Intentive Technologies Pvt Ltd
IndiQube Octagon, Site No. 643,
80 Feet Road, 4th Block,
Koramangala, Bangalore, KA,
India, 560034
www.kommunicate.io

Note: Kommunicate (www.kommunicate.io) is a product from Intentive Technologies Pvt Ltd. Kommunicate adheres to Intentive DPA and its terms of service.

This Intentive Data Processing Agreement ("DPA"), that includes the Standard Contractual Clauses adopted by the European Commission, as applicable, reflects the parties' agreement with respect to the terms governing the Processing of Personal Data under the Intentive Customer Terms of Service (the "Agreement"). This DPA is an amendment to the Agreement and is effective upon its incorporation into the Agreement, which incorporation may be specified in the Agreement, an Order or an executed amendment to the Agreement. Upon its incorporation into the Agreement, the DPA will form a part of the Agreement.

The term of this DPA shall follow the term of the Agreement. Terms not otherwise defined herein shall have the meaning as set forth in the Agreement.

THIS DPA INCLUDES:

(i) Standard Contractual Clauses, attached hereto as EXHIBIT 1.

(a) Annex I to the Standard Contractual Clauses, which includes specifics on the Personal Data transferred by the data exporter to the data importer.

(b) Annex II to the Standard Contractual Clauses, which includes a description of the technical and organizational security measures implemented by the data importer as referenced.

(ii) List of Sub-Processors, attached hereto as Annex III.

1. Definitions

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"Data Protection Law" means all applicable legislation relating to data protection and privacy including without limitation the the GDPR, supplementary laws and regulations to the GDPR and

rules, regulations and binding decisions adopted by competent data protection supervisory authority, together with any national implementing laws in any Member State of the European Union or, to the extent applicable, in any other country, as amended, repealed, consolidated or replaced from time to time. The terms “process”, “processes” and “processed” will be construed accordingly.

“Data Subject” means the individual to whom Personal Data relates.

“GDPR” means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

“Instruction” means the written, documented instruction, issued by Controller to Processor, and directing the same to perform a specific action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).

“Personal Data” means any information relating to an identified or identifiable individual where such information is contained within Customer Data and is protected similarly as personal data or personally identifiable information under applicable Data Protection Law

“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.

“Processing” means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data.

“Processor” means a natural or legal person, public authority, agency or other body that processes Personal Data on behalf of the Controller.

“Standard Contractual Clauses” means the clauses attached hereto as Exhibit 1, set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Intentive Technologies Pvt Ltd
IndiQube Octagon, Site No. 643,
80 Feet Road, 4th Block,
Koramangala, Bangalore, KA,
India, 560034
www.kommunicate.io

2. Details of the Processing

a. 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.

b. 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.

c. Subject-Matter and Nature of the Processing. The subject-matter of Processing of Personal Data by Processor is the provision of the services 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.

d. 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.

e. 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

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, in particular 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 the Data Protection Law. Customer has legally the possibility to give instructions at any time during the term subject to mutual agreement of both Controllers and Processors. Instructions shall initially be specified in the Agreement and may, from time to time thereafter, be amended, amplified or replaced by Controller in separate written instructions (as individual instructions).

Controller shall inform Processor without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the Processing of Personal Data.

4. Obligations of Processor

a. Compliance with Instructions. The parties acknowledge and agree that Customer is the Controller of Personal Data and Intentive is the Processor of that data. Processor shall collect, process and use Personal Data only within the scope of Controller's Instructions. If the Processor believes that an Instruction of the Controller infringes the Data Protection Law, 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 any applicable European Union or Member State law, Processor will (i) promptly notify the Controller of that legal requirement before the relevant Processing to the extent permitted by the Data Protection Law; 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. (iii) Customer bears sole responsibility for assessment of legal admissibility of the instruction and the processing of personal data carried out by the contractor in the context of the contract, with respect to the applicable provisions of Data Protection Act.

If this provision is invoked, the Processor will not be liable to the Controller under the Agreement for any failure to perform the applicable services until such time as the Controller issues new instructions in regard to the Processing.

b. Security. The Processor shall take the appropriate technical and organizational measures to adequately protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data, described under Annex II to the Standard Contractual Clauses. Such measures include, but are not be limited to:

i. the prevention of unauthorized persons from gaining access to Personal Data Processing systems (physical access control),

ii. the prevention of Personal Data Processing systems from being used without authorization (logical access control),

iii. ensuring that persons entitled to use a Personal Data Processing system gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and

Intentive Technologies Pvt Ltd
IndiQube Octagon, Site No. 643,
80 Feet Road, 4th Block,
Koramangala, Bangalore, KA,
India, 560034
www.kommunicate.io

that, in the course of Processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization (data access control),

iv. 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),

v. ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from Personal Data Processing systems (entry control),

vi. ensuring that Personal Data is Processed solely in accordance with the Instructions (control of instructions),

vii. ensuring that Personal Data is protected against accidental destruction or loss (availability control).

Upon Controller's request, Processor may provide a current Personal Data protection and security programme relating to the Processing hereunder.

Processor will facilitate Controller's compliance with the Controller's obligation to implement security measures with respect to Personal Data (including if applicable Controller's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR), by (i) implementing and maintaining the security measures described under Annex II, (ii) complying with the terms of Section 4.4 (Personal Data Breaches); and (iii) providing the Controller with information in relation to the Processing in accordance with Section 5 (Audits).

c. Confidentiality. 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 above-entitled activities.

d. Personal Data Breaches. Processor will notify the Controller without undue delay 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.

e. Data Subject Requests. Processor will provide reasonable assistance, including by appropriate technical and organizational measures and taking into account the nature of the Processing, to enable Controller to respond to any request from Data Subjects seeking to exercise their rights under the Data Protection Law 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 a request is made directly to the Processor, Processor will promptly inform the 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.

f. Sub-Processors. 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 Annex III.

If the Processor intends to instruct sub-Processors other than the companies listed in Annex III, 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. If the Processor and Controller are unable to resolve such an objection, either party may terminate the Agreement by providing written notice to the other party. The Controller shall receive a refund of any prepaid but unused fees for the period following the effective date of termination.

Where Processor engages sub-Processors, Processor will enter into 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-Processors obligations.

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 Data Protection Law, 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.

The provisions of this Section 4.6 shall mutually 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 personal data. If, in the performance of this DPA, Intentive transfers any Personal Data to a sub-processor located outside of the EEA, Intentive shall, in advance of any such transfer, ensure that a legal mechanism to achieve adequacy in respect of that processing is in place.

g. Data Transfers. Controller acknowledges and agrees that, in connection with the performance of the services under the Agreement, Personal Data will be transferred to Intentive. in the United States. 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 Data Protection Law).

h. Deletion or Retrieval of Personal Data. Other than to the extent required to comply with Data Protection Law, following termination or expiry of the Agreement, Processor will delete all Personal Data (including copies thereof) processed pursuant to this DPA. 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.

Controller shall, upon termination or expiration of the Agreement and by way of issuing an Instruction, stipulate, within a period of time set by Processor, the reasonable measures to return data or to delete stored 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

Controller may, prior to the commencement of Processing, and at regular intervals thereafter, audit the technical and organizational measures taken by Processor.

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.

Processor shall, upon Controller's written request and within a reasonable period of time, 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. General Provisions

With respect to updates and changes to this DPA, the terms that apply in the "Amendment; No Waiver" section of "Miscellaneous" in the Agreement shall apply.

In case of any conflict, this DPA shall take precedence over the regulations of the Agreement. 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.

Upon the incorporation of this DPA into the Agreement, the parties indicated in Section 7 below (Parties to this DPA) are agreeing to the Standard Contractual Clauses (where and as applicable) and all appendixes attached thereto. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses in Exhibit 1, the Standard Contractual Clauses shall prevail.

Effective 25 May 2018 Intentive will process Personal Data in accordance with the GDPR requirements contained herein which are directly applicable to Intentive's provision of the Subscription Services.

7. Parties to this DPA

This DPA is an amendment to and forms part of the Agreement. Upon the incorporation of this DPA into the Agreement (i) Controller and the Intentive entity that are each a party to the Agreement are also each a party to this DPA,

The legal entity agreeing to this DPA as Controller represents that it is authorized to agree to and enter into this DPA for, and is agreeing to this DPA solely on behalf of, the Controller.

Intentive Technologies Pvt Ltd
IndiQube Octagon, Site No. 643,
80 Feet Road, 4th Block,
Koramangala, Bangalore, KA,
India, 560034
www.kommunicate.io

EXHIBIT 1

SECTION I

Clause 1

Purpose and scope

a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of personal data to a third country.

b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

c) These Clauses apply with respect to the transfer of personal data specified in Annex I.B.

d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU)

2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 13;

(iv) Clause 15.1(c), (d) and (e);

(v) Clause 16(e);

(vi) Clause 18.

b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

Intentive Technologies Pvt Ltd
IndiQube Octagon, Site No. 643,
80 Feet Road, 4th Block,
Koramangala, Bangalore, KA,
India, 560034
www.kommunicate.io

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

Intentive Technologies Pvt Ltd
IndiQube Octagon, Site No. 643,
80 Feet Road, 4th Block,
Koramangala, Bangalore, KA,
India, 560034
www.kommunicate.io

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data

importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

Intentive Technologies Pvt Ltd
IndiQube Octagon, Site No. 643,
80 Feet Road, 4th Block,
Koramangala, Bangalore, KA,
India, 560034
www.kommunicate.io

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45

Intentive Technologies Pvt Ltd
IndiQube Octagon, Site No. 643,
80 Feet Road, 4th Block,
Koramangala, Bangalore, KA,
India, 560034
www.kommunicate.io

of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent

Intentive Technologies Pvt Ltd
IndiQube Octagon, Site No. 643,
80 Feet Road, 4th Block,
Koramangala, Bangalore, KA,
India, 560034
www.kommunicate.io

necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract

(e) The data importer shall agree a third-party beneficiary clause with the sub- processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub- processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

Intentive Technologies Pvt Ltd
IndiQube Octagon, Site No. 643,
80 Feet Road, 4th Block,
Koramangala, Bangalore, KA,
India, 560034
www.kommunicate.io

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages

the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without

however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III - LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended

Intentive Technologies Pvt Ltd
IndiQube Octagon, Site No. 643,
80 Feet Road, 4th Block,
Koramangala, Bangalore, KA,
India, 560034
www.kommunicate.io

onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation.

Intentive Technologies Pvt Ltd
IndiQube Octagon, Site No. 643,
80 Feet Road, 4th Block,
Koramangala, Bangalore, KA,
India, 560034
www.kommunicate.io

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority,including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

Intentive Technologies Pvt Ltd
IndiQube Octagon, Site No. 643,
80 Feet Road, 4th Block,
Koramangala, Bangalore, KA,
India, 560034
www.kommunicate.io

15.2 Review of legality and data minimization

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

Intentive Technologies Pvt Ltd
IndiQube Octagon, Site No. 643,
80 Feet Road, 4th Block,
Koramangala, Bangalore, KA,
India, 560034
www.kommunicate.io

(i) The data exporter shall be entitled to terminate the contract,insofar as it concerns the processing of personal data under these Clauses, where:

(ii) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(iii) the data importer is in substantial or persistent breach of these Clauses; or

(iv)the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(c) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(d) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Intentive Technologies Pvt Ltd
IndiQube Octagon, Site No. 643,
80 Feet Road, 4th Block,
Koramangala, Bangalore, KA,
India, 560034
www.kommunicate.io

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Federal Republic of Germany.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Berlin, Federal Republic of Germany.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX to the Standard Contractual Clauses

ANNEX I

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.

A. LIST OF PARTIES

Data exporter:

Name: As specified in the Agreement Or Order details if any.

Address: As specified in Agreement Or Specified in Order details if Any.

Contact person's name, position and contact details: As specified in the Agreement Or Order details if any.

Activities relevant to the data transferred under these Clauses: As described under Section B.

Role (controller/processor): Controller

Data importer:

Name: **Intentive Technologies Pvt Ltd.**

Address: IndiQube Octagon, Site No. 643, 80 Feet Road, 4th Block, Koramangala, Bangalore, KA, India, 560034

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

Activities relevant to the data transferred under these Clauses: As described under Section B.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: As described in section 2.a (Refer: "Details of the Processing")

Categories of personal data transferred: As described in section 2.b ((Refer: "Details of the Processing")

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

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

Nature of the processing: As described in section 2.c (Refer: "Details of the

Processing")

Purpose(s) of the data transfer and further processing: As described in section 2.c (Refer: "Details of the Processing")

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: we keep and process the personal data on behalf of the data exporter for as long as they remain a client. When the data exporter terminates its use of the Services, we delete their user/client data within 60 days of the account/subscription termination.

For transfers to sub-processors, also specify subject matter, nature and duration of the processing: we appoint sub-processors in order to facilitate the delivery of our products/Services and to help us to maintain Services effectively and efficiently. The subject matter pertains mainly to new features/tools that we add to our Services in order to develop its functionality. The nature of the processing relates to facilitating usage of our Services, such as but not limited to facilitating document storage, email services, community forum platform.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Notwithstanding any provision to the contrary otherwise agreed to by data exporter, Intentive 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
i) Preventing Unauthorized Product Access

Intentive Technologies Pvt Ltd
IndiQube Octagon, Site No. 643,
80 Feet Road, 4th Block,
Koramangala, Bangalore, KA,
India, 560034
www.kommunicate.io

Outsourced processing: Intentive hosts its Service with outsourced cloud infrastructure providers. Additionally, Intentive maintains contractual relationships with vendors in order to provide the Service in accordance with our Data Processing Agreement. Intentive 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: Intentive hosts its product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are internally audited targeting SOC 2 Type II, among other certifications.

Authentication: Intentive implemented 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 Intentive'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 using an API key or through Oauth authorization.

ii) Preventing Unauthorized Product Use

Intentive 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: Intentive implemented a Web Application Firewall (WAF)

Intentive Technologies Pvt Ltd
IndiQube Octagon, Site No. 643,
80 Feet Road, 4th Block,
Koramangala, Bangalore, KA,
India, 560034
www.kommunicate.io

solution to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

Static code analysis: Security reviews of code stored in Intentive's source code repositories is performed, checking for coding best practices and identifiable software flaws.

Penetration testing: Intentive maintains relationships with industry recognized penetration testing service providers for four annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

iii) Limitations of Privilege & Authorization Requirements

Product access: A subset of Intentive'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. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Employee roles are reviewed at least once every six months.

Background checks: All Intentive 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: Intentive makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces and for free on every customer site hosted on the Intentive products. Intentive's HTTPS implementation uses industry standard algorithms and certificates.

At-rest: Intentive stores user passwords following policies that follow industry standard practices for security. With effect 25 May 2018, Intentive has implemented technologies to ensure that stored data is encrypted at rest. Please note that data encryption at rest comes with a dedicated server option only which carries an extra cost over your subscription.

Intentive Technologies Pvt Ltd
IndiQube Octagon, Site No. 643,
80 Feet Road, 4th Block,
Koramangala, Bangalore, KA,
India, 560034
www.kommunicate.io

c) Input Control

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

Response and tracking: Intentive maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. 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, Intentive will take appropriate steps to minimize product and Customer damage or unauthorized disclosure.

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

d) Availability Control

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones.

Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standard methods.

Intentive Technologies Pvt Ltd
IndiQube Octagon, Site No. 643,
80 Feet Road, 4th Block,
Koramangala, Bangalore, KA,
India, 560034
www.kommunicate.io

Intentive's products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists Intentive operations in maintaining and updating the product applications and backend while limiting downtime.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorized the use of the following sub-processors:

1. Amazon Web Services, Inc.
2. Google, Inc.
3. Cloudflare, Inc.
4. Twilio, Inc.
5. Sendy, Inc.
6. Segment.io, Inc. (Does not have access to end-user data)
7. ActiveCampaign, LLC. (Does not have access to end-user data)
8. UserPilot, Inc. (Does not have access to end-user data)
9. Mixpanel, Inc. (Does not have access to end-user data)
10. Intentive
11. Appmessage
12. Kommunicate

Any other wholly-owned Intentive subsidiary organizations

Intentive Technologies Pvt Ltd
IndiQube Octagon, Site No. 643,
80 Feet Road, 4th Block,
Koramangala, Bangalore, KA,
India, 560034
www.kommunicate.io

Intentive Technologies Pvt Ltd

Name: Adarsh Kumar

Designation: CTO

Contact: support@kommunicate.io

Date:

Authorized Signatory

Customer's Information:

Name:

Designation:

Contact Information:

Date:

Signatory Intentive Customer