DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms part of, and is subject to, the Agreement between the Retensa entity providing the Product (as defined below) under such Agreement (as defined below) and the Client set forth in the Order Form in relation to Retensa's Processing of Client's Protected Data. This DPA shall be effective on the effective date of the Agreement, unless this DPA is separately executed, in which case it is effective on the date of the last signature. Capitalized terms used but not defined herein shall have the meaning assigned to such terms in the Agreement.

1. DEFINITIONS

1.1. "**Agreement**" means: (i) each applicable Order Form and/or Statement of Work for the Product that Client purchases from Retensa, and (ii) the applicable Master Subscription Agreement or other written or electronic terms of service or subscription agreement referenced in the applicable Order Form and/or Statement of Work or signed and executed by and between Client and Retensa;

1.2. "**Controller**" means the entity which determines the purposes and means of the Processing of Protected Data;

1.3. "**Data Subject**" means the identified or identifiable natural person to whom the Protected Data relates;

1.4. "**Data Subject Request**" means a request made by an individual to exercise their rights under Data Protection Laws;

1.5. "**Data Protection Law(s)**" means the laws, regulations, and administrative rules worldwide regarding the protection of data and privacy of individuals, including (if applicable), without limitation, the EU/UK Data Protection Laws, the US Privacy Laws (as defined below) and the Federal Law No. 13.709/2018 (Brazilian General Law on Data Protection (LGPD), but not including any industry-specific or sector-specific laws, regulations, rules, or industry-standards, such as those related to healthcare (including HIPAA, as defined below), financial services, payment or credit card, or government and public bodies;

1.6. "**Data Protection Authority**" means an EU Supervisory Authority, an Information Commissioner or any duly authorized government authority responsible for administering Data Protection Laws;

1.7. "**EU/UK Data Protection Laws**" means: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data on the free movement of such data (General Data Protection Regulation) (the "**EU GDPR**"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); in each case as may be amended or superseded from time to time;

1.8. "**Personal Data**" means any information relating to an identified or identifiable natural person and includes 'personal data', 'personal information' or 'personally identifiable information' as defined under Data Protection Laws;

1.9. "**Personal Data Breach**" means any breach of Retensa's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Protected Data;

1.10. "**Processor**" means the entity which processes Protected Data on behalf of the Controller. For the purpose of this DPA, a "service provider" under US Privacy Laws shall be referred to herein as a Processor;

1.11. "**Processing**" means any operation or set of operations which is performed upon Protected Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, and "**Process**", "**Processes**" and "**Processed**" will be interpreted accordingly;

1.12. "**Protected Data**" means Personal Data in Client Data submitted into the Product by the Client in compliance with the terms of the Agreement;

1.13. "**Purposes**" means: (i) Retensa's provision of the Product as described in the Agreement, including Processing initiated by Authorized Users in their use of the Product; and (ii) further documented, reasonable and lawful instructions from Client agreed upon by the parties in accordance with the terms of this DPA;

1.14. "**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of Protected Data from the European Economic Area ("**EEA**") to a country outside the EEA, which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Protected Data from the United Kingdom to any other country which is not subject based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of Protected Data from Switzerland to any country which is not recognized to provide adequate protection by the Swiss Federal Data Protection and Information Commissioner ("**FDPIC**").

1.15. "**Product**" means the Product pursuant to the Agreement and as further specified in the Documentation;

1.16. "**Standard Contractual Clauses**" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementation Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to the EU GDPR ("**EU SCCs**"); and (ii) where the UK GDPR applies, the UK Addendum (as defined below);

1.17. "**Sub-Processor**" means any Processor engaged by Retensa in order to process Protected Data under this DPA on behalf of Retensa;

1.18. "**Swiss DPA**" means the Swiss Federal Data Protection Act of June 19, 1992, and its corresponding regulations;

1.19. "**UK Addendum**" means the UK Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018;

1.20. "**US Privacy Laws**" means all U.S. state privacy laws applicable to the Personal Data, including where relevant: (i) the California Consumer Privacy Act (the "**CCPA**"), as amended by the California Privacy Rights Act ('CPRA'); and, where applicable, (ii) the Virginia Consumer Data Protection Act ('CDPA'); (iii) the Colorado Privacy Act ('CPA'), when effective; (iv) the Utah Consumer Privacy Act, when effective ('UCPA'); (v) the Connecticut Data Privacy Act ('CTDPA'), when effective; in each case, only to the extent that such law(s) apply to the processing of Personal Data under this DPA, and as well as any regulations that may be issued thereunder.

2. SCOPE AND THE ROLES OF THE PARTIES

2.1. This DPA applies where and only to the extent that Retensa Processes Protected Data on behalf of Client as Processor, in the course of providing the Product.

2.2. Each party acknowledges and agrees that, with respect to the Processing of Protected Data: (i) Client shall be the Controller, "organization", "business", or their equivalent terms, as applicable (and if Client processes the Protected Data on behalf of a third-party – a Processor, or its equivalent terms, as applicable), and; (ii) Retensa shall be the Processor, "service provider", or their equivalent terms, as applicable (and if Client processes the Protected Data on behalf of a third-party – a Sub-Processor, or its equivalent term, as applicable).

2.3. If any Data Protection Law imposes on Retensa additional or overriding obligations to those in this DPA with respect to its Processing of Protected Data or requires Client and Retensa to enter into any additional agreements or to implement any additional security or organizational measures to process Protected Data under the Agreement, Retensa and Client agree to negotiate such additional obligations, agreements, or security measures in good faith.

3. DATA PROCESSING RESPONSIBILITIES

3.1. **Retensa Responsibilities**. Retensa shall: (i) process Protected Data only for the Purposes. The parties agree that the DPA and the Agreement are Client's complete and final documented instructions, and if Client acts as a Processor on behalf of its Controller, then such instructions are consistent with its Controller's instructions. The parties further agree that and any additional instructions, to be provided by Client from time to time, must: (a) be consistent with the terms of the Agreement and this DPA, (b) be accepted by Retensa by amending this DPA, and (c) not contradict any applicable law; and (ii) inform Client if it becomes aware that Client's Processing instructions infringe Data Protection Laws (but without obligation to actively monitor Client's instructions' compliance with such Data Protection Laws).

3.2. **Retensa's Responsibilities under US Privacy Laws**. Retensa shall: (i) not sell Protected Data or share Personal Data for the purposes of targeted or cross-contextual behavioral advertising; (ii) not retain, use or disclose Protected Data for any purpose other than for the specific purpose of performing the Product, or outside the business relationship between Client and Retensa, expect where necessary to provide the Product or as permitted or required under Data Protection Laws; (iii) not combine Protected Data with information received from another source, except where necessary to provide the Product or as permitted or required under Data Protection Laws; (vi) notify Client if it makes a determination that it can no longer meet its obligations under US Privacy Laws, in which case, Client may, upon written notice, and at Client's expense, take reasonable steps to stop and remediate an unauthorized use of Protected Data in accordance with US Privacy Laws, which may include, by way of example, assessments, audits (in accordance with the terms of this DPA) and other technical or operational testing; and (v) provide the same level of privacy protection for the Protected Data as required by the CCPA in order to give effect to consumer requests made, including informing of any consumer request made and cooperating to ensure the information necessary to comply with the request is provided. Retensa certifies that it understands and will comply with the restrictions of this Section 3.2.

3.3. **Client Responsibilities**. Client is solely responsible for its and its Authorized Users' Processing of Protected Data through use of the Product and for the accuracy and quality of the Protected Data. Client shall: (i) comply with all necessary requirements under Data Protection Laws; (ii) provide notice and obtain all consents, permissions and/or rights (as applicable) necessary under Data Protection Laws to disclose or make available any Protected Data to Retensa and ensure Retensa's lawful Processing of the Protected Data (including, without limitation, any sensitive data) under this DPA and the Agreement; (iii) not request or cause Retensa to Process Protected Data in a manner that does not comply with the applicable Data Protection Laws; (iv) be responsible for any communications, notifications, assistance and/or authorizations that may be required by its Controller or in relation to its Controller with regard to this DPA, where Client acts as a Processor on behalf of its Controller; and (v) use the Product in a manner designed to ensure a level of security appropriate to the Protected Data, such as backing-up the Protected Data.

4. RESTRICTED TRANSFERS AND ONWARD TRANSFERS

4.1. **Restricted Transfers.** The parties agree that where the transfer of Protected Data from Client to Retensa is a Restricted Transfer, it shall be subject to the appropriate Standard Contractual Clauses as follows:

(a) In relation to Protected Data that is protected by the EU GDPR, the EU SCCs will be deemed executed, entered into and incorporated into this DPA by this reference as follows:

(i) Module Two will apply to the extent that Client is a Controller of the Protected Data, and Module Three will apply to the extent that Client is a Processor of the Protected Data on behalf of a third-party

Controller;

(ii) in Clause 7, the optional Docking Clause will apply;

(iii) in Clause 9, Option 2 will apply, and the time period for notice of Sub-Processors changes shall be as set out in Section 6.2 of this DPA;

(iv) in Clause 11, the optional language will not apply;

(v) Clause 13(a) shall be deemed completed as indicated in **Exhibit 1.C**;

(vi) in Clause 17, Option 1 will apply, and the EU SCCs will be gov~~erned by Irish~~ law;

(vii) in Clause 18(b), disputes shall be resolved before the courts of Ireland;

(viii) Annex I of the EU SCCs shall be deemed completed with the information set out in **Exhibit 1**

to this DPA; and

(ix) Annex II of the EU SCCs shall be deemed completed with the information set out in **Exhibit 2** to this DPA.

(b) In relation to Protected Data that is protected by the UK GDPR, the UK Addendum will be deemed executed, entered into and incorporated into this DPA by this reference as follows:

(i) the EU SCCs, completed as set out above in Section 4.1(a) of this DPA, shall also apply to transfers of such Protected Data, and the EU SCCs shall be deemed amended as specified by Part 2 of the UK Addendum in respect of the transfer of such Protected Data;

(ii) tables 1 to 3 in Part 1 of the UK Addendum shall be deemed completed with the information set out above at Section 4.1(a) (as applicable), in **Exhibit 1** and in **Exhibit 2** of this DPA;

(iii) table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting “neither party”; and

(iv) any conflict between the terms of the EU SCCs and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

(c) In relation to Protected Data that is protected by the Swiss DPA, the EU SCCs (as set forth in Section 4.1(a) above) shall apply on the following basis:

(i) the EU SCCs, completed as set out above in Section 4.1(a) of this DPA, shall apply and be modified as set out in sub-paragraphs (ii) to (ix) below.

(ii) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA;

(iii) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss DPA;

(iv) references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland" or "Swiss law" (as applicable);

(v) the term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., Switzerland);

(vi) Clause 13(a) shall be deemed completed as indicated in **Exhibit 1.C**;

(vii) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "FDPIC" and "applicable courts of Switzerland";

(viii) in Clause 17, the EU SCCs shall be governed by the laws of Switzerland; and

(ix) the EU SCCs also protect the data of legal entities until the revised Swiss Federal Data Protection Act enters into force.

the parties’ signature to this DPA shall be considered as a signature for the Standard Contractual Clauses.

4.2. **Onward Transfers**. Retensa shall not participate in (nor permit any Sub-Processor to participate in) any other Restricted Transfer of Protected Data (whether as a data exporter or a data importer of such Protected Data) unless the Restricted Transfer is made in full compliance with the EU/UK Data Protection Laws. Subject to the provisions of Section 6 of this DPA, where a Restricted Transfer is protected by the UK GDPR, Client authorizes Retensa to enter into the UK Addendum with any Sub-Processor on its behalf.

5. SECURITY

5.1. Retensa shall implement, maintain, and follow, at its cost and expense, the appropriate technical and organizational measures set forth in **Exhibit 2**, to protect the Protected Data from a Personal Data Breach.

5.2. The technical and organizational measures listed in **Exhibit 2** are subject to technological progress and advancement. As such, Retensa may implement alternative, adequate measures, which meet or exceed the security level of the measures described in **Exhibit 2**.

6. SUB-PROCESSORS

6.1. Retensa appoints its affiliates and the Sub-Processors listed on this website (https://retensa.com/documentation/subprocessors/) ("**Sub-Processor Site**") to perform Processing activities in respect to Protected Data on behalf of Retensa, and Client acknowledges and expressly agrees to such appointment (and where Client is a Processor, it represents that such consent is consistent with the instructions of its Controller). Processing by Sub-Processors is done under a written contract containing data protection obligations no less protective of Protected Data as provided for by this DPA. Retensa shall remain fully responsible for its Sub-Processors' performance of their obligations under their contracts with Retensa. If Retensa adds a new Sub-Processor, or changes a Sub-Processor, Retensa will ensure that data protection obligations are no less protective of Protected Data as provided for by this DPA, and that Sub-Processor will be added to the Sub-Processor Site.

7. PERSONNEL

Retensa shall ensure that only authorized personnel have access to Protected Data. Anyone whom Retensa authorizes to access Protected Data on its behalf is subject to a binding contractual or statutory obligation to protect the Protected Data and keep it confidential, no less than Retensa is required to do under the Agreement and this DPA. Retensa shall ensure that its authorized personnel are appropriately trained regarding their data protection and confidentiality obligations.

8. DATA SUBJECTS' REQUESTS AND DATA PROTECTION AUTHORITIES' INQUIRIES

8.1. Retensa shall promptly notify Client in writing of any Data Subject Requests or other communications received from Data Subjects or Data Protection Authorities (to the extent permitted by law) relating to the Protected Data and for whom Client is responsible, or otherwise identifying Client as its Controller or Processor (as applicable). Client shall be solely responsible for responding to any Data Subject Requests (and in case Client acts as a Processor – cooperating with its Controller to do so). If requested by Client, Retensa shall provide Client with additional commercially reasonable assistance, at Client's expense, with respect to answering and fulfilling Data Subject Requests, as required under Data Protection Laws.

8.2. If Retensa receives a demand from a government agency or any other public authority to disclose Protected Data ("**Government Request**"), then Retensa shall attempt to redirect such Government Request to the Client. Client agrees that Retensa can provide information to such agency/authority to the extent reasonably necessary to redirect the Government Request to Client. If Retensa cannot redirect the Government Request to Client, then Retensa shall, to the extent permitted by law, provide Client with a prompt notice of the Government Request to allow Client to seek a protective order or other appropriate remedy.

8.3. Taking into account the nature of the Product and the nature of the Processing, Client authorizes Retensa, on its behalf and when Client is acting as a Processor - on behalf of its Controllers, to respond to any Data Subject Request or other communications received from Data Subjects, to confirm that Retensa has notified Client in accordance with the provisions of Section 8.1 above. Notwithstanding the foregoing, Retensa may respond to any Data Subject Request or other communications from Data Subjects or Data Protection Authorities if it is required to do so under applicable law.

9. DATA PROTECTION IMPACT ASSESSMENTS AND PRIOR CONSULTATIONS

To the extent that Retensa is required under Data Protection Laws, and to the extent Client does not otherwise have access to the relevant information, Retensa will, at Client's expense, provide reasonably requested information regarding Retensa's Processing of Protected Data under the DPA, to enable Client to carry out a data protection impact assessment or a prior consultation with Data Protection Authorities, as required by law.

10. AUDITS

10.1. Client may review Retensa's compliance with its data protection obligations under this DPA, at its own expense, by itself or by an independent certified auditor who is reasonably acceptable to Retensa (which shall not include any third-party auditors who are competitors of Retensa) ("**Audit**"). If Client wishes to conduct an Audit in accordance with the terms of this Section 10, it will send Retensa a written request for an Audit at least sixty (60) days in advance of its intention to conduct such Audit. Following the receipt by Retensa of such request, the parties shall mutually agree on the details of the audit, including (among others), a reasonable start date, scope and duration of, and the security and confidentiality controls applicable to, any such Audit. While the Audit is being conducted, Client shall ensure that the Audit does not disrupt the regular operations of Retensa. Client will exercise its Audit rights hereunder in good faith and in a proportional manner (taking into account the nature of the Protected Data and the nature of the Product), and shall not exercise its Audit right more than once in any twelve (12) month period, except when Client can provide reasonable evidence that an additional Audit is required by explicit instructions of a Data Protection Authority. Client shall provide to Retensa a copy of any information generated and/or obtained in the Audit, as well as the Audit reports, and shall ensure that such information and reports are kept strictly confidential and will not be shared with any third parties (except as otherwise explicitly required under the applicable Data Protection Law). Retensa may charge a fee (the rates shall be reasonable, taking into account the time and resources expended Retensa) for any such Audit.

10.2. Alternatively, at Retensa's discretion, Retensa may satisfy its obligations under Section 10.1 of this DPA (and any similar obligations under the Standard Contractual Clauses) by presenting sufficient evidence of its compliance with the agreed data protection measures under this DPA, including, without limitation, summary copies of industry-standard audit report(s) and/or third-party certification as to compliance with ISO 27001, ISO 27701 or similar standards.

10.3. Any Audit right under this Section 10 shall not require Retensa to disclose to Client or its third-party auditors: (i) any information of any other Retensa customer; (ii) any internal accounting or financial information; (iii) any trade secret, and/or; (iv) any information that could compromise the security of Retensa's systems or information, or cause

Retensa to breach any applicable law or contractual obligation.

10.4. The parties agree that the audits described in the Standard Contractual Clauses shall be carried out in accordance with Client's rights described in this Section 10, and that such rights are carried out on behalf of Client (and if Client acts process its relevant Controller).

11. BREACH NOTIFICATION

11.1 In respect of any Personal Data Breach, Retensa shall notify Client about the occurrence of such breach without undue delay (not to exceed 72 hours) of becoming aware of the Personal Data Breach. So far as possible without prejudicing the continued security of the Protected Data or any investigation into the Personal Data Breach, Retensa shall provide Client with timely detailed information about the Personal Data Breach. Retensa's notification shall be sent to the email address registered by Client in Client's account for such purposes, and where no such email address is registered, to Client's primary email address as registered in the Client's account. It is the Client's sole responsibility to ensure that Client's account maintain accurate contact information.

11.2 Client acknowledges that since Retensa personnel may not have visibility to the content of the Protected Data, it is unlikely that Retensa will be able to provide information as to the particular nature of the Protected Data (e.g., the identities, number/volume or categories of affected Protected Data or Data Subjects).

11.3 For the avoidance of doubt: (i) the obligations of Retensa herein shall not apply to incidents that are caused by Client or its Authorized Users. Client acknowledges that taking into account the nature of the Processing and of the Product, it is unlikely that Retensa will be able to detect or become aware of Personal Data Breaches or incidents that are caused by Client, Client's Authorized Users or by their respective use of the Product; and (ii) Communications by or on behalf of Retensa with Client in connection with a Personal Data Breach shall not be construed as an acknowledgement by Retensa of any fault or liability by Retensa with respect to the Personal Data Breach.

12. DELETION OR RETURN OF DATA

Retensa shall delete Protected Data of Client in accordance with the provisions of the Agreement. This requirement shall not apply to the extent that Retensa is required by any applicable law to retain some of the Protected Data, or to Protected Data it has archived on back-up systems, in which event Retensa shall isolate and protect such Protected Data from any further Processing except to the extent required by such law, until deletion is possible.

13. MISCELLANEOUS

13.1. In the event of a conflict or an inconsistency between the provisions of this DPA and those of the Agreement in respect of the Processing and protection of Protected Data, the provisions of this DPA shall prevail. With respect to Retensa's Processing of Protected Data as part of a Restricted Transfer, in the event of a conflict between the terms of the Standard Contractual Clauses and this DPA, the Standard Contractual Clauses shall prevail. In the event of a conflict or inconsistency between the provisions of this DPA and those of any Business Associate Agreement executed by Retensa and Client in relation to protected health information regulated by the Health Insurance Portability and Accountability Act ("**HIPAA**") ("**BAA**"), the provisions of the BAA shall prevail. Except as expressly modified herein, all terms and conditions of the Agreement shall remain in full force and effect.

13.2. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions of the Agreement, unless required otherwise by the Data Protection Laws.

13.3. This DPA and the applicable Standard Contractual Clauses will terminate simultaneously and automatically with the termination or expiry of the Agreement. A material breach of this DPA will be treated as a material breach of the Agreement. Without derogating from the foregoing, Client's breach of Section

3.3 above shall be deemed a material breach of this DPA and the Agreement.

13.4. Any claims brought under or in connection with this DPA (including the Standard Contractual Clauses) shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

13.5. No one other than a party to this DPA, its successors and permitted assignees shall have any right to enforce any of the DPA's terms, unless such right is explicitly granted under the Standard Contractual Clauses.

13.6. The parties agree that this DPA shall replace and supersede any existing DPA the parties may have previously entered into, or any security or data protection terms to which the parties may have agreed to, in connection with the Product and such previous DPA or terms (as applicable) are hereby terminated.

Exhibit 1

Data Processing Description

A. List of Parties

Data exporter:

Name	the Client executing the applicable Order Form
Address	as set forth in the Order Form or as otherwise provided to Retensa by Client
Contact person's name, position and contact details	as set forth in the Order Form or as otherwise provided to Retensa by Client
Activities relevant to the Protected Data transferred under this DPA	Retensa's Processing of Protected Data under the Agreement
Role (Controller or Processor)	Controller or Processor (as applicable)

Data importer:

Name:	the Retensa entity named on the applicable Order Form
Address:	Retensa group members' addresses are available https://retensa.com/contact/
Contact details	Ishita Arora, Product Manager: support@retensa.com
Activities relevant to the Protected Data transferred under this DPA	Retensa's Processing of Protected Data under the Agreement
Role (Controller and/or Processor)	Processor

B. Description of Transfer

Categories of Data Subjects whose Protected Data is transferred	The individuals whose Personal Data is contained in the Protected Data, to be provided to Retensa at Client's sole discretion. Such categories of Data Subjects may include, without limitation: Client's and Client's customers, prospects, business partners and vendors, and each of their employees, subcontractors, agents, advisors and any other personnel or collaborators, including any Data Subjects authorized by Client to use the Product
Categories of Protected Data transferred	Data exporter and its authorized users may submit Personal Data as part of the Protected Data, the nature of which is determined and controlled by the data exporter at its sole discretion. Such categories of Protected Data may include, without limitation: • Contact information (such as postal address, phone number, email address, etc.); • Identification information (such as name, IP address, etc.); • Employment information (such as function/title, department, organization/employer name, etc.); • Education and professional training information; • Other personal characteristics (such as professional life data,

	personal life data and location data)
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved.	The Product are made for general use and not intended for the Processing of any sensitive data, such as special categories under the EU GDPR or sensitive personal information under the CCPA (together herein, "**Sensitive Data**"). However, Client may transfer Sensitive Data to the Product, the extent of which is determined and controlled by Client at its sole discretion, provided that Client fully complies with the Data Protection Laws with respect to such transfer. Sensitive Data, if any, may include the following categories of Personal Data: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Client is solely responsible for determining and notifying Retensa (by requesting Retensa to amend this DPA) of the additional restrictions and/or security measures that are needed to be applied to the Sensitive Data transferred by Client
The frequency of the transfer	Continuous basis, depending on the use of the Product by Client
Nature of the Processing	Data analytics and such other Product pursuant to the Agreement and this DPA
Purpose(s) of the data transfer and further Processing	Retensa will Process Protected Data as necessary to perform the Product pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Client in its use of the Product, all subject to the terms of this DPA
The period for which the Protected Data will be retained, or, if that is not possible, the criteria used to determine that period	Subject to Section 12 of the DPA, Retensa will Process Protected Data for the duration of the Agreement, unless otherwise agreed upon in writing
For transfers to (sub-) processors, also specify subject matter, nature and duration of the Processing.	As per Section 6 of the DPA, Sub-Processors will process Protected Data as necessary to perform the Product pursuant to the Agreement. The subject, nature and duration of the Processing shall be as specified in this DPA and the Agreement

C. <u>Competent Supervisory Authority</u>

Identify the competent supervisory authority in accordance with Clause 13 of the EU SCCs	With respect to the Processing of Protected Data to which the EU GDPR applies, the competent supervisory authority, in accordance with Clause 13 of the EU SCCs, is either (i) the supervisory authority applicable to the data exporter in its EEA country of establishment or, (ii) where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the EU GDPR, or (iii) where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the Data Subjects relevant to the transfer are located.

	With respect to the Processing of Protected Data to which the UK GDPR applies, the competent supervisory authority is the Information Commissioner's Office (the ICO). With respect to the Processing of Protected Data to which the Swiss DPA applies, the competent supervisory authority is the FDPIC.

Exhibit 2

Technical and Organizational Measures

Description of the technical and organizational measures implemented by Retensa as per Client's instructions (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

1. For Retensa's Software as a Service (SaaS) Offering

Measures:	Description:
Measures for ensuring ongoing, confidentiality, integrity, availability and resilience of processing systems and services	Retensa has put in place an information security program to design, implement and maintain a coherent set of policies, standards, and systems to manage risks to information assets, conforming to ISO/IEC 27001:2013 and NIST frameworks. The program includes, among others: • A risk management program; • Monitoring for security incidents and maintaining a remediation plan to ensure timely fixes to discovered vulnerabilities; • A written information security policy and incident response plan that explicitly address and provide guidance to its personnel regarding the security, confidentiality, integrity, and availability of customer information; • Penetration testing performed by a qualified third-party on an annual basis; and • Having resources responsible for information security efforts.
Measures for ensuring physical security of locations at which Protected Data is Processed	• For applications hosted by Retensa we operate services via Amazon Web Product (AWS). The physical security controls related to the service have been tested by AWS in their SOC audit report, ISO 27001 certification; • Commercially reasonable steps are taken to assure facilities and equipment are physically protected from unauthorized access, damage, security threats, interference, and environmental hazards in order to prevent loss, damage or compromise of assets and interruption to business activities.
Measures for user identification and authorization	Retensa maintains authentication controls for services with industry standard security practices and maintains audit trails and logs for access in accordance with the applicable data retention periods. Access privileges are updated after any change in personnel or system and are reviewed and confirmed on a quarterly basis. In addition, Retensa has implemented the following additional controls: • Network Access Control: Retensa's internal and external networks are designed with a commitment to secure networking in mind. External connections are carefully managed; third-party network connections are established only after security due diligence has been performed; • Data Access Control: To prevent disclosure, access is granted on the basis of least privilege, need-to-have, and must-know. By role, users and their activities can be uniquely identified and segregated. Administrative privileges are restricted to those who have a legitimate need for them; • System Access Control: A formal provisioning process strictly regulates access. Information systems are password-protected and are managed and controlled by a system administrator; • Multi-factor authentication: Retensa verifies the identity and authentication of personnel with access to systems containing Protected Data and critical technology using a multi-factor authentication method or equivalent controls; • Transmission Control: When transmitting Protected Data through a public network (such as the internet) to and from an external third party, the data is encrypted or sent via a secure channel; and • Separation Control: Network services, systems, users, workstations, and servers are separated based on business purpose.

Measures for ensuring the ability to restore Protected Data in a timely manner	• Retensa has implemented availability controls to protect against the loss of data, backup and redundancy requirements are in place for critical information systems; • Retensa maintains an incident response plan with clearly defined roles and decision-making authority, as well as a logging and monitoring framework, in order to isolate and mitigate incidents; and • Retensa maintains business continuity and disaster recovery management plans, which documented strategies and procedures for analyzing the criticality of applications and/or data and recovering IT services and systems in the event of an emergency or disruption.
Measures for the protection of Protected Data during transit	Protected Data is encrypted in transit, supporting TLS 1.2+.
Measures for the protection of Protected Data at Rest	Retensa encrypts all of Protected Data and metadata at rest using an industry standard AES-256 encryption algorithm.
Measures for ensuring logging of events	Retensa ensures that the logging capabilities of its internal systems are always active and enabled. Logs must be gathered and secured against tampering. Each entry in the log should contain sufficient data for subsequent analysis and effective monitoring. In accordance with our SOC2 Type 2 compliance, all access to customer environments is logged and audited.
Measures for ensuring system configuration	All pertinent infrastructure must comply with applicable industry standards. Retensa will remove all unnecessary operating system configuration utilities and will restrict access rights to the least privilege level; and • Retensa maintains a patch management process to ensure that patches are implemented in a reasonable, risk-based timeframe. • Retensa will ensure operating systems are kept up to date with the latest updates and timely installation of security patches.
Measures IT and security governance management	• Retensa has implemented an information security program in accordance with ISO/IEC 27001:2013 to design, implement, and maintain a coherent set of policies, standards, and systems for managing risks to information assets; • Retensa has defined access roles for each system and service based on least privilege principle. Access to applicable applications is possible only via 2-factor authentication (2FA) with strong password policies; • Retensa requires that its employees use a password manager to ensure that they use unique and complex passwords and store them in a secure vault; • Retensa laptops are equipped with encryption technology that is turned on by default, along with advanced anti-malware software; • Retensa uses email protection solutions designed to prevent malware, zero-day attacks, phishing, Business Email Compromise (BEC) and spam; • Retensa employees receive mandatory data protection and cyber security awareness training as part of their onboarding, as well as ongoing training thereafter. Moreover, employees receive ongoing security education training about topics such as phishing, password management, secure development, and security best practices for operating cloud accounts; and • All vendors at Retensa are subject to risk assessment and review as part of the company's vendor management program. To ensure that data is effectively protected, the due diligence process examines security, data protection, and privacy practices. Retensa will validate their compliance, security posture, and document any shortcomings.

Measures for certification/ assurance of processes and products	• Risks related to security, compliance, and audits are managed by dedicated security personnel at Retensa, who carry out an annual internal audit to make sure our security policies are being followed. • Retensa conducts a set of independent third-party tests per year. Retensa will provide the Client with details regarding third-party tests upon request. Retensa takes timely and appropriate actions to address vulnerabilities of relevant severity that could compromise the system and data.