BRIGHTCOVE

DATA PROCESSING AGREEMENT (the "DPA")
FOR BRIGHTCOVE CUSTOMERS

This DPA is by and between Brightcove Inc., Brightcove K.K., or the other Brightcove entity that is party to the Agreement ("Brightcove") and the entity or individual ("Company") identified in the Order executed by Brightcove and Company that references this DPA and describes certain data processing and transfer obligations of the parties. This DPA is subject to the Brightcove service agreement(s) ("Agreement") pursuant to which Brightcove may Process certain Personal Data on behalf of Company in connection with Company's use of Brightcove products and services ("Brightcove Service" or "Brightcove Services") and is incorporated therein by reference. In the event of any inconsistency between this DPA and the Agreement, or between this DPA and the Order, this DPA shall control. For the avoidance of doubt, acceptance and/or signature of the DPA shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses incorporated herein, including their Annexes.

1. Definitions. In this DPA, the following terms shall have the meanings set out below. Other capitalized terms used but not otherwise defined herein shall have the meanings ascribed to such terms in the Agreement.

1.1 "**Consumer**" means a "consumer" or its equivalent term as such term is defined in U.S. Data Protection Law and the Non-European Data Protection Law.

1.2 "**Controller**" means the party that determines the purposes and means of the Processing of Personal Data.

1.3 "**Data Protection Laws and Regulations**" means all data protection and privacy laws and regulations applicable to a party and its Processing of Personal Data under the Agreement, including: (i) Non-European Data Protection Law; (ii) European Data Protection Law; and (iii) U.S. Data Protection Law.

1.4 "**Data Subject**" means an identified or identifiable natural person, as defined under Data Protection Laws and Regulations, who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.5 "**Europe**" means the member states of the European Economic Area ("**EEA**"), Switzerland and the United Kingdom ("**UK**").

1.6 "**European Data Protection Law**" means: (i) Regulation 2016/679 of the European Parliament and of the Council 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) (the "**EU GDPR**"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**") and the UK Data Protection Act 2018 (collectively, "**UK Data Protection Law**"); (iii) the Swiss Federal Data Protection Act of 19 June 1992 and its corresponding ordinances ("**Swiss DPA**"); (iv) the EU e-Privacy Directive (Directive 2002/58/EC); and (v) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii), (iii) or (iv); in each case as may be amended or superseded from time to time.

1.7 "**Non-European Data Protection Law**" means data protection or privacy laws applicable to Personal Data in force in all jurisdictions outside of Europe, including but not limited to U.S. Data Protection Law.

© Brightcove Inc.

1.8 "**Personal Data**" means any information that is "personal data" (as defined by **European Data Protection Law**) or "personal information" and/or "personal data" (as defined in the **U.S. Data Protection Law** or **Non-European Data Protection Law**), that in each case is Processed by Brightcove on behalf of the Company.

1.9 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by Brightcove in connection with the provision of the Brightcove Services.

1.10 "**Process,**" "**Processes,**" "**Processed**" or "**Processing**" means any operation or set of operations performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.11 "**Processor**" means the party which Processes Personal Data on behalf of the Controller.

1.12 "**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of personal data from the European Economic Area to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; and (ii) where UK Data Protection Law applies, a transfer of personal data from the UK to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of Personal Data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

1.13 "**Sell**" and "**Sale**" have the meaning given in U.S. Data Protection Law.

1.14 "**Share**" has the meaning given in U.S. Data Protection Law.

1.15 "**Standard Contractual Clauses**" or "**SCCs**" means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

1.16 "**Subprocessor**" means any Processor engaged by Brightcove in the provision of Brightcove Services to Company, as further described in Section 2.5 of this DPA.

1.17 "**UK Addendum**" means the International Data Transfer Addendum to the SCCs issued by the Information Commissioners Office under S.119(A) of the UK Data Protection Act 2018, as it is revised under Section 18 therein.

1.18 "**U.S. Data Protection Law**" means data protection or privacy laws in force within the United States of America (U.S.) as applicable to the Personal Data and all regulations thereto, respectively, including but not limited to (i) California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq. ("**CCPA**"), as amended; (ii) Virginia Consumer Data Protection Act, VA Code §§ 59.1-571 et seq, as amended; (iii) Colorado Privacy Act, CRS, §§ 6-1-1301 et seq, as amended; (iv) Connecticut Personal Data Privacy and Online Monitoring Act, Public Act No. 22-15; and (v) Utah Consumer Privacy Act, Utah Code Ann., §§ 13-61-101 et seq.

© Brightcove Inc.

2. Protection of Personal Data

2.1 Relationship of Parties: For the purposes of this DPA and in connection with Company's use of the Brightcove Services pursuant to the Agreement, Company is the Controller and appoints Brightcove to Process Personal Data as a Processor on behalf of Company for the Permitted Purposes (defined below). The Processor and Controller shall each comply with their respective obligations under applicable Data Protection Laws and Regulations and this DPA. For the purposes of U.S. Data Protection Law, the Parties acknowledge and agree that Brightcove will act as a "Service Provider" as such term is defined in the respective U.S. Data Protection Law, in its performance of its obligations pursuant to the Agreement. Service Provider shall be used to refer to obligations of a Processor as that term is used in the respective U.S. Data Protection Law.

2.2 Purpose Limitation: Brightcove shall Process Personal Data in order to provide and maintain the Brightcove Service and to perform Brightcove's obligations under the Agreement as a Processor, all in compliance with the applicable Data Protection Laws and Regulations. The purposes of Processing are as described in the Agreement, including Schedule A to this DPA, and any other exhibits, statements of work or addenda attached to or otherwise incorporated into the Agreement (collectively and individually the "**Permitted Purpose**").

2.3 Restricted Transfers:

The parties agree that when the transfer of Personal Data from Company (as "data exporter") to Brightcove (as "data importer") is a Restricted Transfer, it shall be subject to the Standard Contractual Clauses as follows:

(a) Transfers from the EU. In relation to Personal Data that is protected by the EU GDPR, the SCCs will apply completed as follows:

(i) Module Two (Controller to Processor) will apply;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9, Option 2 will apply, and the time period for prior notice of subprocessor changes shall be as set out in this DPA;

(iv) in Clause 11, the optional language will not apply;

(v) Annex I of the SCCs shall be deemed completed with the information set out in Schedule A to this DPA;

(vi) Annex II of the SCCs shall be deemed completed with the information set out in Schedule B to this DPA;

(vii) in Clause 17, Option 1 will apply, and the SCCs will be governed by Irish law; and

(viii) in Clause 18(b), disputes shall be resolved before the courts of Ireland.

(b) Transfers from the UK. In relation to transfers of Personal Data that are protected by UK Data Protection Law, the SCCs: (i) shall apply as completed in accordance with paragraph (a)(i)-(vii) above; and (ii) shall be deemed amended as specified by the UK Addendum in the form of Schedule C, which shall be deemed executed by the parties and incorporated into and form an integral part of this DPA. Any conflict between the terms of the SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

© Brightcove Inc.

(c) Transfers from Switzerland. In relation to transfers of Personal Data that are protected by the Swiss DPA, the SCCs as implemented under sub-paragraph (a) above will apply with the following modifications:

(i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA;

(ii) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss DPA;

(iii) references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland", or "Swiss law";

(iv) the term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., Switzerland);

(v) Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the Swiss Federal Data Protection and Information Commissioner;

(vi) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection and Information Commissioner" and "applicable courts of Switzerland";

(vii) in Clause 17, the SCCs shall be governed by the laws of Switzerland;

(viii) Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland; and

(ix) the SCCs shall also protect the data of legal entities until the entry into force of the revised Swiss Federal Data Protection Act.

2.4 Onward Transfers: Brightcove shall not participate in any Restricted Transfers of Personal Data to Subprocessors unless they comply with Data Protection Law and Regulations.

2.5 Subprocessing:

2.5.1 Company acknowledges and agrees that Brightcove may engage Subprocessors in connection with the provision of Brightcove Services. A list of approved Subprocessors as of the Effective Date of this DPA is located at https://www.brightcove.com/en/legal/services-subprocessors (the "**Subprocessor List**"). Company may subscribe to receive update alerts when changes are made to the Subprocessor List.

2.5.2 Brightcove will enter into a written agreement with each Subprocessor containing data protection obligations no less protective than those in this DPA or as may otherwise be required by applicable Data Protection Laws and Regulations. Brightcove shall remain liable for any failure by a Subprocessor to fulfill its obligations in relation to Processing Personal Data.

2.6 Brightcove will inform Company of any new Subprocessor engaged during the term of the Agreement by updating the Subprocessor List. If Company reasonably believes that the appointment of a new Subprocessor will have a material adverse effect on Brightcove's ability to comply with applicable Data Protection Laws and Regulations as a Processor, then Company must notify Brightcove in writing, within 30 days following the update to the Subprocessor List, of its reasonable basis for such belief. Upon receipt of Company's written notice, Company and Brightcove will work together without unreasonable delay on an alternative arrangement. If a mutually-agreed alternative arrangement is not found, and Company has a termination right under applicable Data Protection Laws and Regulations, then those Brightcove Services that cannot be provided without the use of the new Subprocessor may be terminated by Company without penalty.

2.7 **Brightcove as a Service Provider under U.S. Data Protection Law:**

Brightcove, in its capacity as a "service provider" or "processor," as those terms are defined under U.S. Data Protection Law, agrees to the following. All capitalized terms shall have the meaning given to them in the DPA.

2.7.1 Brightcove will assist Company in Company meeting its respective obligations related to the security of Processing the Personal Data in accordance with Section 6.2;

2.7.2 As set forth in Sections 2.1 and 2.2, Brightcove will adhere to Company's instructions and not retain, use, or disclose the Personal Data (i) for any purpose, including any commercial purpose, other than the Permitted Purpose or as otherwise permitted by U.S. Data Protection Law; or (ii) outside the direct business relationship between Brightcove and the Company, unless expressly permitted by U.S. Data Protection Law;

2.7.3 Brightcove shall not Sell or Share any Personal Data in accordance with Section 3.2;

2.7.4 Brightcove will notify Company in accordance with Section 5.1 if Brightcove makes a determination that it can no longer meet its obligations under U.S. Data Protection Law;

2.7.5 Brightcove will grant Company the right, upon written notice, to take reasonable and appropriate steps to stop and remediate Brightcove's unauthorized use of Personal Data;

2.7.6 In accordance with Section 3.1, Brightcove will provide reasonable and timely assistance, at Company's request, to enable Company to respond to a consumer seeking to exercise any rights under U.S. Data Protection Law;

2.7.7 Pursuant to Section 6.1, Brightcove employees Processing Personal Data will be bound by a duty of confidentiality regarding Personal Data;

2.7.8 Any written contract with a Subprocessor will comply with Section 2.5 requiring Subprocessors to adhere to U.S. Data Protection Law; and

2.7.9 Brightcove will not attempt to reidentify any deidentified data it receives, shall only use the data in its deidentified form, and contractually prohibit any Subprocessors from re-identifying deidentified data.

© Brightcove Inc.

2.8 **Notices and Consents**:

2.8.1 General: Company shall comply with all applicable Data Protection Laws and Regulations, including: (a) providing all required notices and appropriate disclosures to all Data Subjects regarding Company's, and Brightcove's, Processing and transfer of Personal Data; and (b) obtaining all necessary rights and valid consents from Data Subjects (including Data Subjects within Company's Content) to permit Processing by Brightcove for the purposes of fulfilling Brightcove's obligations, or as otherwise permitted, under the Agreement.

2.8.2 Children; Sensitive Data: Company is responsible for compliance with all applicable Data Protection Laws and Regulations regarding its Content, including without limitation those that regulate content directed toward children (as defined under applicable Data Protection Laws and Regulations; for example, under 13 years old in the United States or under 16 years old in certain other countries). Company's use of Brightcove Services in connection with the distribution of Content and/or Processing of sensitive Personal Data of a Data Subject (such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or an individual's genetic data, biometric data, health data, or data regarding sex life or sexual orientation) must be in compliance with all applicable Data Protection Laws and Regulations, including obtaining any explicit consent from Data Subjects whose Personal Data is provided to Brightcove for Processing.

3. Cooperation and Data Subjects' Rights

3.1 Brightcove will provide reasonable and timely assistance, at Company's request, to enable Company to respond to: (a) a request from a Data Subject to exercise any rights under applicable Data Protection Laws and Regulations (including rights of access, correction, objection, erasure and data portability, as applicable); and (b) any other correspondence, inquiry or complaint received from a Data Subject, regulator or other third party in connection with Processing of Personal Data. If a Data Subject contacts Brightcove directly to request access to, or correction or deletion of, Personal Data in connection with services provided to Company by Brightcove, Brightcove will promptly notify Company of the request.

3.2 No Sale or Sharing of Personal Data: Brightcove shall not Sell or Share any Personal Data to another business or third party without the prior written consent of Company.

4. Investigations and Audits

4.1 Regulatory Audit. Brightcove shall reasonably assist and support Company in the event of an investigation by a data protection regulator or similar authority, if and to the extent that such investigation relates to Brightcove's Processing of Personal Data. Brightcove will grant Company the right to take reasonable and appropriate steps to ensure that Brightcove uses Personal Data in a manner consistent with Brightcove's obligations under US Data Protection Law.

4.2 Company Audit. Upon at least 30 days' advance written request by Company, at mutually agreed times and subject to Brightcove's reasonable audit guidelines, Brightcove shall provide to Company, its authorized representatives and/or independent inspection body designated by Company: (a) reasonable access to records of Brightcove's Processing of Personal Data; and (b) reasonable assistance and cooperation of Brightcove's relevant staff for the purpose of auditing Brightcove's compliance with its obligations under this DPA. Brightcove reserves the right to restrict access to its proprietary information, including but not limited to its network architecture, internal and external test procedures, test results and remediation plans. Company will use best efforts to minimize disruption to Brightcove Services and Brightcove's business operations. Company further agrees that: (W) personnel

(or designated third parties) performing said audits will be bound by the confidentiality obligations set forth in the Agreement; (X) all findings will be deemed Brightcove's Confidential Information; (Y) Company will share all findings with Brightcove; and (Z) Brightcove will classify and remediate all findings in accordance with Brightcove's risk management program.

Company is limited to one audit in any 12-month period, except (i) if and as required by a competent data protection authority; or (ii) Company believes a further audit is necessary as a result of a Personal Data Breach relating to Brightcove Services.

4.3 Data Protection Impact Assessment. Brightcove shall, upon Company's written request, provide Company with reasonable cooperation and assistance to fulfill Company's obligations under applicable Data Protection Laws and Regulations to carry out a data protection impact assessment related to Company's use of Brightcove Services and, if necessary, consult with Company's relevant Supervisory Authority.

5. Notice of Non-Compliance

5.1 If required by applicable Data Protection Laws and Regulations, in the event that Brightcove is unable to comply with its obligations in this DPA, Brightcove shall promptly notify Company, and if Brightcove is unable to take reasonable and appropriate steps to remediate the non-compliance within a mutually-agreed upon timeframe, Company may take any one or more of the following actions: (a) suspend the transfer of Personal Data to Brightcove; (b) require Brightcove to cease Processing Personal Data to the extent technically possible; (c) demand the return or destruction of Personal Data; and/or (d) terminate this DPA in accordance with the Agreement. For the purposes of Section 16(b) of the SCCs, the parties acknowledge that if Brightcove cannot comply with Company's instructions, Brightcove agrees to promptly inform Company of its inability to comply and the parties shall comply with this Section 5.1.

6. Data Security

6.1 Personnel. Brightcove will ensure that all personnel with access to Personal Data are subject to obligations of confidentiality and that Personal Data is Processed only for the Permitted Purpose.

6.2 Security Measures. Brightcove's technical and organizational security measures to protect Personal Data shall be as set forth in the Agreement, this DPA, and/or in any orders or statements of work issued pursuant to the Agreement. Such measures shall be appropriate and take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. At a minimum, such measures shall include those identified in Schedule B to this DPA.

6.3 Breach Notification. If Brightcove becomes aware of a Personal Data Breach involving Brightcove Services, Brightcove shall: (a) promptly, and without undue delay following Brightcove's discovery thereof, notify Company of such Personal Data Breach; (b) investigate, remediate and mitigate the effects of the Personal Data Breach; (c) reasonably cooperate with Company's investigation of the Personal Data Breach to the extent that such cooperation does not compromise Brightcove's security; (d) take any additional actions and provide any additional cooperation to Company as may reasonably be required under applicable Data Protection Laws and Regulations; and (e) upon resolution, provide Company with a written incident report describing the breach, actions taken during the response and plans for future actions to prevent a similar breach from occurring in the future.

© Brightcove Inc.

7. Deletion or Return of Personal Data

7.1 Upon termination or expiration of the Agreement or at any time at Company's written request, Brightcove shall delete or return to Company all Personal Data, except where necessary to comply with applicable laws or in connection with the provision of the Brightcove Service, in which case Brightcove's obligations under this DPA shall continue to apply to any Personal Data retained until such Personal Data is deleted in accordance with Brightcove's policies.

8. Liability

8.1 Any claims brought under the SCCs (including the UK Addendum) shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement between the parties. In no event shall any party limit its liability with respect to any data subject rights under the SCCs.

9. Miscellaneous

9.1 This DPA is effective as of the Effective Date and will terminate automatically when the Agreement terminates or expires, without further action required by either party. Provisions of this DPA that by their nature and on their face should survive, will survive any such termination or expiration.

9.2 Company acknowledges that Brightcove may disclose this DPA (including the Standard Contractual Clauses) and any relevant privacy provisions in the Agreement to the U.S. Department of Commerce, the Federal Trade Commission, a European data protection authority or any other U.S. or European judicial or regulatory body upon their request.

9.3 This DPA shall be governed by and construed in accordance with the governing law set forth in the Agreement, except where otherwise required by applicable Data Protection Laws and Regulations.

9.4 Company agrees that its continued use of Brightcove Services is subject to the sections of Brightcove's posted Privacy Policies, at https://www.brightcove.com/en/legal/brightcove-privacy-policies/, applicable to Company, and consents to the use of its Personal Data in accordance with those Privacy Policies.

(Remainder of Page Intentionally Left Blank)

© Brightcove Inc.

Schedule A
Data Processing Description

This Schedule A forms part of this DPA and describes the Processing of Personal Data that Brightcove will perform on behalf of Company.

Controller
Controller (Company) uploads Content to Brightcove Services, directs distribution of Content via the U/I, elects to collect Viewer data, which may include personal data if using certain Brightcove Services.

Name:	Each of the Company entities identified in the Agreement.
Address:	The addresses of each of the Company entities identified in the Agreement.
Contact person's name, position and contact details:	Data protection enquiries can be addressed to the individual executing the Brightcove Order form on behalf of Controller (Company).

Processor
Processor (Brightcove) is a provider of cloud-based services for publishing, distributing, measuring and monetizing video across devices. Brightcove Services includes analytics and other usage data relating to Company's use of Brightcove Services.

Name:	Each of the Brightcove entities identified in the Agreement.
Address:	The addresses of each of the Brightcove entities identified in the Agreement.
Contact person's name, position and contact details:	Data protection enquiries can be addressed to gdpr@brightcove.com.

Data subjects
The Personal Data to be Processed concerns the following categories of Data Subjects:

- Business information (such as email addresses) of Company's employees who use Brightcove Services ("**Users**").
- End users who view Company's Content ("**Viewers**") (1) via Brightcove Services; (2) via other video platforms through integrations with Brightcove Services; or (3) that subscribe to or sign up for Company's service(s).
- Natural persons whose images (or other Personal Data) are included in Company's video Content.

Categories of data
The Personal Data to be Processed include the following categories of data (some or all of which may not be considered Personal Data under applicable Data Protection Laws and Regulations), and may vary depending on which Brightcove Service and features are utilized:

- Viewers: UserID, IP addresses, location data, names, email, phone numbers, instant messaging user name, title, biography, organization address, industry, login credentials, device ID, subscription confirmation, subscription period, authentication token, video viewing activity (such as in-app downloads, content viewed, favorites or saved content, shared content, amount viewed,

number of unique sessions, session length, in-app searches), interactivity with content (such as poll responses and reactions), images of natural persons.
- Users: Names, email, phone numbers, technical ID, title, industry, biography, organization address, department, login credentials, authentication/authorization tokens, images of natural persons, video sharing and editing activity.
- Images of natural persons included in video Content.

Special categories of data (if appropriate)
The Personal Data to be Processed concern the following special categories of data:

- None, unless Company contacts Brightcove at gdpr@brightcove.com to request a change to this section and the parties agree in writing to the special categories of data to be Processed.

Processing operations
The Personal Data will be subject to the following basic Processing activities:

- Video Content will be transcoded, hosted, transferred and distributed by Brightcove Services in accordance with Company's selections via the U/I or the Brightcove Service's APIs and integrations.
- Name, email, address, title, industry and/or other Personal Data of Viewers may be collected at Company's request if Company is using certain Brightcove Services such as Brightcove Audience Insights.
- IP addresses and approximate location data is collected to operate Brightcove Services and provide Company with video viewing analytics.
- User login credentials and contact information will be used to authenticate User access and to provide Brightcove Services and support to Company.

Frequency of the transfer
The Personal Data will be transferred continuously in accordance with the Company's instructions.

Data retention
The period for which the Personal Data is retained or, if that is not possible, the criteria used to determine that period: Brightcove will process the Personal Data for the duration of the Agreement. Upon termination of the Agreement, it will be deleted in accordance with this DPA.

Processing by Subprocessors, also specify subject matter, nature and duration of the processing:
As described in the Agreement and above.

Competent supervisory authority
Where the EU GDPR applies, the competent supervisory authority shall be the Irish Data Protection Commissioner.

Where UK Data Protection Law applies, the competent supervisory authority shall be the UK Information Commissioner's Office.

(Remainder of Page Intentionally Left Blank)

© Brightcove Inc.

Schedule B
Minimum Security Measures

Brightcove shall use commercially reasonable efforts to implement appropriate network security and encryption technologies, including but not limited to the following technologies or any technologies that provide comparable or enhanced protections:

1. IT Network Security. Brightcove maintains appropriate IT network segmentation, including but not limited to, firewalls, to segregate its internal networks from the internet, and maintains intrusion detection, monitoring, and logging systems to detect and respond to attacks.

2. Application Security. To the extent that Brightcove develops applications or application code on behalf of Company, Brightcove conducts security testing to ensure that the application or application code is secure against the vulnerabilities described in (i) the version of the OWASP Top Ten List available as of the Effective Date, and (ii) any changes to the OWASP Top Ten List after the Effective Date (within a reasonable time after such changes are initially published). The term "OWASP Top Ten List" shall mean the Open Web Application Security Project's Top Ten list (available at https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).

3. Vulnerability and Patch Management. Following receipt of any update release from the manufacturer, Brightcove will apply manufacturer-recommended security updates to all systems, devices, or applications Processing Personal Data within a reasonable period of time, taking into account the nature and severity of the risk. Brightcove will install, within a reasonable period of time following Brightcove's receipt from the manufacturer, any software patches designated by manufacturers, vendors, or Brightcove as "critical". Brightcove conducts regular vulnerability scans and penetration tests of any network storing or processing Personal Data and remediates any identified critical vulnerability in accordance with Brightcove's defined remediation schedule.

4. Access Controls.

   a. Access Management. Only those Brightcove personnel that reasonably need access to Personal Data to perform the services described in the Agreement or to deliver Brightcove Services are granted such access. If Brightcove personnel no longer need access to Personal Data, whether because of termination or re-assignment, then access privileges are promptly disabled.

   b. Usernames and Passwords. Accounts used to access systems, software, equipment, or networks must comply with Brightcove's complex password requirements ("Password Policy") and such Password Policy is automatically enforced by Brightcove's operating system.

   c. Multi-Factor Authentication. Brightcove shall have in place multi-factor authentication for its employees to access Personal Data. For the purposes of this requirement, the implementation and use of appropriate and commercially-reasonable identity verification systems and physical access controls that limit access to systems containing Personal Data may be considered a "factor".

   d. Training. Brightcove personnel that may have access to Personal Data are required to undergo regular training on commercial best practices for data security.

5. Data Transmission. Personal Data is encrypted when transmitted over networks other than those administered by Company or Brightcove. External data transmissions are protected using TLS, current-generation cipher suites and SSL certificates as follows:

   a. Client communications are secured with server-priority based TLS. Backend communications are secured with either TLS for service-to-service communications, AES-based encryption for backend file transfer over SSH or AES/HMAC-based VPN tunnels for inter-datacenter communication; and

b. All SSL certificates are created and updated with 2048-bit key length and SHA-256.

6. Auditing and Testing.

a. Brightcove maintains information system audit records to enable the monitoring, analysis, investigation and reporting of unlawful, unauthorized or inappropriate information system activity.

b. Brightcove's security policies, standards and procedures are designed to monitor and protect the Brightcove Service. Such policies, standards and procedures are reviewed at least annually and updated as necessary.

c. A third party conducts network, system and application vulnerability scanning, and penetration testing, on at least an annual basis, to evaluate the implementation of Brightcove's information security measures. Brightcove conducts regularly-scheduled internal vulnerability scans against its business and production operations networks.

d. Brightcove's physical Data centers and cloud storage providers must provide Brightcove annual SOC 2 or industry equivalent reports attesting to data center controls.

(Remainder of Page Intentionally Left Blank)

© Brightcove Inc.

Schedule C

This Schedule C forms part of this DPA and applies in accordance with Section 2.3(b) (UK Transfers) of the DPA.

Start Date	The date of the underlying agreement	
Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Name: Each of the Company entities identified in the Agreement. Address: The addresses of each of the Company entities identified in the Agreement. Contact person's name, position and contact details: Data protection enquiries can be addressed to the individual executing the Brightcove Order form on behalf of Controller (Company).	Name: Each of the Brightcove entities identified in the Agreement. Address: The addresses of each of the Brightcove entities identified in the Agreement. Contact person's name, position and contact details: Data protection enquiries can be addressed to gdpr@brightcove.com.

Addendum SCCs	The Approved SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the approved SCCs brought into effect for the purposes of this Addendum: See Section 2.3(b) of the DPA.

Appendix Information	See Schedule A

Ending this Addendum when the Approved Addendum changes	Neither Party

Mandatory Clauses	Part 2: Mandatory Clauses of the UK Addendum, as it is revised under Section 18 of those Mandatory Clauses.

(Remainder of Page Intentionally Left Blank)

© Brightcove Inc.