


Data Privacy Agreement (US Version)



between

PTV America Inc.

- hereinafter “**PTV**” -

1530 Wilson Blvd.
Arlington, VA 22209, USA

and

Customer

- hereinafter “**Customer**” -

address

postal code city, country

PTV and the Customer hereinafter jointly referred to as the “**Parties**” and individually as the “**Party**”.

Shorttitle	Data Privacy Agreement – US Version
Version of contract template:	1.0.0 from 2020-10-15

THIS DATA PRIVACY AGREEMENT is made and entered into as of the effective date of the contract, by and between PTV and Customer.

1. Personally Identifiable Information. Names, addresses, phone numbers, social security numbers, dates of birth, IP addresses, unique device identifiers, email addresses, account numbers, and other information relating to an identified or identifiable individual is hereinafter collectively referred to as Personally Identifiable Information (“**PII**”). PTV expressly acknowledges that PII contained within Customer Data, defined in here (“**Customer PII**”) or as otherwise accessed by PTV to perform its obligations under the contract is deemed to constitute Confidential Information and/or Customer Data. PII obtained or accessed by PTV in the performance of the contract, including but not limited to performance of providing the PTV Cloud Service and Support Services, may only be used by PTV to perform its duties and obligations under the contract.

2. Data Security.

A. Technical Controls. PTV, employees of PTV and subcontractors of PTV (collectively employees and subcontractors of PTV are “PTV’s Personnel”) will implement and maintain appropriate technical, logical, administrative, physical, human and organizational measures (such as training and monitoring) and other protections for Customer’s Confidential Information, which PTV expressly acknowledges includes sensitive information and PII, and such measures and protections shall take into account any change in the nature of the data, expanded or different definitions of PII, and shall be in accordance with applicable law, industry standards and federal and state agency guidelines, as such standards, law and guidelines may evolve, including but not limited to controls consistent with and adopted pursuant to DoD, ISO 22301, 27001 and 27002, NIST, the NIST Cybersecurity Framework, and regulatory action and guidance by the Federal Trade Commission, including, without limitation and by example only: (i) host and network based intrusion detection systems, penetration tests (conducted through the use of a vendor other than PTV); (ii) controls against unauthorized access (including, without limitation, viruses and malicious software); (iii) encryption of all Customer PII in transit electronically; and (iv) controls preventing the loading of Customer PII on any laptop computers, USB drives or other portable storage media, unless such Customer PII is encrypted and the loading of such Customer PII on such portable storage media is necessary for PTV to perform under the contract. In regard to Section 2(A)(i) of this Agreement, above, Customer, within its sole discretion and cost, shall select the third party PTV to conduct its own independent penetration and/or vulnerability testing of the PTV Cloud Service at its own expense.

Customer is responsible for maintaining reasonable security of any passwords or other account or User Information (defined below) in its possession or through which it may access the software, and shall be responsible for Customer’s own negligence in failing to adequately protect such password information.

B. Incident Reporting. PTV will promptly and without delay within such time as may be required by law, but in no event later than twenty-four (24) hours from notice of a reportable incident (as described below), report to Customer: (i) any

unauthorized use, loss, disclosure or potential compromise of Customer Data, Customer PII, or other Confidential Information of Customer; or (ii) any other similar event that triggers application of any data breach law. PTV will cooperate fully with Customer in investigating any such unauthorized use, loss, or disclosure, and will take all actions as may be necessary or reasonably requested by Customer to mitigate the problem, including, without limitation, notifying affected individuals and/or governmental entities, minimizing any resulting damage, and reviewing Customer's written recommendations to PTV to enhance its security measures after a forensic investigation or audit (e.g., implementing encryption solutions). PTV agrees that it will not notify affected individuals and/or governmental entities without first attempting to contact Customer in a manner to afford Customer the ability to coordinate and control the notification process or intervene on behalf of itself, with PTV reserving the right to notify governmental entities should it believe such notice is necessary. PTV agrees to ensure that any PTV's Personnel to whom it Transfers (defined below) or discloses Customer Confidential Information (including, without limitation, Customer PII) pursuant to the contract has implemented and maintains a data privacy incident reporting process for the prompt reporting of any privacy or data security breaches to PTV, which, in turn, shall promptly report this information to Customer.

C. Compliance. PTV will cooperate fully with Customer's reasonable requests for access to, correction of, and destruction of Customer PII in PTV's possession, which destruction shall be certified to Customer in writing. Furthermore, Customer, its personnel, and any governmental entity with jurisdiction or oversight authority, may, upon prior notice to PTV, audit PTV's records of Customer's Confidential Information, and, to the extent relevant to the security of Customer's Confidential Information, PTV's security practices and data processing activities, and speak with PTV's Personnel who are familiar with such records, practices and activities. PTV will exercise best efforts to comply with all instructions or other requirements provided or issued by Customer from time-to-time relating to Customer PII. If PTV does not believe such compliance is appropriate, it shall promptly notify Customer in writing, and PTV and Customer will discuss and determine how to proceed.

D. PTV Assessments. PTV will ensure that PTV's Personnel, vendors, and subcontractors who have access to Customer Data are at all times in compliance with applicable laws, industry standards and best practices as PTV itself is obligated to comply with pursuant to the contract and applicable laws and standards. PTV shall from time-to-time, no less frequently than once every twenty-four (24) months or otherwise more frequently in accordance with industry standards and applicable law, conduct an ongoing privacy assessment and security validation of those PTV's Personnel or its contracted third parties, if any, to whom it has transferred Customer PII or other Customer Confidential Information pursuant to the contract. PTV shall notify Customer in writing if any PTV's Personnel or contracted third parties that PTV uses to provide the PTV Cloud Service under the contract, in fact perform any portion of such PTV Cloud Service outside the United States and receive or have access to Customer PII or

other Customer Confidential Information. During the Term of the contract, PTV shall provide prior written notice when any PTV's Personnel that is to assist PTV in providing the PTV Cloud Service under the contract will have access to Customer's Confidential Information.

3. Privacy and Data Security Laws.

A. Consent. The Parties agree that PTV shall not provide Customer with any PII obtained or accessed by PTV for any purpose unrelated to Customer Data or providing PTV Cloud Service ("PTV PII"). However, in the event PTV provides PTV PII to Customer in violation of this Section 3(A) of this Agreement, PTV acknowledges and agrees that PTV PII may be collected, Processed (as defined below), and/or transferred (each, a "Transfer(s)") across international boundaries to Customer's software systems. To the extent that PTV PII requires consent from any personnel or PTV's Personnel prior to subsequent Transfer by Customer, PTV agrees that it shall be solely responsible for obtaining legally compliant consent permitting the Transfer of such PTV PII.

B. Limited Processing and Disclosure. PTV will: (i) Process (as defined below) Customer PII only on Customer's written instruction and consistent with the contract and applicable law; (ii) not Process Customer PII for any other purpose; (iii) absent prior written authorization from Customer, only Process Customer PII in the country in which Customer originally delivered the PII to PTV or to which access was granted by Customer unless otherwise approved by Customer in writing; (iv) immediately stop Processing (as defined herein) Customer PII upon written request from Customer; and (v) not disclose, Transfer or provide access to Customer PII to any third party, including PTV's Personnel, or its contracted third parties, without Customer's prior written approval.

For purposes of this Agreement, "Process," "Processed" or "Processing" means any operation or set of operations which is performed upon PII, whether or not by automatic means, including but not limited to, collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, Transfer, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

C. U.S., Mexico, Canada and International Data Protection Laws. PTV represents and warrants that it and its vendors, suppliers, subcontractors and PTV's Personnel shall comply with all applicable United States, Mexican, Canadian and international laws governing or relating to privacy, data protection, data security and the handling of data security breaches when Processing Customer Data or otherwise relating to Customer PII, as such laws may be amended or superseded by other laws. When and as required by Customer from time-to-time, PTV shall promptly execute and cause PTV's Personnel to promptly execute, supplemental security and data protection terms, and controller-to-processor data transfer agreements, on such other terms and conditions as shall be mutually agreed upon and as required for the Processing or Transfer of Customer PII in accordance with the applicable requirements of United States, Canadian, Mexican, and/or international law. For the avoidance of doubt and in

regard to Canada, PTV, PTV's Personnel and its employees, vendors, suppliers, and subcontractors shall comply with the Personal Information Protection and Electronic Documents Act ("PIPEDA") and any substantially similar national, provincial and/or local legislation relating to privacy, data protection, data security and the handling of data security breaches when Processing Customer PII or otherwise relating to Customer PII, including but not limited to, British Columbia's Personal Protection Act, Alberta's Personal Information Protection Act, Quebec's Act Respecting the Protection of Personal Information in the Private Sector, as such laws may be amended or superseded. For the avoidance of doubt and in regard to Mexico, PTV, PTV's Personnel and PTV's employees, vendors, suppliers, and subcontractors shall comply with Article 26 of the Law on the Protection of Personal Data Held by Private Parties ("Data Protection Law").

D. European Union. To the extent that PTV shall Process any Customer Data or otherwise access PII governed by laws implementing the European Union Data Privacy Directive (95/46/EC) superseded by the General Data Protection Regulation (2016/679) as such laws may be amended or superseded by other laws governing or relating to privacy, data protection, data security, and the handling of data security breaches ("EU Privacy Laws"), PTV shall Process such Customer PII: (i) in the European Economic Area ("EEA") or in a country considered by the European Commission as providing adequate data privacy protection; or (ii) outside the EEA provided PTV ensures that the Transfer of such Customer PII outside the EEA and its subsequent Processing is done in compliance with applicable law by means of: (a) PTV's participation, to Customer's satisfaction, in the EU-U.S. Privacy Shield Framework; (b) entering into the appropriate controller-to-processor data transfer agreement approved by the European Commission (i.e. the current approved version of the Standard Contractual Clauses applicable to the Parties relationship); and/or (c) other mechanism acceptable to Customer that effectively complies with EU Privacy Laws or other requirements under applicable law.

E. Data Controller/Data Processor. The Parties agree that for any Processing of Customer PII in any medium or format governed by EU Privacy Laws, Customer shall be the "data controller" and PTV shall be the "data processor," pursuant to such laws.

F. Complaints or Requests; Data Subject Requests. PTV shall promptly notify Customer upon receipt of any complaint or request (including "data subject access" requests) relating to PTV's obligations under the relevant data protection law that may impact Customer, and such impact shall be deemed a loss pursuant to which PTV will indemnify Customer under the Agreement. PTV shall provide cooperation and assistance in relation to such complaint or request as reasonably requested by Customer, including acting timely in accordance with Customer's instructions and timetables. When and as required by Customer, PTV will assist Customer in identifying, copying, preserving, or producing Customer PII that is: (i) in the possession of PTV and/or PTV's Personnel; or (ii) stored in facilities under management or control of PTV and/or PTV's Personnel, including for purposes of

Customer satisfying the order or request of a governmental entity or a third party with access rights over the Customer PII. Notwithstanding anything to the contrary in this Agreement, PTV agrees that it shall not, without the prior written consent of Customer, process Customer Data on servers located outside of the United States.

4. PTV Systems.

A. Unauthorized Access. PTV shall be solely responsible for the information technology infrastructure, including all computers, software, databases, electronic systems (including database management systems) and networks used by or for PTV in connection with the PTV Cloud Service and Licensed Computer System (defined below) (collectively, the “PTV Systems”) and shall prevent unauthorized access to Customer Data through the PTV Systems.

(i) Unless otherwise specifically provided, and in addition to the other defined terms set forth herein, the following term will have the meanings set forth below: “Licensed Computer System” means the configuration of hardware, software and documentation, including infrastructure equipment, database storage and other hardware storage, cloud based storage, cloud-based systems, website or web-based storage locations used to run and support the PTV Cloud Service offered to Customer and Authorized Users, including (a) all computer programs (both source code and object code, unless otherwise indicated) including, without limitation, software, firmware, application programs, operating systems, files, and utilities; (b) supporting documentation for such computer programs, including, without limitation, input and output formats, program listings, narrative descriptions, operating instructions and procedures, user and training documentation, special forms, and source code; (c) the tangible media on which such programs are recorded, including without limitation chips, CDs, tapes, back up tapes, archive systems, cloud-based storage locations, hard drives, servers and disks; and (d) any maps or other navigational information acquire for use with the PTV Cloud Service by PTV.

B. Regulatory and Compliance Audits. Any authorized representative of any regulatory agency, taxing authority or private entity that functions in a quasi-regulatory manner that has jurisdiction over Customer in connection with its regulatory functions (each, a “Regulator”) shall, upon request, have the right to audit in accordance applicable law. PTV shall cooperate with all individuals conducting such audits and comply with all reasonable recommendations that result from such inspections, tests and audits within reasonable time frames. Without limiting any of PTV’s other obligations under this Section 4(B) of this Agreement, PTV may engage a third party auditor to perform a Statement on Standards for Attestation Engagements No. 16 (SSAE 16) audit of PTV’s overall operations, information security program or disaster recovery/business continuity plan (or “Plan;” defined below), PTV shall provide on an annual yearly basis a copy of the audit report to Customer thirty (30) days after PTV’s receipt of such report. Any such audit reports shall be PTV’s Confidential Information.

C. Nonexclusive Remedy for Security Breach. Any failure of the PTV Cloud Service to meet the requirements of this Agreement with respect to the security of any Customer Data, Customer PII or other Confidential Information of Customer, including any related backup, disaster recovery or other policies, practices or procedures, is a material breach of this Agreement for which Customer, at its option, may terminate this Agreement immediately on written notice to PTV without any notice or cure period. Without limiting any remedy, PTV shall be responsible, as such rates, costs and charges are incurred, including but not limited to, paying all costs of notice of affected individuals in the event of a security event, credit monitoring services as are deemed reasonable by Customer, other fraud and identity remediation costs and expenses for affected individuals, including all costs and attorneys' fees incurred in investigating and responding to a security incident. PTV will defend, indemnify and hold Customer harmless for all Losses (whether occurring before or after termination), losses, damages, costs, fees, forensic investigation and remediation services and other remediation services (including but not limited to Customer credit monitoring services) arising from any data compromise occurring by virtue of PTV'S failure to observe a reasonable standard of care or requirements of this Agreement.

5. Data Compromise. Without limiting any remedy, PTV shall be responsible, as such rates, costs and charges are incurred, for paying all costs of notice of affected individuals in the event of a security event, credit monitoring services as are deemed reasonable by Customer, and other fraud and identity remediation costs and expenses for affected individuals. PTV will defend, indemnify and hold Customer harmless for all Losses (whether occurring before or after termination), losses, damages, costs, fees, remediation services (including but not limited to Customer credit monitoring services) arising from any data compromise occurring by virtue of PTV's failure to observe a reasonable standard of care or the provisions of this Agreement. Customer is responsible for maintaining reasonable security of any passwords or other account or User Information in its possession or through which Customer may access the PTV Cloud Service, and shall be responsible for Customer's own negligence in failing to adequately protect such password information, to the fullest extent permitted by applicable law.

6. Security; User Information and Usage Data; Data Breach Procedures.

A. Security. PTV shall employ security measures at least as protective as those set forth herein to ensure against unauthorized access to the hosting environment and Customer materials, including all PTV Cloud Service administrative functionality (including any administrative tools, applications, or facilities).

B. User Information and Usage Data. PTV acknowledges that all information collected by PTV from a User ("User Information") and data collected by PTV about any Authorized User ("Usage Data") is Customer's Confidential Information. PTV shall not collect, store, process, record, reproduce, transfer, disclose, use, or perform any other acts, or cause, authorize, or permit any Person to undertake any of the foregoing, with respect to any Usage Data or User Information, other than as strictly necessary to provide the PTV Cloud Service for

the benefit of Customer in accordance with the terms and conditions of this Agreement and, provided, that any Person receiving access to Usage Data is bound by written confidentiality agreements that are at least as protective of, and impose such obligations with respect to, such information as are set forth in this Agreement. “Person” means an individual, corporation, partnership, joint venture, limited liability company, governmental authority, unincorporated organization, trust, association, or other entity.

7. Redundancy, Data Backup and Disaster Recovery.

A. Scope. PTV shall maintain or cause to be maintained disaster avoidance procedures in accordance with this Section 7 during the Term and at all times in which PTV is obligated to provide the PTV Cloud Service. For the avoidance of doubt, “**Customer Data**” shall also mean and include all information relating to Customer or any Registered User or their businesses that Customer or Authorized User uploads to or stores on or transmits through or otherwise processes by the PTV Cloud Service or that PTV otherwise collects by, through or from them, including but not limited to any and all information reflecting the access or use of the PTV Cloud Service by or on behalf of Customer or any Authorized User, including any End-user profile-, visit-, session-, impression-, click through- or click stream- data and any statistical or other analysis, information, Customer PII, and/or data based on or derived from any of the foregoing.

B. Redundancy and Connectivity. PTV shall simultaneously operate as the secondary hosting environment a mirrored production environment at a hardened data center facility that is geographically remote from the primary hosting environment (the “**Secondary Backup Facility**”). Except for its location and housing facility, the mirror system shall: (i) be identical in all respects to the primary system; (ii) have hardware and software, network connectivity, power supplies, backup generators and other similar equipment and PTV Cloud Service that operate independently of the primary system; (iii) have fully current backups of all Customer Data stored on the primary system; and (iv) have the ability to provide the PTV Cloud Service in accordance with this Agreement, during the performance of routine and remedial maintenance or any outage or failure if the primary system fails. PTV shall operate, monitor and maintain such mirror system so that it may be activated and Available.

C. Data Backup. PTV shall conduct or have conducted daily backups of Customer Data and perform or cause to be performed other periodic backups of Customer Data on at least a weekly basis and store such backup Customer Data in a commercially reasonable location and manner and, in addition, no less than daily at the Secondary Backup Facility, as agreed to by the Parties. Customer will extract its own Customer Data at its own cost.