VIDYARD CUSTOMER DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is entered into by and between Buildscale, Inc. (dba and referred to herein as "**Vidyard**") and Customer, and forms part of the services agreement(s) previously entered into by and between Vidyard and Customer (the "**Agreement**").

Vidyard agrees that it shall comply with the following provisions with respect to all Personal Information collected, used, transmitted or maintained for Customer. This Addendum stipulates privacy, confidentiality, and security requirements and demonstrates compliance with applicable privacy, security and data protection laws. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

Except as amended by this DPA, the Agreement will remain in full force and effect. In the event of a conflict between this DPA and the Agreement, this DPA will control, but only to the extent of the conflict. If Vidyard and Customer have entered into a previous version of this DPA, upon execution by Customer, this DPA will replace and supersede, in its entirety, the previous version of this DPA. This DPA shall only become legally binding between Vidyard and Customer upon Customer's execution of this DPA. This DPA may be executed in two or more counterparts, including facsimile or e-mail counterparts, which together shall constitute a single agreement.

HOW TO EXECUTE THIS DPA:

1. To complete this DPA, Customer must:
   a. Complete the information in the signature block and sign on Page 8;
   b. Complete the information requested on Pages 19, 20, 23 and 29 and sign each page; and
   c. Complete the information on Page 30.

2. Submit the completed and signed DPA to Vidyard via email to privacy@vidyard.com

The DPA will only become legally binding between Vidyard and Customer upon the completion of all steps listed under "How to Execute this DPA". Any modifications, alterations or amendments to the content of this DPA (including, but not limited to, striking out any portion of the Agreement or inserting any content to the Agreement) will fully prevent the formation of a binding and enforceable agreement between the parties. FOR CLARITY, VIDYARD WILL NOT BE LIABLE FOR ANY AMOUNTS CLAIMED UNDER AN AGREEMENT THAT (I) HAS NOT STRICTLY MET ALL REQUIREMENTS SET OUT FOR FORMATION OF THE AGREEMENT OR (II) HAS MADE ANY MODIFICATIONS TO THE AGREEMENT.

1. Definitions.

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

(b) "**Applicable Laws**" means all statutes, cods, rules, regulations, by-laws, judicial or arbitral or administrative or ministerial or departmental or regulatory judgments, orders, decisions, rulings or awards, policies, guidelines, or any provisions of the foregoing, including general principles of common and civil law and equity, binding on or affecting the person referred to in the context in which such word is used.

(b) **"CCPA"** means the California Consumer Privacy Act of 2018.

(c) "**Customer**" means the party to the Agreement that receives a subscription to the Services.

(d) **"Customer Personal Information"** means any Personal Information originated by Customer

that Customer submits, collects or provides in the course of using the Services.

(e) "**EEA Personal Data**" means personal data (as defined in GDPR) pertaining to individuals in the European Economic Area ("**EEA**") and Switzerland.

(f) "**GDPR**" means the EU GDPR and the UK GDPR, where:
(i) "**EU GDPR**" means the General Data Protection Regulation (EU) 2016/679; and
(ii) "**UK GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation) (as implemented by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020).

(g) "**Internal Control Report**" means a Type II Service Organizational Control (SOC) report (based on the SSAE 16 or ISAE 3402 model) or any successor report thereto.

(h) "**Personal Information**" means any and all data (regardless of format) that (i) identifies or can be used to identify, contact or locate a natural person, or (ii) pertains in any way to an identified natural person. Personal Information includes obvious identifiers (such as names, addresses, email addresses, phone numbers and identification numbers) as well as biometric data, EEA Personal Data and UK Personal Data, and any and all information about an individual's computer or mobile device or technology usage, including (for example) IP address, MAC address, unique device identifiers, unique identifies set in cookies, and any information passively captured about a person's online activities, browsing, application or hotspot usage or device location.

(i) "**Privacy Laws**" means all Applicable Laws that regulate the Processing of Personal Information. In particular, "Privacy Laws" includes the GDPR, UK Data Protection Law, the CCPA, and other Applicable Laws that specify privacy, security or security breach notification obligations that affect the Personal Information or the provision of the Services by Vidyard .

(j) "**Processing**" means any operation or set of operations which is performed upon Personal Information, whether or not by automatic means, such as collection, compilation, use, disclosure, duplication, organization, storage, alteration, Transfer, transmission, combination, redaction, erasure, or destruction.

(k) "**Security Breach**" means a "personal data breach" (as defined in the GDPR), a "breach of the security of a system" or similar term (as defined in any other applicable Privacy Law) or any other event that compromises the security, confidentiality or integrity of Personal Information.

(l) "**Services**" means any and all services that Customer requests Vidyard to perform under the Agreement or any other contract or agreement that involves Processing of Personal Information.

(m) "**Subprocessor**" means any third party (including an Affiliate of Vidyard) that provides any services to Vidyard and that may have access (including inadvertent access) to any Customer Personal Information.

(n) "**Third Countries**" means all countries outside the scope of the applicable Privacy Laws of either the EEA or the United Kingdom, excluding countries approved as providing adequate protection:

(i) with respect to EEA Personal Data, by the European Commission from time to time; and

(ii) with respect to UK Personal Data, the UK Secretary of State and/or Information Commissioner's Office from time to time.

(o) "**Transfer**" means to disclose or otherwise make the Personal Information available to a third party (including to any affiliate or Subprocessor of Vidyard), either by physical movement of the Personal Information to such third party or by enabling access to the Personal Data by other means.

(p) "**UK Data Protection Law**" means the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003, and the UK GDPR.

(q) "**UK Personal Data"** means personal data (as defined in the UK Data Protection Act 2018) pertaining to individuals in the United Kingdom.

2. General Obligations.

(a) Vidyard shall only Process or Transfer Customer Personal Information as authorized by Customer and as necessary to perform the Services.

(b) Vidyard shall promptly inform Customer in writing: (i) if it cannot comply with any material term of its Agreement with Customer regarding the Services and this DPA (if this occurs, Vidyard shall use reasonable efforts to remedy the non-compliance, and Customer shall be entitled to terminate Vidyard's further Processing of Customer Personal Information); (ii) of any request for access to any Customer Personal Information received from an individual who is (or claims to be) the subject of the data; (iii) of any request for access to any Customer Personal Information received by Vidyard from any government official (including any data protection agency or law enforcement agency) unless it is explicitly prohibited by law from notifying Customer of the request; (iv) of any other requests with respect to Customer Personal Information received from Customer's employees or other third parties, other than those set forth in the agreement. Vidyard understands that it is not authorized to respond to these requests, unless explicitly authorized by Customer or the response is legally required under a subpoena or similar legal document issued by a government agency that compels disclosure by Vidyard.

(c) Vidyard shall not (i) sell, rent, lease, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing or by electronic means, any Customer Personal Information to another business or third party for monetary or other valuable consideration; or (ii) retain, use or disclose any Customer Personal Information for any purpose other than for the specific purpose of performing the Services and to fulfil Customer's operational business purposes, including retaining, using or disclosing the Personal Information to any third party, except to the extent necessary for the performance of the Services pursuant to the Agreement or except to the extent such disclosure is required by Applicable Laws.

(d) Each party must use reasonable efforts to stay informed of the legal and regulatory requirements for its Processing of Personal Information. Vidyard's Processing shall comply with all Privacy Laws that are applicable to the Processing, as well as Vidyard's own privacy

notices. Vidyard certifies that it is now and shall remain in compliance with all applicable Privacy Laws.

(e) Customer certifies that its collection and submission of Customer Personal Information is now and shall remain in compliance with all applicable Privacy Laws.

(f) If the Services involve the collection of Personal Information directly from individuals, Vidyard will provide the individuals with a clear and conspicuous privacy notice, provided that such notice must indicate that Vidyard is processing the data as a processor on behalf of its clients.

(g) If the Customer Personal Information will include EEA Personal Data or UK Personal Data, Vidyard and Customer shall ensure adequate protection respectively for the EEA Personal Data or UK Personal Data. Each party shall comply with the provisions of GDPR, UK GDPR and other Privacy Laws applicable to it, as a "controller" or a "processor" (as defined in GDPR or UK GDPR, as applicable). In the event of any Transfers of EEA Personal Data or UK Personal Data, the parties shall document adequate protection for the EEA Personal Data or UK Personal Data by using an approved means in accordance with section 4(e) below.

(h) Vidyard shall reasonably cooperate with Customer and with its affiliates and representatives in responding to inquiries, incidents, claims and complaints regarding the Processing of the Customer Personal Information or as otherwise needed for Customer to demonstrate compliance with the Privacy Laws applicable to it and to respect individuals' rights under such Privacy Laws.

3. Confidentiality and Data Access.

(a) Consistent with the confidentiality provisions of the Agreement, Customer Personal Information is considered Confidential Information of Customer and Vidyard must maintain all Customer Personal Information in strict confidence. Vidyard may disclose Personal Information to its employees and contingent workers, but only to the extent such individuals require access to the Customer Personal Information to perform the Services.

(b) Prior to allowing any employee or contingent worker to Process any Personal Information, Vidyard shall (i) conduct an appropriate background investigation of the individual as permitted by law (and receive an acceptable response), (ii) require the individual to execute an enforceable confidentiality agreement, and (iii) provide the individual with appropriate privacy and security training. Vidyard will also monitor its employees and contingent workers for compliance with the privacy and security program requirements.

4. Approvals for Transfers and Subprocessors.

(a) Customer acknowledges and agrees that (a) Vidyard's Affiliates may be retained as Subprocessors; and (b) Vidyard and Vidyard's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. Vidyard and Vidyard's Affiliates shall not Transfer the Customer Personal Information to any Subprocessors or other third parties unless such Processing is required to perform the Services. Customer may provide an email address via http://www.vidyard.com/dpanotice to subscribe to notifications of new Subprocessors for each applicable Service, to which Customer shall subscribe, and if Customer subscribes, Vidyard shall provide notification of a new Subprocessor(s) before authorizing any new Subprocessor(s) to Process Customer Personal Information in connection with the provision of the applicable Services.

(b) In order to exercise its right to object to Vidyard's use of a new Subprocessor, Customer shall notify Vidyard promptly in writing within ten (10) business days after receipt of Vidyard's notice in accordance with the mechanism set out in Section 4(a). In the event Customer objects to a new Subprocessor, and that objection is not unreasonable, Vidyard will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Customer Personal Information by the objected-to new Subprocessor without unreasonably burdening the Customer. If Vidyard is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Sales Order(s) with respect only to those Services which cannot be provided by Vidyard without the use of the objected-to new Subprocessor by providing written notice to Vidyard. Vidyard will refund Customer any prepaid fees covering the remainder of the term of such Sales Order(s) following the effective date of termination with respect to such terminated Services.

(c) Notwithstanding the preceding paragraphs, Customer understand that Vidyard has a contractual relationship with the Subprocessors listed below (the "**Authorized Subprocessors**"), and each Authorized Subprocessor is bound by a contract with Vidyard containing terms materially the same as those contained herein that requires it to protect all Customer Personal Information to which it may be exposed. Customer hereby authorizes Vidyard to make routine transfers of Personal Information in the normal course of business on its corporate systems to the Authorized Subprocessors:

Subprocessor:	**Services Provided:**	**Location:**
Amazon Web Services, Inc.	Hosting	Virginia, USA
Yahoo Edgecast Canada ULC	Content Delivery Network	Ontario, Canada
Fastly, Inc.	Content Delivery Network	California, USA
Ninja Partners, Inc.	International Customer Support	Texas, USA Clark, Philippines

(d) In addition, Customer authorizes Vidyard to make routine Transfers of Customer Personal Information in the normal course of business on its corporate systems to itself in the following other countries: Canada, the Philippines and the United States, or to other entities in the same group of companies. To the extent that these Transfers include any EEA Personal Data or UK Personal Data, Vidyard agrees to comply with the provisions paragraph 4(e) below regarding the Transfers of EEA Personal Data.

(e) With regard to Transfers of EEA Personal Data or UK Personal Data, the parties shall assure adequate protection for the EEA Personal Data or UK Personal Data by entering into the controller to processor standard contractual clauses attached hereto as Schedule 1 and the UK Addendum attached hereto as Schedule 2 unless the Transfer is to a third country that is subject to a determination by the European Commission or the UK Secretary of State (as

applicable) has decided that the third country, a territory or one or more specified sectors within that third country ensures an adequate level of protection. For Transfers of EEA Personal Data, the standard contractual clauses in Schedule 1 shall apply. For Transfers of UK Personal Data, the UK Addendum in Schedule 2 shall apply. In the event that EU authorities, UK authorities, or courts determine that the Transfer mechanism set out herein is no longer an appropriate basis for Transfers, Vidyard and Customer shall promptly take all steps reasonably necessary to demonstrate adequate protection for the EEA Personal Data or UK Personal Data, using another approved mechanism. Vidyard understands and agrees that Customer may terminate the Transfers as needed to comply with applicable Privacy Laws.

5. Information Security Requirements.

(a) Vidyard shall have implemented and documented appropriate administrative, technical and physical measures set forth in the Agreement, as applicable, to protect Personal Information against accidental or unlawful destruction, alteration, unauthorized disclosure or access. Vidyard will regularly test and monitor the effectiveness of its safeguards, controls, systems and procedures. Vidyard will periodically identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of the Personal Information, and ensure that these risks are addressed.

(b) Vidyard shall have implemented and documented appropriate business continuity and disaster recovery plans to enable it to continue or resume providing Services (including restoring access to the Personal Information) in a timely manner after a disruptive event. Vidyard will regularly test and monitor the effectiveness of its business continuity and disaster recovered plans. At appropriate intervals or as otherwise requested by Customer, Vidyard will provide a copy of its written business continuity and disaster recovery plans to Customer.

(c) If the Processing involves the transmission of Personal Information over a network, Vidyard shall have implemented appropriate supplementary measures to protect the Personal Information against the specific risks presented by the Processing. Personal Information may not be transmitted over any insecure network unless it has been appropriately encrypted.

(d) Upon request, and subject to the confidentiality obligations set forth in the Agreement, Vidyard shall provide Customer (or Customer's independent, third-party auditor that is not a competitor of Vidyard) information regarding Vidyard's compliance with the obligations set forth in this DPA in the form of Vidyard's Internal Audit Report. Customer may contact Vidyard in accordance with the "Notices" Section of the Agreement to request an on-site audit of the architecture, systems and procedures relevant to the protection of Customer Personal Information. Customer shall reimburse Vidyard for any time expended by Vidyard or its third-party sub-processors for any such on-site audit at Vidyard's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Vidyard shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by the Vidyard, or its third-party sub-processors. Customer shall promptly notify Vidyard with information regarding any non-compliance discovered during the course of an audit. In the event that any such audit reveals material gaps or weaknesses in Vidyard's security program, Customer shall be entitled to terminate Vidyard's Processing of Personal Information until such issues are resolved. Such audits will

be limited to once per year; provided however, that Customer may audit at any time in the event of a security breach or suspected material violation by Vidyard of its obligations under this DPA. Vidyard shall also cooperate with any audits conducted by any regulatory agency that has authority over Customer as needed to comply with Applicable Laws. In the case of Vidyard's Subprocessor, Amazon Web Services, Inc., Customer acknowledges that no on-site audit is available and that Vidyard relies on publicly available third party security reports.

(e) Vidyard will promptly and thoroughly investigate all allegations of unauthorized access to, use or disclosure of Customer Personal Information. Vidyard will notify Customer within forty-eight (48) hours upon discovery of any Security Breach. Notifications should be sent in accordance with the "Notices" Section of the Agreement. Vidyard shall provide Customer with all information about the Security Breach reasonably needed by Customer to assess its incident response obligations. Such notification shall as a minimum (i) describe the nature of the Security Breach, the categories and numbers of data subjects concerned, and the categories and numbers of personal data records concerned; (ii) communicate the name and contact details of Vidyard's data protection officer or other relevant contact from whom more information may be obtained; (iii) describe the likely consequences of the Security Breach; and (iv) describe the measures taken or proposed to be taken to address the Security Breach.

(f) Vidyard shall bear all costs associated with resolving a Security Breach, including (without limitation), conducting an investigation, engaging appropriate forensic analysis, notifying individuals, regulators and others as required to by Applicable Laws and responding to individual, regulator and media inquiries.

(g) When the Vidyard ceases to perform Services for Customer (and at any other time, upon request), Vidyard will either, at Customer's option (i) return the Personal Information (and all media containing copies of the Personal Information) to Customer, or (ii) with Customer's prior written consent, purge, delete and destroy the Customer Personal Information. Electronic media containing Customer Personal Information will be disposed of in a manner that renders the Personal Information unrecoverable. Vidyard will provide Customer with an Officer's Certificate to certify its compliance with this provision upon request. If Vidyard is required by Applicable Laws to retain any Personal Information, Vidyard warrants that it shall (i) ensure the continued confidentiality and security of the Personal Information, (ii) securely delete or destroy the Personal Information when the legal retention period has expired, and (iii) not actively Process the Personal Information other than as needed for to comply with Applicable Laws.

(remainder of this page is blank)

IN WITNESS WHEREOF, the parties have executed this DPA by their respective, duly authorized officers on _____.

BUILDSCALE, INC.	**CUSTOMER: _____**
1 Queen Street North Unit #301 Kitchener, ON N2H 2G7	
By: _____	By: _____
Name: Matt Hodgson	Name: _____
Title: CFO	Title: _____
Email: privacy@vidyard.com	Email: _____

Schedule 1 -

Schedule 1 - EEA Standard Contractual Clauses (processors)

Controller to 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 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 8.1(b), 8.9(a), (c), (d) and (e);
(iii) Clause 9(a), (c), (d) and (e);
(iv) Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18(a) and (b).

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

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 – Optional

Not used. Intentionally deleted.

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

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. 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 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).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17

Governing law

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

Clause 18

Choice of forum and jurisdiction

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

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

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

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

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Signature……

On behalf of the data importer: Buildscale, Inc.
Name: Matthew Hodgson

Position: Chief Financial Officer

Address: 1 Queen Street North, Unit #301, Kitchener, ON N2H 2G7, Canada

Signature……

ANNEX I

A. LIST OF PARTIES

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

Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

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

Name: Buildscale, Inc. on behalf of itself and its wholly-owned operating entities

Address: 1 Queen Street North, Unit #301, Kitchener, ON N2H 2G7, Canada

Contact person's name, position and contact details: Matt Hodgson, Chief Financial Officer

1 Queen Street North, Unit #301, Kitchener, ON N2H 2G7, Canada

Tel.: 800-530-3878; e-mail: legal@vidyard.com and privacy@vidyard.com

Activities relevant to the data transferred under these Clauses:

Buildscale, Inc., dba Vidyard is a provider of video marketing and sales services which involves processing personal data provided by, and pursuant to the instructions and directions of, the data exporter in accordance with the terms of the Agreement. The activities may include compute, storage, transmission and display.

DATA EXPORTER

Name:……

Authorised Signature ……

DATA IMPORTER

Name: Buildscale, Inc.

Authorised Signature ……

B. DESCRIPTION OF TRANSFER

DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

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

- Customer employees, contractors, agents, and/or representatives
- Customer customers and affiliates, and their employees, contractors, agents, representatives, prospects, and website visitors (some of which may be end users of Buildscale's software products and services)

Categories of personal data transferred

The personal data transferred may include following categories of data

- Standard contact information such as name, title, email address physical address, phone number, etc.
- Information about an individual's computer or mobile device or technology usage, including (for example) IP address, MAC address, unique device identifiers set in cookies, and any information passively captured about a person's online activities, browsing, application or hotspot suage or device location.

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

- N/A

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

- Continuous basis given the use of the Services as determined by the Customer

Nature of the processing

- Processing activities in performance of the video marketing and sales services as set forth in the Agreement, such as storing, copying, summarizing, aggregating, deleting data.
- Processing is required for the functionality and delivery of the Buildscale Services and the Vidyard Platform

Purpose(s) of the data transfer and further processing

- Purpose of processing personal data is to provide video sales services through the Vidyard Platform.

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

- The Term as set forth in the Agreement including 90 days post termination plus one archival cycle of seven days.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Subprocessor:	**Services Provided:**	**Duration:**
Amazon Web Services, Inc.	Hosting	The Term as set forth in the Agreement
Yahoo Edgecast Canada ULC	Content Delivery Network	The Term as set forth in the Agreement
Fastly, Inc.	Content Delivery Network	The Term as set forth in the Agreement
Ninja Partners, Inc.	International Customer Support	The Term as set forth in the Agreement

C. COMPETENT SUPERVISORY AUTHORITY

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

The Data Protection Commission of the Republic of Ireland, 21 Fitzwilliam Square South, Dublin 2, D02 RD28, Ireland

DATA EXPORTER

Name:……

Authorised Signature ……

DATA IMPORTER

Name: Buildscale, Inc.

Authorised Signature ……

ANNEX II

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

Integrity and Ethical Values

Buildscale, Inc. d/b/a Vidyard (the "Company" or "Vidyard") has developed employee guidelines, expectations, and policies that address acceptable business practices, conflicts of interest, and expected standards of ethical and moral behavior. The Company has also developed employee confidentiality agreements that prohibit inappropriate use and disclosure of customer or Company information. These documents are available to all new employees. All employees are required to sign an acknowledgement that they have received and agree to follow the confidentiality agreement. Employees and contractors who violate these guidelines are subject to disciplinary actions.

Board of Directors

The Company has a Board of Directors that follows documented responsibilities for oversight of the Company. The board meets quarterly and is consulted on and involved in all significant business decisions. Based on that strategy, management and the board annually establish or update the Company's overall business objectives, including objectives for operations, compliance, and reporting. The Company has Security and Privacy Committees that exercise oversight of the development and performance of internal control. The Committees report to the Audit Committee of the Board of Directors.

Organizational Structure

The Company has established lines of reporting that facilitate the flow of information to the appropriate personnel. The Company uses a centralized organizational model to support Company applications and technology. Roles and responsibilities are segregated based on functional requirements. The Company has an organization chart that sets forth the Company's lines of reporting and is updated, as necessary.

Management's Philosophy and Operating Style

The Company's management philosophy and operating style is direct and open. Commitment to open and honest communication and full transparency is considered a strong core value. Issues and hot topics are addressed quickly and communicated by the management team through various channels, including the Company's internal messaging tool, weekly Company-wide town halls, and monthly management meetings. Quarterly, the Company seeks feedback from the employees and leaders that helps ensure that the style and format of the operating style is effective. Direct and open communication, along with timely and ongoing bidirectional communication, allows for issue identification and quick resolution in accordance with Vidyard's policies and procedures.

Authority and Responsibility

Vidyard demonstrates assignment of authority and responsibility through job descriptions that outline both the level of authority and key areas of responsibility. The level of authority indicates capacity to make a decision or take action. For example, only managers or above have the authority to hire or authorize budget spending. In addition to job descriptions, Vidyard manages and maintains an organizational chart that shows team structure and alignment to managers. The level assigned to each position provides the basis for accountability control.

Human Resources

Vidyard's management team reviews competency for jobs prior to posting roles for recruitment. Job descriptions are reviewed by the direct manager and the manager's executive leader prior to being posted.

Vidyard's Talent and Recruiting teams then source candidates that match the desired profile for

interviewing. All employees are subject to background checks as part of the hiring process.

Vidyard's HR team ensures that employees adhere to expected levels of integrity, ethical behavior, and competence by setting foundational expectations on day one of employment. Each new hire attends a live onboarding session that provides a comprehensive overview of the Company's values and culture. Any violation of policy may result in a written warning or termination. Employees are provided regular communication on policy changes and updates, and copies of all policies are available to employees in the Company HR information system.

COMMUNICATION AND INFORMATION

The Company has documented policies, procedures, and system environment descriptions that are updated annually and communicated to authorized users. System changes are also communicated to authorized users when they occur. The Company uses various tools for internal alerting, messaging, collaboration, and document sharing. Security reports and alerts from network and application support hosts are aggregated and sent to the appropriate teams, and documentation is created where appropriate.

External events that affect the Vidyard Platform are captured inorganically by alerting messages from various vendors and services and organically through news services and peer discussion.

The Company obtains or generates and uses relevant information to support the function of internal control through the following:

- Control self-assessment tool
- Log management tool
- External penetration testing

As is typical business practice by most organizations, Vidyard restricts communication of matters related to the functioning of the Vidyard Platform to only those stakeholders and business partners who have a need to know such information. This information may be communicated via mediums appropriate to the nature of the information and the urgency of the situation, which may include conference calls, email, memoranda, or in-person meetings. In the rare instances when public disclosure of such matters would be necessary or appropriate, Vidyard's legal counsel and corporate communications representative are responsible for

jointly distributing and communicating such disclosures.

Customers are notified of system changes that may affect their processing. Customers are provided a means to report system failures, incidents, concerns, or other complaints, as well as technical support resources relating to system operations.

Risk Assessment and Mitigation

Vidyard makes use of various internal monitoring processes to observe, classify, and mitigate risks to its service delivery to customers. Quantitatively, risks such as performance and availability are captured with Vidyard's monitoring utilities. Data and confidentiality risk assessments regarding third-party applications and new features of Vidyard services are performed using an internal auditing tool.

The Company has a risk assessment process to identify and manage risks that could affect the Company's ability to provide reliable services to its clients and conducts a risk assessment annually. This process requires management to identify significant risks in its areas of responsibility and to implement measures to address those risks. In designing its controls, the Company has considered the risks that could prevent it from effectively addressing the criteria under the security, availability, and confidentiality Trust Services Categories.

The Company ensures that risks are evaluated and that controls are designed, implemented, and operated to address all areas, as appropriate, to detect, respond to, mitigate, and recover from security

events based on the assessed risks. Areas for evaluation include systems development, computer operations, program changes, and access to programs and data. Implemented controls include preventive and detective controls, such as manual, automated, or IT- dependent controls based on the environment in which the entity operates, the nature and scope of the entity's operations, and its specific characteristics. The Company identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. The Company's risk assessment process includes an

analysis of possible threats and vulnerabilities relative to each of the objectives. The risk identification process includes the consideration of both internal and external factors and their impact on the achievement of the objectives.

The Company considers the potential for fraud when assessing risks to the achievement of objectives. The assessment of fraud risk considers fraudulent reporting, possible loss of assets or data, and corruption resulting from the various ways that fraud and misconduct can occur. It also considers opportunities for unauthorized acquisition, use, or disposal of assets, altering of the entity's reporting records, or committing other inappropriate acts and how management and other personnel might engage in or justify inappropriate actions.

The Company identifies and assesses changes that could significantly impact the system of internal control. The risk identification process considers changes to the regulatory, economic, and physical environment in which the Company operates. The Company considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations, rapid growth, and new technologies on the system of internal control. Identified risks are analyzed through a process that includes estimating the potential significance of the risk.

The Company's risk assessment process includes considering how the risk should be managed and whether to accept, avoid, mitigate, or share the risk. The Company determines mitigation strategies for the risks that have been identified and designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy.

Security risks related to external parties (such as contractors and vendors) are identified and addressed based on Vidyard's procurement process. Designated responsibilities are defined in reviewing risks associated with external parties and establishing relevant agreements. Purchase orders to engage a third party require a vendor agreement and signed non-disclosure agreement (NDA) to be established.

The Company's vendor and business partner oversight program requires that all contracts with vendors or business partners clearly address (a) the size, scope, and nature of services being provided; (b) the hardware, software, and information requirements related to the provision of such services; (c) the responsibilities of each party; (d) the requirements for information security to meet Vidyard's standards; (e) the ability to perform independent audits of the effectiveness of internal control processes; and (f) the requirement to obtain and review a third-party attestation report.

Disclosure of any confidential information to a vendor or business partner is provided only as needed and only if the vendor or business partner has enacted appropriate information security and confidentiality controls. All vendors and business partners with access to confidential information are subject to confidentiality agreements and other contractual confidentiality provisions, which must be signed and acknowledged before access to Vidyard's systems and data is granted.

Vidyard considers the inherent risk of working with vendors and business partners as part of the annual risk assessment performed by the information security team. Internal and external cyber threats and vulnerabilities are identified and assessed based on the likelihood that they could prevent the entity from achieving its objectives. Consideration is given to the cyber threats and vulnerabilities such relationships may present and whether Vidyard's controls reduce such risks to a level consistent with the Company's objectives and risk acceptance.

Monitoring

The Company selects, develops, and performs ongoing or separate evaluations to ascertain whether the

components of internal control are present and functioning. Internal personnel use an automated control monitoring tool to perform assessments and tests of internal controls that include (a) working with process owners and IT support personnel to identify specific security threats and vulnerabilities and how the associated risk is being addressed and (b) tests of the design, implementation, and operating effectiveness of internal controls that address risks. Members of the internal assessment team have the requisite knowledge of and experience with cybersecurity risks and controls.

Vidyard also uses external parties to independently evaluate the state of the control environment. Penetration tests are performed annually by an external service provider to identify specific technical threats and vulnerabilities and benchmark the environment against leading cybersecurity practices. The penetration testing scope is determined based on Vidyard's areas of risk and compliance requirements.

Both internal and external evaluations are made using a risk-based approach that may vary the nature, timing, and extent of testing. The criteria for such evaluations, including the nature and frequency of such evaluations, are reviewed during the annual risk assessment and modified as needed, with consideration for changes to Vidyard's operational processes. These considerations include changes to the size, scope, and operational nature of the business, recent security threats or incidents, new or emerging risks, and changes in industry standards.

The results of all monitoring activities, regardless of source, are entered into a vulnerability tracking system for the evaluation and identification of remediation activities that may be needed. Identified vulnerabilities are assessed with regard to the likelihood and magnitude of exploitation. All vulnerabilities evaluated are identified for remediation or additional monitoring. Responsibilities for corrective action plans are assigned and completion dates determined.

Control Activities

The Company's control activities are defined through its established policies and procedures. Policies are dictated through management or board member statements of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Control activities are deployed through policies that establish what is expected and procedures that enforce those policies.

Logical Access

Logical access to Vidyard systems, applications, and data is limited to properly authorized individuals, and user rights are kept to a minimum based on job responsibility. The Director of Information Security, at the direction of the Chief Technology Officer (CTO), controls network and server passwords. All user account authentication to the network is managed via JumpCloud, along with AWS Identity and Access Management (IAM). System passwords are managed by the Director of Information Security who adheres to a strict password policy as set forth in the Vidyard Information Security Policy.

The Vice President (VP) of Engineering is responsible for maintaining the data integrity of the production environment and determining end-user access rights. All access granted to systems, applications, and data is password protected using role-based security. All new access granted to systems, applications, and data is reviewed and signed off on by the Director of Information Security and Privacy Officer.

Vidyard's servers run on Linux inside of the AWS offering. User workstation OS software is predominantly based on the Mac OS platform, with Microsoft Windows and Linux where necessary. All applicable workstations are members of the Vidyard domain and have policies enforced that restrict user rights to authorized business needs.

Vidyard maintains rapid response support agreements with all critical hardware and software vendors. Sophos AV is used for anti-malware and AV, and JumpCloud is used for mobile device management (MDM) on all Vidyard-owned laptops.

System Operations

All production endpoints are equipped with logging capabilities. The resulting data is sent to both Datadog for troubleshooting and metrics analysis and ELK for SIEM analytics. Critical events are sent over

integrations with Slack for incident management and tracking.

AWS Key Management Service (KMS) and Elastic Container Service (ECS) are used to orchestrate configuration management across all sites and technology stacks.

Change Management

Software development is performed primarily on the local host using test data. Once completed and ready for quality assurance (QA), code is run through various linters prior to being deployed to the staging environment. Once QA-approved, a GitHub pull request is created and subject to further peer review and approval before it is deployed to production.

Infrastructure changes follow a similar process as the production application. Infrastructure changes use Terraform for an infrastructure-as-code approach to changes.

Availability

The Company has implemented a secure backup system infrastructure to provide secure backup, retention, and restoration of data in the AWS environment. Processes have been implemented for the backup of critical system components and data. Backups are managed by the InfoSec team and scheduled on a regular cadence established by the respective component teams.

The Company utilizes AWS to provide data redundancy to minimize disruptions to the availability of customer data. The data redundancy is achieved through fragmentation of data into extents, which are copied onto multiple nodes within a region. This approach minimizes the impact of isolated storage node failures and loss of data.

Vidyard maintains a comprehensive business continuity and disaster recovery plan, which is tested annually. From this testing, changes to other policy documents such as the Vidyard Information Security Policy, Cybersecurity Incident Response Plan, Disaster Recovery/Business Continuity Plan (DR/BCP), and various runbooks are generated.

Confidentiality

The Company has a data classification policy to classify data in the various categories, as described in the Data section above, based on how it is used or may be used in the service environment. All data, regardless of classification, is transmitted using only secure transmission protocols such as HTTPS (Transport Layer Security [TLS] 1.2) and stored using industry standard cryptographic functions.

Retention periods, and policies for ensuring retention during the specified period and proper disposal of data at the end of the retention period, are also outlined in the data classification policy. The retention period assigned to data is based on the (1) classification of the data, (2) regulatory requirements and legal statutes, and (3) the general requirements of the business. During the designated retention period, the Company ensures that backup media (whether offline or online) is stored in a protected environment for the duration of the designated document retention period. When the retention period has ended, the Company destroys the information securely.

Customer information is securely disposed of by proven means, NIST800-88 governed disposal techniques certified by The Company's CSP, AWS.

ANNEX III

LIST OF SUB-PROCESSORS

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

Subprocessor:	Services Provided:	Location:
Amazon Web Services, Inc.	Hosting	Virginia, USA
Yahoo Edgecast Canada ULC	Content Delivery Network	Ontario, Canada
Fastly, Inc.	Content Delivery Network	California, USA
Ninja Partners, Inc.	International Customer Support	Texas, USA Clark, Philippines

DATA EXPORTER

Name:……

Authorised Signature ……

DATA IMPORTER

Name: Buildscale, Inc.

Authorised Signature ……

Schedule 2 - UK Addendum

This UK Addendum is deemed to be entered into by the parties referenced herein and attached to the Standard Contractual Clauses attached as Schedule 1 hereto.

Table 1: Parties

Start date	Effective Date of the DPA to which this Schedule 2 is attached.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Buildscale, Inc. Trading name (if different): Vidyard Main address (if a company registered address): 1 Queen Street North, Unit #301, Kitchener, ON N2H 2G7, Canada Official registration number (if any) (company number or similar identifier): Ontario 1942177	Full legal name: _____ Trading name (if different):_____ Main address (if a company registered address): _____ _____ _____ Official registration number (if any) (company number or similar identifier): _____
Key Contact	Full Name (optional): Matt Hodgson Job Title: Chief Financial Officer Contact details including email: see address above; email: dpo@vidyard.com	Full Name (optional): _____ Job Title: _____ Contact details including email: _____

1 Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: See Effective Date of the DPA to which this Schedule is attached. Reference (if any): N/A Other identifier (if any): N/A

		Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:				
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	N/A	N/A	N/A	N/A	N/A	N/A
2	N/A	N/A	N/A	N/A	N/A	N/A
3	N/A	N/A	N/A	N/A	N/A	N/A
4	N/A	N/A	N/A	N/A	N/A	N/A

2 Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Schedule 1, Annex IA to this DPA.
Annex 1B: Description of Transfer: See Schedule 1, Annex IB to this DPA.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Schedule 1, Annex II to this DPA.
Annex III: List of Sub processors (Modules 2 and 3 only): See Schedule 1, Annex III (*Permitted Subcontractors and Subprocessors*) to this DPA.

3 Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum	Which Parties may end this Addendum as set out in Section **Error! Reference source not found.**: ☐ Importer ☒ Exporter

changes	☐ neither Party

Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses, is incorporated by reference herein.