THIS DATA PROCESSING AGREEMENT IS ENTERED INTO BY AND BETWEEN INTERVISION SYSTEMS, LLC ("INTERVISION") AND THE CUSTOMER. CUSTOMER SHALL INCLUDE ANY AFFILIATES OF CUSTOMER TO WHOM INTERVISION IS PROVIDING SERVICES (AS DEFINED BELOW).

DATA PROCESSING AGREEMENT

1. Scope and Order of Precedence

This InterVision Data Processing Agreement ("DPA") applies to InterVision's Processing of Personal Data provided to the Customer as part of the services (the "Services") as further specified in the applicable Master Services Agreement, Statement of Work, Service Orders and/or other documents (collectively the "Agreement") by and between Customer and InterVision.

This DPA applies where InterVision processes Personal Data on behalf of the Customer in the course of providing the Services and such Personal Data is subject to Data Protection Laws of the United States, Canada, the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom. The parties agree to comply with the terms and conditions in this DPA in connection with such Personal Data.

This DPA is an amendment to and incorporated into the Agreement. The DPA is subject to the terms of the Agreement.

With respect to updates and changes to this DPA, the terms included in the "Miscellaneous" section of the Agreement shall apply.

In case of any conflict, the DPA shall take precedence over the terms of the Agreement. Where individual provisions of this DPA are invalid or unenforceable, the validity and forcibility of the other provisions of this DPA shall not be affected.

The legal entity agreeing to this DPA as Customer represents that it is authorized to agree to and enter into this DPA for and is agreeing to this DPA solely on behalf of, the Customer.

This DPA is comprised of the below General Terms and the following Attachments A-B attached herein, which are incorporated by reference:

ATTACHMENT A: INTERVISION SECURITY STANDARDS
ATTACHMENT B: STANDARD CONTRACTUAL CLAUSES

2. Definitions

"CCPA" means the California Consumer Privacy Act of 2018.

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data.

"Customer" means the Customer that has executed the Agreement.

"Data Protection Law" means all applicable legislation relating to data protection and privacy, including the General Data Protection Regulation 2016/679, the Personal Information Protection and Electronic Documents Act, California Consumer Privacy Act of 2018, and all Federal, State and local laws and regulations which amend or replace any of the referenced regulations. The terms "process", "processes", and "processed" will be construed accordingly.

"Data Subject" means the individual to whom Personal Data relates.

"Data Transfer" means a transfer of Personal Data from the Controller to a Processor, or the onward transfer of Personal Data to a contracted Sub-Processor.

"EEA" means countries and territories comprising the European Economic Area.

"GDPR" means the EU General Data Protection Regulation 2016/679.

"Personal Data Breach" means any 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.

"Personal Data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one 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.

"PIPEDA" means the Personal Information Protection and Electronic Documents Act, which regulates the privacy and protection of Personal Data for residents of Canada.

"Processing" means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data.

"Processor" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf on the Controller.

"Services" means services provided by or on behalf of InterVision under the terms of the Agreement.

"Sub-Processor" means any natural or legal person, public authority, agency or other body which processes personal data on behalf of InterVision (including any Affiliate of InterVision).

3. Data Processing

Nature of Processing: The parties acknowledge and agree that Customer is the Controller of Personal Data and InterVision is the Processor of that data (as each term is defined in the GDPR). The Customer as Controller may submit Personal Data to InterVision or may direct the collection of Personal Data by InterVision. InterVision, acting as Processor, will Process Personal Data only as a service provider to Customer (a) as needed to provide the Services, (b) in accordance with Customer's documented instructions (including any instructions regarding data transfers to third countries) and (c) as needed to comply with applicable law (in which case InterVision shall provide prior notice to Customer of such legal requirement, unless applicable law prohibits disclosure). With respect to any written instructions received by InterVision, the parties will negotiate in good faith with respect to any change in the Services and/or fees resulting from such instructions. If compelled to disclose Personal Data to a law enforcement or governmental entity or pursuant to other legal process, InterVision will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other remedy to the extent InterVision is legally permitted to do so.

Categories of Data Subjects: Data subjects may include but are not limited to: (i) Customer's prospects, customers, business partners, vendors of Customer; (ii) employees or contact persons of Customer's prospects, customers, business partners and vendors; (iii) employees, agents, advisors, freelancers or Customers; and (iv) representatives and end users, such as employees, applicants, contractors, collaborators, partners of any of the foregoing listed in (i) through (iii) . Data subjects also include individuals attempting to communicate or transfer Personal Data to users of the Services.

Types of Personal Data: Types of Personal Data processed may include office email, personal contact information (name, address, contact details), office contact information (name, address, title, contact details), financial information (credit card details, account details, payment information), employment details (employer, job title, geographic location, area of responsibility), computer device tracking information (IP addresses, cookies data, location data), system usage data and other electronic data submitted, stored, or transmitted by the Customer, or the Customer's end users, via systems InterVision uses to deliver Services to the Customer.

Duration of Processing: The duration of the Processing shall be for the duration of the provision of Services under the Agreement and will remain in effect until, and will automatically expire upon, deletion of all Personal Data as described in this DPA.

4. Controller Responsibilities

Data Protection Impact Assessment: The Customer as Controller is responsible for performing risk and impact assessments with respect to Personal Data it submits to InterVision pursuant to Articles 35 and 36 of the GDPR. Accordingly, the Customer is responsible for determining the appropriate technical and administrative controls required to mitigate risks identified and comply with applicable Data Protection Laws.

Compliance with Data Protection Law: Within the scope of this DPA, the Agreement and its use of the services, Customer as Controller shall be solely responsible for complying with the statutory requirements related to data protection and privacy, particularly regarding the disclosure and transfer of Personal Data to InterVision for the Processing of Personal Data. The Customer's instructions to InterVision for the Processing of Personal Data shall comply with the applicable Data Protection Law.

Processing Instructions: Additional instructions outside the scope of this DPA will require prior written agreement between the parties as additional charges may apply. Instructions shall initially be specified in the Agreement and may thereafter be amended, amplified, or replaced by the Customer as a Change or addendum to the original Agreement. Customer is responsible that all of its instructions are lawful and the Processing of Personal Data in accordance with such instructions will not violate applicable Data Protection Laws.

Information Security: The Customer as Controller is responsible for validating the integrity, completeness, and accuracy of Personal Data it submits to InterVision. Transfers of data outside

of InterVision's hosted environment may require unencrypted communications. The content of communications (including sender and recipient addresses) sent through email or messaging services may not be encrypted. Controller determines the suitability of communication and transfer protocols for Personal Data it submits to InterVision. Controller opts to use unencrypted file transfer protocols or email to transmit Personal Data to InterVision as Processor, the Customer as Controller is solely responsible for its decision.

a. The Customer is responsible for the security policies, procedures, and configuration settings for its operating systems and applications environments housed on InterVision's hosted platforms, including but not limited to, password configuration settings, auditing settings, operating server settings, and application settings.

b. The Customer is responsible for the encryption of Personal Data stored within its operating system and application environments housed on InterVision's hosted platforms.

c. The Customer is responsible for reviewing and updating authorized contact lists provided to InterVision on a regular basis to ensure lists are complete and accurate and unauthorized parties are promptly removed.

d. The Customer is responsible for managing access of its users of Personal Data Processing systems managed by InterVision and promptly notifying InterVision of user terminations.

e. The Customer is responsible for vetting and approving change requests made to Personal Data Processing systems managed by InterVision.

f. The Customer is responsible for requesting Processing of Personal Data from Data Subjects residing within the United States.

Supervisory Authorities: The Customer is responsible for communication, consultation, and reporting with Supervisory Authorities as required under Data Protection Law.

Retrieval of Personal Data: Personal Data owned by the Customer will be deleted by InterVision upon termination of the Agreement. The Customer is responsible for communicating, in writing, alternative directives regarding the retention, archive, or transfer of Personal Data. As with other changes to Data Processing Instructions, additional instructions for the disposition of Customer's data are outside the scope of this DPA will require prior written agreement between the parties as additional charges may apply.

5. Processor Responsibilities

Compliance with Instructions: InterVision shall collect, process and use Personal Data only within the scope of Customer's Instructions. If InterVision believes that an Instruction of the Customer infringes the Data Protection Law, it shall immediately inform the Customer without delay. If InterVision cannot process Personal Data in accordance with Instructions due to a legal requirement under any applicable statutory provision, if shall (i) promptly notify the Customer of that legal requirement prior to Processing, and (ii) cease all Processing in violation of statutory provision until such time as the Customer issues new instructions which InterVision is able to comply. If this provision is invoked, InterVision will not be liable to the Customer under the Agreement for failure to perform Services until such time as the Customer issues new instructions for Processing.

Information Security: In assessing the appropriate level of security implemented, InterVision shall take into account the particular of the risks that are presented by processing, in particular, from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Personal Data transmitted, stored or otherwise processed. See ATTACHMENT A: InterVision Security Standards for further information.

Confidentiality: InterVision shall ensure that any personnel whom InterVision authorizes to process Personal Data or access Personal Data Processing systems has been advised of and has acknowledged confidentiality obligations regarding Personal Data. Confidentiality obligations shall continue after the termination of InterVision's personnel.

Legal Actions: Except as otherwise required by law, InterVision will promptly notify the Customer of any subpoena, judicial, or other legal order or demand from an administrative agency or governmental authority that it receives and that relates to the Personal Data owned by the Customer. At the Customer's request, InterVision will provide Customer with reasonable information in its possession that may be responsive to the foregoing and any assistance reasonably required for Customer to respond in a timely manner. Customer acknowledges that InterVision has no responsibility to interact with the entity seeking the Personal Data.

Deletion or Return of Personal Data: Upon expiration or termination of the Agreement, Customer-owned data residing on the InterVision's hosted service platforms will be deleted. Additionally, any Customer-owned Personal Data will be purged from contact lists in applications used by the InterVision to deliver services. Customer-owned data will NOT be deleted if the InterVision is required to retain copies under applicable law. If Customer-owned data must be retained, the InterVision will make reasonable efforts to isolate and protect Customer-owned

data from further Processing, except to the extent required by applicable law.

6. Sub-Processors

Customer acknowledges and agrees to the engagement of third-party Sub-Processors by InterVision to fulfill its contractual obligations under this DPA or to provide certain services on its behalf, such as providing support services.

Where InterVision engages a Sub-Processor:

a. InterVision will restrict the Sub-Processor's access to Customer Data only to what is necessary to maintain the Services or to provide the Services to Customer;
b. InterVision will enter into a written agreement with the Sub-Processor that imposes on the Sub-Processor that same obligations that apply to the InterVision under this DPA; and
c. InterVision remains liable to the Customer for the performance of Sub-Processors obligations.

InterVision shall make available to Customer a current list of Sub-Processors for the respective Services with the identities of those Sub-Processors ("Sub-Processor List") upon Customer's reasonable request.

7. Rights of Data Subject

Data Subject Requests: Processor (InterVision) will promptly notify Controller (Customer) if it receives any inquiry, communication or complaint from a Data Subject or regulator relating to its processing of Personal Data or a request from a Data Subject to access, rectify, erase, transfer or port Personal Data. If a Data Subject request is made directly to the InterVision, InterVision will promptly inform Customer and will advise Data Subject to submit request to the Customer. InterVision will NOT respond to any such Data Subject request without Customer's prior written consent except to confirm that the request relates to Customer.

Complaints or Notices related to Personal Data: In the event InterVision receives any official compliant, notice, or communication that relates to InterVision's Processing of Personal Data or either Party's compliance with mandatory applicable law in connection with Personal Data, to the extent legally permitted, InterVision shall promptly notify Customer and, to the extent applicable, InterVision shall provide Customer with appropriate technical and organizational assistance in relation to any such complaint, notice, or communication The Customer shall reimburse InterVision for commercially reasonable costs arising from this assistance.

8. Security Breach Notification

Data Breach: For the purposes of this Section, "Data Breach" means the misappropriation of Personal Data in the custody of the InterVision or the compromise the security, confidentiality or integrity of the Personal Data Processing System maintained by the InterVision.

Security Breach Notification: Upon becoming aware of a Data Breach, InterVision shall without undue delay (and in no event later than 72 hours of becoming aware of such Data Breach) inform the Controller (Customer) and provide written details of the Data Breach, including the type of data affected, the identity of affected person(s), the likely consequences of the Personal Data Breach, any other information the Customer may reasonably request concerning the affected persons, and the measures taken or proposed to be taken to address it, as soon as such information becomes known or available to the InterVision.

Security Breach Investigation: InterVision will promptly take reasonable steps to contain, investigate and mitigate any Data Breach. InterVision will provide timely information about the Data Breach including, but not limited to, the nature and consequences of the Data Breach, the measures, taken and/or proposed by InterVision to mitigate or contain the Data Breach, the status of the InterVision's investigation of the Data Breach, a contact point from which additional information may be obtained and the categories and approximated number of data records concerned. Since InterVision does not have visibility to the content of the Personal Data, or where applicable, the identities, number or categories or affected Data Subject, InterVision may not be able to provide information pertaining thereto. InterVision's communications with Customer in connection with a Data Breach shall not be construed as an acknowledgment by InterVision of any fault or liability with respect to the Data Breach.

Public Communications and Disclosures: The parties agree to coordinate in good faith on developing the content of any related public statements or any required notices for the affected persons and/or the relevant legal authorities, except as otherwise required by applicable law. In the event of a Personal Data Breach, the InterVision will provide timely information and cooperation as the Customer may require to fulfill Customer's Data Breach reporting obligations under applicable law; take such measures and actions as are appropriate to remedy or mitigate the effects of the Data Breach; and shall keep Customer up-to-date about all developments in connection with the Personal Data Breach.

9. Audit Rights

The Processor (InterVision) shall, in accordance with Data Protection Laws and in response to a reasonable written request by the Customer, make available to Customer such information

related to the InterVision's compliance with the terms of this DPA.

The Customer may, upon written request and with at least 30 days' notice to the InterVision, during regular business hours and without interruption to InterVision's business operations, conduct an inspection of InterVision's business operations.

The Customer may audit InterVision's compliance with the terms of this DPA up to once per year. InterVision shall, upon Customer's written request and with at least 30 days' notice, provide Customer with the following information:

a. A SSAE18 System and Organization Controls (SOC) 2 Type II Report on the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability, and Confidentiality Trust Services Criteria.
b. Copy of the *InterVision Data Protection Policy*
c. Inventory of Personal Data owned by Customer in InterVision's Custody
d. Log of Data Subject Requests pertaining to Personal Data owned by Customer
e. List of Sub-Processors of Personal Data owned by Customer
f. SSAE18/SOC 2 Type 2 Report or alternative due diligence assessment for Sub-Processors of Personal Data owned by Customer.

The Customer agrees to accept results of the InterVision's annual SSAE18 SOC 2 Type 2 examination in lieu of an audit of the controls covered in the scope of this engagement, provided the engagement period end was no more than 12 months from the current date and the InterVision confirms, in writing, there are no known material changes to control processes.

If additional audit procedures are required, costs of the audit shall be borne by the Customer. InterVision will provide Customer with all information necessary to demonstrate compliance with this DPA, to the extent that such information is within InterVision's control and InterVision is not precluded from disclosing said information by applicable law, a duty of confidentiality, or any other obligation owed to a third party.

10. Data Transfers

Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom shall be referred to as "EU Data".

Customer acknowledges and agrees that InterVision stores and processes EU Data (defined above) in data centers located in the United States. Personal Data will not be transferred outside of the United States.

InterVision will process Personal Data in accordance with the GDPR requirements directly applicable to InterVision's provisioning of its services. Any transfers of EU data outside of European Union, the European Economic Area and/or their member states, Switzerland and/or United Kingdom shall be governed by the Standard Contractual Clauses set forth in Attachment B to this DPA, to the extent such transfers are subject to such Data Protection Laws and Regulations.

The Customer authorizes InterVision to process EU Data to destinations outside of the EU to operate, store and process Personal Data within the scope of Customer's Instructions.

11. Relationship with Agreement

The parties agree that this DPA will replace and supersede any existing data processing agreement, attachment, addendum or exhibit that the parties may have entered in connection with the standard services.

Except as provided in this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent applicable to any Personal Data. Notwithstanding, if there is a business associate agreement (a "BAA") between Customer and InterVision, then as and between the DPA and BAA the BAA shall prevail solely with respect to protected health information regulated by HIPPA or similar federal and state laws.

Notwithstanding anything to the contrary in the Agreement or this DPA, the liability of each party and each party's Affiliates shall be subject to the limitations on liability in the Agreement. Without limiting either of the parties obligations under the Agreement, each party agrees that any regulatory penalties incurred by one party in relation to the Personal Data that arise as a result of, or in connection with, the other party's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce the incurring party's liability under the Agreement as if it were liability to the other party under the Agreement.

In no event shall this DPA or any party restrict or limit the rights of any Data Subject or any governmental body.

This DPA will be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement

ATTACHMENT A: INTERVISIONS SECURITY STANDARDS

1. Purpose and Scope

InterVision shall maintain an Information Security and Protection Program designed to secure Customer's systems and data from unauthorized access, unlawful disclosure, system disruption and data loss.

The scope of internal controls set forth in this document pertain to all personnel, equipment, and facilities InterVision uses to perform any part of the agreement.

2. Audits and Certifications

InterVision shall engage an external auditor to perform a SSAE 18 Service Organization Control (SOC) 2, Type II examination on a minimum annual basis. The scope of the examination shall include the Trust Services Criteria (TSC) relevant to Security, Availability, and Confidentiality of customer systems and data residing on InterVision's Managed Services Platform, which include the following service offerings:

- Managed Security Services
- Managed Resiliency Services
- Managed Hosting Services
- Managed Network Services
- Managed Collaboration Services
- Managed Carrier Services
- Managed Help Desk Services
- Managed Server and Storage
- Managed Cloud Services
- Monitoring Services
- Client Service Management

A copy of the final SOC 2 Type II report shall be made available to the Customer upon request. InterVision shall address and resolve any deficiencies identified in the SOC 2 Type II report in a transparent and timely manner.

3. Administrative Controls

InterVision has implemented and shall maintain the following administrative controls designed to protect Customer systems and data from disruption, loss, destruction or alternation, authorized access or unlawful disclosure:

a. Risk Management- InterVision has implemented and shall maintain formal processes for identifying and assessing risks to Customer's systems and data. A documented Risk Assessment shall be performed to identify threats to the confidentiality, integrity and availability of Customer's systems and data at least once annually. Risks shall also be continuously monitored and updated on a minimum quarterly basis.

b. Policies and Procedures- InterVision has implemented and shall maintain formal policies and procedures to avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security or other security requirements.

c. Workforce Management- InterVision has implemented and shall maintain processes for screening and vetting job applicants, communicating non-disclosure and confidentiality commitments to workforce members, as well as training workforce members on data privacy and protection protocols.

d. User Access Control- InterVision has implemented and shall maintain formal processes for provisioning and de-provisioning users accessing both InterVision's Corporate resources and Managed Systems. Periodic access reviews of administrative and other sensitive access levels shall be performed on a minimum annual basis.

e. Physical Access Control- Critical infrastructure supporting customer systems and data are housed in 3rd party colocation centers. Colocation centers provide 24X7X365 manned security desks, active monitoring of surveillance systems, and security zone restrictions. Entry to data center suites requires badge and biometric authentication. InterVision has implemented and shall maintain processes for colocation oversight, including, but not limited to annual control evaluations and inspection of independent audit reports (e.g. SOC 2, SOC 1) to validate operating effectiveness of stated controls. Additionally, periodic access reviews of colocation centers and data center suites shall be performed on a minimum quarterly basis.

f. Change Management- InterVision has implemented and shall maintain formal change management processes to prevent the introduction of unauthorized or untested changes to the Managed Services Platform.

g. Vendor Management- InterVision has implemented and shall maintain a formal process for vetting and periodically evaluating security and privacy processes of critical service providers impacting the Managed Services Platform.

h. Vulnerability Management- InterVision has implemented and shall maintain processes for scanning external and internal managed systems for vulnerabilities. External penetration tests shall be performed by an independent, 3rd party assessor on a minimum annual basis.

i. Incident Response- InterVision has implemented and shall maintain a documented incident response plan. Incident Response procedures shall be reviewed and tested on a minimum annual basis.

j. Disaster Recovery- InterVision has implemented and shall maintain a documented disaster recovery plan. Recovery of

systems critical for delivery of services to customers shall be tested on a minimum annual basis.

4. Technical Controls

InterVision has implemented and shall maintain the following technical controls designed to protect Customer systems and data from disruption, loss, destruction or alternation, authorized access or unlawful disclosure:

a. *Firewalls*- All traffic to and from the public internet shall traverse through firewalls. Firewall alerts shall be actively monitored. Firewalls rules shall be reviewed and assessed on a minimum annual basis.
b. *Remote Access*- Connections to Customer's systems and data from the public internet maintained by InterVision shall use VPN or other secure, encrypted connection mechanisms. Furthermore, multifactor authentication, defined as something you know, something you have, or something you are, shall be required for remote connections managed by InterVision. Note, however, the Customer shall be responsible for the security of any connections with InterVision that the Customer owns and manages.
c. *Device Authentication*- Wired and wireless device connections to the InterVision Corporate and Managed environments shall use 802.1x authentication protocols.
d. *Data Encryption*- customer backup data shall be encrypted using either 128 or 256-bit ciphers.
e. *Monitoring*- monitoring systems shall be maintained to communicate system security and performance alerts to the technical team.
f. *End Point Protection*- InterVision-managed workstations shall be equipped with desktop management software to enforce device encryption, monitoring, and system updates. Antivirus solutions shall be deployed on all vulnerable endpoints, including workstations and Windows Servers.
g. *Backup and replication*- Critical systems supporting Customer's systems and data shall be replicated to a secondary data center, located in another region of the United States. Backup and replication processes shall be monitored to validate successful completion.

5. Data Privacy and Protection Program

InterVision has implemented and shall maintain a formal Data Privacy and Protection program designed to comply with the requirements of state, federal, and international privacy laws such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act of 2018 (CCPA).

InterVision has implemented and shall maintain a formal Privacy Policy applicable to customers and business partners. The Privacy Policy can be viewed at https://www.intervision.com/privacy-policy/.

InterVision has implemented and shall maintain documented policies, procedures, and protocols for collection, transmission, processing, and storage of personal data by its workforce members. InterVision shall instruct its workforce members on data protection policies, procedures, and protocols through published documents and formal training sessions provided of a minimum annual basis.

All personal data shall be deemed "Confidential" in accordance with InterVision's Data Classification Standard and shall only be transmitted, processed and stored via approved and authorized applications and/or service providers. All requests for release of personal data shall be coordinated by InterVision's Data Protection Officer (DPO). No Customer data shall be released to a third party without the express written consent of the Customer.

ATTACHEMENT B: STANDARD CONTRACTUAL CLAUSES

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection (These can be located in their original text on the European Commission website here: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm).

For purposes of this Attachment A:

- any reference to "data exporter" means Customer, acting as data exporter on behalf of its EEA or Swiss customer(s) where applicable, and
- any reference to "data importer" means InterVision
-

each a "party"; together "the parties".

The parties have agreed on the following Standard Contractual Clauses (the Clauses) in order to adduce 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 the personal data specified in Appendix 1.

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, unauthorized 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 organizational security measures specified in the Data Processing Agreement;

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

4. 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 its 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

CLAUSE 9: GOVERNING LAW

The Clauses shall be governed by the law of the Member State in which the data controller 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 controller 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 ATTACHEMENT A: STANDARD CONTRACTUAL CLAUSES

This Appendix 1 forms part of the Clauses.

Data exporter

The data exporter is Customer, acting as data exporter on behalf of itself or a customer where applicable. Activities relevant to the transfer include the performance of services for Customer and its customer(s).

Data importer

The data importer is InterVision. Activities relevant to the transfer include the performance of services for Customer and customers.

Data subjects

The personal data transferred may concern the following categories of data subjects: Employees, contractors, business partners, representatives and end customers of customers, and other individuals whose personal data is processed by or on behalf of Customer or Customer's customers and delivered as part of the Services.

Categories of data

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

Personal Data related directly or indirectly to the delivery of services or Performance, including online and offline customer, prospect, partner, and InterVision data, and personal data provided by customers in connection with the resolution of support requests.

Special categories of data

The personal data transferred may concern the following special categories of data:

Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union memberships, and data concerning health or sex life, and data relating to offenses, criminal convictions or security measures.

Processing operations

The personal data transferred may be subject to the following basic processing activities, as may be further set forth in contractual agreements entered into from time to time between Customer and customers: (a) customer service activities, such as processing orders, providing technical support and improving offerings, (b) sales and marketing activities as permissible under applicable law, (c) consulting, professional, security, storage, hosting and other services delivered to customers, including services offered by means of the products and solutions described by InterVision, and (d) internal business processes and management, fraud detection and prevention, and compliance with governmental, legislative, and regulatory requirements.