DATA PROCESSING AMENDMENT
TO
THE BRIGHTCOVE SERVICE AGREEMENT

Brightcove Inc., Brightcove K.K., or the other Brightcove entity that is party to the Service Agreement (as defined below) ("**Brightcove**") and Company (indicated on the signature block below) have entered into an agreement or agreements (the "**Service 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 (collectively, "**Brightcove Services**"). This amendment (the "**Amendment**") incorporates the DPA (attached hereto) into the Service Agreement (as amended by the DPA, the "**Agreement**") and describes certain data processing and transfer obligations of the parties. This Amendment shall be effective as of the date of last signature below (the "**Effective Date**"). In the event of any inconsistency between the DPA and the Service Agreement, the DPA shall control.

By signing below, each party agrees to be bound by the terms of this Amendment and the DPA.

BRIGHTCOVE	**COMPANY:**
Signature	Signature
Name	Name
Title	Title
Date	Date

(Remainder of Page Intentionally Left Blank)

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

This DPA is by and between Brightcove Inc. ("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 Master 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.

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 "**CCPA Consumer**" means a "consumer" as such term is defined in the CCPA.

1.2 "**CCPA Personal Information**" means the "personal information" (as defined in the CCPA) that Brightcove processes on behalf of Company in connection with the Brightcove's provision of the Brightcove Services.

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

1.4 "**Data Protection Laws and Regulations**" means laws and regulations applicable to the Processing of Personal Data under the Agreement, including: (i) California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq. ("**CCPA**"); and (ii) applicable laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, and the United Kingdom, including without limitation 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**" or "**GDPR**") and EU Directive 2002/58/EC on Privacy and Electronic Communications ("**e-Privacy Directive**") or, the superseding Regulation on Privacy and Electronic Communications ("**e-Privacy Regulation**"), once effective.

1.5 "**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.

1.6 "**Personal Data**" means any information relating to a Data Subject that is Processed by Brightcove on behalf of Company pursuant to the terms of the Agreement, including "**personal data**" (as defined in the GDPR) and CCPA Personal Information.

1.7 **"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.

1.8 **"Proccess," "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.

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

1.10 **"Sell"** and **"Sale"** have the meaning given in the CCPA.

1.11 **"Standard Contractual Clauses"** means the standard contractual clauses for the transfer of personal data from the European Union to processors established in third countries as set out in the Annex to Commission Decision 2010/97/EU (as may be updated from time to time) and in Schedule C to this DPA.

1.12 **"Subprocessor"** means any Processor engaged by Brightcove in the provision of Brightcove Services to Company, as further described in Section 2.4 of this DPA.

2. Protection of Personal Data

2.1 Relationship of Parties: For the purposes of the Agreement, Company is the Controller and appoints Brightcove as a Processor to Process Personal Data on behalf of Company in connection with Company's use of Brightcove Services pursuant to the Agreement. The Processor and Controller shall each comply with their respective obligations applicable to it under the Data Protection Laws and Regulations and this DPA.

For the purposes of the CCPA, the Parties acknowledge and agree that Brightcove will act as a "Service Provider" as such term is defined in the CCPA, in its performance of its obligations pursuant to the Agreement.

2.2 Purpose Limitation: Brightcove shall Process Personal Data in order to perform Brightcove's obligations, or as otherwise permitted, under the Agreement as a Processor, 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 (the "**Permitted Purpose**").

Brightcove shall not retain, use or disclose CCPA Personal Information for any purpose other than for the specific purpose of providing the Brightcove Services, or as otherwise permitted by the CCPA. Brightcove acknowledges and agrees that it shall not retain, use or disclose CCPA Personal Information for a commercial purpose other than for the Permitted Purpose.

2.3 Cross-Border Transfers: If Personal Data is transferred under the Agreement from the European Economic Area or Switzerland by Company as Controller to Brightcove as Processor, or otherwise by Brightcove as Processor, to a jurisdiction which the European Commission or, where relevant, the Swiss Federal Data Protection and Information Commissioner, has determined does not ensure an adequate level of protection of Personal Data, then the Standard Contractual Clauses attached hereto as Schedule C will apply, or Brightcove will take such other measures as may be required under applicable Data Protection Laws and Regulations.

2.4 Subprocessing:

2.4.1 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.

2.4.2 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.

2.4.3 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.

2.5 **Notices and Consents**:

2.5.1 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.

2.5.2 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 of CCPA Personal Information:

Brightcove shall not Sell any CCPA Personal Information 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.

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 fullfil 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.

6. Data Security

6.1 Brightcove will ensure that all personnel with access to Personal Data are subject to written 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.

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: return to Company or destroy all Personal Data, except as otherwise permitted by applicable Data Protection Laws and Regulations.

8. Government Access to Personal Data

8.1 Notwithstanding any other provision of this DPA, if Brightcove become aware that any government authority (including law enforcement) wishes to obtain access to or a copy of some or all of the Personal Data, whether on a voluntary or a mandatory basis, then unless legally prohibited or under a mandatory legal compulsion that requires otherwise:

(a) it will immediately notify Company;

(b) it will inform the relevant government authority that Brightcove is a Processor of the Personal Data and that Company has not authorised Brightcove to disclose the Personal Data to the government authority;

(c) it will inform the relevant government authority that any and all requests or demands for access to the Personal Data should therefore be notified to or served upon Company in writing; and

(d) it will not provide access to the Personal Data unless and until authorised by Company.

8.2 In the event Brightcove is under a legal prohibition or a mandatory legal compulsion that prevents you from complying with Clauses 8.1 (a) to (d) above in full, then Brightcove shall use reasonable and lawful efforts to challenge such prohibition or compulsion (though Company acknowledges that such challenge may not always be reasonable or possible in light of the nature, scope, context and purposes of the intended government authority access). If Brightcove successfully challenges the prohibition or compulsion, then Clauses 8.1 (a) to (d) will apply. In either case, if Brightcove makes disclosure to the government authority (either with Company authorisation or due to a mandatory legal compulsion), then Brightcove will only disclose the Personal Data to the extent it is legally required to do so and in accordance with applicable lawful process.

8.3 Clauses 8.1 and 8.2 shall not apply in the event that, taking into account the nature, scope, context and purposes of the intended government authority access to the Personal Data, Brightcove has a reasonable and good-faith belief that urgent disclosure is necessary to prevent an imminent risk of serious harm to any individual. In such event, Brightcove shall notify the Company as soon as possible following disclosure and provide the Company with full details of the same, unless and to the extent legally prohibited.

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 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.

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.

Processor
Processor (Brightcove) is a provider of cloud solutions for transcoding, hosting and delivering video to internet-connected devices. Brightcove Services includes analytics and other usage data relating to Company's use of Brightcove Services.

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**") via Brightcove Services.
- 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):

- Viewers: UserID, IP addresses, location data, names, email, address, title, industry, login credentials, device ID.
- Users: Names, phone numbers, email and login credentials.
- 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.
- 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 Audience.
- IP addresses and geolocation 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.

(Remainder of Page Intentionally Left Blank)

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 SecurityProject'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)

Schedule C

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

(pursuant to Article 26(2) of Directive 95/46/EC)

Brightcove Inc. and its affiliates ("**Brightcove**") (also referred to herein as "**data importer**") and **Company** (also referred to herein as "**data exporter**") have entered into one or more agreements (the "**Agreement**") pursuant to which Brightcove may Process Personal Data on behalf of Company, as well as a Data Processing Addendum (the "**DPA**"), which refers to and incorporates the following Standard Contractual Clauses (also referred to herein as the "**Clauses**") in order to ensure adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of Personal Data of residents of the European Union or Switzerland (or, if Company so notifies Brightcove in writing, of any other country that has adopted Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 or substantially equivalent laws or regulations) under the Service Agreement. Capitalized terms used but not otherwise defined herein shall have the meanings ascribed to those terms in the DPA.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 1;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or

accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights

against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses

The details of the transfer and in particular the special categories of Personal Data where applicable are specified in Schedule A to the DPA.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

As set forth in Schedule B to the DPA.

APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix sets out the parties' interpretation of their respective obligations under specific clauses identified below. Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the clauses.

Clause 4(h) and 8: Disclosure of these Clauses

1. Data exporter agrees that these Clauses constitute data importer's Confidential Information as that term is defined in the Agreement and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to the Agreement. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8.

Clause 5(a): Suspension of data transfers and termination:

1. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.
2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, it agrees to inform promptly the data exporter of its inability to comply and the parties shall comply with Section 5.1 of the DPA.

Clause 5(f): Audit:

1. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described in Section 4.2 of the DPA.

Clause 5(j): Disclosure of subprocessor agreements

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.

2. The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.

3. Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably in connection with such subprocessing agreement to data exporter.

Clause 6: Liability

1. Any claims brought under the Clauses 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 these Clauses.

Clause 11: Onward subprocessing

1. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "*FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC*" the data exporter may provide a general consent to onward subprocessing by the data importer.

2. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer's compliance with the requirements in Section 2.4 of the DPA, which collectively ensure that the onward subprocessor will provide adequate protection for the personal data that it processes.

