This Partner Data Processing Addendum **("Partner DPA**") to the Master Partner Agreement (this "**MPA**"), including the corresponding data sheets set forth in **Annex C** ("**Data Sheets**"), applies to the Processing of Partner Personal Data by Acoustic, on behalf of Partner or Partner's Affiliate(s), in compliance with Data Protection Laws (as defined below). This Partner DPA applies to the Processing of both Partner Personal Data and Customer Data, where Acoustic acts as a Processor of Partner Personal Data and a sub-processor of Customer Data in those cases where Acoustic has no direct contractual relationship with the Customer.

1. DEFINITIONS

1.1 Unless otherwise set out below, capitalized terms used but not defined in this Partner DPA shall have the same meaning as set forth in applicable Data Protection Laws, the MPA or the applicable Data Sheet. In this Partner DPA, unless the context requires otherwise:

"**Affiliate(s)**" means any entity that is controlled by or under common control with Partner and who is a beneficiary of the Services under the Agreement.

"**Anonymized Data**" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular individual or household.

"**ADPA**" means the Argentine Data Protection Act, Law No. 25,326 and its Implementing Decree No. 1558/2001 (amended by Decree No. 1160/10), as amended from time to time.

"**Australian Privacy Act**" means Australia's Privacy Act 1988 (Cth).

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq., and any amendments or implementing regulations thereto that are or become effective on or after the effective date of this Partner DPA.

"**Colombian General Data Protection Regime**" means the Colombian General Data Protection Regime enclosed in Colombian Law 1581 of 2012 and Decree 1074 of 2015.

"**Controller**" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Information.

"**Partner Personal Data**" means (a) any information relating to a Data Subject that Acoustic Processes as a Processor on behalf of the Partner and/or the Partner's Affiliate(s) in connection with Acoustic's provision of Services, including any Personal Information; and (b) Customer Data.

"**Data Protection Laws**" means any Law intended to protect the privacy rights of natural persons with regard to the Processing of Partner Personal Data, including the GDPR, the CCPA, the ADPA, the Australian Privacy Act, the Colombian Data Protection Regime, the Indian Privacy Laws, the PDPA and the LGPD.

"**Data Subject**" means an identified or identifiable natural person.

"**Customer**" means the end user customer named in the Quote governed by the MPA.

"**Customer Data**" means any information relating to a Data Subject that Acoustic Processes as sub-processor on behalf of the Partner and/or Partner Affiliate(s) and includes Personal Data.

"**GDPR**" means the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council and any national Law of the European Economic Area member states ("**EEA**") implementing or supplementing this regulation, in each case as amended, replaced or superseded from time to time

and all applicable Laws of the European Union or the EEA member states privacy rights with regard to the Processing of Personal Information, as well as corresponding data privacy Law in the United Kingdom.

"**LGPD**" means the Brazilian General Data Protection Law, No. 13,709/2018.

"**Indian Privacy Laws**" means the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

"**PDPA**" means the Personal Data Protection Act of Singapore.

"**Personal Information**" means any information within the scope of the definition of that term under the CCPA, any information within the scope of "personal data" as such term is defined in the GDPR, and any information within the scope of another reasonably equivalent term under another applicable Data Protection Law.

"**Processing**" means any operation or set of operations that is performed on Personal Information, or on sets of Personal Information, whether or not by automated means, and "**Process**" and "**Processes**" will be interpreted accordingly.

"**Processor**" means, as applicable, (a) the entity that Processes Personal Information on behalf of a Controller, (b) the "**data intermediary**" as such term is defined in the PDPA, and (c) the "**service provider**" as such term is defined in the CCPA.

"**Services**" means the service(s) provided by Acoustic to Partner pursuant to the Agreement.

1.2 This Partner DPA amends the Agreement with respect to any Processing of Partner Personal Data and replaces all prior agreements regarding this subject matter. In the event of conflict between the Partner DPA and the terms of the Agreement, the terms of the Partner DPA shall prevail. Additional details regarding the Processing under this Partner DPA are set forth in the relevant Data Sheet.

1.3 **Role of the Parties**. Partner and Acoustic agree that:

(a) For purposes of the GDPR and any and all other applicable Data Protection Laws, Partner and/or Partner's Affiliate(s), as applicable, is the Controller of Partner Personal Data (except Customer Data), and Acoustic is the Processor of such data, except when Partner or Partner's Affiliate(s) act as a Processor of Partner Personal Data (where the Customer is the Controller), in which case Acoustic is a sub-processor. Partner will identify and inform Acoustic of other Controllers, if any, prior to providing their Partner Personal Data in accordance with the Data Sheet.

(b) For purposes of the CCPA, Acoustic will act as a "service provider" (as defined in Cal. Civ. Code §1798.140), in its performance of its obligations under the Agreement. Acoustic will not retain, use, or disclose any "personal information" (*ibid.*) included in the Partner Personal Data for any purpose other than Acoustic's performance of its obligations under the Agreement, or as otherwise permitted by the CCPA.

1.4 If Partner Personal Data of Partner's Affiliate(s) is Processed, Partner's Affiliate(s) providing such data shall have the same rights as the Partner under this Partner DPA.

2. SPECIFICATION OF THE DATA PROCESSING

2.1 A list of categories of Data Subjects, types of Partner Personal Data, including information on special categories of Personal Information, subject matter and nature and purpose of Processing is set out in the Data Sheet corresponding with each Service. When Acoustic is providing Professional Services, Acoustic shall take reasonable measures to avoid access to Personal Information, however, the Parties understand and acknowledge that incidental access to Personal Information stored within the Partner's data processing system cannot be excluded. Unless provided for otherwise in the Agreement, the subject matter of the Processing will be in this case providing the Professional Services for the Partner.

2.2 Services are provided on the assumption that their use is limited to the categories of Data Subjects and types of Partner Personal Data, including information on special categories of Personal Information, as described in the Data Sheets. If Partner believes that certain types of Partner Personal Data or Data Subjects are not (or not sufficiently) covered by the corresponding Data Sheet, Partner shall inform Acoustic and seek Acoustic's consent before any such Processing can take place. Such consent shall not be unreasonably withheld; reasonable bases for withholding consent exist where: (a) the quality of Processing would be degraded or (b) the sensitivity of the data to be Processed would change in such a way that Acoustic would need to modify its technical or organizational security measures, for example, if such modification would be required to satisfy legal requirements related to the Processing of such data. Any use of the Services in deviation of what has been agreed to in the Data Sheets constitutes a breach of contract and is the sole responsibility of the Partner, in which case Partner shall hold harmless and indemnify Acoustic from any direct, indirect, consequential or other claims, damages, losses, liabilities and expenses (including all fees and charges of internal or external counsel with whom Acoustic may consult and all expenses of litigation and preparation therefore) that may be asserted against Acoustic by any person, entity or governmental or supervisory authority.

2.3 In addition to the subject matter, nature and purpose of the Processing as set out in the corresponding Data Sheet, the Parties agree that anonymizing the Partner Personal Data for the benefit of Acoustic is an additional subject matter of the Processing.

2.4 The duration of the Processing corresponds to the duration of the Services, unless otherwise stated in the Data Sheet.

3. INSTRUCTIONS AND COMMUNICATION BETWEEN THE PARTIES

3.1 Unless otherwise required by applicable Law, Acoustic will Process Partner Personal Data according to Partner's instructions provided in electronic or written form (referred to collectively as "in writing") or, if provided verbally, confirmed in writing. Such instructions may include transfers of Partner Personal Data to a country not providing an adequate level of protection pursuant to the applicable Data Protection Laws ("**Third Country**") or an international organization. If Acoustic is required by applicable Law to Process Partner Personal Information in a manner other than as instructed by Partner and is not prohibited by applicable Law from disclosing such legal requirement, then Acoustic will inform Partner of such legal requirement before engaging in such Processing.

3.2 The scope of Partner's instructions for the Processing of Partner Personal Data is defined by the Agreement, and, if applicable, Partner's and its authorized users' use and configuration of the Services. Partner shall notify Acoustic, in writing, of the names of the persons authorized to issue instructions to Acoustic.

3.3 If Acoustic believes an instruction violates applicable Law, Acoustic will inform Partner without undue delay, and may suspend the performance of such instruction until Partner has modified or confirmed its lawfulness in writing.

3.4 Partner may provide further legally required instructions regarding the Processing of Partner Personal Data ("**Additional Instructions**") as described in Section 11. If Acoustic notifies Partner that an Additional Instruction is not feasible, the Parties shall work together to find a reasonable alternative. If Acoustic notifies the Partner that neither the Additional Instructions nor an alternative is feasible, Partner may terminate the affected Service, in accordance with any applicable terms of the Agreement.

3.5 Partner authorizes Acoustic to anonymize the Partner Personal Data and to use the Anonymized Data for its own purposes, e.g., to improve the Services and for analytics purposes.

3.6 Partner shall serve as the single point of contact for Acoustic in regard to this Partner DPA. As other Controllers may have certain direct rights against Acoustic, Partner undertakes to exercise all such rights on their behalf and to obtain all necessary permissions from such Controllers. Acoustic shall be discharged of its obligation to inform or notify another Controller when Acoustic has provided such information or notice to Partner. Similarly, Acoustic will serve as the single point of contact for Partner with respect to its obligations as a Processor under this Partner DPA. Partner shall provide written notice to Acoustic with the name and contact information of the person designated by Partner to be responsible for dealing with questions relating to applicable Data Protection Laws and data security in the context of performing this Partner DPA.

4. ACOUSTIC'S OBLIGATIONS

4.1 Acoustic will comply with Data Protection Laws applicable to Acoustic in its role as Processor in performing the Services. Acoustic is not responsible for determining the legal requirements applicable to Partner's business, or for determining whether a Service meets any such requirements.

4.2 Acoustic shall take reasonable steps to ensure that natural persons acting under its authority have committed themselves to confidentiality and do not process Partner Personal Data except as provided under this Partner DPA, the Agreement, according to Partner's instructions or as required by Law.

4.3 Acoustic will inform Partner of requests Acoustic receives directly from Data Subjects exercising their Data Subject rights regarding Partner Personal Data under applicable Data Protection Laws (*e.g.*, including access to, rectification, deletion and blocking of data). Partner shall be responsible for handling such requests. Acoustic will make reasonable efforts to assist Partner in handling such requests in accordance with Section 11.

4.4 If a Data Subject brings a claim directly against Acoustic for alleged violation of Data Subject rights, Partner will reimburse Acoustic for any direct, indirect or consequential cost, charge, damages, expenses or loss arising from such claim, provided that Acoustic has notified Partner about the claim and given Partner the opportunity to cooperate with Acoustic in the defence and settlement of the claim. Subject to the terms of the Agreement, Partner may claim from Acoustic damages resulting from Data Subject claims for violation of Data Subject rights proximately and directly caused by Acoustic's breach of this Partner DPA and/or the corresponding Data Sheet.

4.5 Acoustic will assist Partner by providing appropriate technical and organizational measures for the fulfilment of Partner's obligation to respond to Data Subject rights requests under the Data Protection Laws.

4.6 Taking into account the nature of the Processing and the information available to Acoustic, Acoustic shall assist Partner in complying with the obligations pursuant to the Data Protection Laws, including Art. 32 through 36 GDPR (Security of Processing, Data Security Breach Notification, Data Protection Impact Assessment, Consultation with Data Protection Supervisory Authorities).

4.7 Acoustic will implement technical and organisational data-security measures, pursuant to the Data Protection Laws, including Art. 32 GDPR, and in accordance with Section 6 of this Partner DPA.

4.8 For the purpose of enabling Partner to comply with its own notification obligations with regard to any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Partner Personal Data ("**Security Incident**") pursuant to Data Protection Laws, including Art. 33 para 1 and Art. 34 para 1 GDPR,

Acoustic shall notify Partner without undue delay after becoming aware of any Security Incident.

4.9 In the case claims based on Art. 82 GDPR are raised against Partner, Acoustic shall reasonably support Partner with its defence to the extent such claims arise in connection with the Processing of Partner Personal Data by Acoustic.

4.10 Acoustic will inform Partner of the name and the official contact details of its data protection officer if Acoustic is legally required to appoint one. The data protection officer may serve as the single point of contact pursuant to Section 3.6 of this Partner DPA.

5. PARTNER'S OBLIGATIONS

5.1 As between the Parties, Partner is responsible for the lawfulness of the Processing of the Partner Personal Data, including, to the extent required under applicable Data Protection Laws, by ensuring Data Subjects have received adequate notice of, exercised adequate consent with regard to or otherwise adequately authorized the Processing of their Personal Information. Partner is also responsible for complying with Data Subject requests. Partner will not use the Services in a manner that would violate applicable Law.

5.2 In the case claims based on Art. 82 GDPR are raised against Acoustic, Partner shall reasonably support Acoustic with its defence to the extent such claims arise in connection with the Processing of Partner Personal Data by Acoustic.

6. TECHNICAL AND ORGANISATIONAL MEASURES

6.1 Acoustic will implement and maintain the technical and organizational measures ("**TOM**") set forth in the Data Security and Privacy Principles, annexed as **Annex A** to the Partner DPA, or the corresponding Data Sheet, reasonably designed and implemented to provide a level of security appropriate to the risk. In assessing the appropriate level of security, due consideration shall be given to the risks presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Partner Personal Data transmitted, stored or otherwise Processed.

6.2 Acoustic reserves the right to modify the TOM provided that the overall functionality and security of the Services are not degraded. Modifications to the TOM must be reasonably designed and implemented to provide an appropriate level of security. Acoustic shall make available to Partner a description of any material modifications to the TOM which enables Partner to assess compliance with the Data Protection Laws, including Art. 32 GDPR. If Acoustic provides notification to Partner of any such material modifications, Partner may object in writing to the proposed modifications within two (2) weeks of their provision by Acoustic. Partner shall only be entitled to object to modifications that are not reasonably designed and implemented to provide an appropriate level of security. If Partner fails to provide timely and valid written objection, such failure shall be deemed consent and any objection waived. In case of timely and valid objection, Acoustic may suspend the affected portion of the Services. Partner shall not be entitled to a pro-rata refund for the suspended portion of the Services unless Partner can demonstrate that the modified TOM are not reasonably designed and implemented to provide an appropriate level of security.

7. SUBPROCESSOR

7.1 Acoustic may engage other Processors to Process Partner Personal Data ("**Sub-processors**").

7.2 Any Sub-processor is obliged, before initiating the Processing, to commit itself in writing for the benefit of Partner and Partner Affiliate(s) to comply with the same data protection obligations as the ones under this Partner DPA.

7.3 The agreement with the Sub-processor must provide at least the level of data protection required by this Partner DPA, including requirements to implement appropriate TOM. Where the Sub-processor fails to fulfil its data protection obligations, Acoustic shall remain fully liable to Partner for the performance of the Sub-processor's obligations.

7.4 Where a Sub-processor refuses to be bound by the same data protection obligations as the ones under this Partner DPA, Partner may consent thereto, whereby such consent shall not be unreasonably withheld.

7.5 By entering into this Partner DPA, Partner authorizes engagement of the Sub-processors identified in the corresponding Data Sheet. Upon Partner's written request, Acoustic shall provide Partner with relevant information on data protection obligations of Sub-processors, including granting Partner appropriate access to relevant contractual documents.

7.6 Acoustic shall audit its Sub-processors on a regular basis and will, upon Partner's written request, confirm Sub-processor compliance with Data Protection Laws and data processing agreements. Where Partner demonstrates legitimate grounds, Partner may instruct Acoustic in writing to provide additional information regarding Sub-processor data protection compliance, and Acoustic shall undertake reasonable efforts to comply with such requests.

7.7 Acoustic will notify Partner in advance of any addition to or replacement of the current Sub-processors. Such notice may be provided by posting the updated information on a website accessible to Partner, or by providing another form of written notice to Partner listing all Sub-processors with access to Partner Personal Data, along with a description of the services provided by the Sub-processors.

7.8 Within thirty (30) days after notification of any intended change in Sub-processors, Partner may object in writing if the change would cause Partner to violate applicable Law. Any such written objection shall include Partner's specific reasons for its objection and proposed options to mitigate alleged risk, if any. In the absence of timely and valid objection, Sub-processors identified by Acoustic to Partner may be commissioned to Process Partner Personal Data.

7.9 If Partner provides timely and valid objection to the addition of a Sub-processor and Acoustic cannot reasonably accommodate Partner's objection, Acoustic will notify Partner. Partner may then terminate the affected Services as set out in the Agreement, if the Parties cannot find a feasible solution in accordance with the dispute resolution process set forth in the Agreement. If Partner issues an objection to a proposed Sub-processor that is either untimely, invalid or both, Acoustic may terminate the Agreement and this Partner DPA with thirty (30) days prior written notice. Until the termination of the Agreement, Acoustic may suspend the portion of the Services affected by the Partner's objection. Partner shall be entitled to a pro-rata refund for Services only where Partner provides timely and valid objection to the addition of a Sub-processor.

8. INTERNATIONAL TRANSFERS OF PARTNER DATA

8.1 In the case of a transfer of Partner Personal Data to a Third Country, the Parties shall cooperate to ensure compliance with applicable Data Protection Laws as set out in the following Sections. If Partner believes the measures set out below are insufficient to satisfy legal requirements under any particular circumstances, Partner shall provide written notice of its grounds for such opinions to Acoustic and the Parties shall work together to find a mutually agreeable alternative.

8.2 By entering into the Agreement, and provided the Partner and/or another Controller are located in the European Union, if Partner is acting on behalf of other Controllers, Partner is entering into EU Standard Contractual Clauses ("**EU SCC**") as set forth in **Annex B** to this Partner DPA with (i) each Sub-processor listed in the Data Sheet that is an Acoustic Affiliate located in a Third Country ("**Acoustic Data Importers**") and (ii) Acoustic, if located in a Third Country, as follows:

(a) if Partner is a Controller of all or part of the Partner Personal Data, Partner is entering into the EU

SCC in respect to such Partner Personal Data; and

(b) if Partner is acting as Processor on behalf of other Controllers of all or part of the Partner Personal Data, then Partner is entering into the EU SCC:

(i) as back-to-back EU SCC in accordance with Clause 11 of the EU Standard Contractual Clauses ("**Back-to-Back SCC**"), provided that Partner has entered into separate EU Standard Contractual Clauses with the Controllers; or

(ii) on behalf of the other Controller(s).

8.3 Partner agrees in advance that any new Acoustic Data Importer engaged by Acoustic in accordance with this Section 8 shall become an additional data importer under the EU SCC and/or Back-to-Back SCC. Partner herewith authorizes Acoustic to enter into the EU SCC or Back-to-Back SCC with Acoustic Data Importers in the name of and on behalf of the Partner.

8.4 If a Sub-processor located in a Third Country is not an Acoustic Data Importer ("**Third Party Data Importer**") and EU SCC are entered into in accordance with Section 8.2, then, Acoustic or an Acoustic Data Importer shall enter into Back-to-Back SCC with such a Third Party Data Importer, provided Acoustic or an Acoustic Data Importer is located in a Third Country.

8.5 If Partner is unable to agree to the EU SCC or Back-to-Back SCC on behalf of another Controller, as set out in Sections 8.2 through 8.4, Partner will procure the agreement of such other Controller to enter into those agreements directly. Additionally, Partner agrees and, if applicable, procures the agreement of other Controllers that the EU SCC or the Back-to-Back SCC, including any claims arising from them, are subject to the terms set forth in the Agreement, including the exclusions and limitations of liability.

8.6 In case of conflict between this Partner DPA and the EU SCC or Back-to-Back SCC, the EU SCC and Back-to- Back SCC shall prevail.

9. AUDIT

9.1 In response to Partner's written request and subject to a non-disclosure agreement, Acoustic shall provide to Partner sufficient documentation related to the TOM to demonstrate compliance with this Partner DPA. The effectiveness of Acoustic's TOM may be demonstrated on an annual basis by documentation provided by an independent third-party evaluating the TOM, for example an ISO/IEC 27001 Certificate, an SSAE18 SOC 2 Type II or equivalent attestation report, or similar certification or attestation. Acoustic will reasonably cooperate with Partner where requested, by providing available additional information concerning the TOM, to help Partner better understand such TOM.

9.2 If Partner provides legitimate grounds to allege, or raise serious concerns about, the potential non- compliance of Acoustic's TOM, Partner is, subject to a non-disclosure agreement and no more frequently than once per year (absent specific indicators warranting differently), entitled to audit Acoustic with respect to its TOM compliance.

9.3 This audit right can be exercised by (i) requesting additional information in writing, such as documentation on the processing of Partner Personal Data or (ii) by inspecting Acoustic's working premises where Partner Personal Data is accessible, provided that such inspection shall be conducted in a manner that minimizes the risk of Partner access to data of other Partners or to Acoustic's confidential information. Alternatively, Partner may designate an independent, qualified third-party to perform such tasks on its behalf. Any such designated third-party must agree to a non-disclosure agreement, shall not be a direct competitor of Acoustic and must be able to demonstrate industry-recognized credentials and qualifications to conduct such audits.

9.4 The costs associated with such audits and/or for providing additional information shall be borne by Partner,

unless factual evidence conclusively demonstrates a material breach of this Partner DPA by Acoustic.

10. RETURN OR DELETION OF PARTNER PERSONAL DATA

10.1 Upon termination or expiration of the Agreement Acoustic will, at the choice of the Partner, either delete or return Partner Personal Data, provided such deletion or return does not conflict with superseding legal obligations.

10.2 The Parties agree that, if the Partner has not made a choice pursuant to Section 10.1 within ten (10) days of termination of the Agreement, Partner will be deemed to have chosen to have the Partner Personal Data deleted by Acoustic and waived any objection to such deletion, unless such deletion would conflict with superseding legal obligations.

11. ADDITIONAL INSTRUCTIONS

If Partner's instructions lead to a change from, or increase of, the agreed Services, or in the case of Acoustic's compliance with its obligations pursuant to this Partner DPA to assist Partner with Partner's own statutory obligations, Acoustic is entitled to charge reasonable fees for such tasks, based on the prices agreed for rendering the Services and/or communicated to Partner in advance.

12. LIABILITY

Unless explicitly stated differently in the Agreement, the Parties agree on the following provisions in regard to liability:

(a) Partner and Acoustic shall be each liable for damages of affected Data Subjects according to the Data Protection Laws, including Art. 82 GDPR (external liability).

(b) Either Party shall be entitled to claim back from the other Party, Acoustic or Partner, that part of the compensation, corresponding to the other Party's part of responsibility for the damage of that other Party ("internal liability").

(c) As regards internal liability and without any effect as regards liability towards Data Subjects, the Parties agree that, notwithstanding anything contained hereunder, when providing the Services, Acoustic's liability for breach of this Partner DPA shall be subject to the liability limitations agreed in the Agreement. Partner will indemnify Acoustic against any claims and losses that exceed the liability limitations in the Agreement suffered by Acoustic in connection with any claims of Data Subjects based on alleged breach of the Data Protection Laws or this Partner DPA.

ANNEX A

DATA SECURITY AND PRIVACY PRINCIPLES

The technical and organizational measures provided in this Data Security and Privacy Principles annex ("**DSP**") apply to Acoustic SaaS Products, including any underlying applications, platforms, and infrastructure components operated and managed by Acoustic in providing the SaaS Product ("**Components**"), except where Partner is responsible for data security and privacy or otherwise specified in writing between Acoustic and Partner. Partner is responsible for: a) determining whether the SaaS Product is suitable for Partner's use and; b) implementing and managing security and privacy measures for elements not provided and managed by Acoustic within the SaaS Product described in applicable attachments ("**Attachments**") to this document, the Data Protection Agreement (DPA) or the Agreement (such as systems and applications built or deployed by Partner, or Partner end-user controls to restrict and protect access to Software as a Service offerings). The measures implemented and maintained by or on behalf of Acoustic within each SaaS Product will be subject to annual certification of compliance by International Business Machines Corporation ("IBM"), Acoustic's sub-contractor in respect of the SaaS Product, and/or by Acoustic with ISO 27001 or SSAE SOC 2 or both.

1. DATA PROTECTION

1.1 Security and privacy measures for each SaaS Product are designed in accordance with Acoustic's secure-engineering and privacy-by-design practices to protect Partner data and files ("**Content**") input into a SaaS Product, and to maintain the availability of such Content pursuant to the Agreement, including applicable Attachments and transaction documents. Partner is the sole Controller for any Personal Data included in the Content and appoints Acoustic as a processor to process such personal data (as those terms are defined in Regulation (EU) 2016/679, General Data Protection Regulation). Acoustic will treat all Content as confidential by not disclosing Content except to Acoustic employees, contractors, and sub- processors, and only to the extent necessary to deliver the SaaS Product, unless otherwise specified in an Attachment.

1.2 Acoustic will verify that physical storage media intended for reuse are securely sanitized prior to such reuse and will verify the destruction of such media not intended for reuse, consistent with National Institute of Standards and Technology, United States Department of Commerce (NIST), guidelines for media sanitization.

1.3 Upon written request, Acoustic will provide reasonable evidence of stated compliance and accreditation, which may, where available, comprise certificates, attestations, or reports resulting from accredited independent third-party audits, such as ISO 27001, SSAE SOC 2, and/or other industry standards as specified in an Attachment, and which may be held by IBM who for the time being operate the infrastructure, hosting, support and related services in respect of the SaaS Product and/or by Acoustic itself. Where applicable, the accredited independent third-party audits will occur at the frequency required by the relevant standard to maintain the SaaS Product's stated compliance and accreditation.

1.4 Additional data security and privacy information specific to a SaaS Product may be available in a relevant Attachment (such as a Data Sheet) or other standard documentation to aid in Partner's initial and ongoing

assessment of a SaaS Product's suitability for use. Such information may include evidence of stated certifications and accreditations, information related to such certifications and accreditations, data sheets, FAQs, and other generally available documentation. Acoustic will direct Partner to available standard documentation if asked to complete Partner-preferred questionnaires or forms, and Partner agrees such documentation will be utilized in lieu of any such request. Acoustic may charge an additional fee to complete any Partner-preferred questionnaires or forms or to provide consultation to Partner for such purposes.

2. SECURITY POLICIES

2.1 Acoustic will maintain and follow information-technology ("**IT**") security policies and practices that are integral to Acoustic's business and mandatory for all Acoustic employees. The Chief Information Security Officer, Chief Information Officer, or equivalent will maintain responsibility and executive oversight for such policies, including formal governance and revision management, employee education, and compliance enforcement.

2.2 Acoustic will review its, and procure that IBM, whist acting as sub-contractor in respect of the SaaS Product, will review its IT security policies at least annually and amend such policies as Acoustic or IBM (as appropriate) deems reasonable to maintain protection of SaaS Products and Content processed therein.

2.3 Acoustic will maintain and follow its standard mandatory employment verification requirements for all new hires and will extend such requirements to wholly owned Acoustic subsidiaries. In accordance with Acoustic internal process and procedures, these requirements will be periodically reviewed and may include criminal background checks, proof of identity validation, and additional checks as deemed necessary by Acoustic. Each Acoustic company is responsible for implementing such requirements in its hiring process as applicable and permitted under local Law.

2.4 Acoustic employees will complete security and privacy education annually and certify each year that they will comply with Acoustic's ethical business conduct, confidentiality, and security policies. Additional policy and process training will be provided to persons granted administrative access to SaaS Product Components that is specific to their role within Acoustic's operation and support of the SaaS Product, and as required to maintain compliance and any certifications stated in the relevant Attachment.

3. SECURITY INCIDENTS

3.1 Acoustic will maintain and follow, and procure that IBM as long as it is acting as sub-contractor for the SaaS Product will maintain and follow, documented incident-response policies consistent with NIST guidelines for computer security incident handling and will comply with data-breach notification terms of the Agreement.

3.2 Acoustic will investigate unauthorized access to and unauthorized use of Content of which Acoustic becomes aware, and, within the SaaS Product scope, Acoustic will define and execute an appropriate response plan. Partner may notify Acoustic of a suspected vulnerability or incident by submitting a technical support case.

3.3 Acoustic will notify Partner without undue delay upon confirmation of a security incident that is known or reasonably suspected by Acoustic to affect Partner. Acoustic will provide Partner, in response to a reasonable written request, information about such security incident and the status of any Acoustic remediation and restoration activities, including, if required by applicable Data Protection Laws, (i) a description of the security incident, including the date and time the security incident was discovered; (ii) an overview of the affected Personal Information; (iii) the number of affected Data Subjects; (iv) the expected consequences of the security incident; (v) a description of the measures taken by Acoustic to restrict such consequences.

4. PHYSICAL SECURITY AND ENTRY CONTROL

4.1 Acoustic will, and as long as IBM is a sub-contractor procure that IBM will, verify the maintenance of appropriate physical-entry controls, such as barriers, card-controlled entry points, surveillance cameras, and manned reception desks, to protect against unauthorized entry into Acoustic facilities used to host the SaaS Product ("**Data Centers**"). Auxiliary entry points into Data Centers, such as delivery areas and loading docks, will be controlled and isolated from computing resources.

4.2 Access to Data Centers and controlled areas within Data Centers will be limited by job role and subject to authorized approval. Use of an access badge to enter a Data Center and controlled areas will be logged, and such logs will be retained for not less than one year. Acoustic will revoke or procure the revocation of access to controlled Data Center areas upon separation of an authorized employee. Acoustic will follow formal documented separation procedures that include prompt removal from access-control lists and surrender of physical access badges.

4.3 Acoustic will ensure, including the securing of relevant contractual commitments from third party vendors, that any person duly granted temporary permission to enter a Data Center facility or a controlled area within a Data Center will be registered upon entering the premises; must provide proof of identity upon registration, and will be escorted by authorized personnel. Any temporary authorization to enter, including deliveries, will be scheduled in advance and require approval by authorized personnel.

4.4 Acoustic will verify that the operators of the Data Centers take all necessary and required precautions to protect the SaaS Product's physical infrastructure against environmental threats, both naturally occurring and man-made, such as excessive ambient temperature, fire, flood, humidity, theft, and vandalism.

5. ACCESS, INTERVENTION, TRANSFER AND SEPARATION CONTROL

5.1 Documented security architecture of networks managed by or on behalf of Acoustic in its operation of the SaaS Product will be maintained. Such network architecture, including measures designed to prevent unauthorized network connections to systems, applications and network devices, will be reviewed for compliance with secure segmentation, isolation, and defense-in-depth standards prior to implementation. SaaS Product networks do not use wireless-networking technology. Wireless-networking technology may be used in the maintenance and support of the SaaS Product and associated Components. Such wireless networks, if any, will be encrypted, will require secure authentication, and will not provide direct access to SaaS Product networks.

5.2 Measures that are designed to logically separate and prevent Content from being exposed to or accessed by unauthorized persons will be maintained for each SaaS Product. Appropriate isolation of its production and non-production environments will be maintained, and, if Content is transferred to a non-production environment, for example in order to reproduce an error at Partner's request, security and privacy measures designed to provide the same level of protection as in the production environment will be maintained in the non-production environment.

5.3 To the extent described in the relevant Attachment, Content not intended for public or unauthenticated viewing will be encrypted when transferred over public networks, and the SaaS Product shall enable use of a cryptographic protocol, such as HTTPS or SFTP, for Partner's secure transfer of Content to and from the SaaS Product over public networks.

5.4 Content will be encrypted at rest when and as specified in an Attachment. If the SaaS Product includes management of cryptographic keys, documented procedures will be maintained for secure key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use.

5.5 If access to Content is required, it will be restricted to the minimum level required. Such access, including administrative access to any underlying Components ("**Privileged Access"**), will be individual, role- based, and subject to approval and regular validation by authorized personnel following the principles of segregation of duties. Adequate measures will be maintained to identify and remove redundant and dormant accounts with Privileged Access and such Privileged Access will promptly be revoked upon the account owner's separation from Acoustic or upon the request of authorized personnel, such as the account owner's manager.

5.6 Consistent with industry standard practices, and to the extent natively supported by each Component managed by or on behalf of Acoustic within the SaaS Product, technical measures will be maintained enforcing timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, strong password or passphrase authentication, and measures requiring secure transfer and storage of such passwords and passphrases.

5.7 Use of Privileged Access will be monitored and maintained and security information and event management measures will be maintained designed to: a) identify unauthorized access and activity; b) facilitate a timely and appropriate response; and c) enable internal and independent third-party audits of compliance with documented policy.

5.8 Logs in which Privileged Access and activity are recorded will be retained in compliance with Acoustic's records-management plan. Measures designed to protect against unauthorized access, modification, and accidental or deliberate destruction of such logs will be maintained.

5.9 To the extent supported by native device or operating system functionality, computing protections for its end-user systems will be maintained that include endpoint firewalls, full-disk encryption, signature-based malware detection and removal, time-based screen locks, and endpoint-management solutions that enforce security configuration and patching requirements.

6. SERVICE INTEGRITY AND AVAILABILITY CONTROL

6.1 Acoustic will: a) ensure security and privacy risk assessments of its SaaS Products are carried out at least annually; b) ensure penetration testing and vulnerability assessments, including automated system and application security scanning and manual ethical hacking, are carried out before production release and annually thereafter; c) ensure a qualified independent third-party performs penetration testing at least annually; d) ensure automated management and routine verification of underlying Components' compliance with security-configuration requirements are carried out; and e) remediate identified vulnerabilities or noncompliance with its security configuration requirements based on associated risk, exploitability, and impact.

6.2 Acoustic will take reasonable steps to avoid SaaS Product disruption when performing tests, assessments, scans, and execution of remediation activities.

6.3 Acoustic will maintain policies and procedures designed to manage risks associated with the application of changes to its SaaS Products. Prior to implementation, material changes to a SaaS Product, including its systems, networks, and underlying Components, will be documented in a registered change request that includes a description and reason for the change, implementation details and schedule, a risk statement addressing impact to the SaaS Product and its Partners, expected outcome, rollback plan, and documented approval by authorized personnel.

6.4 Acoustic will maintain an inventory of all information-technology assets used in its operation of the SaaS Product. Acoustic will continuously monitor and manage the health, including capacity, and availability of the SaaS Product and underlying Components.

6.5 Each SaaS Product will be separately assessed for business-continuity and disaster-recovery requirements pursuant to documented risk-management guidelines. Each Acoustic SaaS Product will have, to the extent warranted by such risk assessment, separately defined, documented, maintained, and annually validated business-continuity and disaster-recovery plans consistent with industry-standard practices. Recovery-point and recovery-time objectives for the SaaS Product, if provided, will be established with consideration given to the SaaS Product's architecture and intended use, and will be described in the relevant Attachment. Partner's Content on physical media intended for off-site storage, if any, such as media containing SaaS Product backup files, will be encrypted prior to transport.

6.6 Acoustic will maintain measures designed to assess, test, and apply security patches to the SaaS Product and its associated systems, networks, applications, and underlying Components within the SaaS Product scope. Upon determining that a security patch is applicable and appropriate, Acoustic will implement the patch pursuant to documented severity and risk-assessment guidelines. Implementation of security patches will be subject to Acoustic change-management policy.

[END OF ANNEX]

ANNEX B

EU STANDARD CONTRACTUAL CLAUSES FOR PROCESSORS

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Each of the EU Partner Affiliate(s) expressly identified as a data exporter in **Appendix 3** is hereinafter referred to as the "**Data Exporter**" with respect to the personal data provided by the respective Data Exporter.

Acoustic is hereinafter referred to as the "**Data Importer**".

The Data Exporter(s) and the Data Importer, each a "**party**" and collectively "**the parties**" HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Data Exporter to the Data Importer of the personal data specified in **Appendix 1**.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* has the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the Data Exporter'* means the controller who transfers the personal data;

(c) *'the Data Importer'* means the processor who agrees to receive from the Data Exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) the *'Subprocessor'* means any processor engaged by the Data Importer or by any other subprocessor of the Data Importer who agrees to receive from the Data Importer or from any other subprocessor of the Data Importer personal data exclusively intended for processing activities to be carried out on behalf of the Data Exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the Applicable Data Protection Law'* means the Law protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the Data Exporter is established;

(f) *'Technical and Organisational Security Measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the Data Exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the Data Importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the Data Exporter has factually disappeared or has ceased to exist in Law unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of Law, as a result of which it takes on the rights and obligations of the Data Exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the Subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in Law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of Law as a result of which it takes on the rights and obligations of the Data Exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the Subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national Law.

Clause 4

Obligations of the Data Exporter

The Data Exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the Applicable Data Protection Law (and, where applicable, has been notified to the relevant authorities of the Member State where the Data Exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the Data Importer to process the personal data transferred only on the Data Exporter's behalf and in accordance with the Applicable Data Protection Law and the Clauses;

(c) that the Data Importer will provide sufficient guarantees in respect of the Technical and Organisational Security Measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the Applicable Data Protection Law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the Data Importer or any Subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the Data Exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a Subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the Data Importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the Data Importer

The Data Importer agrees and warrants:

(a) to process the personal data only on behalf of the Data Exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the Data Exporter of its inability to comply, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the Data Exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the Data Exporter as soon as it is aware, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the Technical and Organisational Security Measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the Data Exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal Law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the Data Exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the Data Exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the Data Exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the Data Exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the Data Exporter;

(h) that, in the event of subprocessing, it has previously informed the Data Exporter and obtained its prior written consent;

(i) that the processing services by the Subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the Data Exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or Subprocessor, is entitled to receive compensation from the Data Exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the Data Exporter, arising out of a breach by the Data Importer or his Subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the Data Exporter has factually disappeared or ceased to exist in Law or has become insolvent, the Data Importer agrees that the data subject may issue a claim against the Data Importer as if it were the Data Exporter, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract of by operation of Law, in which case the data subject can enforce its rights against such entity.

   The Data Importer may not rely on a breach by a Subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the Data Exporter or the Data Importer referred to in paragraphs 1 and 2, arising out of a breach by the Subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in Law or have become insolvent, the Subprocessor agrees that the data subject may issue a claim against the data Subprocessor with regard to its own processing operations under the Clauses as if it were the Data Exporter or the Data Importer, unless any successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of Law, in which case the data subject can enforce its rights against such entity. The liability of the Subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The Data Importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the Data Importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the Data Exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of Law.

Clause 8

Cooperation with supervisory authorities

1. The Data Exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the Applicable Data Protection Law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the Data Importer, and of any Subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the Data Exporter under the Applicable Data Protection Law.

3. The Data Importer shall promptly inform the Data Exporter about the existence of legislation applicable to it or any Subprocessor preventing the conduct of an audit of the Data Importer, or any Subprocessor, pursuant to paragraph 2. In such a case the Data Exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the Law of the Member State in which the Data Exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The Data Importer shall not subcontract any of its processing operations performed on behalf of the Data Exporter under the Clauses without the prior written consent of the Data Exporter. Where the Data Importer subcontracts its obligations under the Clauses, with the consent of the Data Exporter, it shall do so only by way of a written agreement with the Subprocessor which imposes the same obligations on the Subprocessor as are imposed on the Data Importer under the Clauses (This requirement may be satisfied by the Subprocessor co-signing the contract entered into between the Data Exporter and the Data Importer which is based on the terms and conditions of this Agreement.). Where the Subprocessor fails to fulfil its data protection obligations under such written agreement the Data Importer shall remain fully liable to the Data Exporter for the performance of the Subprocessor's obligations under such agreement.
2. The prior written contract between the Data Importer and the Subprocessor shall also provide for a third- party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the Data Exporter or the Data Importer because they have factually disappeared or have ceased to exist in aw or have become insolvent and no successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of Law. Such third-party liability of the Subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the Law of the Member State in which the Data Exporter is established.
4. The Data Exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the Data Importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the Data Exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the Data Importer and the Subprocessor shall, at the choice of the Data Exporter, return all the personal data transferred and the copies thereof to the Data Exporter or shall destroy all the personal data and certify to the Data Exporter that it has done so, unless legislation imposed upon the Data Importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the Data Importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The Data Importer and the Subprocessor warrant that upon request of the Data Exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE EU STANDARD CONTRACTUAL CLAUSES FOR PROCESSORS

This Appendix forms part of the Clauses and is incorporated by reference into the DPA.

Data Exporter(s)

The Data Exporter(s) is/are one or more entities for whom the Services are being provided by the Data Importer.

Data Importer

The Data Importer is a software company which offers marketing software as a service (SaaS) solutions.

Data subjects

*Please refer to the information provided in **Annex C** of the DPA.*

Categories of data

*Please refer to the information provided in **Annex C** of the DPA*

Special categories of data (if appropriate)

*Please refer to the information provided in **Annex C** of the DPA*

Processing operations

*Please refer to the information provided in **Annex C** of the DPA*

APPENDIX 2 TO THE EU STANDARD CONTRACTUAL CLAUSES FOR PROCESSORS

This Appendix forms part of the Clauses and is incorporated by reference into the DPA.

Description of the Technical and Organizational Security Measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The Technical and Organizational Security Measures are described in **Annex A** of the DPA.

APPENDIX 3 TO THE EU STANDARD CONTRACTUAL CLAUSES FOR PROCESSORS

This Appendix forms part of the Clauses and is incorporated by reference into the DPA.
The following EU Partner Affiliate(s) is/are data exporters for purposes of the Clauses:

- Please refer to the applicable EU Partner Affiliate(s) identified in the Quote (if any).

[END OF ANNEX]

ANNEX C

DATA SHEETS

The relevant Data Sheet(s) can be found here: acoustic.com/acoustic-terms.