DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is entered between MoEngage (including its Affiliates) and Customer and its Affiliates to enable MoEngage to process the Customer Personal Data as per the Applicable Data Privacy Laws while providing Services to the Customer ("Services"). The DPA shall form an integral part of the Agreement and shall come into effect on the same date as the Agreement.

In the course of providing the Services to Customer pursuant to the Agreement, MoEngage may Process Personal Data on behalf of Customer, and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

DATA PROCESSING TERMS

1. DEFINITIONS

1.1 **"Affiliate"** means any legal entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.2 **"Authorized Affiliate"** means any of Customer's Affiliate(s) which (i) is subject to the data protection laws and regulations and (ii) is permitted to use the Services pursuant to the Agreement between Customer and MoEngage.

1.3 **"Data Controller"** means the Customer who determines the purposes and means of the Processing of Personal Data.

1.4 **"Customer Personal Data"** means any Personal Data that the Customer shares with or permits MoEngage to access, store, host, share, delete and Process for the performance of the Services which includes all electronic data or information submitted by or on behalf of Customer to, or collected from the Customer by MoEngage.

1.5 **"End Users/Consumer"** means any end user of the Customers mobile applications or websites or offline channels such as physical stores to whom the Customer sends any communication through the Platform.

1.6 **"Data Protection Laws and Regulations"** means all data protection laws and regulations, which includes US federal and state privacy laws, EU Data Protection Laws and any other laws pertaining to data protection in any territory of the world that may be applicable to the Processing of Personal Data under the Agreement.

1.7 **"Data Subject"** means the identified or identifiable natural person to whom Personal Data relates to.

1.8 **"Equivalent Protection Area"** means the area that comprises (a) countries within the European Union, including Iceland, Liechtenstein, and Norway, and (b) countries that the European Commission may from time to time recognize as ensuring an adequate level of protection as provided for in article 45 of the GDPR, which includes Switzerland and the United Kingdom.

1.9 **"Processing"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by

transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.10 **"Data Processor"** means the entity which Processes Personal Data on behalf of the Controller.

1.11 **"Data Breach"** means a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, transmitted, stored or otherwise Processed by MoEngage or its Sub-processors of which MoEngage becomes aware.

1.12 **"Standard Contractual Clauses"** or **"SCC"** means the contractual clauses set out in Annex 1 to this DPA pursuant to the European Commission's decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the transfer of Personal Data to Processors established in third party countries which do not ensure an adequate level of protection, and any further approved set of contractual clauses as approved by the competent authority from time to time.

1.13 **"Sub-processor"** means any Processor engaged by MoEngage or its Affiliates engaged in the Processing of Personal Data.

1.14 **"Services"** shall mean services provided to the Customer under the Agreement.

1.15 **"EEA"** means European Economic Area.

1.16 **"Transfer"** means any Processing, which includes accessing, sharing, disclosing or otherwise making Personal Data available, whether by a MoEngage affiliate, its suppliers or the Customer, from another location than where the Processing initially occurs, which includes:)

i) any transfer of Customer Personal Data from the Customer to MoEngage and/ or a MoEngage Affiliate;

ii) an onward transfer of Customer Personal Data from MoEngage to a MoEngage Affiliate; or

iii) an onward transfer of Customer Personal Data from MoEngage and/ or a MoEngage Affiliate to another Sub-Processor,

in each case, where such Transfer would be prohibited by Applicable Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of appropriate safeguards and any lawful mechanisms for such Transfers, which includes the use of Standard Contractual Clauses.

2. PROCESSING OF PERSONAL DATA

1.1 **Details of the Processing.** The parties acknowledge and agree that with regard to the Processing of Customer Personal Data, Customer is the Data Controller, MoEngage is the Data Processor and that MoEngage or its Affiliates engaged in the Processing of Customer Personal Data will engage Sub-processors pursuant to the requirements set forth in Section 6 "Sub-processors" below. The subject-matter of Processing of Personal Data by MoEngage is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 3 (Details of the Processing) to this DPA.

1.2 **Customer's Processing of Customer Personal Data.** Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions for the Processing of Customer Personal Data shall comply with Data Protection Laws and Regulations. This DPA and the Agreement are, Customer's complete and final documented instructions to MoEngage

for the Processing of Customer Personal Data, and Customer's configuration of the Services shall constitute an additional instruction to MoEngage. Any additional or alternate instructions must be agreed upon separately. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired the Customer Personal Data. The Customer represents and warrants that it has undertaken to provide all necessary notices to Data Subjects and received all necessary permissions and consents, as required for MoEngage to Process the Customer Personal Data under this DPA and pursuant to the Applicable Data Protection Laws in their respective country and state (if applicable).

1.3 **MoEngage's Processing of Customer Personal Data.** MoEngage shall treat Personal Data as Confidential Information and shall only Process Customer Personal Data on behalf of Customer and in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement; (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement. MoEngage will Process Customer Personal Data in compliance with applicable Data Protection Laws and Regulations, provided however that MoEngage shall not be in violation of this contractual obligation in the event that MoEngage's Processing of Customer Personal Data is not-compliant with applicable Data Protection Laws and Regulations due to the Customer.

3. RESPONSIBILITIES OF CUSTOMER

2.1 The Customer:

i) instructs MoEngage and each MoEngage Affiliate (and authorises MoEngage and each MoEngage Affiliate to instruct each Subprocessor) to:

a) Process Customer Personal Data; and

b) in particular, transfer Customer Personal Data to any country or territory, as reasonably necessary for the provision of the Services and consistent with the Agreement;

ii) warrants and represents that it is and will at all relevant times remain duly and effectively authorized to give the instruction set out in section 3.1; and

iii) warrants and represents that it has complied with all the obligations that it has under the Applicable Data Protection Laws with respect to its being the Data Controller of Customer Personal Data. The Customer further represents and warrants that it has collected the Customer Personal Data in accordance with Applicable Data Protection Laws and has provided all the necessary notices and received all necessary permissions and consents.

2.2 Customer's instructions to MoEngage and each MoEngage Affiliate for the Processing of Customer Personal Data shall comply with Applicable Data Protection Laws. Customer shall be responsible for the Customer Personal Data and the means by which Customer acquired Customer Personal Data.

2.3 The Customer agrees to defend, indemnify and hold harmless MoEngage and/or the relevant MoEngage Affiliate from and against all claims, actions, third party claims, direct losses, damages and expenses incurred by MoEngage and/ or the relevant MoEngage Affiliate as a result of or in connection with the Customer's non-compliance with the Applicable Data Protection Laws.

2.4 The Customer shall issue instructions to MoEngage in writing/ via e-mail. MoEngage will duly cooperate with and make commercially reasonable efforts to assist the Customer in complying with Customer's obligations pursuant to the Applicable Data Protection Laws, taking into account the nature of processing, technical and organizational feasibility, and the

information available to MoEngage. The Customer may reimburse costs and expenses for any cooperation and assistance services provided to the Customer in that regard.

4. RIGHTS OF DATA SUBJECTS

3.1 **Data Subject Requests.** The Customer shall remain fully responsible to comply with any Data Subject requests and any deadline to comply with a request as required by Applicable Data Protection Laws. The Customer shall provide any such instruction to MoEngage sufficiently in advance prior to any regulatory or legal deadline in order for MoEngage to process and comply with the Customer's instruction.

3.2 MoEngage shall, to the extent legally permitted and to the extent MoEngage is able to identify that the request comes from a Data Subject whose Personal Data was submitted to the Services by Customer, promptly notify Customer if MoEngage receives a request from a Data Subject (customer's End Users) in relation to the exercise of any Data Subject Right ("**Data Subject Request**"). MoEngage shall not respond to a Data Subject Request without Customer's prior written consent except to confirm that such request relates to Customer, to which Customer hereby agrees.

3.3 Taking into account the nature of the Processing, MoEngage shall assist Customer by providing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations.

5. MOENGAGE PERSONNEL

4.1 **Confidentiality.** MoEngage shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities.

4.2 **Reliability.** MoEngage shall take commercially reasonable steps to ensure the reliability of any MoEngage personnel engaged in the Processing of Personal Data.

4.3 **Limitation of Access.** MoEngage shall ensure that MoEngage's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

4.4 **Data Protection Officer.** MoEngage shall comply fully with its obligations with respect to the employment of a data protection officer as required under Data Protection Laws and Regulations.

6. SUB-PROCESSORS

5.1 **Appointment of Sub-processors.** Customer acknowledges and agrees that (a) MoEngage's Affiliates may be retained as Sub-processors; and (b) MoEngage and MoEngage's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. MoEngage or a MoEngage Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor.

5.2 **List of Current Sub-processors and Notification of New Sub-processors.** The updated list of Sub-processors for the Services is present here. Such Sub-processor list shall include the

identities of those Sub-processors, their country of location as well as the type of processing they perform. MoEngage will notify Customer of a new Sub-processor(s) before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.

5.3 **Objection Right for New Sub-processors.** Customer may object to MoEngage's use of a new Sub-processor by notifying MoEngage promptly in writing within ten (10) business days after receipt of MoEngage's notice in accordance with Section 6.2. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, MoEngage will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Customer Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If MoEngage is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Order Form(s) with respect to only those Services which cannot be provided by MoEngage without the use of the objected-to new Sub-processor, by providing written notice to MoEngage.

5.4 **Liability for Sub-processors.** MoEngage shall be liable for the acts and omissions of its Sub-processors to the same extent MoEngage would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

7. SECURITY

6.1 **Controls for the Protection of Customer Data. (a)** MoEngage shall maintain appropriate technical and organizational measures for the protection of the security (including protection against Personal Data Breach), confidentiality and integrity of Customer Data, as set forth in the Security, Privacy and Architecture Datasheet attached hereto as Schedule 1. MoEngage regularly monitors compliance with these measures. The customer is responsible for reviewing the information made available by MoEngage relating to data security and making an independent determination as to whether the Services meet the Customer's requirements and legal obligations under Data Protection Laws and Regulations. The customer acknowledges that the security measures described within the Security, Privacy and Architecture Datasheet are subject to technical progress and development and that MoEngage may update or modify such document from time to time provided that such updates and modifications do not result in a material decrease of the overall security of the Services during a subscription term; **(b)** Without prejudice to MoEngage and its Affiliate's obligations under this Section 7 (security), the Customer:

i) shall remain solely responsible for its use of the Services, including: (a) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Personal Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the Services; and

ii) acknowledges that MoEngage and its Affiliates have no obligation to protect Customer Personal Data that Customer elects to store or transfer outside of MoEngage and its Affiliate's and its Sub-processors' systems (for example, offline or online premises storage).

6.2 **Customer Data Incident Management, Notification and Remediation.** MoEngage maintains security incident management policies and procedures specified in the Security, Privacy and Architecture Datasheet and shall notify Customer without undue delay after becoming aware of a Personal Data Breach. MoEngage shall provide information to Customer necessary to enable Customer to comply with its obligations under Data Protection Laws and Regulations. The content of such communication to Customer shall include (a) the nature of Processing and the information available to MoEngage (b) a description of the nature of the Data Breach including, where possible, the categories and an approximate number of

individuals concerned and the categories and an approximate number of Personal Data records concerned; (c) a description of the likely consequences of the Personal Data Breach; and (d) a description of the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects. MoEngage shall make commercially reasonable efforts to identify the cause of such Data Breach and take those steps as MoEngage deems necessary and reasonable in order to remediate the cause of such Data Breach to the extent the remediation is within MoEngage's reasonable control. The obligation to remediate the cause of a Data Breach shall not apply to Personal Data Breaches that are caused by Customer or Customer's Users.

6.3 **Third-Party Certifications and Audits.** MoEngage has obtained the third-party certifications and audits set forth in the Security, Privacy and Architecture Datasheet. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, MoEngage shall allow for and contribute to audits and inspections ("**Audits**") conducted by Customer (or Customer's independent, third-party auditor that is not a competitor of MoEngage by providing any information regarding MoEngage's compliance with the obligations set forth in this DPA in the form of a copy of MoEngage's then most recent third-party audits or certifications, as applicable, that MoEngage makes available to its customers generally. Customer may perform an Audit remotely or on-site, up to one (1) time per year, with at least three (3) weeks' advance written notice, unless otherwise required by Customer's regulators or applicable law. If Customer requests an on-site Audit, the following terms shall apply: (a) such Audit shall be limited to facilities operated by MoEngage and shall not exceed one (1) business day; (b) before the commencement of any such on-site Audit, Customer and MoEngage shall mutually agree upon the scope and timing of the Audit; (c) Customer shall reimburse MoEngage for actual expenses and costs incurred in connection with such Audit; (d) It is expressly clarified that MoEngage and/or the relevant MoEngage Affiliate will not be able to provide access to the SaaS platform operated by MoEngage and/or the relevant MoEngage Affiliate or otherwise let the auditors interact with the platform.

8. RETURN AND DELETION OF CUSTOMER DATA

MoEngage shall return Customer Data by enabling Customer to export its Customer Data as set forth in the Agreement and shall delete Customer Data, in accordance with the Agreement, applicable laws and the Security, Privacy and Architecture Datasheet.

9. AUTHORIZED AFFILIATES

8.1 **Relationship between MoEngage and Customer's Authorized Affiliates.** The parties acknowledge and agree that, by executing the Agreement, the Customer enters into this DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing an independent DPA between MoEngage and each such Authorized Affiliate, subject to the provisions of the Agreement and this Section 9 and Section 10. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For sake of clarity, an Authorized Affiliate is not and does not become a party to the Agreement, and is only a party to this DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

8.2 **Communication.** The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with MoEngage under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

8.3 **Rights of Authorized Affiliates.** Where an Authorized Affiliate executes a DPA with MoEngage, it shall to the extent required under applicable Data Protection Laws and Regulations, be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

8.3.1 Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against MoEngage directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together.

9.3.2 The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an on-site Audit, take all reasonable measures to limit any impact on MoEngage and its Sub-Processors by combining, to the extent reasonably possible, several Audit requests carried out on behalf of different Authorized Affiliates in one single Audit.

10. EUROPEAN SPECIFIC PROVISIONS

9.1 **Data Protection Impact Assessment.** Upon Customer's request, MoEngage shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to MoEngage. MoEngage shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority (as defined in the GDPR) in the performance of its tasks relating to this Section 10.1 of this DPA, to the extent required under the GDPR.

9.2 **Infringing instructions. MoEngage** shall immediately inform the Customer if, in its opinion, an instruction infringes GDPR.

9.3 **Transfer mechanism(s) for data transfers.** As of the Effective Date of this DPA, with regard to any transfers of Personal Data under this DPA from the European Union, Switzerland, the European Economic Area and/or their member states and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws and Regulations, MoEngage makes available the following transfer mechanism(s) which shall apply, in the order of precedence as set out below, if applicable:

i. The Standard Contractual Clauses, in accordance with the following terms:

1. For purposes of the SCC, when and as applicable, Customer and any applicable Authorized Affiliates are each the data exporter, and Customer's signing of this DPA or an Agreement referencing this DPA, or a Customer's Affiliate signing an Order Form under an Agreement referencing this DPA, shall be treated as signing of the SCC and their appendices. MoEngage's signature of this DPA or an Agreement referencing this DPA shall be treated as signing of the SCC and their

appendices Details required under the SCC's Appendix 1 are available in Schedule 3 to this DPA and under the SCC's Appendix 2 are outlined in Schedule 1 to this DPA. In the event of any conflict or inconsistency between this DPA and the SCC, the SCC shall prevail.

2. Section 6 of this DPA represents Customer's express consent regarding existing and new Sub-processors under Clause 5(h) of the SCC. Copies of the Sub-processor agreements that must be provided by MoEngage to Customer pursuant to Clause 5(j) of the SCC may have all commercial information, or clauses unrelated to the SCC or their equivalent, removed by MoEngage beforehand; such copies will only be provided by MoEngage upon request by Customer.

3. Audits pursuant to Clause 5(f) and Clause 12(2) of the SCC shall be carried out in accordance with Section 6.3 of this DPA.

4. The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the SCC shall only be provided by MoEngage to Customer upon Customer's request.

11. RETENTION OF CUSTOMER DATA

During the Term of the DPA, and subject to MoEngage's retention obligations under applicable laws, including Data Protection Laws, MoEngage shall adhere to Customer's instructions with regard to retention (including, without limitation, deletion) of Customer Data Processed pursuant to the DPA. Further, and subject to MoEngage's retention obligations under applicable laws, including Data Protection Laws, MoEngage shall, and shall cause its Subcontractors to, immediately securely destroy (by making unreadable, unreconstructable, and indecipherable) any or all Customer Data upon the earlier to occur of the following: (a) termination or expiration of the DPA or any applicable order form; or (b) cessation of MoEngage's need to retain such Customer Data to perform the Services. If Customer requests return or transfer of all or a portion of such Customer Data prior to the destruction described above, MoEngage shall promptly return to Customer all such Customer Data, through a secure method designated by Customer, or shall promptly transfer such Customer Data to Customer's designee, in accordance with the instructions of, and using the secure method prescribed by, Customer, following Customer's written demand therefore. In either event, MoEngage shall promptly provide Customer with a certification by an officer of MoEngage that all Customer Data has been removed from MoEngage's and any Subcontractor's possession and/or control.

12. GOVERNING LAW & SETTLEMENT OF DISPUTES

Without prejudice to the Standard Contractual clauses:

11.1 The Parties to this Agreement hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Agreement, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

11.2 This DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

11.3 Any dispute arising between the parties hereto in respect of the interpretation of this DPA and the performance of obligations hereunder shall be settled amicably by mutual consultations as

far as practicable. In the event a claim, controversy or dispute between the parties arises out of or in connection with this DPA or the transactions and business contemplated hereby, including the validity, construction or enforcement thereof, whether by way of contractual breach, tort or quasi-delict, the parties agree that the matter will be referred to an independent mediator mutually agreed upon by the parties. Where the parties cannot agree on a mediator, the parties agree to submit the dispute to either ad hoc or institutional arbitration, the choice of venue, law and rules of procedure of which shall be mutually agreed upon. All dispute resolution proceedings and records shall be in English. Issuance of an arbitration demand shall suspend the effect of any default entailed by such claim, controversy or dispute and any judicial or administrative proceedings instituted in connection therewith, for the duration of the arbitration proceedings.

11.4 The parties agree to participate in good faith in any mediation or arbitration begun under this paragraph. Any mediation or arbitral award shall be binding upon the parties, and shall be final and unappealable except on grounds provided under the applicable Alternative Dispute Resolution and Arbitration Laws, Rules and Procedures.

11.5 It is understood that where the parties have mutually agreed upon a mode of dispute resolution, the same shall be the exclusive remedy in the event such mode of dispute resolution is agreed upon, except that parties shall be entitled to obtain equitable relief, such as injunctive relief, from any court of competent jurisdiction in order to protect its rights while such proceeding is pending or in support of any award made pursuant to such arbitration.

List of Schedules:
Schedule 1: Technical and organisational measures to ensure the security of the data, privacy and architecture
Schedule 2: Details of the Processing

The Parties' authorized signatories have duly executed this DPA

MoEngage India Private Limited:	
Signature:	Signature:
Name: I V Narasimha Reddy	Name:
Title: CFO	Title:
Email: narasimha@moengage.com	Email:
Date:	Date:

ANNEX 1

STANDARD CONTRACTUAL CLAUSES

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 as 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

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

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), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

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

Clause 4

Interpretation

(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 - Optional

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.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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 Schedule 1 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 its content or exercise his/her rights. On request, the Parties shall provide the data subject (customer's end users) 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 security 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 data masking, tokenization, 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 Schedule 1. 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.

(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[2] (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 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;

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(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.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION 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 10 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.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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 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 Schedule 1 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.

(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) [Where the data exporter is established in an EU Member State:] 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 behaviour 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 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[4];

(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. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If 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. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

---

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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.

15.2 Review of legality and data minimisation

(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).

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

(i) 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;

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

(iii) 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.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. 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.

(e) 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

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 Ireland.

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.

(f) The Parties agree that those shall be the courts of Ireland.

(g) 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.

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

SCHEDULE 1

TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA, PRIVACY AND ARCHITECTURE

MoEngage takes data protection practices very seriously and has placed several controls and standards to diligently follow protocols protecting customers' data. MoEngage is committed to abiding by increased transparency regarding processing personal information.

A. Organization of Information Security & Data Privacy

- **Ownership**. MoEngage has appointed a Data Governance team under the Head of Security & Privacy Role, responsible for coordinating and monitoring Information security & Data privacy requirements and procedures. This team has the knowledge, experience, and authority to serve as the owner(s) of, with responsibility and accountability for, Information security & Data Privacy within the organization.

- **Roles and Responsibilities**. MoEngage has defined and allocated Data Governance responsibilities and implemented policies for Information security & data privacy in line with ISMS ISO 27001:2022 and PIMS ISO 27701:2019. Such policies (or summaries thereof) are published and communicated to respective stakeholders required to comply with such policies.

- **Project Management**. MoEngage addresses Information Security and Data Privacy in project management to identify and appropriately address security and privacy risks.

- **Risk Management**. MoEngage follows a risk management framework and conducts periodic risk assessments of its environment and systems to understand its risks and applies appropriate controls to manage and mitigate risks before Processing Protected Data.

B. Human Resources Security

- **General.** MoEngage ensures that its personnel are under a Non-Disclosure Agreement (NDA) that includes the protection of Protected Data and will provide adequate training about relevant privacy and security policies, procedures and regulatory requirements. MoEngage further informs its personnel of the possible consequences of breaching MoEngage's security policies and procedures, including disciplinary actions, with the possibility of termination of employment for MoEngage employees and termination of contract or assignment for Representatives and temporary personnel.

- **Training**. MoEngage personnel with access to Protected Data receive appropriate, periodic education and training regarding privacy and security procedures for services to aid in the prevention of unauthorized use (or inadvertent disclosure) of Protected Data and training regarding how to effectively respond to security incidents. Training is provided before MoEngage personnel are granted access to Protected Data or begin providing services to customers. Training is regularly reinforced through refresher training courses, emails, posters, notice boards, and other training and awareness materials.

- **Background Checks.** MoEngage conducts professional history, criminal and other relevant background checks of all personnel and evaluates the results to ensure that there is no indication that the personnel may present a risk for theft of confidential data in compliance with Applicable Laws and MoEngage's policies.

C. Trusted Device Standards.

- MoEngage personnel who access Customers' confidential data:
    - Only use trusted Devices that are configured with security software (i.e., anti-virus, encryption, MDM, DLP etc.);
    - Follow MoEngage IT Security and Acceptable Usage policy when accessing Protected Data. These policies specify the requirements that user device ("Devices") must satisfy to be trusted when accessing Protected Data via a restricted network [VPN]. Devices that fail to comply with this standard will not be entitled to access the Network.

- MoEngage IT Security and Acceptable Usage policy includes, at a minimum, the following:
    - Each Device is uniquely associated with a specific, individual user;

- All operating system and application security patches are installed within the timeframe recommended or required by the issuer of the patch;
- Devices are encrypted (i.e., full disk) and secured with a protected (SSO, two Factor Authentication), and screens are locked with the automatic activation feature.;
- Devices are periodically scanned for restricted/prohibited software; and
- Devices run an acceptable industry standard anti-malware solution.

- **Storage**. MoEngage has implemented policies designed to prevent the storage of Protected Data even on trusted devices or any physical storage media without prior written authorization from the MoEngage Data Governance team and Customer. MoEngage takes appropriate measures to prevent accidental exposure of Protected Data using solutions like Data Loss Prevention (DLP) and Mobile Device Management (MDM) on all laptops.

D. Personnel Access Controls

- **Access**

  - **Limited Use.** MoEngage understands and acknowledges that the Customer may grant MoEngage access to sensitive and proprietary information. MoEngage will not (i) access the Protected Data for any purpose other than as necessary to perform its obligations to Customer; or (ii) use any system to access information or log-in credentials to gain unauthorized access to Protected Data or to exceed the scope of any authorized access.

  - **Authorization**. MoEngage follows the Principle of Least Privilege and restricts, by default and provides access to Protected Data solely to those Representatives whose access is necessary to performing MoEngage's obligations to the Customer.

  - **Suspension or Termination of Access Rights.** At Customer's reasonable request, MoEngage will promptly and without undue delay suspend or terminate the access rights to Protected Data for any MoEngage's personnel or its Representatives reasonably suspected of breaching any of the provisions of the agreement with Customer; and MoEngage ensures removal of access rights of all employees and external party users upon suspension or termination of their employment, or engagement.

  - **Information Classification**. MoEngage internally classifies all Customer's PII-Data as Restricted while Non-PII Data as Confidential. MoEngage categorizes, and/or tags Protected Data to help identify it and to allow for access and use to be appropriately restricted as per the defined classification level.

- **Access Policy.** MoEngage determines appropriate access control rules, rights, and restrictions for each specific user's roles towards their assets. MoEngage maintains a record of the security privileges of its personnel who have access to Protected Data, networks, and network services.

E. Access Authorization.

- MoEngage has user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to SaaS Infrastructure and Protected Data of the customer. MoEngage makes use of an enterprise access control system that requires revalidation of its personnel by managers and governance team at regular intervals based on the principle of "least privilege" and need-to-know criteria based on job role/Performance obligations.

- For systems that process Protected Data, MoEngage revalidates (or where appropriate, deactivates) access of users who change reporting structure and deactivates authentication credentials that have not been used for some time, not exceeding three (3) months.

- MoEngage restricts access to program source code and associated items such as software object code, designs, specifications, verification plans, and validation plans, to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

F. Network Design. For systems that process Protected Data, MoEngage has implemented controls to avoid personnel assuming access rights beyond those that they have been assigned to gain unauthorized access to Protected Data.

G. Authentication

- Where authentication mechanisms are based on passwords, MoEngage will require the password to conform to strong password control parameters (e.g., length, character complexity, and/or non-repeatability).

- MoEngage ensures that de-activated or expired identifiers and log-in credentials are not granted to other individuals.

- MoEngage monitors repeated failed attempts to gain access to the information system.

- MoEngage maintains industry standard procedures to deactivate log-in credentials that have been corrupted or inadvertently disclosed.

- MoEngage makes use of industry-standard log-in credential protection practices, including practices designed to maintain the confidentiality and integrity of log-in credentials when they are assigned and distributed, and during storage. Such practices are designed to ensure strong, confidential log-in credentials.

H. Cryptography and Key management

- MoEngage ensures a policy on the use of cryptographic controls based on assessed risks.

- MoEngage assesses and manages the lifecycle of cryptographic algorithms, hashing algorithms, etc. and deprecates and disallows usage of weak cypher suites and insufficient bit and block lengths.

- MoEngage has procedures for distributing, storing, archiving, and changing/updating keys; recovering, revoking/destroying, and dealing with compromised keys; and logging all transactions associated with such keys.

I. Physical and Environmental Security

MoEngage provides a completely [IaaS] Cloud-based SaaS Infrastructure to host its SaaS Infrastructure and related services to its customers. MoEngage only ensures Logical and administrative security of its SaaS infrastructure and relies on its IaaS Cloud Service provider for the Physical Security of data centres hosting physical resources.

- **Physical Access to Facilities**

    - MoEngage ensures its IaaS Cloud Service provider has
        - limited access to facilities where systems that Process Protected Data are located to authorized individuals.
        - defined Security perimeters and uses them to protect areas that contain Protected Data and Processing facilities.
        - Facilities that are monitored and access-controlled at all times (24x7).
        - controlled access through key card and/or appropriate sign-in procedures for facilities with systems Processing Protected Data.

- **Physical Access to Equipment.** Physical systems hosting MoEngage services used to process or store Protected Data are protected using industry-standard processes to limit access to authorized individuals by IaaS Cloud Service provider.

- **Protection from Disruptions**. MoEngage IaaS Cloud Service provider has implemented appropriate measures designed to protect against loss of data due to power supply failure or line interference.

- **Clear Desk**. MoEngage has policies requiring a “clean desk/clear screen” to prevent inadvertent disclosure of Protected Data.

J. Operations Security

- **Operational Policy.** MoEngage maintains written policies describing its security and privacy measures and the relevant procedures and responsibilities of its personnel who have access to Protected Data and to its systems and networks. MoEngage communicates its policies and requirements to all persons involved in the Processing of Protected Data and has implemented the appropriate management structure and control designed to ensure

compliance with such policies and with applicable aaws concerning the processing and protection of Protected Data.

- **Security and Processing Controls.**

  - **Areas**. MoEngage maintains, documents, and implements standards and procedures to address the configuration, operation, and management of systems, networks and services that store or Process Protected Data.

  - **Standards and Procedures**. Such standards and procedures include security controls, identification and patching of security vulnerabilities, change control processes and procedures, and incident prevention, detection, remediation, and management.

- **Logging and Monitoring.** MoEngage maintains logs of administrator and operator activity and data recovery events related to Protected Data.

K. Communications Security and Data Transfer

- **Networks.** MoEngage ensures following controls to secure its networks that access or Process Protected Data:

  - Network traffic passes through next generation firewalls [NGFW], which is monitored at all times. NGFW also acts as EDR and IPS for flowing traffic.

  - Cloud-based Network devices used for administration utilize industry-standard cryptographic controls when Processing Protected Data.

  - Anti-spoofing filters and controls are enabled at cloud gateways and at each processing resource.

  - Network, application, and server authentication passwords are required to meet minimum complexity guidelines (at least 8 characters with all of the following four classes: upper case, lower case, numeral, special character) and to be changed at least every 90 days; utilized along with Two Factor authentication.

  - Initial user passwords are required to be changed at first log-on. MoEngage has a policy prohibiting the sharing of user IDs, passwords, or other log-in credentials.

- **Data Transfer.** MoEngage has formal data transfer policies in place to protect the transfer of information through the use of all types of communication facilities that adhere to the requirements of the agreement with the customer. Such policies are designed to protect transferred information from unauthorized interception, copying, modification, corruption, routing and destruction.

L. System Acquisition, Development, and Maintenance

- **Security Requirements.** MoEngage adopts security requirements for the purchase, use, or development of information systems, including for application services delivered through public networks.

- **Development Requirements**. MoEngage has policies for secure development, system engineering, and support. MoEngageconducts appropriate tests for application security as part of acceptance testing processes. MoEngage also supervises and monitors the activity of outsourced system development, if any.

M. Penetration Testing and Vulnerability Scanning & Audit Reports

- **Testing.** MoEngage performs periodic audits and penetration tests on SaaS infrastructure, Application and Processing Resources. These tests are conducted by both internal and external assessment teams. Upon written request from the Customer, MoEngage will provide a Vulnerability & Penetration testing report conducted by an independent 3rd party at the organization level which may include an executive summary of the results and not the details of actual findings.

- **Audits**. MoEngage will respond promptly to and cooperate with reasonable requests by Customers for security audits, scanning, discovery, and testing reports.

- **Remedial Action**. If any audit or penetration testing exercise reveals any deficiencies, weaknesses, or areas of non-compliance, MoEngage will promptly take such steps as may be required, in MoEngage's reasonable discretion, to remedy those deficiencies, weaknesses, and areas of non-compliance as soon as may be practicable given the circumstances. Upon request, MoEngage will keep Customer informed of the status of any remedial action that is required to be carried out and will certify to Customer as soon as may be practicable that all necessary remedial actions have been completed.

N. Contractor Relationships

- **Policies.** MoEngage ensures information security policies or procedures are used by Representatives who impose requirements consistent with service agreements with customers.

- **Monitoring**. MoEngage ensures the monitoring and audit of service delivery by its Representatives. MoEngage reviews its Representatives' security practices against the security requirements outlined in MoEngage's agreements with such Representatives. MoEngage manages changes in Representative services that may have an impact on security.

O. Management of Information Security Incidents and Data breaches

- **Responsibilities and Procedures.** MoEngage ensures procedures for quick, effective, and orderly response to Information Security Incidents & Data Breaches.

- **Reporting**. MoEngage ensures to reports Information Security Incidents and Data breaches through appropriate management channels to customers within 72 hrs.

- **Reporting Information Security Weaknesses**. MoEngage has implemented procedures to monitor, report and manage any observed or suspected information security and privacy weaknesses in systems or services.

- **Assessment of and Decision on Information Security Events**. MoEngage has an incident classification scale in place to decide whether a security/privacy event should be classified as an Information Security Incident or Data breach. The classification scale is based on the impact and extent of an incident or breach.

- **Response Process**. MoEngage maintains a record of Information Security Incidents and Data Breaches with a description of the incident/breach, the effect of the incident/breach, the name of the reporter and to whom the incident/breach was reported, the procedure for rectifying the incident/breach, and the remedial action taken to prevent future security incidents/data breaches.

P. Information Security Aspects of Business Continuity Management

- **Planning.** MoEngage maintains emergency and contingency plans for all storage and processing resources that process Protected Data. MoEngage verifies the established and implemented information security continuity controls at regular intervals.

- **Data Recovery.** MoEngage ensures that redundant storage and procedures for recovering data in a manner are sufficient to reconstruct Protected Data in its original state as found on the last recorded backup.

Q. Notification and Communication Obligations

- **Notification.** MoEngage, without undue delay (i.e., within 72 hours from confirmation) notify Customer if any of the following events occur:

    - any unmitigated, material security vulnerability, or weakness of which MoEngage has actual knowledge in (i) Customer's systems, or networks, or (ii) MoEngage's systems or networks, that have compromised Protected Data;

    - an Information Security Incident/data breach that compromises or is likely to compromise the security of Protected Data and weaken or impair business operations of Customer.

    - an Information Security Incident/data breach that negatively impacts the confidentiality, integrity, and availability of Protected Data; or

- Known and wilful failure or inability to maintain material compliance with requirements of agreement with customers and Applicable Laws.

- **Cooperation.**

MoEngage will: (i) respond promptly to any Customer's reasonable requests for information, cooperation, and assistance in any post-incident investigation, remediation, and communication efforts.

- **Information Security Communication.**

Except as required by Applicable Laws or by existing applicable contractual obligations, MoEngage agrees that it will not inform any third party of any of the events described above in this Section referencing, or identifying Customer, without Customer's prior written consent. MoEngage will fully cooperate with Customer and law enforcement authorities concerning any unauthorized access to Customer's systems or networks, or Protected Data. Such cooperation will include the retention of all information and data within MoEngage's possession, custody, or control that is directly related to any Information Security Incident. If disclosure is required by law, MoEngage will work with Customer regarding the timing, content, and recipients of such disclosure. To the extent MoEngage was at fault, MoEngage will bear the cost of reproduction or any other remedial steps necessary to address the incident or compromise.

SCHEDULE 2
DETAILS OF THE PROCESSING

Nature and Purpose of Processing
MoEngage will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Customer in its use of the Services.

Duration of Processing
MoEngage will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects
Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of Data Subjects:

1.
2.
3.

Type of Personal Data
Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

1.
2.
3.

Annex I.A to Standard Contractual Clauses

A. LIST OF PARTIES

Data exporter(s):

1. Name: …

Address: …

Contact person's name

Position and contact details:

Activities relevant to the data transferred under these Clauses:

Signature and date: …

Role (controller/processor): … Controller

2.**Data importer(s):**

1. Name: MoEngage India Private Ltd

Address: 1st Floor, #32, Salarpuria Tower II, Chikku Lakshmaiah Layout, Luskar Hosur Road, Koramangala, Bangalore - 560029, India

Contact person's name, position and contact details: Nitin Kotwal, dpo@moengage.com

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role…Processor

Annex I. B. to Standard Contractual Clauses

Data exporter

The data exporter is the Customer or a Customer Authorized Affiliate, i.e., a company that wishes to manage its customer engagement via the MoEngage Services.

Data importer

The data importer is MoEngage, a company which processes Personal Data upon the instruction of the data exporter in accordance with the terms of the Agreement.

Data subjects

The personal data transferred concern the following categories of data subjects: the data subjects listed above in Schedule 2 "Categories of Data Subjects", in particular the data exporter's Users of the MoEngage Services and End-Users.

Categories of data

The personal data transferred concerns the following categories of data: Event data, application data, email address, location data, application settings and preferences, campaign data, connections with social networks or other platforms, and device data.

Special categories of data (if appropriate)

The personal data transferred concerns the following special categories of data:

Processing operations

The personal data transferred will be subject to the following basic processing activities. The Personal Data transferred is stored by the data importer and accessible by the data exporter within a web interface to enable the data exporter to segment their user audience and create targeted multi-channel messaging.

Annex I. C to Standard Contractual Clauses

Competent Supervisory Authority

Data Protection Commission, Ireland.