be construed as precluding either party from releasing such information to the other or to service providers so that each can perform its respective responsibilities. Customer represents and warrants that it is authorized to process such information, including any Education Records contained therein, and make such information available to Rev as set out in the Agreement or this DPA.

b. The limitations set forth in Section 13(a) shall not apply to information which Rev receives independent of the Agreement with Customer or pursuant to consent of a student user's parent or guardian or a student user who is at least 18 years of age or the age of majority in such user's jurisdiction of residence.

14. **Return and Destruction**. Rev shall destroy all Personal Data at Customer's written request, except to the extent Applicable Law requires storage of the Personal Data. Additionally, Rev can support the earlier return or deletion of Personal Data upon request of Customer and at its reasonable cost. Please contact legal@rev.com for further information regarding its data retention policy regarding files created for security, back-up and business continuity purpose.
15. **Survival**. The obligations placed upon the Rev under this DPA (including, to the extent applicable, the SCCs) shall survive so long as Rev and/or its Subprocessors processes Personal Data on behalf of Customer.
16. **Modifications**. If Privacy Laws require modifications to this DPA, Customer and Rev agree to negotiate such changes in good faith as necessary to comply with Privacy Laws.

Schedule 1

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name: The Customer who is a party to the Agreement.

Address: As set out in the Agreement

Contact person's name, position and contact details: As set out in the Agreement.

Activities relevant to the data transferred under these Clauses: Data importer will process the data in order to provide the Services pursuant to the Agreement.

Role: Controller

Data importer(s):

1. Name: Rev.com, Inc.

Address: 1717 W 6th St, Suite 310. Austin, TX 78703

Contact person's name, position and contact details: General Counsel, legal@rev.com

Activities relevant to the data transferred under these Clauses: Data importer will process the data in order to provide the Services pursuant to the Agreement.

Role: Processor

B. DESCRIPTION OF TRANSFER

The categories of data subjects whose personal data is transferred:

The categories of Data Subjects about whom Rev processes Personal Data are determined and controlled by Customer, in its sole discretion, which may include, but are not limited to, the following. Each category includes current, past and prospective members of the category. Where any of the following is a business or organization, it includes their staff.

- employees including volunteers, agents, temporary and casual workers
- customers and clients (including their employees, volunteers, agents, temporary and casual workers)
- suppliers (including their employees, volunteers, agents, temporary and casual workers)
- social media members or supporters
- shareholders
- relatives, guardians and associates of the data subject
- complainants, correspondents and enquirers
- experts and witnesses
- advisers, consultants and other professional experts
- students, pupils, and university staff and officials

Categories of personal data transferred:

Customer may submit Personal Data in audio or video files to the Services. Customer controls the types of Personal Data submitted, which may include, but is not limited to Personal Data relating to the following categories of data:

- Personal details, including any information that identifies the data subject and their personal characteristics.
- Family, lifestyle and social circumstances.
- Education and training details.
- Employment details.
- Goods or services provided and related information, including details of the goods or services supplied, licenses issued, and contracts.

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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

None

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

Ad-hoc or regular transfers for the duration of the Agreement.

Nature of the Processing:

The Personal Data Processed shall be subject to the following basic Processing activities:

- Receiving audio and video files and other data, including, collection, accessing, retrieval, recording, and data entry
- Holding data, including storage, organization and structuring
- Using data, including analyzing, consultation, testing, automated decision making and profiling
- Updating data, including correcting, adaptation, alteration, alignment and combination
- Protecting data, including restricting, encrypting, and security testing
- Sharing data, including disclosure, dissemination, allowing access or otherwise making available
- Returning data to the data exporter or data subject
- Erasing data, including destruction and deletion

Purpose(s) of the data transfer and further processing:

To provide the Services pursuant to the Agreement.

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

For the duration of the Agreement and for such time thereafter as is required for Rev to return and/or delete the Personal Data in accordance with the Agreement, except where otherwise required by Applicable Law.

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

Subprocessors described in Schedule 3 to the DPA. Ancillary service providers supporting the Data Importer in its provision of the Services.

Third countries or international organizations to which the personal data will be transferred, if applicable:

Transfer to and from the U.S. from the originating jurisdiction of the data exporter.

C. COMPETENT SUPERVISORY AUTHORITY

To the extent legally permissible, the Competent Supervisory Authority shall be the Irish Data Protection Commission.

Schedule 2

ANNEX II – TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Rev has implemented and shall maintain commercially reasonable and appropriate technical and organizational measures to protect Personal Data against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction, including the policies, and procedures and internal controls set forth in this Schedule 2.

More specifically, to the extent that Customer provides to Rev or Rev otherwise accesses Customer's Personal Data in connection with the DPA, Rev shall implement an Information Security Program that includes administrative, technical and physical safeguards to ensure the confidentiality, integrity and availability of Personal Data, protect against any reasonably anticipated threats or hazards to the confidentiality, integrity and availability of Personal Data, and protect against unauthorized access, use, disclosure, alteration or destruction of Personal Data. In particular, Rev's Information Security Program shall include, but not be limited to the following safeguards where appropriate or necessary to ensure the protection of Personal Data:

(i)Access Controls – policies, procedures and physical and technical controls designed: (i) to limit physical access to its information systems and the facility or facilities in which they are housed to properly authorized persons; (ii) to ensure that all members of its workforce who require access to Personal Data have appropriately controlled access, and to prevent those workforce members and

others who should not have access from obtaining access; (iii) to authenticate and permit access only to authorized individuals and to prevent members of its workforce, including its contractors and agents from providing Personal Data or information relating thereto to unauthorized individuals; and (iv) to encrypt Personal Data where appropriate.

(ii)Security Awareness and Training – a security awareness and training program for all members of Company's workforce which includes training on how to implement and comply with its Information Security Program.

(iii)Security Incident Procedures – policies and procedures to detect, respond to and otherwise address security incidents, including procedures to monitor systems and to detect actual and attempted attacks on or intrusions into Personal Data or information systems relating thereto, and procedures to identify and respond to suspected or known security incidents, mitigate harmful effects of security incidents, and document security incidents and their outcomes.

(iv)Contingency Planning – policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages Personal Data or systems that contain Personal Data, including a data backup plan and a disaster recovery plan.

(v)Audit Controls – hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports concerning these security requirements and compliance therewith.

(vi)Data Integrity – policies to ensure the confidentiality, integrity and availability of Personal Data and protect it from disclosure, improper alteration or destruction.

(vii)Storage and Transmission Security – technical security measures to guard against unauthorized access to Personal Data that is being transmitted over an electronic communications network, including a mechanism to encrypt electronic information whenever appropriate, such as while in transit or in storage on networks or systems to which unauthorized individuals may have access.

(ix)Assigned Security Responsibility – Rev shall designate a security official responsible for the development, implementation and maintenance of its Information Security Program. Rev shall inform Customer as to the person responsible for security.

(x)Testing – Rev shall regularly and no less than one time per year test the key controls, systems and procedures of its Information Security Program to ensure that they are properly implemented and effective in addressing the threats and risks identified. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

(xi)Business Continuity and Operational Resilience – business continuity and disaster recovery procedures that include monitoring and communication and reporting capability.

(xii)Security Incident Management – Rev utilizes its own incident response plan and breach notification policies.

(xiii)Adjust the Program – Rev shall monitor, evaluate and adjust, as appropriate, the Information Security Program in light of any relevant changes in technology or industry security standards, the sensitivity of Personal Data, internal or external threats to Rev or Personal Data, requirements of applicable work orders, and Rev's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to information systems.

Schedule 3

ANNEX III – LIST OF SUB-PROCESSORS

LIST OF SUBPROCESSORS

Customer has authorized the use of the following Subprocessors:

1. Rev's employees and individual contractors and agents may have access to Personal Data in order to provide the Services.
2. Additional Subprocessors:

a. AWS a. Country of Jurisdiction: USA b. Brief Description of Processing: cloud computing services c. Affected Products: All (human and ASR)
b. eClerx Services Limited a. Country of Jurisdiction: India b. Brief Description of Processing: Freelancer services c. Affected Products: Human services
c. Speechmatics a. Country of Jurisdiction: US/UK b. Brief Description of Processing: non-English speech-to-text subprocessor c. Affected Products: Rev.ai (for certain non-English languages only) and Rev.ai
d. Rammer Technologies Inc. a. Country of Jurisdiction: USA b. Brief Description of Processing: Natural language processing subprocessor c. Affected Products: Rev.ai (Insights – Topic extraction/sentiment)
e. Azure a. Country of Jurisdiction: USA b. Brief Description of Processing: cloud computing services c. Affected Products: All (human and ASR)