HIGHER LOGIC

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") forms part of the Master Subscription Agreement (the "Agreement") between Higher Logic, LLC ("Higher Logic") and Subscriber for the purchase of Software Services (as defined in the Agreement) from Higher Logic (hereinafter referred to as the "Service"), and reflects the parties' agreement with regard to the Processing of Personal Data.

Subscriber enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent Higher Logic Processes Personal Data for which such Authorized Affiliates qualify as the Controller. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. In providing the Service to Subscriber pursuant to the Agreement, Higher Logic may Process Personal Data on behalf of Subscriber, and the parties agree to comply with the following provisions with respect to any Personal Data.

For purposes of this DPA, Subscriber and Higher Logic agree that Subscriber is the Controller of Personal Data and Higher Logic is the Processor of such data, except when Subscriber acts as a Processor of Personal Data, in which case Higher Logic is a Sub-processor. This DPA applies to the Processing of Personal Data by Higher Logic on behalf of Subscriber. This DPA does not limit or reduce any data protection commitments Higher Logic makes to Subscriber in the Master Subscription Agreement or other agreement between Higher Logic and Subscriber. This DPA does not apply where Higher Logic is a Controller of Personal Data.

APPLICATION OF THIS DPA

If the Subscriber entity signing this DPA is a party to the Agreement, then this DPA is an addendum to, and forms part of, the Agreement. In such case, the Higher Logic entity that is party to the Agreement is party to this DPA.

If the Subscriber entity signing this DPA has executed an Order Form with Higher Logic or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, then this DPA is an addendum to that Order Form and applicable renewal Order Forms, and the Higher Logic entity that is a party to such Order Form is a party to this DPA.

If the Subscriber entity signing this DPA is neither a party to an Order Form nor the Agreement, then this DPA is not valid and therefore is not legally binding. Such entity should request that the Subscriber entity who is a party to the Agreement executes this DPA.

This DPA shall not replace any comparable or additional rights relating to Processing of Subscriber Data contained in the Agreement.

DPA DEFINITIONS

“Affiliate” means any entity that directly or indirectly controls, is controlled by, or is under common control with the Subscriber entity signing this Agreement, or with Higher Logic, as the case may be.

“Authorized Affiliate” means any of Subscriber's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Service pursuant to the Agreement between Subscriber and Higher Logic, but has not signed its own Order Form with Higher Logic and is not a "Subscriber" as defined under the Agreement.

"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.

“Controller” means the entity which determines the purposes and means of the Processing of Personal Data.

“Data Protection Laws and Regulations” means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

“Data Subject” means the identified or identifiable person to whom Personal Data relates.

“GDPR” means the 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, and repealing Directive 95/46/EC (European Union General Data Protection Regulation or “EU GDPR”) and the EU GDPR in such form as incorporated into the laws of the United Kingdom (“UK GDPR”).

“Higher Logic” means the Higher Logic entity which is a party to this DPA, as specified in the section “Application of this DPA” above, being Higher Logic, LLC, a limited liability company formed under the laws of Delaware, or an Affiliate of Higher Logic, as applicable.

“Higher Logic Group” means Higher Logic and its Affiliates engaged in the Processing of Personal Data.

“Personal Data” means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each of (i) or (ii), such data is Subscriber Data.

“Processing” (including its root word, “Process”) 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.

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

"Subscriber Data" means all electronic data submitted by or on behalf of Subscriber, or an Authorized Affiliate, to the Service.

"Standard Contractual Clauses" means the clauses approved with Commission Implementing Decision (EU) 2021/914 of June 4, 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended, supplemented, updated or replaced from time to time.

"Sub-processor" means any Processor engaged by Higher Logic or a member of the Higher Logic Group.

"Supervisory Authority" means an independent public authority which is established pursuant to the Data Protection Laws and Regulations.

DPA TERMS

Higher Logic and Subscriber hereby enter into this DPA as of the last date of execution by a party.

1. Provision of the Service. Higher Logic provides the Service to Subscriber under the Agreement. In connection with the Service, the parties anticipate that Higher Logic may Process Subscriber Data that contains Personal Data relating to Data Subjects.

2. Subscriber Responsibilities. Subscriber shall, in its use of the Service, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Subscriber's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Subscriber shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Subscriber acquired Personal Data. Subscriber instructs Higher Logic (and authorizes Higher Logic to instruct each Sub-processor) to: (a) Process Subscriber Data, which may include Personal Data, and (b) in particular, transfer Subscriber Data and Personal Data to any country or territory, as reasonably necessary for the provision of the Service and consistent with the Agreement. Subscriber warrants and represents that it is and will at all relevant times remain duly and effectively authorized to give the instruction set out in this Section 2 on behalf of each relevant Authorized Affiliate.

3. Processing Purposes. Higher Logic shall keep Personal Data confidential and shall only Process Personal Data on behalf of and in accordance with Subscriber's

documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Service; and (iii) Processing to comply with other documented, reasonable instructions provided by Subscriber (for example, via email) where such instructions are consistent with the terms of the Agreement. Higher Logic shall not be required to comply with or observe Subscriber's instructions if such instructions would violate the Data Protection Laws and Regulations.

4. Scope of Processing. The subject-matter of Processing of Personal Data by Higher Logic is the performance of the Service 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 as set forth in the Agreement and in Schedule 2 of this DPA.

5. Data Subject Requests. To the extent legally permitted, Higher Logic shall promptly notify Subscriber if Higher Logic receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request"). Factoring into account the nature of the Processing, Higher Logic shall assist Subscriber by appropriate organizational and technical measures, insofar as this is possible, for the fulfilment of Subscriber's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Subscriber, in its use of the Service, does not have the ability to address a Data Subject Request, Higher Logic shall, upon Subscriber's request, provide commercially-reasonable efforts to assist Subscriber in responding to such Data Subject Request, to the extent that Higher Logic is legally authorized to do so, and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Subscriber shall be responsible for any reasonable costs arising from Higher Logic's provision of such assistance.

6. Higher Logic Personnel. Higher Logic 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 regarding their responsibilities, and have executed written confidentiality agreements. Higher Logic shall take commercially-reasonable steps to ensure the reliability of any Higher Logic personnel engaged in the Processing of Personal Data. Higher Logic shall ensure that Higher Logic's access to Personal Data is limited to those personnel assisting in the provision of the Service in accordance with the Agreement.

7. Data Protection Officer. Higher Logic shall appoint a data protection officer if and whereby such appointment is required by Data Protection Laws and Regulations.

8. Higher Logic's Sub-processors. Subscriber has instructed or authorized the use of Sub-processors to assist Higher Logic with respect to the performance of Higher Logic's obligations under the Agreement and Higher Logic agrees to be responsible for the acts or omissions of such Sub-processors to the same extent as Higher Logic would be liable if performing the services of the Sub-processors under the terms of the Agreement. Higher Logic shall ensure that the arrangement between Higher Logic and each Sub-processor is governed by a written contract including terms which offer at least the same level of protection for Subscriber Personal Data as those set out in this DPA and in GDPR Article 28(3)-(4) or equivalent applicable provisions of the Data Protection Laws and Regulations. Higher Logic shall make available to Subscriber Higher Logic's list of its then-current Sub-processors at https://www.higherlogic.com/legal/subprocessors. Subscriber acknowledges and agrees that (a) Higher Logic's Affiliates may be retained as Sub-processors; and (b) Higher Logic and Higher Logic's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Service. Higher Logic shall provide a mechanism by which Subscriber may subscribe to notifications of new Sub-processors for the Service at https://resources.higherlogic.com/notification-of-sub-processor-change and if Subscriber subscribes, Higher Logic shall provide notification of a new Sub-processor(s) at least ten (10) business days before authorizing any new Sub-processor(s) to process Personal Data in connection with the provision of the Service. In order to exercise its right to object to Higher Logic's use of a new Sub-processor, Subscriber shall notify Higher Logic promptly in writing within ten (10) business days after receipt of Higher Logic's notice. In the event Subscriber objects to a new Sub-processor, and that objection is not unreasonable, Higher Logic will use reasonable efforts to make available to Subscriber a change in the Service or recommend a commercially-reasonable change to Subscriber's configuration or use of the Service to avoid Processing of Personal Data by the objected- to new Sub-processor without unreasonably burdening the Subscriber. If Higher Logic is unable to make available such change within a reasonable time period, which shall not exceed thirty (30) days, Subscriber may terminate the applicable Order Form(s) with respect only to a Service which cannot be provided by Higher Logic without the use of the objected-to new Sub-processor by providing written notice to Higher Logic within ten (10) days following such thirty (30) day cure period. Higher Logic will refund Subscriber any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Service. The parties agree that the copies of the Sub- processor agreements that must be provided by Higher Logic to Subscriber pursuant to the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Higher Logic beforehand; and, that such copies will be provided by Higher Logic, in a manner to be determined in its discretion, only upon request by Subscriber.

9. Liability for Sub-processors. Higher Logic shall be liable for the acts and omissions of its Sub-processors to the same extent Higher Logic would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

10. Security Measures. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Higher Logic shall, in relation to Subscriber Data, implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR. Higher Logic regularly monitors compliance with these measures. In assessing the appropriate level of security, Higher Logic shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data breach. Higher Logic will not materially decrease the overall security of the Service during Subscriber's and/or Authorized Affiliates' subscription term.

11. Notifications Regarding Subscriber Data. Higher Logic has in place reasonable and appropriate security incident management policies and procedures, and shall notify Subscriber without undue delay of the unlawful or accidental destruction, alteration or damage or loss, unauthorized disclosure of, or access to, Subscriber Data, including Personal Data, transmitted, stored or otherwise Processed by Higher Logic or its Sub-processors of which Higher Logic becomes aware (hereinafter, a "Subscriber Data Incident"), as required to assist the Subscriber in ensuring compliance with its obligations to notify the Supervisory Authority in the event of Personal Data breach. Higher Logic shall make reasonable efforts to identify the cause of such Subscriber Data Incident, and take those steps as Higher Logic deems necessary and reasonable in order to remediate the cause of such a Subscriber Data Incident, to the extent that the remediation is within Higher Logic's reasonable control. The obligations set forth herein shall not apply to incidents that are caused by either Subscriber or Subscriber's Users.

12. Return or Deletion of Subscriber Data. Higher Logic shall, at Subscriber's election, return all Subscriber Data to Subscriber and, to the extent allowed by applicable law, automatically delete any and all copies of Subscriber Data within thirty (30) days of the request in accordance with Higher Logic's backup policy, unless the retention of the data is required by applicable Data Protection Laws and Regulations; provided that Higher Logic shall ensure the confidentiality of such retained Subscriber Data, and shall ensure that such data is only processed for the purposes specified under such laws requiring its storage for the period specified therein and for no other purpose. The parties agree that the certification of deletion of Personal Data that is described in the Standard Contractual Clauses shall be provided by Higher Logic to Subscriber only upon Subscriber's request.

13. Authorized Affiliates. The parties agree that, by executing the DPA, the Subscriber enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliate(s), thereby establishing a separate DPA between Higher Logic and each such Authorized Affiliate, subject to the provisions of the Agreement. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. An Authorized Affiliate is not and does not become a

party to the Agreement, and is only a party to the DPA. All access to and use of the Service by Authorized Affiliate(s) must comply with the terms and conditions of the Agreement and any violation thereof by an Authorized Affiliate shall be deemed a violation by Subscriber.

14. Communications. The Subscriber that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Higher Logic under this DPA, and shall be entitled to transmit and receive any communication in relation to this DPA on behalf of its Authorized Affiliate(s).

15. Exercise of Rights. In the event that an Authorized Affiliate becomes a party to the DPA, 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, except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Higher Logic directly by itself, the parties agree that (i) solely the Subscriber 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 Subscriber that is the contracting party to the Agreement shall exercise any such rights under this DPA in a combined manner for all of its Authorized Affiliates together, instead of doing so separately for each Authorized Affiliate.

16. Liability. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Higher Logic, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. Higher Logic's total liability for all claims from the Subscriber and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Subscriber and all Authorized Affiliates, and shall not be understood to apply individually and severally to Subscriber and/or to any Authorized Affiliate that is a contractual party to any such DPA. Each reference to the DPA herein means this DPA, including its Appendices.

17. Data Protection Laws and Regulations. Higher Logic will Process Personal Data in accordance with the Data Protection Laws and Regulations' requirements directly applicable to Higher Logic's provision of the Service.

18. Data Protection Impact Assessment. Upon Subscriber's request, Higher Logic shall provide Subscriber with reasonable cooperation and assistance needed to fulfil Subscriber's obligation under the GDPR to carry out a data protection impact assessment related to Subscriber's use of the Service, to the extent Subscriber does not otherwise

have access to the relevant information, and to the extent such information is available to Higher Logic. Higher Logic shall provide reasonable assistance to Subscriber in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks to the extent required under the GDPR (to include GDPR Articles 35 and 36).

19. Cross-Border Transfers of Personal Data.

(i) With respect to the transfer of Personal Data originating from the European Union, the European Economic Area and their member states, the United Kingdom and Switzerland, the parties agree to comply with the Standard Contractual Clauses attached hereto at Schedule 1. Where Higher Logic is a Processor, Higher Logic shall comply with all the obligations of the "data importer" under Module Two (Transfer Controller to Processor) of the Standard Contractual Clauses. Where Higher Logic is a Sub-processor, Higher Logic shall comply with all the obligations of the "data importer" under Module Three (Transfer Processor to Processor) of the Standard Contractual Clauses. In each case, Subscriber shall comply with the obligations, and shall have the rights, of the "data exporter" under Module Two and Module Three, respectively, of the Standard Contractual Clauses.

(ii) Insofar as the transfer of Personal Data is subject to, respectively, the Data Protection Laws and Regulations of Switzerland ("Swiss Data Protection Laws") and the Data Protection Laws and Regulations of the United Kingdom ("UK Data Protection Laws"), the following provisions apply: (a) the Swiss Federal Data Protection and Information Commissioner (FDPIC) and the Information Commissioner will be the competent supervisory authorities for, respectively, transfers of Personal Data from Switzerland and transfers of Personal Data from the United Kingdom under Clause 13 of the Standard Contractual Clauses; (b) the parties agree to abide by the EU GDPR standard in relation to all Processing of Personal Data that is governed by Swiss Data Protection Laws and by the UK Data Protection Laws standard in relation to all Processing of Personal Data that is governed by UK Data Protection Laws; (c) the term 'Member State' in the Standard Contractual Clauses will not be interpreted in such a way as to exclude Data Subjects in Switzerland and the UK from the possibility of suing for their rights in their place of habitual residence (Switzerland or the UK, as applicable) in accordance with Clause 18(c) of the Standard Contractual Clauses; (d) references to the 'GDPR' and its provisions in the Standard Contractual Clauses will be understood as references to Swiss Data Protection Laws or, as applicable, UK Data Protection Laws; (e) all references to the "European Economic Area" or the "European Union" in the Standard Contractual Clauses shall be deemed to refer to, respectively, Switzerland and the UK, (f) for transfers of Personal Data governed by UK Data Protection Laws, Clause 17 of the Standard Contractual Clauses is replaced to provide that the Standard Contractual Clauses are governed by the laws of England and Wales, and for transfers of Personal Data governed by Swiss Data Protection Laws, Clause 17 of the Standard Contractual Clauses is replaced to provide that the Standard Contractual Clauses are governed by the laws of Switzerland; and (g) for transfers of

Personal Data governed by UK Data Protection Laws, the courts under Clause 18 of the Standard Contractual Clauses shall be the courts of England and Wales, and for transfers of Personal Data governed by Swiss Data Protection Laws, the courts under Clause 18 of the Standard Contractual Clauses shall be the competent courts of Switzerland. In respect of data transfers governed by Swiss Data Protection Laws, the Standard Contractual Clauses also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity.

(iii) In each case, the Standard Contractual Clauses apply to (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and its Authorized Affiliates and, (ii) all Affiliates of Subscriber which have signed Order Forms for the Service and are subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom. For the purpose of the Standard Contractual Clauses the aforementioned entities shall be deemed "data exporters."

20. Audits. The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications: following Subscriber's written request, and subject to the confidentiality obligations set forth in the Agreement, Higher Logic shall make available to Subscriber information regarding the Higher Logic Group's compliance with the obligations set forth in this DPA, to include, if and to the extent that Higher Logic makes them generally available to its Subscribers, third-party certifications and audits. Subscriber may contact Higher Logic in accordance with the "Notices" Section of the Agreement to request an onsite audit of the procedures relevant to the protection of Personal Data. Subscriber may not request more than one audit per year (unless otherwise permitted under Data Protection Laws and Regulations) and all audits shall be conducted with a representative of Higher Logic present at all times, shall be subject to Higher Logic's policies during Higher Logic's regular business hours and shall not unreasonably interfere with Higher Logic's business activities. If a third party is to conduct such audit, the third party must be mutually agreed to by Subscriber and Higher Logic and must execute a confidentiality agreement acceptable to Higher Logic before conducting the audit. Subscriber shall reimburse Higher Logic for any time expended for any such on-site audit at the Higher Logic Group's then current professional services rates, which shall be made available to Subscriber upon request. Before the commencement of any such on- site audit, Subscriber and Higher Logic shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Subscriber shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Higher Logic. Subscriber shall promptly notify Higher Logic and provide information about any actual or suspected non-compliance discovered during an audit and shall provide Higher Logic with a copy of the audit report. Subscriber may only use the audit report to confirm Higher Logic's compliance with

this DPA and the audit report will be Confidential Information of both parties under the Agreement. If the requested audit scope is addressed in an SOC 2, ISO, NIST or other similar audit report performed by a qualified third party auditor within the prior twelve months and Higher Logic confirms that there are no known material changes in the controls audited, Subscriber agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.

The provision in this section shall by no means derogate from or materially alter the provisions on audits as specified in the Standard Contractual Clauses.

21. Order of Precedence. This DPA is incorporated into and forms part of the Agreement. For matters not addressed under this DPA, the terms of the Agreement apply. With respect to the rights and obligation of the parties vis-à-vis each other, in the event of a conflict between the terms of the Agreement and this DPA, the terms of this DPA will control. In the event of a conflict between the terms of the DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail.

[*Signature Page Follows*]

IN WITNESS WHEREOF, the parties hereby execute this Data Processing Addendum, effective as of the Effective Date.

SUBSCRIBER

Signature: _____

Company Name: _____

Printed Name: _____

Title: _____

Date:

HIGHER LOGIC, LLC

Signature: DocuSigned by: Kevin M. Boyce 385D8C0E58CB46C...

Company Name: Higher Logic

Printed Name: Kevin M. Boyce

Title: CEO

Date: 9/30/2021

Schedule 1 – Standard Contractual Clauses

The parties agree to that with respect to the implementation of the Standard Contractual Clauses under the DPA, either one or both of Module Two: Controller to Processor of the Standard Contractual Clauses ("**Module Two**," otherwise defined in the DPA as "**C2P SCCs"**) and Module Three: Processor to Processor of the Standard Contractual Clauses ("**Module Three**," otherwise defined in the DPA as "**P2P SCCs**") shall apply, and both Module Two and Module Three are referenced herein. To the extent Module Two and Module Three differ, those differences are highlighted below. Where Module Two and Module Three do not differ, the identical provisions are referenced only once.

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) 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 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. For Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); For Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

iii. For Module Two: Clause 9(a), (c), (d) and (e); For Module Three: 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

(Intentionally left blank)

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.

FOR MODULE TWO: TRANSFER CONTROLLER TO PROCESSOR

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 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.

(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 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.

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.

FOR MODULE THREE: TRANSFER PROCESSOR TO PROCESSOR

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

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 controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix 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 with the reasons for the redactions, to the extent possible without revealing the redacted information.

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 rectify or erase 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 controller 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, they 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 subject. 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 or the controller. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out 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 controller, as communicated to the data importer by 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 of Regulation (EU) 2016/679 that covers the onward transfer;

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

(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 or the controller 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 controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) 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.

(g) 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

FOR MODULE TWO: TRANSFER CONTROLLER TO PROCESSOR

(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 ten (10) business 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. 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 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.

FOR MODULE THREE: TRANSFER PROCESSOR TO PROCESSOR

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten (10) business days in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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. 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 or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. 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

FOR MODULE TWO: TRANSFER CONTROLLER TO PROCESSOR

(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.

FOR MODULE THREE: TRANSFER PROCESSOR TO PROCESSOR

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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 controller, as communicated by 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 subprocessor) 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.

(b) 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.

(c) 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.

(d) 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;

(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). For Module Three: The data exporter shall forward the notification to the controller.

(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 [for Module Three: if appropriate in consultation with the controller]. 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 [for Module Three: the controller or] 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.

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.

For Module Three: The data exporter shall forward the notification to the controller.

(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.). For Module Three: The data exporter shall forward the information to the controller.

(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. For Module Three: The data exporter shall make the assessment available to the controller.

(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 [for Module Three: and the controller] 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.

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

(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

Annex I
To the Standard Contractual Clauses

A. LIST OF PARTIES

Data exporter(s): *Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*

Name:	The Subscriber listed in the Agreement.
Address:	As provided in the Agreement.
Contact person's name, position and contact details:	As provided in the Agreement.
Activities relevant to the data transferred under these Clauses:	A customer of the data importer.
Signature and date:	Signature _____ Name _____ Title _____ Date Signed _____
Role (controller/processor):	Controller (under the C2P SCCs) or Processor (under the P2P SCCs).

Data importer(s): *Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*

Name:	Higher Logic, LLC
Address:	1919 N Lynn Street, Suite 500, Arlington, VA 22209, United States.
Contact person's name, position and	Kevin Boyce, CEO; Tel.: +1 (202) 360-4402, privacy@higherlogic.com.

contact details:	
Activities relevant to the data transferred under these Clauses:	Provider of cloud based engagement platforms.
Signature and date:	Signature DocuSigned by: Kevin M. Boyce 386D8C0E58CB46C... Name Kevin M. Boyce Title CEO Date Signed 9/30/2021
Role (controller/processor):	Processor (under the C2P SCCs) or sub-Processor (under the P2P SCCs).

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:
As described in Schedule 2 of the DPA.

Categories of personal data transferred:
As described in Schedule 2 of the DPA.

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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:
Subscribers are prohibited from including sensitive data or special categories of data as part of the Subscriber Data.

The frequency of the transfer (eg. whether the data is transferred on a one-off or continuous basis):
The frequency of the transfer is continuous (for as long as Subscriber uses the Service).

Nature of the processing:
As described in Schedule 2 of the DPA.

Purpose(s) of the data transfer and further processing:
As described in Schedule 2 of the DPA.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:
For the duration of the Master Subscription Agreement, with the addition of thirty (30) days in accordance with Higher Logic's backup policy, and subject to Section 12 of the DPA (Return or Deletion of Subscriber Data).

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
As described at https://www.higherlogic.com/legal/subprocessors.

C. COMPETENT SUPERVISORY AUTHORITY

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

The authority identified by the data exporter as its competent supervisory by notice to Higher Logic at privacy@higherlogic.com. If the data exporter does not submit such notice, the competent supervisory authorities will be determined based on the criteria specified in Clause 13 of the Standard Contractual Clauses.

Annex II
To the Standard Contractual Clauses

Technical And Organisational Measures Including Technical And Organisational Measures To Ensure The Security of The Data:

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

As described in Schedule 3 of the DPA.

Schedule 2 – Description of Processing

Purpose and Nature of Processing:
The purpose of Processing of Personal Data by Higher Logic is the performance of the Service pursuant to the Agreement. Processing activities include but are not limited to collection, storage, retrieval, use, disclosure and access to Personal Data to provide the Service.

Categories of Data Subjects:
Customers or prospective customers of Subscriber (natural persons), individuals, employees, agents, contractors, and affiliates of Subscriber.

Categories of Personal Data:
The Personal Data that may be Processed under the Agreement, as submitted by Subscriber to or through the Service, may include, but is not limited to first, middle and last name; email address; company name, and title. Subscribers are prohibited from including sensitive data or special categories of data as part of the Subscriber Data.

Subject matter and duration of the Processing:
The subject matter of the Processing of Personal Data is the provision of the Service to Subscriber. Personal Data will be Processed for the duration of the Agreement and in accordance with the DPA terms.

Obligations and rights of the Controller:
As described in the DPA and the Agreement.

Schedule 3 – Security Measures

Higher Logic maintains administrative, physical and technical safeguards for the protection of the security, confidentiality and integrity of Personal Data uploaded to the Service. Higher Logic staff are subject to background checks and sign confidentiality agreements protecting client data. Platform security practices include application firewalls, endpoint protection, intrusion detection, and log management. Active analysis is provided by a security operations center.

Policy Controls

Security and data privacy are governed with policies which address a range of business processes, organizational and technical requirements.

Higher Logic implements the following policies:

- Acceptable Use of Assets
- Access Control
- Business Continuity
- Communications Security
- Compliance
- Cryptography
- Disaster Recovery
- Human Resource
- Incident Response
- Information Security
- Maintenance Communication
- Policy Performance Evaluation
- Operations Security
- Organization of Information Security
- Physical Security
- Record Retention
- Risk Management
- Security Awareness Training
- Secure Systems Development

- Security Roles and Responsibilities
- Vendor Management

Technical Controls

To support policy requirements, technical controls are implemented as features of infrastructure, operating systems, management systems and applications. These controls allow Higher Logic to scale it's operations in a high assurance manner in alignment with documented information security controls. Technical controls align with access control, monitoring, security detection and response, deployment and capacity management controls.

Security Program Oversight

Security, data privacy and compliance operate under oversight from Higher Logic's executive management team. The program is evaluated for effectiveness, alignment with industry trends and customer expectations. We undergo multiple third-party audits annually including audits for ISO 27001, SOC 2, an internal IT audit and annual penetration testing conducted by Offensive Security Certified Professionals (OSCP) certified security engineers.

Risk Management

At least annually, we conduct a comprehensive risk assessment. The risk assessment considers a variety of possible risks including:

- effectiveness of security controls
- technical implementations
- operations processes
- human resource
- business continuity
- compliance with laws and regulations

Our risk management is also continuous. Risks may be identified, reported and remediated at any time in parallel with our comprehensive annual assessment.

Vendor Management

Our vendor management program tracks and qualifies all vendors. Sub-processors that handle customer data undergo additional scrutiny, are subject to a Data Processing Agreement, become added to our sub-processors list and undergo an annual review. Any risks identified are managed through our risk assessment process.

Backup Management

Data is backed up daily. Additionally, database logs are backed up every 20 minutes. Backups are stored as snapshots which allow for discrete point in time backups. Backups are securely, retained for up to 30 days and are for the purpose of site recovery and service continuity.

Disaster Recovery

Higher Logic has a documented Disaster Recovery Plan which is tested at least annually. The plan addresses all current platforms including Online Community and Marketing Automation. Our Software as a Service (SaaS) platform is designed to provide protection against incidents which would otherwise result in loss of availability.

Business Continuity

Annually, as part of our disaster recovery plan test, business continuity preparedness and procedures are reviewed. Our business systems are cloud based which allow for employees to work remotely in circumstances where one or more of our offices may be unavailable.

Network Security Model

Higher Logic operates our service production environment as an "air-gapped" network, isolated from our development, QA and corporate networks. All services within our production environment are self-contained with separate authentication, accounts and resources.

Intrusion Detection and Prevention

A comprehensive intrusion detection and prevention (IDS/IPS) system operates within our production environment. Every server, whether Internet facing or internal is installed with an IDS agent. An IDS server, local to the environment collates and correlates IDS data and forwards event data to our MSSP for real time analysis. Security events automatically evaluated as being a potential threat are escalated via an application programming interface (API) which is consumed by our perimeter security devices and used to trigger an immediate block of all network traffic from the attacker. The system operations run 7x24x365 and is automated. Additionally, a security operations center (SOC) analyst may trigger blocks base on analysis of real time log data, event correlation and other threat information.

Log Management

Production servers and services are configured for central spooling of log data to our MSSP. Logs are automatically analyzed for event correlation and are retained for 13 months. Higher Logic personnel do not have the ability to alter log data.

Anti-malware / Anti-virus

All production servers run artificial intelligence based anti-malware software which is centrally administered. The anti-malware solution used is not signature based. An attribute matrix

resulting from a machine learning model provides a higher degree of adaptability than signature-based methods.

Endpoint Security

For our corporate desktop systems, comprehensive endpoint security agents are used which provide protection from malware, viruses and malicious web sites. Encryption of endpoint storage devices is enforced with a minimum of AES-128 encryption. Remote management capabilities allow devices to be remotely wiped in the case of loss or theft.

Vulnerability Management

Production systems are scanned daily for known vulnerabilities. Vulnerabilities are reviewed and resolved based on risk assessment of severity.

Maintenance and Patching

Systems receive maintenance patches and updates quarterly. Scheduled system maintenance is disruptive and requires up to 8 hours of service downtime. Maintenance schedules are published on our customer support community. Critical patches are applied within 7 days.

Software Development Life Cycle (SDLC)

Application development and deployment follows Agile methodology. Changes specified and approved by Product Management are developed during a two week sprint schedule. Source control and automated unit testing are employed to provide an automated testing baseline for each release. Security reviews of architecture and application code are conducted when specific change management criteria are met.

We use a deployment method that stages new releases on server tiers that are rapidly deployed via changes to proxy routes. This method of deployment also provides a rapid reversion capability if, for any reason, a release containing a critical bug were to be deployed.

Penetration Testing

At least annually, each production platform is tested by a third party penetration testing firm. Vulnerabilities found are documented and remediated by our Engineering department. Penetration test reports are available to customers under a non-disclosure agreement.

Data Disposal

Our data disposal process complies with the NIST 800-88 standard for data disposal. For production server environments, we employ a technique known as cryptographic erasure, where data that is encrypted on a storage volume is disassociated from the encryption key, rendering the encrypted data unrecoverable.

Incident Response

An incident response plan (IRP) is in place which serves to improve the consistency of our response to incidents as well as improve the timeliness of our response activities. A documented cross functional incident response team (IRT) is in place that will assess and manage the incident through to resolution.

An incident affecting confidentiality, integrity or availability of customer data will be communicated, once confirmed, within 48 hours.

Privacy Practice

Our privacy practices are audited annually by a third party.