COMPLINITY DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms part of the Complinity's Terms of Service or other written or electronic agreement ("**Agreement**") including any written or electronic service orders, purchase orders or other order forms (each an "**Order Form**") entered into between Complinity and Customer, pursuant to which Complinity provides Services (as defined in the Agreement) to the Customer.

The purpose of this DPA is to reflect the parties' agreement about the transfer and processing of any Personal Data that is entitled to protection under the EU Data Protection Laws, while providing the Services.

This DPA will take effect on the DPA Effective Date and, notwithstanding expiry of the Term, will remain in effect until, and automatically expire upon, deletion of all Customer Data by Complinity as described in this DPA.

This DPA includes the Standard Contractual Clauses attached hereto as **Exhibit 1** along with (i) **Appendix 1** to the Standard Contractual Clauses, which includes specifics on the Personal Data transferred by the data exporter to the data importer; **Appendix 2** to the Standard Contractual Clauses, which includes a description of the technical and organizational security measures implemented by the data importer as referenced; and (iii) **Appendix 3** to the Standard Contractual Clauses, which sets forth the List of Sub-Processors.

1. DEFINITIONS

1) "**Controller**" means the Customer.
2) "**Customer Data**" means any information, data or materials received by Complinity from Customer and its end users in connection with the use of the Services
3) "Data Subject" means the natural person to whom Personal Data relates.

4) "**DPA Effective Date**" means, as applicable, (a) Aug 15, 2020 if Customer has been availing the Services prior to such date; or (b) the date from which the Customer avails the Services, if such date is on or after Aug 15, 2020.

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as transposed into domestic legislation of each Member State of the European Union, and as amended, replaced, or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR.

6) "**GDPR**" means the European Union's General Data Protection Regulation 2016/679.

7) "**Instructions**" means the written, documented instructions, issued by Controller to Processor regarding the processing of Personal Data (including, but not limited to, depersonalizing, blocking or deletion).

8) "**Personal Data**" means any information relating to an identified or identifiable natural person where such information is contained within Customer Data and is entitled to protection under the EU Data Protection Laws.

9) "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

10) "**Processing**" means any operation or set of operations which is performed on Personal Data, whether by automated 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 of Personal Data.

11) "**Processor**" means Complinity.

12) "**Standard Contractual Clauses**" means the clauses attached hereto as Exhibit 1.

13) **Terms not defined but used** herein shall have the meanings assigned to them in the Agreement or the GDPR.

2. DETAILS OF THE PROCESSING

1) **CATEGORIES OF DATA SUBJECTS.** Controller's Contacts and other end users including Controller's employees, contractors, collaborators, customers, prospects, suppliers, and subcontractors. Data Subjects also include individuals attempting to communicate with or transfer Personal Data to the Controller's end users.

2) **TYPES OF PERSONAL DATA**. Contact Information, the extent of which is determined and controlled by the Customer in its sole discretion, and other Personal Data such as navigational data (including website usage information), email data, system usage data, application integration data, and other electronic data submitted,

stored, sent, or received by end users via the Subscription Service. Customer confirms that it will not be providing sensitive or special categories of Personal Data to Complinity.

3) **SUBJECT-MATTER AND NATURE OF THE PROCESSING**. The subject-matter of Processing of Personal Data is the provision of the Services by the Processor to the Controller that involves the Processing of Personal Data. Personal Data will be subject to those Processing activities as may be specified in the Agreement and an Order Form.
4) **PURPOSE OF THE PROCESSING**. Personal Data will be Processed for purposes of providing the Services set out and otherwise agreed to in the Agreement and any applicable Order Form.
5) **DURATION OF THE PROCESSING**. Personal Data will be Processed for the duration of the Agreement, subject to Section 4 of this DPA.

3. CUSTOMER RESPONSIBILITY

1) Within the scope of the Agreement and in its use of the Services, Controller shall be solely responsible for complying with the statutory requirements relating to data protection and privacy, regarding the disclosure and transfer of Personal Data to the Processor and the Processing of Personal Data. For the avoidance of doubt, Controller's instructions for the Processing of Personal Data shall comply with all applicable laws and regulations, including the EU Data Protection Laws. Instructions shall initially be specified in the Agreement and in this DPA and may, from time to time thereafter, be amended, amplified, or replaced by Controller in separate written instructions (as individual instructions).
2) Controller shall inform Processor without undue delay and comprehensively about any errors, corrections or irregularities related to the Personal Data and statutory provisions on the Processing of Personal Data.

4. OBLIGATIONS OF PROCESSOR

1) COMPLIANCE WITH INSTRUCTIONS. The parties acknowledge and agree that Customer is the Controller of Personal Data and Complinity is the Processor of that data. Processor shall process and use the Personal Data only within the scope of Controller's Instructions. If the Processor believes that an Instruction of the Controller infringes the EU Data Protection Laws, it shall immediately inform the Controller without delay. If Processor cannot process Personal Data in accordance with the Instructions due to a legal requirement under the EU Data Protection Laws, Processor will (i) promptly notify the Controller of that legal requirement before the relevant Processing to the extent permitted by the EU Data Protection Laws; and (ii) cease all

Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as the Controller issues new Instructions with which Processor is able to comply. If this provision is invoked, Processor will not be liable to the Controller under the Agreement for any failure to perform the Services until such time as the Controller issues new Instructions regarding the Processing.

2) SECURITY. Processor shall take the appropriate technical and organizational measures to adequately protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, described under **Appendix 2** to the Standard Contractual Clauses. Such measures include, but are not be limited to:
    1. the prevention of unauthorized persons from gaining access to Personal Data Processing systems (physical access control),
    2. the prevention of Personal Data Processing systems from being used without authorization (logical access control),
    3. ensuring that persons entitled to use a Personal Data Processing system gain access only to such Personal Data as they are entitled to accessing and for the time period as required in accordance with their access rights, and that, while Processing or use and after storage, Personal Data cannot be read, copied, modified, or deleted without authorization (data access control),
    4. ensuring that Personal Data cannot be read, copied, modified, or deleted without authorization during electronic transmission, transport, or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control),
    5. ensuring the establishment of an audit trail to document whether and by whom Personal Data has been entered, modified, or removed from Personal Data Processing systems (entry control),
    6. ensuring that Personal Data is Processed solely in accordance with the Instructions (control of instructions), and
    7. ensuring that Personal Data is protected against accidental destruction or loss (availability control).

    Processor will also facilitate Controller's compliance with the Controller's obligation to implement security measures with respect to Personal Data under the EU Data Protection laws.

3) PROCESSOR shall ensure that any personnel whom Processor authorizes to process Personal Data on its behalf is subject to confidentiality obligations with respect to that

Personal Data. The undertaking to confidentiality shall continue after the termination of the Processing activities.

4) PERSONAL DATA BREACHES. Processor will notify the Controller as soon as practicable after it becomes aware of any Personal Data Breach affecting any Personal Data. At the Controller's request, Processor will promptly provide the Controller with all reasonable assistance necessary to enable the Controller to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if Controller is required to do so under the Data Protection Law. Processor shall also take necessary actions to mitigate the effects of Personal Data Breaches and prevent the recurrence of such breaches.

5) DATA SUBJECT REQUESTS. Processor will provide reasonable assistance, including by appropriate technical and organizational measures and considering the nature of the Processing, to enable Controller to respond to any request from Data Subjects seeking to exercise their rights under the EU Data Protection Laws with respect to Personal Data (including access, rectification, restriction, deletion, or portability of Personal Data, as applicable), to the extent permitted by the law. If such request is made directly to Processor, Processor will promptly inform Controller and will advise Data Subjects to submit their request to the Controller. Controller shall be solely responsible for responding to any Data Subjects' requests. Controller shall reimburse Processor for the costs arising from this assistance.

6) SUB-PROCESSORS.
    1. Processor shall be entitled to engage sub-Processors to fulfil Processor's obligations defined in the Agreement only with Controller's written consent. For these purposes, Controller consents to the engagement as sub-Processors of Processor's affiliated companies and the third parties listed in Appendix 3. For the avoidance of doubt, the above authorization constitutes Controller's prior written consent to the sub-Processing by Processor for purposes of Clause 11 of the Standard Contractual Clauses.
    2. If the Processor intends to instruct sub-Processors other than its affiliates or the companies listed in Appendix 3, the Processor will notify the Controller thereof in writing (email to the email address(es) on record in Processor's account information for Controller is sufficient) and will give the Controller the opportunity to object to the engagement of the new sub-Processors within 30 days after being notified. The objection must be based on reasonable grounds (e.g., if the Controller proves that significant risks for the protection of its Personal Data exist at the sub-Processor). If the Processor and Controller are unable to resolve such objection, either party may terminate the Agreement by providing written notice to the other party.

3. Where Processor engages sub-Processors, Processor will enter a contract with the sub-Processor that imposes on the sub-Processor the same obligations that apply to Processor under this DPA. Where the sub-Processor fails to fulfil its data protection obligations, Processor will remain liable to the Controller for the performance of such sub-Processor's obligations.
4. Where a sub-Processor is engaged, the Controller must be granted the right to monitor and inspect the sub-Processor's activities in accordance with this DPA and the EU Data Protection Laws, including to obtain information from the Processor, upon written request, on the substance of the contract and the implementation of the data protection obligations under the sub-Processing contract, where necessary by inspecting the relevant contract documents.
5. The provisions of this Section 4 (f)shall apply if the Processor engages a sub-Processor in a country outside the European Economic Area ("EEA") not recognized by the European Commission as providing an adequate level of protection for Processing of Personal Data or to an entity not registered under the EU-US Privacy Shield framework. If, in the performance of this DPA, Complinity transfers any Personal Data to a sub-Processor located outside of the EEA, Complinity shall, in advance of any such transfer, ensure that requisite safeguards are in place in respect of that Processing.

7) DATA TRANSFERS. Controller acknowledges and agrees that, in connection with the performance of the Services, Personal Data will be transferred to Complinity servers outside the EEA. The Standard Contractual Clauses at Exhibit 1 will apply with respect to Personal Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the EU Data Protection Laws) or to an entity not registered under the EU-US Privacy Shield framework.

8) DELETION OR RETRIEVAL OF PERSONAL DATA.

1. Other than to the extent required to comply with EU Data Protection Laws or any other laws to which the Processor is subject, Processor will delete all Personal Data (including copies thereof) processed pursuant to this DPA upon completion of a period of 30 (thirty) days following termination or expiry of the Agreement. If Processor is unable to delete Personal Data for technical or other reasons, Processor will apply measures to ensure that Personal Data is blocked from any further Processing.
2. Controller shall, upon termination or expiration of the Agreement and by way of issuing an Instruction, stipulate, within the aforesaid period of 30 (thirty) days, reasonable measures to return Personal Data or to delete stored Personal Data.

Any additional cost arising in connection with the return or deletion of Personal Data after the termination or expiration of the Agreement shall be borne by Controller.

5. AUDITS

1. Controller may, prior to the commencement of Processing, and at regular intervals thereafter, audit the technical and organizational measures taken by Processor. The cost associated with such audit, including cost of professional services from any third party, will be completely borne by the Controller. For such purpose, Controller may, e.g.,
   - obtain information from the Processor;
   - request Processor to submit to Controller an existing attestation or certificate by an independent professional expert; or
   - upon reasonable and timely advance agreement, during regular business hours and without interrupting Processor's business operations, conduct an on-site inspection of Processor's business operations or have the same conducted by a qualified third party which shall not be a competitor of Processor.
2. Processor shall, upon Controller's written request and within a reasonable period, provide Controller with all information necessary for such audit, to the extent that such information is within Processor's control and Processor is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party.

6. INDEMNIFICATION

1. Controller shall defend, indemnify and hold Complinity harmless against any claims, losses, damage, liabilities, expenses and costs (including reasonable attorneys' fees), including against any claims by Data Subjects or actions by supervisory authorities under the EU Data Protection Laws, that Processor may incur or be subject to in relation to the Processing of Personal Data (i) so long as Processor is Processing the Personal Data as per the Instructions received; or (ii) where such claims, losses, damage, liabilities, expenses and costs have arisen due to Controller's breach of EU Data Protection Laws.

7. GENERAL PROVISIONS

1. General provisions of the Agreement shall, in so far as they are not inconsistent herewith, apply to this DPA.
2. In case of any conflict between the terms of this DPA and the Agreement, the terms of this DPA shall take precedence in so far as the subject matter to which it relates. Where individual provisions of this DPA are invalid or unenforceable, the validity and enforceability of the other provisions of this DPA shall not be affected.

8. OTHERS

1. The organization ensures that the contract to process PII addresses the organization's role in aiding with the customer's obligations.
2. The Agreement considers following and follows:
    1) Privacy by Design and default
    2) Achieving Security of Processing
    3) Notification of breaches involving PII to a Supervisory authority
    4) Notification of breaches involving PII to Customers and PII Principals
    5) Conducting Privacy Impact Assessment
    6) Assurance of Assistance by the PII Processors if prior consultations with relevant PII Protection authorities are needed.
    7) Complinity Technologies Pvt Ltd shall inform the customer if in its opinion a processing instruction infringes applicable legislation or regulation.
    8) The organization does not use PII processed under a contract for the purposes of Marketing and Advertising
    9) Coordinate with Clients for helping Audit the systems. The organization provides the customer with the appropriate information so that it can demonstrate compliance with their obligations
    10) Complinity Technologies Pvt Ltd shall use AWS and PIPL as sub processors with Security and Privacy requirements full filled.
    11) The organization shall comply with all statutory and regulatory requirements, ISO 27001:2013, ISO 27701:2019 and EU GDPR requirements.
    12) The Data shall be deleted or de-identified after the processing is complete (This is after the retention period selected is complete).
    13) Complinity Technologies Pvt Ltd shall inform 24 hours in advance to clients in case of any legally binding requests for disclosure of PII.
    14) For Access, Correction and/or Erasure of PII of Data subjects can be done by contacting the Data Protection Officer (DPO) below. Also, for raising concerns and/or any complaints related with PII that can be done by contacting the Data Protection Officer below:

        Name: Neera Singh

        Email ID: neera.singh@complinity.com

        Contact Number: 8800499040

EXHIBIT 1

Standard Contractual Clauses (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,

The Customer, as defined in the Complinity Customer Terms of Service (the "data exporter") with details as follows:

Name of the data exporting organization:

Customer's Name and Address, as set out in the Order Form

And

Name of the data importing organisation;

each a 'party;' together '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.

1. DEFINITIONS

For the purposes of the Clauses:

1. 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have 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;
2. 'the data exporter' means the controller who transfers the personal data;

3. ‘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;
4. ‘the sub-processor’ means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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;
5. ‘the applicable data protection law’ means the legislation 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;
6. ‘technical and organizational security measures’ means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. DETAILS OF THE TRANSFER

1. Complinity Technologies Pvt Ltd is certified to Information Security Management as per ISO 27001:2013. Complinity Technologies Pvt Ltd shall notify Client in writing without undue delay if it can no longer comply with its obligations under the Privacy compliance, and, in such a case, Complinity Technologies Pvt Ltd will have the option of (i) promptly taking reasonable steps to remediate any non-compliance with applicable obligations under this Addendum, or (ii) engaging in a good faith dialogue with Client to determine a new data transfer mechanism to carry out the purposes of the Terms. Complinity Technologies Pvt Ltd acts as a Processor with respect to Personal Data received pursuant to a data transfer.
2. In the event the Privacy Compliance is invalidated, Client and each Client Affiliate (on behalf of the relevant Controller(s), as the case may be), if applicable (as "data exporter") and Complinity Technologies Pvt Ltd (as "data importer"), with effect from the commencement of the relevant transfer, shall enter into the Controller to Processor SCCs (mutatis mutandis, as the case may be) in respect of any transfer (or onward transfer) from Client or Client Affiliate to Complinity Technologies Pvt Ltd, where such transfer would otherwise be prohibited by applicable Data Protection Laws or by the terms of data transfer agreements put in place to address applicable Data Protection Laws.
3. 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.

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 sub-processor 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 sub-processor 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.

4. OBLIGATIONS OF THE DATA EXPORTER

The data exporter agrees and warrants:

1. that the processing, including the Appendix 1 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;
2. 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;
3. that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;

4. 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, unauthorized 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;
5. that it will ensure compliance with the security measures;
6. 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;
7. to forward any notification received from the data importer or any sub-processor 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;
8. to make available to the data subjects upon request a copy of the Clauses, except for Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing 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;
9. that in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor 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
10. that it will ensure compliance with Clause 4(a) to (i).

5. OBLIGATIONS OF THE DATA IMPORTER

The data importer agrees and warrants:

1. 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;
2. 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;

3. that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;
4. that it will promptly notify the data exporter about:
    1. 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;
    2. any accidental or unauthorized access; and
    3. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;
5. 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 regarding the processing of the data transferred;
6. 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;
7. to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, except for 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;
8. that in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
9. that the processing services by the sub-processor will be carried out in accordance with Clause 11;
10. to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

7. MEDIATION AND JURISDICTION

1. The data importer agrees that if the data subject invokes against its third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
    1. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
    2. 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 national or international law.

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 sub-processor, 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 sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

9. GOVERNING LAW

1. The Clauses shall be governed by the law of the Member State in which the data exporter is established.

10. VARIATION OF THE CONTRACT

1. 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 if they do not contradict the 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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor 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 sub-processor ’s obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor 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 law 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 sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing 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 sub-processing 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.

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 sub-processor 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 sub-processor 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 Standard Contractual Clauses

This Appendix forms part of the Clauses. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

1. **Data exporter**

The data exporter is the Customer, as defined in the Complinity Customer Terms of Service ("**Agreement**").

2. **Data importer**

The data importer is Complinity – India's Leading Compliance Software

3. **Data subjects**

Categories of data subjects set out under Section 2 of the Data Processing Addendum to which the Clauses are attached.

4. **Categories of data**

Categories of personal data set out under Section 2 of the Data Processing Addendum to which the Clauses are attached.

5. **Special categories of data (if appropriate)**

The parties do not anticipate the transfer of special categories of data.

6. **Processing operations**

The processing activities set out under Section 2 of the Data Processing Addendum to which the Clauses are attached.

Appendix 2 to the Standard Contractual Clauses (Technical and Organizational Security Measures)

This Appendix forms part of the Clauses.

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):

Complinity currently observes the security practices described in this Appendix 2. Notwithstanding any provision to the contrary otherwise agreed to by data exporter, Complinity may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Agreement.

a) Access Control

- Preventing Unauthorized Product Access Outsourced processing: Complinity hosts its Services with outsourced cloud infrastructure providers. Additionally, Complinity maintains contractual relationships with vendors in order to provide the Services in accordance with our Data Processing Addendums. Complinity relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors. Physical and environmental

security: Complinity hosts its product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are aligned with SOC 2 Type II and ISO 27001, among other standards. Authentication: Complinity implements a uniform password policy for its customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public Customer Data. Authorization: Customer data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of Complinity's products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set. Application Programming Interface (API) access: Public product APIs may be accessed over secured socket layer (SSL) or Transport Layered Security (TLS) based HTTPS using and security API key only.

- Preventing Unauthorized Product Use

Complinity implements industry standard access controls and detection capabilities for the internal networks that support its products. Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules. Intrusion detection and prevention: As part of its commitment to protecting customer data and websites, access to Complinity is aligned with best practice guidelines documented by the Open Web Application Security Project (OWASP) in the OWASP Top 10 and similar recommendations. Protections from Distributed Denial of Service (DDoS) attacks are also incorporated, helping to ensure that customers' sites and other parts of the Complinity products are available continuously. Complinity is configured with a combination of industry standard and custom rules that are capable of automatically enabling and disabling appropriate controls to best protect our customers. We employ tools that actively monitor real-time traffic at the application layer with ability to alert or deny malicious behaviour based on behaviour type and rate. Static code analysis: Security reviews of code stored in Complinity's source code repositories is performed, checking for coding best practices and identifiable software flaws. Penetration testing: Complinity maintains relationships with industry recognized penetration testing service providers for penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

- Limitations of Privilege & Authorization Requirements Product access: A subset of Complinity's employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through "just in time" requests for access; all such requests are logged. Background checks: All Complinity employees undergo a third-party background check prior to being extended an employment offer, in accordance with the applicable laws. All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

b) Transmission Control

In-transit: Complinity makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces. Complinity's HTTPS implementation uses industry standard algorithms and certificates.

All sensitive interactions with the Complinity products (e.g., API calls, login, authenticated sessions to the customer's portal, etc.) are encrypted in-transit with TLS 1.2.

Certain information is encrypted or hashed at rest, based on the sensitivity of the information. For instance, user passwords are hashed. Contact Data like Lead information is encrypted at rest. Other information, like public web content, images, documents are not encrypted at rest.

c) Input Control

Detection: Complinity designed its infrastructure to log extensive information about the system behaviour, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Complinity personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: Complinity maintain a security incident response and tracking mechanism. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, Complinity will take appropriate steps to minimize product and Customer damage or unauthorized disclosure.

Communication: If Complinity becomes aware of unlawful access to customer data stored within its products, Complinity will: 1) notify the affected customers of the incident; 2) provide a description of the steps Complinity is taking to resolve the incident; and 3) provide status updates to the Customer contact, as Complinity deems necessary. Notification(s) of incidents, if any, will be delivered to one or more of the Customer's contacts in a form Complinity selects, which may include via email or telephone.

d) Availability Control

Complinity maintains business continuity and disaster recovery plans focusing both on preventing outage through redundancy of telecommunications, systems, and business operations, and on rapid recovery strategies in the event of an availability or performance issue. Whenever customer-impacting situations occur, Complinity's goal is to quickly and transparently isolate and address the issue. Identified issues are published on Complinity's status site and are subsequently updated until the issue is resolved.

Business continuity testing is part of Complinity normal processing. Complinity recovery processes are validated continuously through normal maintenance and support processes. We follow continuous deployment principles and create or destroy many server instances as part of our regular daily maintenance and growth. We also use those procedures to recover from impaired instances and other failures, allowing us to practice our recovery process every day.

Complinity primarily relies on infrastructure redundancy, real time replication and backups. All Complinity product services are built with full redundancy. Server infrastructure is strategically distributed across 2 distinct availability zones within our data centre provider.

Complinity ensures data is replicated and backed up in multiple durable data-stores. The retention period of backups depends on the nature of the data. Data is also replicated across data-centre availability zones in order to provide fault-tolerance within an availability zone as well as scalability and responsive recovery, when necessary. In addition, the following policies have been implemented and enforced for data resilience:

- Customer (production) data is backed up leveraging multiple online replicas of data for immediate data protection. All production databases have no less than 1

primary (master) and 1 replica (slave) copy of the data live at any given point in time. Ten days' worth of backups are kept for any database in a way that ensures restoration can occur easily.

- Because we leverage private cloud services for hosting, backup, and recovery, Complinity does not implement physical infrastructure or physical storage media within its products. Complinity does also not generally produce or use other kinds of hard copy media (e.g., paper, tape, etc.) as part of making our products available to our customers.
- By default, all backups will be protected through access control restrictions on Complinity product infrastructure networks, access control lists on the file systems storing the backup files and/or through database security protections.

Appendix 3 to the Standard Contractual Clauses (List of Sub-Processor)

- Amazon Web Services, Inc.
- Complinity
- Google LLC
- CloudThat