VBrick Systems, Inc. General Data Protection Addendum

This Data Protection Addendum ("**Addendum**") amends and supplements the cloud services agreement entered into between your party, acting on its own behalf and on behalf of each Customer Affiliate ("**Customer**"), and VBrick Systems, Inc. d/b/a Vbrick, acting on its own behalf and on behalf of each Vbrick Affiliate (**"Vbrick"),** as amended to date (the "**Original Agreement**").

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Original Agreement. Except as modified below, the terms of the Original Agreement shall remain in full force and effect.

Data Protection Laws (defined below) require that Customer and Vbrick or, where applicable, Vbrick Affiliates, have in place written contracts setting out certain mandatory provisions. In consideration of the mutual obligations set out in the Original Agreement, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Original Agreement for the purposes of complying with Data Protection Laws. Except where the context requires otherwise, references in this Addendum to the Original Agreement are to the Original Agreement as amended by, and including, this Addendum. Without limiting Customer's rights under the Original Agreement(s), the Parties agree as follows:

1. Definitions

1.1 In this Addendum, the following terms have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Adequate Territory**" means a territory outside of the European Economic Area that has been designated by the European Commission as ensuring an adequate level of protection pursuant to EU Data Protection Laws;

1.1.2 "**Adequate Transfer Mechanism**" means: (a) transferring Personal Data to a recipient that has achieved binding corporate rules authorisation in accordance with EU Data Protection Laws; (b) transferring Personal Data to a recipient that has executed Standard Contractual Clauses in circumstances that are appropriate for their use; or (c) any other mechanism that is recognised by the European Commission from time to time as providing adequate safeguards for the transfer of Personal Data to a third country while such mechanism is in force and provided that the relevant transfer is made in circumstances that are appropriate for its use;

1.1.3 "**Applicable Laws**" means all applicable law, statute, regulation, order, regulatory policy, guidance or industry code, rule of court or directives or requirements of any regulatory body, delegated or subordinated legislation, including applicable Data Protection Laws and laws that are enacted or become effective after the Effective Date;

1.1.4 "**CCPA**" means the California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100 *et seq.*) and its regulations, as amended;

1.1.5 "**Customer Affiliate**" means with respect to Customer, any current or future entity that, directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with Customer. Affiliate includes any successor (whether by dissolution, merger, consolidation, reorganization, or otherwise) to such entity or its business and assets;

1.1.6 "**Customer Group Member**" means Customer or any Customer Affiliate;

1.1.7 "**Customer Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a Customer Group Member pursuant to or in connection with the Original Agreement;

1.1.8 "**Contracted Processor**" means Vbrick or a Subprocessor;

1.1.9 "**Data Protection Laws**" means any of the following in respect of which any Customer Group Member is subject with respect to any Customer Personal Data: (a) EU Data Protection Laws; and (b) any other Applicable Laws with respect to data protection or privacy of any other country, which may include the CCPA;

1.1.10 "**EEA**" or "European Economic Area" means the Member States of the European Economic Area as it is made up from time to time, comprising the Member States of the European Union and such other countries that are party to the Agreement on the European Economic Area that entered into force on 1 January 1994;

1.1.11 "**EU Data Protection Law**" means all Applicable Laws relating to data protection, the processing of Personal Data and privacy, including: (a) the GDPR; (b) Directive 2002/58/EC; and (c) any applicable national laws and regulations that implement the GDPR or Directive 2002/58/EC ; (d) the proposed Regulation on Privacy and Electronic Communications if and when that Regulation comes into force in the European Union; (e) the United Kingdom version of the General Data Protection Regulation; (f) the Data Protection Act 2018; and any other law relating to data protection, the processing of personal data and privacy in the European Union or United Kingdom;

1.1.12 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.13 "**Permitted Derogation**" means any of the circumstances in which a transfer of Personal Data outside the European Economic Area is permitted in the absence of an adequacy decision pursuant to Article 45(3) GDPR or of appropriate safeguards pursuant to Article 46 GDPR, subject to the conditions set out in Article 49 GDPR as interpreted by Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 adopted by the European Data Protection Board on 25 May 2018;

1.1.14 "**Personal Data**" means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household;

1.1.15 "**Restricted Transfer**" has the meaning given to it in Section 12.1;

1.1.16 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Vbrick for Customer Group Members pursuant to the Original Agreement;

1.1.17 "**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of Personal Data to Processors established in third countries approved by the European Commission from time to time;

1.1.18 "**Subprocessor**" means any person (including any third party and any Vbrick Affiliate, but excluding an employee of Vbrick) appointed by or on behalf of Vbrick or any Vbrick Affiliate to Process Customer Personal Data on behalf of any Customer Group Member in connection with the Original Agreement;

1.1.19 "**Vbrick Affiliate**" means with respect to Vbrick, any current or future entity that, directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with Vbrick. Affiliate includes any successor (whether by dissolution, merger, consolidation, reorganization, or otherwise) to such entity or its business and assets; and

1.1.20 "**Vbrick Group Member**" means Vbrick or any Vbrick Affiliate.

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly. The terms "**Sale**" and "**Sell**" shall have the same meaning as in the CCPA.

1.3 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Authority

Vbrick warrants and represents that, before any Vbrick Affiliate Processes any Customer Personal Data on behalf of any Customer Group Member, Vbrick's entry into this Addendum as agent for and on behalf of that Vbrick Affiliate will have been duly and effectively authorized (or subsequently ratified) by that Vbrick Affiliate.

3. Processing of Customer Personal Data

3.1 Vbrick and each Vbrick Affiliate shall:

3.1.1 comply with all applicable Data Protection Laws in the Processing of Customer Personal Data;

3.1.2 not collect, retain, use, disclose, or Sell Customer Personal Data for any purpose other than for business purposes specified in the Original Agreement, or as otherwise permitted by law;

3.1.3 not share Customer Personal Data for the purpose of online advertising;

3.1.4 not retain, use, or disclose Customer Personal Data outside of the direct business relationship between Customer and Vbrick;

3.1.5 not combine Customer Personal Data with any Personal Data that Vbrick receives from an individual or any other person; and

3.1.6 only Process Customer Personal Data on documented written instructions from Customer Group Member unless Processing is required by Applicable Laws to which the Contracted Processor is subject, in which case Vbrick or the relevant Vbrick Affiliate will to the extent permitted by law inform the relevant Customer Group Member of the legal requirement before Processing the Personal Data.

3.2 Each Customer Group Member:

3.2.1 instructs Vbrick and each approved Vbrick Affiliate (and authorizes Vbrick and each Vbrick Affiliate to instruct each approved Subprocessor) to:

3.2.1.1 Process Customer Personal Data; and

3.2.1.2 in particular, subject to Section 12, transfer Customer Personal Data to any country or territory,

as reasonably necessary for the provision of the Services and consistent with the Original Agreement and this Addendum; and

3.2.2 warrants that it is and will at all relevant times remain duly and effectively authorized to give the instructions set out in Section 3.2.1 and 3.2.2 on behalf of each relevant Customer Affiliate and that such instructions shall not violate, or require any Contracted Processor to violate, any Applicable Laws.

To the extent a Customer Group Member provides instructions to any Contracted Processor regarding the Processing of Customer Personal Data other than those in Section 3.2.1 that would cause such Contracted Processor to incur additional costs or risks or have more than a de minimis impact upon such Contracted Processor's business or operations, Vbrick and the Customer Group Member shall negotiate in good faith to address such Customer Group Member instructions and any associated terms and conditions, costs, and reimbursements through the applicable change management process in the Original Agreement before any Contracted Processor is required to comply with such additional instructions.

3.3 The Vbrick or Vbrick Affiliate shall immediately inform the relevant Customer Group Member if, in its opinion, an instruction infringes Data Protection Laws. For the avoidance of doubt, neither Vbrick nor any Vbrick Affiliate shall have any affirmative obligation to monitor Customer Group Member instructions for compliance with applicable Data Protection Laws.

4. Vbrick and Vbrick Affiliate Personnel

Vbrick and each Vbrick Affiliate shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to Customer Personal Data, taking reasonable steps to ensure in each case that access is strictly limited to those individuals who need to know / access the relevant Customer Personal Data, as necessary for the purposes of the Original Agreement and this Addendum, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, and ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security

5.1 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, Vbrick and each Vbrick Affiliate shall in relation to Customer Personal 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.

5.2 In assessing the appropriate level of security, Vbrick and each Vbrick Affiliate shall take into account the risks that are presented by Processing, in particular from a Personal Data Breach.

5.3 At minimum, each Contracted Processor shall implement appropriate security protections and safeguards that are designed to comply with Applicable Laws and protect Customer Personal Data. Vbrick and each Vbrick Affiliate shall comply with the requirements set forth in the Data and Systems Security Schedule, attached as Annex II.

6. Subprocessing

6.1 Each Customer Group Member provides general written authorization for Vbrick and each Vbrick Affiliate to continue to use those Subprocessors already engaged by Vbrick or any Vbrick Affiliate previously approved by Customer as at the date of this Addendum, subject to Vbrick and each Vbrick Affiliate in each case as soon as practicable meeting the obligations set out in Section 6.3.

6.2 Vbrick shall keep an up to date list of its Subprocessors posted with its privacy policy at https://vbrick.com/privacy-policy/#0--privacy-policy.

6.3 With respect to each Subprocessor, Vbrick or the relevant Vbrick Affiliate shall:

6.3.1 before the Subprocessor first Processes Customer Personal Data (or, where relevant, in accordance with Section 6.2), carry out reasonable due diligence designed to ensure that the Subprocessor is capable of providing the level of protection for Customer Personal Data required by the Original Agreement and this Addendum and provide Customer with the opportunity to object to the engagement of the Subprocessor;

6.3.2 ensure that the arrangement between on the one hand (a) Vbrick, or (b) the relevant Vbrick Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract, including terms which offer a similar level of protection for Customer Personal Data as those set out in this Addendum and meets the requirements of article 28(3) of the GDPR; and

6.3.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) Vbrick, or (b) the relevant Vbrick Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, in accordance with Section 12.

6.4 To the extent a Subprocessor fails to fulfil its data protection obligations, Vbrick and each Vbrick Affiliate shall remain fully responsible and liable to Customer (subject to any disclaimers and limitations of liability in the Original Agreement) as if the Subprocessor were party to this Addendum in place of Vbrick.

7. Data Subject Rights

7.1 Taking into account the nature of the Processing, Vbrick and each Vbrick Affiliate shall assist each Customer Group Member by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer Group Members' obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

7.2 Where any Customer Group Member requests assistance from any Vbrick Group Member with respect to Data Subject rights under Data Protection Laws, and such Customer Group Member requires the Vbrick Group Member's assistance to respond to a request to exercise Data Subject rights under Data Protection Laws (such as, for example and without limitation, where the Customer Group Member does not have or have access to information necessary for the Customer Group Member to respond to a request to exercise Data Subject Rights under Data Protection Laws), that Vbrick Group Member shall promptly provide such reasonable assistance, cooperation or information requested by Customer Group Member within the timescales required for Customer Group Member to satisfy its obligations under Data Protection Laws, at each Customer Group Member's cost and expense.

7.3 Without prejudice to Sections 7.1 and 7.2, Vbrick shall:

7.3.1 promptly notify Customer if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data; and

7.3.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of Customer or the relevant Customer Affiliate or as required by Applicable Laws to which the Contracted Processor is subject, in which case Vbrick shall to the extent permitted by Applicable Laws inform Customer of that legal requirement before the Contracted Processor responds to the request.

8. Personal Data Breach

8.1 Vbrick shall notify Customer without undue delay and in any event within 48 hours upon Vbrick or any Subprocessor becoming aware of a Personal Data Breach affecting Customer Personal Data and shall provide Customer with reasonable cooperation and assistance to allow each Customer Group Member to meet any obligations to report or inform Data Subjects and/or government regulators of the Personal Data Breach as required under the Data Protection Laws.

Such notification shall as a minimum, to the extent known at the time of notification:

8.1.1 describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

8.1.2 communicate the name and contact details of Vbrick's data protection officer or other relevant contact from whom more information may be obtained;

8.1.3 describe the likely consequences of the Personal Data Breach; and

8.1.4 describe the measures taken or proposed to be taken to address the Personal Data Breach.

8.2 Vbrick shall reasonably co-operate with Customer and each Customer Group Member and take such reasonable commercial steps to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

9.1 Taking into account the nature of the Services and the information available to Vbrick, Vbrick and each Vbrick Affiliate shall provide reasonable assistance to each Customer Group Member, at each Customer Group Member’s cost and expense, with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required of any Customer Group Member by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9.2 Upon Customer reasonable request, Vbrick shall make available all information in its possession reasonably necessary to demonstrate Vbrick’s compliance with Applicable Laws.

10. Retrieval and deletion of Customer Personal Data

10.1 Customer will have access to and the sole responsibility to delete or retrieve all video files (and supplemental files thereto) and all application metadata, including any Customer Personal Data therein, prior to expiration or termination of the Original Agreement. Customer can retrieve or delete such data using the application user interface, an API provided by Vbrick, or if the Customer deems it necessary to meet Customer specific requirements, through a mutually agreed upon professional services engagement with Vbrick. All Customer data, including any Customer Personal Data therein, that has not been retrieved or deleted by Customer prior to expiration or termination of the Original Agreement, shall be deleted by Vbrick per Vbrick's data retention policy.

10.2 Each Contracted Processor may retain Customer Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Vbrick and each Vbrick Affiliate shall continue to maintain the confidentiality of all such Customer Personal Data and shall implement controls to ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

10.3 Upon timely written request from Customer, Vbrick shall provide written certification to Customer that it, and any applicable Vbrick Affiliate, has fully complied with this Section 10.

11. Audit rights

11.1 Vbrick will verify the adequacy of its security measures at least annually based on NIST 800-53 revision 4 standards, and Vbrick and each Vbrick Affiliate shall make available to each Customer Group Member on written request any reasonably requested information necessary to demonstrate compliance with this Addendum.

11.2 Customer agrees to exercise any right it may have to conduct an audit or inspection, including under the Standard Contractual Clauses if they apply, by instructing Vbrick to carry out the audits described in Section 11.1. If Customer wishes to change this instruction regarding the audits, then Customer has the right to request a change to this instruction by sendingVbrick written notice as provided for in the Original Agreement. If Vbrick declines to follow any reasonable instruction requested by Customer regarding audits or inspections, Customer is entitled to terminate this Addendumand the Original Agreement. If the Standard Contractual Clauses apply, nothing in this Section varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses.

11.3 Information and audit rights of Customer Group Members under Section 11.1 shall be without prejudice to any other information and audit rights under the Original Agreement.

12. Vbrick Rev Special Terms

12.1 This Section 12 shall apply only to Vbrick Rev Customers.

12.1.1 Sections 3, 7, 8-11 of this Addendum do not apply to the processing of Customer Personal Data through Vbrick Rev.

12.2 The parties acknowledge and agree that with regarding to Customer Personal Data Processed by Vbrick Rev, Customer is an independent controller and Vbrick is an independent controller. For clarity, Customer is not a joint controller with Vbrick.

12.3 Each party shall comply with its obligations under applicable Data Protection Laws, and this Addendum, when Processing Customer Personal Data. Vbrick warrants that it has obtained all necessary rights, consents, and permissions to collect, process, share, use and transfer personal data as contemplated in this Addendum. Upon request, Vbrick shall make available any and all records, disclosures or documentation relating to such consents or other permissions.

12.4 For purposes of Section 13, the Standard Contractual Clauses applicable to this Section are attached as Appendix 1 (including Annexes 1-2), and Appendix 2 does not apply.

13. International Transfers

13.1 Vbrick shall not permit (and shall implement controls designed to ensure that Vbrick Affiliates and Subprocessors do not permit) any processing of Customer Personal Data that originated within the European Economic Area or is otherwise subject to EU Data Protection Laws outside the European Economic Area (a "**Restricted Transfer**") unless:

13.1.1 the processing takes place in an Adequate Territory;

13.1.2 Vbrick (or Vbrick Affiliate or Subprocessor) first puts in place an Adequate Transfer Mechanism to ensure the transfer is in compliance with Data Protection Laws; or

13.1.3 Vbrick (or Vbrick Affiliate or Subprocessor) can undertake the processing in accordance with a Permitted Derogation and first obtains Customer's prior written consent to transfer Customer Personal Data outside of the European Economic Area in accordance with the relevant Permitted Derogation.

13.2 Unless Vbrick (or Vbrick Affiliate or Subprocessor) relies on Section 13.1.1 or implements a mechanism other than the Standard Contractual Clauses in accordance with Section 13.1.2 or 13.1.3, then each Customer Group Member (as "data exporter") and each Vbrick Group Member, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from that Customer Group Member to that Vbrick Group Member in accordance with the remaining provisions of this Section 13. Each party warrants that it has the right to enter into the Standard Contractual Clauses as provided in this Section 13.2 as agent for and on behalf of its Affiliates.

13.3 The Standard Contractual Clauses shall come into effect under Section 13.2 upon commencement of the relevant Restricted Transfer, subject to Sections 13.4 and 13.5 and the following conditions:

13.3.1 the Standard Contractual Clauses are attached as Appendix 2;

13.3.2 the appropriate Customer Group Member will be deemed to have entered into the Standard Contractual Clauses in its own name and on its own behalf in relation to Customer Personal Data disclosed to the appropriate Vbrick Group Member (and on behalf of any third party controller on behalf of whom Customer Group Member processes Customer Personal Data that is transferred to the appropriate Vbrick Group Member);

13.3.3 the appropriate Vbrick Group Member will be deemed to have entered into the Standard Contractual Clauses in its own name and on its own behalf in relation to Customer Personal Data disclosed to it by the Data Exporter(s);

13.3.4 the security measures referred to in Section 5 will be deemed to be set out in Annex 2 of the Standard Contractual Clauses (where relevant);

13.3.5 where and to the extent that the Standard Contractual Clauses apply pursuant to this Section 13, if there is any conflict between this Addendum or the Original Agreement and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail.

13.4 In the event that a Customer Group Member is located within the European Economic Area or an Adequate Territory and is acting as a Processor with respect to any Customer Personal Data, and wishes to transfer Customer Personal Data to a Vbrick Group Member, then that Customer Group Member shall be deemed to have entered into the Standard Contractual Clauses in accordance with Section 13.3 as agent for and on behalf of the Controller of Customer Personal Data (whether the Controller is another Customer Group Member or a third party) with respect to the transfer of Customer Personal Data to the relevant Vbrick Group Member.

13.5 In the event that a Vbrick Group Member is located within the European Economic Area or an Adequate Territory and wishes to transfer Customer Personal Data to a Contracted Processor located in a territory outside of the European Economic Area that is not an Adequate Territory, then Vbrick Group Member shall ensure that the Contracted Processor first enters into Standard Contractual Clauses with Customer Group Member from whom Customer Personal Data has originated on substantially the same terms as those set out in Section 13.3.

13.6 For the avoidance of doubt, where Vbrick Group Member has entered into the Standard Contractual Clauses pursuant to this Section 13 and wishes to undertake a subsequent transfer to a Subprocessor, then Vbrick Group Member shall enter into the Standard Contractual Clauses with such Subprocessor as provided in the Standard Contractual Clauses to which it is a party with Customer or Customer Group Member. At the request of a Customer Group Member, Vbrick Group Member shall use commercially reasonable efforts to procure that the Subprocessor enters into Standard Contractual Clauses directly with Customer Group Member to facilitate such subsequent transfer.

14. General Terms

Governing law and jurisdiction

14.1 Without prejudice to and save as and to the extent provided in clauses 17 (Governing Law) and 18 (Choice of Forum and Jurisdiction) of the Standard Contractual Clauses:

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

14.1.2 this Addendum 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 Original Agreement.

Order of precedence

14.2 Nothing in this Addendum reduces Vbrick's or any Vbrick Affiliate's obligations under the Original Agreement in relation to the protection of Personal Data or permits Vbrick or any Vbrick Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Original Agreement. In the event of any conflict or inconsistency between

this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

14.3 Subject to Section 13.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Original Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

Changes in Data Protection Laws, etc.

14.4 The parties may agree to revise this Addendum by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement) or by revising the form of Standard Contractual Clauses that are deemed to be entered into pursuant to Section 12. Neither Customer nor Vbrick shall require the consent or approval of any Customer Affiliate or Vbrick Affiliate or Subprocessor to amend this Addendum pursuant to this Section 13.4.

14.5 *Severance*

Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

APPENDIX 1: STANDARD CONTRACTUAL CLAUSES (Vbrick as Controller)

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) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

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

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(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 omitted

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 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. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties 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.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

8.5 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 personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (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.

(a) The Parties have agreed on the technical and organisational measures set out 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 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 personal data breach, including measures to mitigate its possible adverse effects.

(d) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information

can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(e) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(f) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 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 or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data 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") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it 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 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

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

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9 omitted

Clause 10

Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the

enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge :

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter "automated decision"), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

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) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.

(c) 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.

(d) The Parties agree that if one Party is held liable under paragraph (c), 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.

(e) The data importer may not invoke the conduct of a processor or 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;

(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.

(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.

(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.

(a) 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.

(b) 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

OPTION 1: 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 Germany.

OPTION 2: These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

Clause 18

Choice of forum and jurisdiction

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

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

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

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

APPENDIX 2: STANDARD CONTRACTUAL CLAUSES (Vbrick as Processor)

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) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

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

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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

Clause 4

Interpretation

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

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

(e) 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 omitted

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 Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where

possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

(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.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing (including elctronic communications) of any intended changes to that list through the addition or replacement of sub-processors at least fifteen (15) 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.

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

(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;

(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.

(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.

(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

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

(e) 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).

(f) 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.

(g) 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.

(h) 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

OPTION 1: 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 Germany.

OPTION 2: These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

Clause 18

Choice of forum and jurisdiction

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

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

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

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

ANNEX I TO THE STANDARD CONTRACTUAL CLAUSES

This Annex forms part of the Clauses and must be completed and signed by the parties.

A. List of Parties

Data exporter
The data exporter is:

Customer as detailed in Original Agreement

Description of Activities Relevant to the Transfer:

Data importer
The data importer is:

Name: VBrick Systems, Inc. d/b/a Vbrick

Address: 607 Herndon Parkway, Suite 300, Herndon VA 20170 USA

Contact Person:

Tel.: 1.866.827.4251; e-mail: privacy@vbrick.com

Role: Processor

Description of Activities Relevant to the Transfer:

B. Description of Transfer

Data subjects
The personal data transferred concern the following categories of data subjects:

Customer videos will be transferred by the data exporter (the customer) to the service in the Cloud via encrypted HTTPS protocol and stored in the Cloud service for later access. Recordings of live events which have been hosted using our webcast platform may also be stored on our service. The Data exporter (the customer) will also likely export LDAP directory data to our service to allow for the creation of user identities for their users. This information usually entails only a user name, email address and last name of the user. Other than values for these three fields, no other personal data for individuals is necessary, but the customer may choose to upload optional information such as full name, a phone number (presumably for their work phone) and their title.

Categories of data
The personal data transferred concern the following categories of data:

The Data exporter has complete control over what video data is uploaded to our service and may upload data at any time. The Cloud service undertakes automated processing to reformat the videos in the format chosen by the customer, but no manual work or processing is done by Vbrick staff. All administration of a customer's tenant is done by customer assigned administrators or users granted permissions by those administrators.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data:
NA

Frequency of the transfer:

At Data exporter's discretion and control.

Nature of the processing:
The personal data transferred will be subject to the following basic processing activities:

Video data uploaded to the Cloud service is run through a video reformatter to allow the video to be stored in a format which is able to be played in both web and mobile platforms. This usually consists of producing HLS video data for multi-bitrate streaming.

Webcasts or video conferences which are recorded are uploaded to the Cloud service and reformatted in a similar fashion to video files. The difference is that the recording is produced for conference calls in real time before the video is formatted and made available for viewing. This is all automated.

LDAP or other Directory data uploaded to Rev is used to create both user identities and user groups based on the customer's existing corporate directory structure. The customer can control what groups and users are uploaded to the Cloud service. These identities are stored in a database and used to attach permissions for that user as well as group membership.

Purpose of the data transfer and further processing:

Enterprise video streaming, management, and storage.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

Dependent on the term of the applicable subscription license(s) Data exporter purchases from Data controller.

C. Competent Supervisory Authority

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 shall act as competent supervisory authority.

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 shall act as competent supervisory authority.

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 shall act as competent supervisory authority.

ANNEX II TO THE STANDARD CONTRACTUAL CLAUSES

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

This Annex forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clause 8.6 and 10(b)

Vbrick shall establish, maintain, and enforce security measures that meet or exceed the requirements of this Schedule that are designed to protect against the destruction, loss, unauthorized access, use, or alteration of Customer Confidential Information, which is defined as Customer Personal Data, video content, hosted by Vbrick for Customer in its virtual private cloud environment,. Notwithstanding the requirements of this Schedule, for so long as Vbrick retains Customer's Confidential Information or has access to Customer's Confidential Information including Customer Personal Data, computer systems, or networks, Vbrick shall: (a) use commercially reasonable efforts to meet the ever-evolving risks facing the security of Confidential Information and computer systems and networks; and (b) comply with all applicable privacy and security laws, regulations, and standards. In the event that Vbrick subcontracts, outsources, or otherwise relies on a third-party in support of Customer or Vbrick's obligations under the Agreement, Vbrick shall ensure that such third-parties (including Subcontractors) meet information security obligations consistent with the following requirements, and that Vbrick uses reasonable effort to exercise oversight over such third parties, to the extent applicable to the third party's performance.

1. ACCESS CONTROL

a. **Access**: Vbrick uses measures designed to deny all access to information systems and resources by default. Access is granted by request for specific business purposes and requires approval by management. Vbrick maintains usage restrictions and configuration/connection requirements for information systems (including wireless) access, which requires prior authorization for access to the systems prior to allowing such connections.

b. **Account Management**: Vbrick configures its information systems and resources in a manner designed to enforce access control policies and standards. This includes the use of mechanisms designed to support information system account management, which remove and/or disable temporary, emergency, and inactive accounts after a pre-determined time period for each type of account and mechanisms that require and/or force users to log out after a pre-determined amount of inactivity.

c. **Access Control for Mobile Devices**: Vbrick maintains usage restrictions, configuration/connection requirements, and implementation guidance for organization-controlled mobile devices, and authorizes (as described above) the connection of mobile devices to organizational information systems.

d. **Separation of Duties**: Vbrick employs the principle of separation of duties of individuals to reduce the risk of potential abuse and malevolent activity, documents the separation of such duties and individuals, and defines information system access authorizations.

e. **Least Privilege**: Vbrick employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks and business functions. Vbrick controls the use of administrative privileges by tracking, preventing, and correcting the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

f. **Premises Access:** Vbrick agrees that Customer in its sole discretion, but in compliance with law, may require Vbrick to remove a person or entity within Vbrick's authority or control from Customer property or prevent the access of a person or entity within Vbrick's authority or control to Customer's systems, in which case that person or entity may not be reassigned to another Customer location.

2. AWARENESS AND TRAINING

a. **Security Awareness Training/Role-Based Training**: Vbrick maintains, documents, and distributes a security awareness and training policy that addresses the purpose, scope, roles, responsibilities, coordination among organizational entities, and compliance with the policy. Vbrick maintains procedures that implement the security awareness training policy. The program is reviewed and updated regularly to reflect changes in the organizational risk management strategy and industry best practices and standards. Vbrick provides role-based security training to personnel with assigned security roles and responsibilities before authorizing access to applicable information systems and as Vbrick determines is needed thereafter.

b. **Security Training Records**: Vbrick documents and retains individual information security training activities, including basic security awareness training and specific information system security training.

3. AUDIT AND ACCOUNTABILITY

a. **Audit Records**:

i. Vbrick's information systems generate audit records for certain types of events containing the type of event, the date and time of the event, the location of the event, the source of the event, the outcome of and response to the event, the individual(s) associated with the event and any other information relevant to the event and provide such information to Customer upon request.

ii. Vbrick agrees that Customer may, upon reasonable request (but not more than once every twelve (12) months) and with reasonable prior written notice (not less than thirty (30) days), conduct a security audit, based on NIST 800-53 revision 4 standards, of Vbrick systems and physical facility which may cover, Vbrick's security measures for its computer systems (subject to any applicable restrictions or requirements, including without limitation confidentiality, security, and nondisclosure obligations and policies, imposed by third parties or Subcontractors) and physical facilities and its security policies, procedures, and controls, and may involve preparing a confidential report thereon ("Security Report"). Such audit, which will occur during Business Hours, may be conducted by Customer's personnel. Customer shall bear its own costs and expenses and reimburse Vbrick for all costs and expenses Vbrick incurs, in connection with any such audit.

b. **Standardized Audit Reporting**: The Vbrick security program is based on NIST 800-53 revision 4 standards and is audited annually as part of our FedRAMP Continuous monitoring program. Access to reports is restricted to authorized Federal Agencies, however status can be validated on the FedRAMP Marketplace. The scope of such audit will include attestations of availability, security, privacy, processing integrity, disaster recovery, backup, and contingency plans and systems, and confidentiality, as Vbrick deems appropriate.

c. **Non-Repudiation**: Information systems are designed to enforce non-repudiation to protect against an individual (or process acting on behalf of an individual) falsely denying having performed certain tasks, including creating information, sending and receiving messages, approving information, signing contracts, and approving procurement requests.

d. **Audit Information**:

i. Information systems are designed to protect audit information, including audit records, audit settings, audit reports, and audit tools from unauthorized access, modification, and deletion. Audit information is backed up onto a physically different system or system component than the system or component being audited. The information systems implement cryptographic protection designed to ensure the integrity of audit information.

ii. Vbrick retains audit records for reasons including, without limitation, to provide support for after-the-fact investigations of Security Incidents and to meet regulatory and organizational information retention requirements.

4. SECURITY ASSESSMENT AND AUTHORIZATION

a. **System Interconnections**: Vbrick documents the interface characteristics, security requirements, and the nature of the information communicated for each interconnection, and reviews and updates the Interconnection Security Agreements regularly.

b. **Security Authorization**: Vbrick assigns a senior-level executive or manager as the authorizing official for the information systems, implements processes to ensure that such official authorizes the information systems for processing before commencing operations, and periodically updates the security authorization as needed.

c. **Continuous Monitoring**: Vbrick maintains a continuously monitors information systems in a manner designed to prevent data exfiltration, mitigate the effects of exfiltrated data, and protect the privacy and integrity of sensitive information. Vbrick's continuous monitoring program includes establishing metrics to be monitored, the frequency for monitoring, and ongoing security control assessments and ongoing security status monitoring of organization-defined metrics, in accordance with Vbrick's continuous monitoring strategy, correlation and analysis of security-related information generated by assessments and monitoring, response actions to address the results of such analysis, and reporting the security status of Vbrick and information systems to the appropriate personnel.

5. CONFIGURATION MANAGEMENT

a. **Baseline Configuration**: Vbrick develops, documents, and maintains a current baseline configuration of the information systems. Baseline configurations are formally reviewed, and regularly listd, including when Vbrick deems necessary, as an integral part of information system component installations and updates. Vbrick retains previous versions of baseline configurations of the information systems to support rollback, and maintains a baseline configuration for information system development and test environments that is managed separately from the operational baseline configuration. Vbrick establishes, implements, and actively tracks, corrects, and reports on the security configuration of network infrastructure devices using a configuration management and change control process designed to prevent attackers from exploiting vulnerable services and settings.

b. **Configuration Change Control**: Vbrick establishes, implements, and actively manages the security configuration of network infrastructure devices using a configuration management and change control process designed to, in part, prevent attackers from exploiting vulnerable services and settings. Vbrick: (a) determines the types of changes to the information systems that are configuration-controlled; (b) reviews proposed configuration-controlled changes to the information systems and approves or disapproves such changes with explicit consideration for security impact analyses; (c) documents configuration change decisions; (d) implements approved changes; (d) retains records of changes; (e) audits and reviews activities associated with configuration-controlled changes to the systems; and (f) coordinates and provides oversight for configuration change control activities. Vbrick employs automated mechanisms to document proposed changes to the information system. Vbrick tests, validates, and documents changes to the information systems before

implementing the changes on the operational systems, and requires that an information security representative be a member of the configuration change control team.

c. **Information System Component Inventory**: Vbrick develops and documents an inventory of information system components that reflect the current information systems, which includes all components within the authorization boundary of the system, is at the level of granularity Vbrick deems appropriate for tracking and reporting, and is reviewed and updated regularly and on an as needed basis. Vbrick tracks hardware devices on its non-public networks in a manner designed to ensure that only authorized devices are given access.

d. **Configuration Management Plan**: Vbrick develops, documents, and implements a configuration management plan for the information systems that addresses roles and responsibilities, as well as defines detailed processes and procedures for how configuration management is used to support the system development lifecycle. The plan describes how to move changes through the system, how to update baselines and configuration settings, how to maintain system component inventories, and how to control development, test, and operational environments.

6. CONTINGENCY PLANNING AND BUSINESS CONTINUITY / DISASTER RECOVERY

a. **Contingency Plan**: Vbrick develops a contingency plan for the information systems, which identifies essential business missions/functions and associated contingency requirements, provides recovery objectives and restoration responses, addresses contingency roles and responsibilities, addresses maintaining essential business functions in the event of system disruption or failure, and addresses full system restoration without deterioration of the security safeguards in place. Such plan is be regularly reviewed and updated as Vbrick deems necessary.

b. **Contingency Training**: Vbrick provides contingency training to information system users consistent with assigned roles and responsibilities when an individual assumes a contingency role or responsibility, whenever required by information system changes, and periodically thereafter. Such training may include simulated events and automatic training environments to provide thorough and realistic contingency training.

c. **Alternate Storage Site**: Vbrick maintains alternate storage locations permitting storage and retrieval of information system backup information. Vbrick requires such locations to maintain information security safeguards no less protective than the primary site.

d. **Information System Backup**: Vbrick conducts backups of user-level information, system-level information, and system documentation including security-related documentation, and implements safeguards and controls designed to protect the confidentiality, integrity, and availability of backup information at storage locations.

e. **Information System Recovery and Reconstitution**: Vbrick's contingency plans are designed to promote the recovery and reconstitution of the information systems to a known state after disruption, compromise, or failure. This recovery plan includes transaction-based recovery, and is designed to protect backup and restoration hardware, software, and firmware.

7. IDENTIFICATION AND AUTHENTICATION

a. **Identification and Authentication (Organizational Users)**: Vbrick information systems are designed to uniquely identify and authenticate organizational users, or processes (*e.g.* service accounts) acting on behalf of organizational users. Vbrick information systems implement multifactor authentication where available for network and local access to both privileged and non- privileged accounts, such that one of the factors is provided by a device separate from the system gaining access. Vbrick's systems provide for single-sign on capabilities and implement replay- resistant authentication mechanisms.

b. **Identification and Authentication (Non-Organizational Users)**: Vbrick information systems are designed to uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).

c. **Authenticator Management**: Vbrick manages information system authenticators by: (a) using mechanisms designed to verify the identity of the individual, group, role, or device receiving the authenticator; (b) establishing initial authenticator content for authenticators defined by Vbrick (c) using authenticators of a reasonable strength for their intended use; (d) maintaining administrative procedures for initial authenticator distribution, for lost, compromised, or damaged authenticators, and for revoking authenticators; (e) changing default content of authenticators prior to information system installation; (f) establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; (g) changing/ refreshing authenticators; (h) using safeguards and controls designed to protect authenticator content from unauthorized disclosure and modification; (i) requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and (j) changing authenticators for group/role accounts when membership to those accounts changes. Vbrick takes into consideration the type of authentication (e.g., hardware token-based, PKI-based, password-based, biometric-based, etc.) and applies additional security controls as it deems appropriate.

8. INCIDENT RESPONSE

a. **Incident Response Training**: Vbrick provides incident response training to information system users consistent with assigned roles and responsibilities upon assuming an incident response role or responsibility, when required by system changes, and regularly thereafter.

b. **Incident Handling**: Vbrick implements security incident handling procedures that: (a) cover preparation, detection, analysis, containment, eradication, and recovery capabilities, (b) are designed to coordinate incident handling activities with contingency planning activities, and (c) incorporate past security incidents into ongoing response procedures, training, and testing. Vbrick coordinates with external organizations to correlate and share incident information to achieve cross-organizational awareness and more effective incident responses. This includes coordinating incident handling activities involving supply chain events with other organizations involved in the supply chain.

c. **Incident Notification**: In the event that Vbrick becomes aware of any security incident or Personal Data Breach impacting Customer Personal Data or Confidential Information, Vbrick shall in addition to any notification obligations in the Agreement or the Addendum, (i) promptly, in consultation with Customer, investigate the security incident or Personal Data Breach; (ii) remediate and/or mitigate the risk to Customer Personal Data or Confidential Information or systems or effects of the Security Incident; (iii) preserve relevant records and other evidence; (iv) implement a plan designed to prevent such a Personal Data Breach from reoccurring; and (v) take all other actions required under this Addendum. Vbrick maintains automated mechanisms designed to assist in the reporting of Security Incidents.

9. MAINTENANCE

a. **Nonlocal Maintenance**: Vbrick: (a) approves and monitors nonlocal maintenance and diagnostic activities; (b) allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; (c) employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions; (d) maintains records for nonlocal maintenance and diagnostic activities; and (e) terminates session and network connections when nonlocal maintenance is completed. Vbrick protects nonlocal maintenance sessions by employing replay-resistant authenticators and separating the maintenance

sessions from other network sessions by either physically or logically separated communication paths based upon encryption.

b. **Timely Maintenance**: Vbrick endeavors to obtain maintenance support, or spare parts, or both for information system components in a timely manner following system or component failure. Vbrick performs preventative maintenance on critical information system components at regular intervals.

10. MEDIA PROTECTION

a. **Media Use**: Vbrick prohibits the transfer of Confidential Information outside of the Vbrick virtual private cloud environment (excluding transfer to virtual private cloud environments used for disaster recovery by Vbrick). Further, Vbrick shall use encryption to protect information stored in the Vbrick virtual private cloud environment ("Covered Information").

b. **Media Storage**: Vbrick physically controls and securely stores both digital and non-digital media, and uses security controls and safeguards designed to protect information system media until such media are destroyed or sanitized using secure data destruction techniques that render data unrecoverable. Vbrick employs mechanisms designed to restrict access to media storage areas and to audit access attempts and access gained.

c. **Media Sanitation**: Vbrick and its hosting provider sanitizes information system media prior to disposal, release from organizational control, or release for reuse in accordance with organizational policies, employing sanitation mechanisms with the strength and integrity commensurate with the security category or classification of the information. Vbrick: tracks and documents the media sanitation process, including personnel who handled such media, and verifies that that sanitation of the media was effective prior to disposal. The information systems, system components, and system devices are capable of being purged/wiped remotely to protect data obtained by unauthorized individuals.

11. PHYSICAL AND ENVIRONMENTAL PROTECTION

a. **Physical Access Control**: For facilities housing the Vbrick virtual private cloud systems, Vbrick's hosting services provider: (a) enforces physical access authorizations at facility entrance/exit points by verifying individual access authorizations before granting access to the facility; (b) maintains physical access audit logs for entry/exit points; (c) physical access control devices (*e.g.* alarms, card swipe, keypads); (d) escorts visitors and monitors their activity; (e) secures, through direct and indirect means, physical access devices (*e.g.* keys, cards, combinations, credentials); (f) inventories physical access devices regularly; and (g) changes physical access devices when lost or compromised, or when individuals who are possession thereof are transferred or terminated.

b. **Power Equipment and Cabling**:

i. Vbrick implements measures designed to protect power equipment and power cabling for the information systems from damage and destruction.

ii. Vbrick employs physically separate, redundant power cables in a manner designed to ensure that power continues to flow to the hosted system environment in the event that one cable is cut or otherwise damaged, as well as automatic voltage controls for critical information system components.

c. **Location of Information System Components**: Vbrick positions information system components within the facility in a manner designed to minimize potential damage from environmental hazards (*e.g.* flooding, fire, tornados, earthquakes, hurricanes, vandalism, acts of

terrorism, electromagnetic pulse, electrical interference, etc.) as well as physical hazards, including the opportunity for unauthorized access.

12. PERSONNEL SECURITY

a. **Personnel Screening**: Vbrick screens individuals prior to authorizing access to the information system and performs rescreening on individuals Vbrick deems necessary.

b. **Personnel Termination**: Upon termination of an individual, Vbrick promptly: (a) disables the individual's information system access; (b) terminates/revokes any authenticators/credentials associated with the individual; (c) conducts exit interviews that include information security topics; (d) retrieves all security-related organizational information system-related property (*e.g.* hardware authentication tokens, system administration technical manuals, keys, identification cards, building passes, etc.); and (e) retains access to organizational information and information systems formerly controlled by terminated individual.

13. RISK ASSESSMENT

a. **Risk Assessment**: Vbrick annually: (a) conducts a risk assessment, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information systems and the information they process, store, or transmit; (b) documents and reviews the risk assessment results; and (c) updates the risk assessment regularly, and whenever there are significant changes to the information system or environment of operation (*e.g.* the identification of new threats and vulnerabilities).

b. **Vulnerability Scanning**: Vbrick: (a) scans for vulnerabilities in the information systems and hosted application at least monthly and when new vulnerabilities potentially affecting the system/applications are identified and reported; (b) employs vulnerability scanning tools and techniques that are designed to facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for enumerating platforms, software flaws, and improper configurations, formatting checklists and test procedures, and measuring vulnerability impact; (c) analyzes vulnerability scan reports and results from security control assessments; (d) remediates or mitigates material vulnerabilities in accordance with the organizational risk assessment; (e) shares information from the vulnerability scanning and security control assessments with appropriate personnel to help eliminate similar vulnerabilities in other information systems; g) employs annual vulnerability scanning and periodic penetration testing to assess the overall strength of Vbrick's safeguards.

14. SYSTEM SERVICES AND ACQUISITION

a. **System Development Life Cycle**: Vbrick manages information systems using an industry standard System Development Life Cycle ("SDLC") that incorporates information security considerations, defines and documents information security roles and responsibilities throughout the SDLC, identifies individuals having such roles or responsibilities, and integrates Vbrick's information security risk management process into SDLC activities.

b. **Developer Security Testing and Evaluation**: Vbrick requires Developer to: (b) perform unit, integration, system, and regression testing and evaluation, and produce evidence and results thereof; (c) implement a verifiable flaw remediation process; and (d) remediate identified flaws. Vbrick employs static code analysis tools to identify common flaws and document the results of such analysis.

c. **Supply Chain Protection**: Vbrick (a) protects against supply chain threats to the information systems, components, or service by employing security safeguards as part of a comprehensive information security strategy, including the use of secure acquisition strategies, contract, tools, and

procurement methods for purchasing of information systems, components, and services from suppliers; (b) conducts supplier reviews prior to engaging into a contractual agreement to acquire information systems, components, or services; (c) maintains security safeguards designed to limit harm from potential adversaries targeting the organizational supply chain; and (d) conducts assessments of the information systems, components, or services prior to selection, acceptance, or update.

15. SYSTEM AND COMMUNIATIONS PROTECTION

a. **Security Function Isolation**: Vbrick information systems are designed to isolate security functions from non-security functions using isolation boundaries designed to control access to and protect the integrity of hardware, software, and firmware that perform security functions, and implement code separation. Vbrick implements security functions as a layered structure minimizing interactions between layers of the design and designed to avoid dependence by lower layers on the functionality or correctness of higher layers.

b. **Boundary Protection**: Vbrick information systems are designed to monitor and control communications at the external boundary of the system and at key internal boundaries within the system, implement sub-networks for publicly accessible system components that are physically and logically separated from internal Vbrick networks, and connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture. Vbrick limits the number of external network connections. Information systems at managed interfaces are designed to deny network communications traffic by default and allow network communications traffic by exception for both inbound and outbound communications. Vbrick manages the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

c. **Transmission Confidentiality and Integrity**: Vbrick information systems are designed to protect the confidentiality and integrity of transmitted information through the use of both physical and logical means, including employing protected distribution procedures and limiting access to peripherals (*e.g.* servers, computers, printers, scanners, facsimile machines), and through the use of encryption.

d. **Protection of Information at Rest**: Vbrick information systems are designed to protect the confidentiality and integrity of information at rest through the use of encryption or other suitable measures (*e.g.* storing such information off-line in a secure location).

e. **Encryption**: Any Covered Information retained or transmitted by a Vbrick information system shall be encrypted at a rate of at least 256-bit encryption.

16. SYSTEM AND INFORMATION INTEGRITY

a. **Flaw Remediation**: Vbrick: (a) implements processes designed to identify, report, and correct information system flaws; and (b) installs security-relevant software and firmware updates once they are available.

b. **Malicious Code Protection**: Vbrick: (a) employs malicious code protection mechanisms at information system exit and entry points (including web browsers and email) designed to detect and eradicate malicious code; (b) updates Malicious Code protection mechanisms and maintains organizational configuration management policy and procedures for managing such updates; (c) configures Malicious Code protection mechanisms to perform periodic scans of the information systems and real-time scans of files from external sources, as the files are downloaded, opened, or executed; and (d) blocks, quarantines, or both, Malicious Code and maintains systems that send alerts to system administrator(s) in response to Malicious Code detection.

c. **Information System Monitoring**: Vbrick: (a) monitors the information systems to detect attacks; indicators of potential attacks; unauthorized local, network, and remote connections; and unauthorized use of the information system; (b) implements safeguards designed to protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; and (c) provides information system monitoring information to appropriate personnel as needed.

d. **Software, Firmware, and Information Integrity**: Vbrick maintains integrity verification tools designed to detect unauthorized changes to software, firmware, and information. Vbrick performs regular integrity checks and employs tools that provide notification to personnel upon the discovery of discrepancies during integrity verification.

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorized the use of the sub-processors detailed at https://portal.vbrick.com/dpasubs/