VTEX Global Data Processing Addendum

Este **Data Processing Agreement** de VTEX (**"DPA"**) sirve como Apéndice 2 del Master Service Agreement ("MSA") disponible en https://vtex.com/us-es/Contratos, firmado por el Cliente y VTEX. En conjunto, el Master Service Agreement ("MSA"), el Order Form - Commercial Proposal y este DPA, se denominan "**Contrato**".

En consideración de los supuestos mutuos establecidos en este DPA, el Cliente y VTEX acuerdan que:

1 Tipos de datos y finalidades del procesamiento

A continuación se detallan los tipos de datos personales, categorías de Interesados, propósitos y puntos y métodos de recopilación de datos personales que serán procesados.

Datos personales	*Identificadores personales:* - Nombre y/o apellidos, seudónimo, firma, correo electrónico, dirección o teléfono - Documento de identificación gobierno (por ejemplo, CPF, CNPJ, RUT, número de pasaporte, número de licencia de conducir) *Información de pago:* - Número de tarjeta de crédito o débito (cifrado según los estándares PCI-DSS) *Datos generados oen línea:* - Identificador personal único o identificador electrónico (por ejemplo, cookies o dirección IP) - Información de acceso (por ejemplo, nombre de usuario y/o contraseña cifrada) - información de actividad (por ejemplo, historial de navegación, historial de búsqueda, información del carrito, historial de pedidos, historial de tarjetas de regalo, historial de contactos de soporte o interacciones con contenido y anuncios) - Inferencias derivado de preferencias y comportamiento
A a quién pertenecen los datos (categorías de Interesados)	- Los consumidores finales del Cliente (por ejemplo, compradores o compradores, visitantes del sitio web o suscriptores) - Empleados del cliente
Propósitos para procesamiento de datos	- Servicios de desempeño en virtud del Contrato (por ejemplo, mantener o proporcionar cuentas, brindar servicios al Cliente, cumplir con pedidos y transacciones, procesar pagos, brindar publicidad o servicios de marketing según las instrucciones del Cliente) - Auditoría relacionada con una interacción actual (por ejemplo, contar y verificar impresiones de anuncios) - Detectar, prevenir e investigar incidentes de seguridad, actividades fraudulentas o ilegales - Depurar errores que perjudiquen la funcionalidad y mantengan o mejoren la disponibilidad de los Servicios - Mejora y desarrollo de productos. - Realizar análisis, agregación y/o desidentificación de datos, incluso para desarrollar conocimientos en beneficio del Cliente.
Punto de recogida de datos	- Sitio web, aplicación móvil o servicio digital similar del cliente

Método de recopilación de datos	- Formularios completados directamente por el Interesado (por ejemplo, suscripción al boletín, encuesta, formulario de registro) - Cookies, píxeles, etiquetas, SDK y tecnologías similares

2 Definiciones e Interpretación.

Cualquier término escrito en mayúscula se define: (i) en **Leyes de protección de datos** aplicables, como por ejemplo "**Responsable de datos**", "**datos personales**", "**Encargado de datos**" y "**Sub-Encargado**"; (ii) por el significado que se les da en el MSA; o (iii) en esta cláusula. Para los fines de este DPA, "**datos personales**" significa cualquier información relativa a una persona física identificada o identificable, protegida por las Leyes de Protección de Datos aplicables, proporcionada por el Cliente, en la posición de Responsable de Datos, a VTEX, en la posición de Encargado de Datos, en el contexto de la ejecución del Contrato.

"**Afiliado**" significa cualquier entidad que directa o indirectamente controle, esté controlada o esté bajo control común con el Cliente. "Control", a los efectos de esta definición, significa propiedad o control directo o indirecto de más del 50% de las participaciones con derecho a voto de la entidad en cuestión.

"**Usuarios autorizados**" significa cualquier persona a quien el Cliente haya otorgado acceso al entorno de la Plataforma VTEX de acuerdo con los requisitos establecidos en el Contrato.

"**Cliente**" significa la entidad identificada en el *Order Form - Commercial Proposal* que firme este DPA en su nombre y en nombre de cualquier Afiliado del Cliente.

"**Afiliado del cliente**" significa cualquier Afiliado(s) del Cliente autorizado a utilizar los Servicios de conformidad con el MSA entre el Cliente y VTEX. Si y en la medida en que VTEX procese datos personales en nombre de dicho(s) Afiliado(s), el Afiliado calificará como Responsable.

"**Datos personales del cliente**" significa cualquier dato personal relacionado con los Usuarios Autorizados recibidos con el fin de autorizar el acceso a los Servicios, o con los representantes del Cliente o Afiliados en relación con la ejecución y administración del Contrato, cuyos datos personales VTEX trata como Responsable.

"FAP" significa los mecanismos para transferir datos personales a los Estados Unidos de la Unión Europea/Espacio Económico Europeo, el Reino Unido (y Gibraltar) y Suiza de conformidad con el *UE-EE.UU. Marco de privacidad de datos* ("**UE-EE.UU. FAP**"), con el *Extensión del Reino Unido a la UE-EE.UU. Marco de privacidad de datos* ("**Extensión del Reino Unido a la UE-EE.UU. FAP**"), y con el *Suiza-EE.UU. Marco de privacidad de datos* ("**Suiza-EE.UU. FAP**"), basado en la decisión de adecuación de la Comisión Europea vigente el 10 de julio de 2023.

"Leyes de Protección de Datos" significa todas las leyes, regulaciones de las autoridades supervisoras de protección de datos y órdenes judiciales/administrativas en cualquier jurisdicción a la que el Cliente esté obligado en relación con los Servicios proporcionados en virtud del Contrato, incluidas aquellas relacionadas con: (a) privacidad; (b) la seguridad, pérdida o uso indebido de datos, (c) marketing y publicidad comercial; y (d) uso responsable y protección de datos.

"SCC" significa las secciones I, II, III y IV (según corresponda) en la medida en que hagan referencia al Módulo Dos (Responsable a Encargado) dentro de las Cláusulas Contractuales Estándar (o *Standard Contractual Clauses*) para la transferencia de datos personales a países terceros de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo aprobado por Decisión de Ejecución (UE) 2021/914 de la Comisión Europea de 4 de junio de 2021, tal y como está

establecido actualmente en https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj, según enmendado, reemplazado o requerido para ser implementado en relación con las CEC de vez en cuando.

"**SCC del Reino Unido**" significa el SCC transpuesto a la legislación nacional del Reino Unido mediante la operación de la sección 3 de la Ley (Retirada) de la Unión Europea de 2018 y modificada por las Regulaciones de Protección de Datos, Privacidad y Comunicaciones Electrónicas (Enmienda, etc.) (Salida de la UE) de 2019 ("**RGPD del Reino Unido**"), de conformidad con el artículo 46 del RGPD del Reino Unido.

"Violación de Seguridad" significa el acceso, pérdida, alteración o divulgación accidental o no autorizado de datos personales procesados. Una violación de seguridad incluye, entre otras, una "fuga de datos personales" u otro término similar según se define en las Leyes de Protección de Datos.

"**Autoridad de Supervisión**" significa una autoridad reguladora independiente responsable de hacer cumplir las leyes de protección de datos.

3 Detalles del tratamiento.

3.1 **Roles de las Partes.** A los efectos de este DPA, el Responsable de datos es el Cliente (como se define en el Order Form - Commercial Proposal) y cualquier Afiliado del Cliente; el Encargado de Datos es VTEX (según se define en el Order Form - Commercial Proposal); y los Sub-Encargados son AWS (Región de Virginia Norte - EE.UU.) y VTEX Brasil Tecnología para E-commerce Ltda.

3.2 **Transferencias Internacionales de Datos**. Cuando VTEX procese datos personales de Interesados ubicados en el Espacio Económico Europeo, Suiza o Reino Unido en un país que no haya recibido una decisión de adecuación de la Comisión Europea o de las autoridades suizas o del Reino Unido, según corresponda, dicha transferencia se realizará con base sobre Certificación VTEX en el DPF. Si el DPF se declara inválido, o si VTEX no puede recertificarse según el DPF, entonces la transferencia de datos personales estará sujeta al SCC o al SCC del Reino Unido, según corresponda, que las partes acuerdan que se incorporarán por referencia a este DPA. Las partes acuerdan que, con respecto a aquellos elementos de las CEC y las CEC del Reino Unido que requieren aportes de las partes, los Schedules 1 a 4 contienen toda la información relevante.

3.3 **Alcance del procesamiento.** El Contrato contiene las instrucciones completas y finales del Cliente en el momento de la ejecución del DPA para el Tratamiento de datos personales. Cualquier instrucción adicional o alternativa deberá solicitarse por separado y por escrito a VTEX. VTEX siempre deberá: (i) procesar datos personales únicamente con el fin de proporcionar los Servicios al Cliente como se describe en la tabla de las páginas 1 y 2 y Schedules 1-4 para los fines de las CEC; (ii) de acuerdo con las instrucciones documentadas del Cliente; y (iii) no tratar datos personales para fines propios o de terceros. VTEX notificará de inmediato al Cliente por escrito, a menos que esté prohibido por las Leyes de Protección de Datos u otras leyes aplicables, si: (a) toma conocimiento o cree que alguna instrucción de procesamiento de datos del Cliente viola las Leyes de Protección de Datos o no cumple. con las instrucciones de procesamiento de datos del Cliente; y/o (b) no puede cumplir con los términos del Contrato que se relacionan o rigen el procesamiento y/o la seguridad de los datos personales.

3.4 **Obligaciones mutuas.** En la medida aplicable al desempeño o uso de los Servicios por parte de cada parte, según corresponda, incluso en la medida en que cada parte recopile datos personales directamente de individuos, cada parte declara y garantiza que: (i) cumplirá con las Leyes de Protección de Datos en relación con a cualquier dato personal recibido, recopilado, procesado, compartido o almacenado por dicha parte, incluidas las directrices, marcos o códigos de autorregulación aplicables de la industria; (ii) mantener avisos de privacidad visibles para el consumidor, divulgaciones de cookies y/u otras declaraciones requeridas legalmente que revelen con precisión todas las prácticas de seguridad, uso, intercambio, divulgación y recopilación de datos

aplicables; (iii) obtener los permisos necesarios y los consentimientos de participación o exclusión voluntaria de las personas y respetar esas elecciones de los consumidores; (iv) establecer y mantener procesos legales para el ejercicio de los derechos de los Propietarios y cumplir con cualquier solicitud de derechos válida relacionada con los datos personales y los datos personales del Cliente, según corresponda a cada parte; y (v) garantizar que las personas con acceso a datos personales estén sujetas a una obligación de confidencialidad contractual o legal adecuada.

4 Obligaciones del cliente.

4.1 **Base legal**. El Cliente es el único responsable de la exactitud, calidad y licitud de los datos personales y del medio por el cual adquirió los datos personales proporcionados a VTEX. El Cliente garantiza que tiene una base legal para compartir datos personales con VTEX y para que VTEX procese datos personales según lo previsto en el Contrato.

5 Obligaciones VTEX.

5.1 **Schedules Regionales.** VTEX se compromete a incluir obligaciones adicionales de acuerdo con las leyes vigentes en el país y/o territorio aplicables a Cliente, según lo establecido en el Order Form. Dichas obligaciones están previstas en el Schedule CCPA, Schedule LATAM, Schedule GDPR y otros Schedule, cada uno en la medida aplicable al procesamiento de datos personales realizado por VTEX de acuerdo con la ley aplicable y los territorios establecidos en la MSA. En la medida en que exista algún conflicto entre un Schedule y el cuerpo principal de este DPA, prevalecerá el Schedule.

5.2 **Derechos del Interesado y Cooperación.**

5.2.1 VTEX cooperará con el Cliente para permitirle responder a cualquier pedido, queja u otras comunicaciones válidas de individuos, organismos reguladores o judiciales, u otras entidades relevantes, relacionadas con el procesamiento de datos personales (**"Solicitud"**), incluidas las Solicitudes de personas para ejercer sus derechos según las leyes de protección de datos. Si dicha Solicitud se realiza directamente a VTEX, VTEX deberá notificar al cliente por escrito dentro de los 2 (dos) días hábiles.

5.2.2 Si VTEX recibe una citación, orden judicial, orden judicial u otro requisito legal de un tercero (incluidas autoridades policiales u otros servicios públicos o de protección de datos). autoridades supervisoras) que buscan la divulgación de datos personales, en la medida en que no lo prohíba la ley, VTEX notificará de inmediato al Cliente por escrito sobre dicha Solicitud y cooperará razonablemente con el Cliente si el Cliente desea limitar, objetar o proteger contra dicha divulgación.

5.3 **Sub-Encargados y Empleados.** El Cliente reconoce y acepta que (a) los Afiliados de VTEX son Sub-Encargados bajo este DPA especialmente para fines de soporte técnico y (b) VTEX y los Afiliados de VTEX pueden contratar con Sub-Encargados de terceros, como AWS, Región de Virginia del Norte, EE. UU., en relación con la prestación de los Servicios. Una lista actualizada de Sub-Encargados contratados por VTEX para brindar los Servicios está disponible en https://vtex.com/es-pt/privacidad-y-Contratos/Sub-Encargadoes/ ("**Lista de Sub-Encargadoes**"). VTEX impondrá contractualmente el mismo o mayor nivel de protección a los Sub-Encargados para el procesamiento de datos personales según lo previsto en este DPA. VTEX debe garantizar que los empleados autorizados a procesar datos personales estén: (i) obligados a mantener la confidencialidad de los datos personales; y (ii) estar debidamente capacitado en el procesamiento de datos personales según las leyes de protección de datos aplicables.

5.4 **Evaluación de impacto de la protección de datos.** En la medida en que el Cliente no tenga acceso a la información relevante, VTEX brindará al Cliente la cooperación y asistencia razonables necesarias para llevar a cabo una evaluación de impacto de la protección de datos, o cualquier evaluación similar requerida por las Leyes de Protección de Datos, relacionada con el uso

de los Servicios. por el Cliente, cuando un tipo de tratamiento pueda resultar en un alto riesgo para los derechos y libertades de las personas físicas.

5.5 **Medidas de seguridad y auditorías de cumplimiento.**

5.5.1 VTEX: (i) implementará medidas de seguridad técnicas y organizativas apropiadas para proteger los datos personales de una Violación de Seguridad utilizando medidas apropiadas a los riesgos presentados por la naturaleza del procesamiento de datos personales (y dichas medidas cumplirán o excederán las identificadas en el Schedule 3; (ii) monitorear periódicamente el cumplimiento de dichas medidas; (iii) previa solicitud, poner a disposición del Cliente una copia de los resultados de sus auditorías de terceros más recientes o certificaciones relacionadas con dichas medidas, en la medida en que VTEX las ponga a disposición de sus clientes de manera general; y (iv) responder oportunamente a las solicitudes anuales del Cliente relativas al cuestionario de seguridad y privacidad de la información de VTEX. Si, según la determinación razonable del Cliente, la información proporcionada en (iii) y (iv) es inadecuada o en caso de una Violación de Seguridad, VTEX acepta permitir una auditoría o inspección de un tercero independiente (siempre que dicha auditoría o inspección se realice por un auditor mutuamente acordado por las partes, a cargo exclusivo del Cliente y no más de una vez al año, excepto si la auditoría o inspección ocurre en respuesta a una Violación de Seguridad). Antes del comienzo de cualquier auditoría o inspección independiente, el Cliente y VTEX acordarán mutuamente el alcance, el momento y la duración de la auditoría o inspección y VTEX brindará asistencia y cooperación razonables para permitir dicha auditoría o inspección. Cuando lo requieran las Leyes de Protección de Datos, VTEX mantendrá un plan y/o política integral por escrito relacionado con la implementación de dichas medidas y proporcionará un resumen de dicho plan y/o política al Cliente cuando lo solicite.

5.5.2 **Auditorías.** El Cliente podrá auditar el cumplimiento por parte de VTEX de las Medidas Técnicas y Organizativas relevantes a los datos personales procesados por VTEX (“**Auditoria del Cliente**") previa solicitud y sólo si:

(a) VTEX no ha proporcionado evidencia suficiente de su cumplimiento de las Medidas Técnicas y Organizativas establecidas en el Schedule 3, 3.3, por ejemplo, ISO 27001, SOC 2 - Tipo 2, u otras normas definidas en las certificaciones (“**Informes de Auditoría y Certificaciones**"); o

(b) se ha producido una violación de datos personales; o

(c) la autoridad de protección de datos del Cliente solicita formalmente una auditoría; o

(d) u, la Ley de Protección de Datos establece un derecho de auditoría directa.

5.5.3 **Especificaciones de auditoría.** Antes de iniciar una solicitud de auditoría, el Cliente revisará los Informes de Auditoría y Certificaciones de VTEX. El Cliente o su auditor externo independiente (razonablemente aceptable para VTEX, actuando en nombre del Cliente) deberá notificar con al menos sesenta (60) días de anticipación cualquier Auditoría del Cliente, a menos que una Ley de Protección de Datos o la autoridad de protección de datos del Cliente requiera un aviso más corto. . La fecha de inicio, el momento y el alcance de cualquier Auditoría del Cliente se acordarán mutuamente entre las partes actuando de manera razonable. A menos que las Leyes de Protección de Datos exijan auditorías más frecuentes, la frecuencia de una Auditoría del Cliente no excederá una vez cada 12 meses. Los recursos de VTEX para soportar las Auditorías de Clientes se limitarán a un máximo equivalente a 3 (tres) días hábiles durante el horario comercial normal de VTEX, no interrumpirán las operaciones comerciales normales de VTEX y estarán sujetos a los requisitos de confidencialidad de VTEX. EL Cliente compartirá cualquier informe resultante de una Auditoría de Cliente a VTEX.

5.5.4 **Costos de auditoría**. Si se realiza una auditoría fuera de las especificaciones proporcionadas en 5.5.3, entonces el cliente cubrirá todos los costos razonables de dicha auditoría y cualquier trabajo requerido de VTEX a las tarifas vigentes en ese momento. Si la Auditoría del Cliente revela un incumplimiento material de este DPA por parte de VTEX, entonces VTEX realizará su propia auditoría para confirmar dicho incumplimiento material. En

este caso, se aplicarán los procedimientos de remediación establecidos en el Contrato.

5.6 **Violación de Seguridad.**

5.6.1 En caso de una Violación de Seguridad, VTEX:

(i) De inmediato, y en ningún caso más tarde de 72 (setenta y dos) horas después de tener conocimiento de dicha Violación de Seguridad, informar al Cliente y proporcionar detalles por escrito de la Violación de Seguridad, incluidos, si corresponde, los tipos de datos personales afectados y la identidad del persona(s) afectada(s) tan pronto como dicha información sea conocida o esté disponible para VTEX;

(ii) Proporcionar información oportuna y cooperación según lo requiera el Cliente para cumplir con sus obligaciones de informar sobre violaciones de datos según las Leyes de Protección de Datos o para cumplir o responder a cualquier consulta de una autoridad de protección de datos o cualquier acción legal que surja de la Violación de Seguridad, excepto cuando dicha información incluya información confidencial. información de terceros;

(iii) Investigar la violación de seguridad y realizar un análisis de la causa raíz;

(iv) Tomar medidas y acciones apropiadas para remediar o mitigar los efectos de la Violación de Seguridad y mantener al Cliente actualizado sobre los desarrollos relacionados con la Violación de Seguridad; y

(v) Si el análisis de la causa raíz demuestra que la Violación de Seguridad fue causada únicamente por VTEX, VTEX reembolsará al Cliente cualquier costo y gasto razonable incurrido en relación con una Violación de Seguridad, incluido el costo de notificaciones a individuos y servicios de monitoreo y resolución de robo de identidad (incluyendo servicios de seguimiento de crédito) a las partes afectadas de acuerdo con la cláusula 6. Responsabilidad.

5.6.2 El contenido y la provisión de cualquier aviso, comunicación pública/regulatoria o comunicado de prensa relacionado con la Violación de Seguridad serán únicamente del Cliente, a menos que las Leyes de Protección de Datos exijan lo contrario o haya referencia a VTEX en dichos anuncios; en ese caso, VTEX deberá aprobar el contenido por escrito y con antelación para cualquier publicidad.

5.7 **Eliminación y/o transferencia**. VTEX, en cualquier momento, pero no después de la terminación del Contrato, proporcionará los medios para que el Cliente extraiga una copia completa de todos los datos personales en posesión de VTEX o, en ausencia de instrucciones del Cliente, destruirá de forma segura dichos datos personales. El Cliente reconoce que VTEX podrá cumplir con la obligación anterior proporcionando las interfaces necesarias para que el Cliente recupere datos personales por sus propios medios, en el propio entorno administrativo del Cliente en la Plataforma VTEX. Esta opción permanecerá disponible, por defecto, hasta la fecha de terminación del Contrato.

6 Responsabilidad.

6.1. La responsabilidad de cada parte y de todas sus Afiliadas, en conjunto, que surja de o esté relacionada con este DPA, y todos los DPA entre el Cliente y las Afiliadas y VTEX, ya sea por contrato, agravio o bajo cualquier otra teoría de responsabilidad, están sujetos a la sección "**LIMITACIÓN DE RESPONSABILIDAD DE VTEX**" del MSA. Cualquier referencia en esta sección a la responsabilidad de una parte significa la responsabilidad agregada de esa parte y todas sus Afiliadas según el MSA. En particular, no debe entenderse que el conjunto de todas las reclamaciones se aplica individual y conjuntamente al Cliente y/o a cualquier Afiliado que sea parte contractual del MSA. VTEX será responsable de los actos y omisiones de sus Sub-Encargados en la misma medida que lo sería si prestara los servicios de cada Sub-Encargado directamente bajo este DPA.

7 Ley aplicable y resolución de disputas

Según lo establecido en la Cláusula "**LEY APLICABLE Y ARBITRAJE**" del MSA.

Como excepción a lo anterior, en relación con las transferencias restringidas únicamente en el Reino Unido, el "**legislación aplicable**" será la ley de Inglaterra y Gales.

Lugar, fecha y firmas en el Order Form - Commercial Proposal

POR CUANTO, este DPA se celebra y se convierte en una parte vinculante del Contrato.

Schedule 1: Transferencias Internacionales - Descripción del Procesamiento y Sub-Encargados

Actividad de tratamiento	**El Cliente divulga sus datos personales a VTEX para proporcionar, operar y mantener los Servicios VTEX.**	**El cliente contacta a VTEX para soporte técnico**	**El cliente procesa datos personales de usuarios finales/datos personales de compradores en los Servicios VTEX**
Tipos de datos y finalidades del tratamiento	Ver "Tipos de datos y finalidades del tratamiento" en la DPA.		
Situación de las Partes	VTEX y el Cliente son Responsables del Tratamiento	VTEX y el Cliente son Responsables del Tratamiento	VTEX es un Encargado de Datos El cliente es el Responsable del Tratamiento
Categorías de datos personales tratados	Registro de cuenta, contenido de usuario, comunicación, tecnologías de seguimiento, uso de Servicios y cuentas de terceros (según las integraciones elegidas por el Cliente).	Registro de cuenta, contenido de usuario, comunicaciones, uso de Servicios y cuentas de terceros (según integraciones elegidas por el Cliente).	Según lo determine el Cliente (ver sección "Tipos de datos y finalidades del procesamiento" en la DPA).
Categorías de datos personales sensibles tratados	Ninguno	Ninguno	Según lo determine el Cliente
Frecuencia de transferencia	Continuo	Continuo	Según lo determine el Cliente
Módulo SCC aplicable	Módulo 1	Módulo 1	Módulo 2
Sub-Encargados	Para obtener una lista completa, consulte https://vtex.com/es-pt/privacidad-y-Contratos/Sub-Encargadoes/		

	Exportador de datos: Cliente nombrado en el Contrato **Importador de datos:** Entidad VTEX indicada en el Contrato **Sub-Encargado 1**: VTEX Brasil Tecnología para E-commerce Ltda. para fines de soporte técnico **Sub-Encargado 2**: Amazon Web Services Inc., Región de Virginia del Norte, EE. UU.

Schedule 2: Información para SCC - Módulo 1

1. Plazos de conservación

VTEX conserva los datos personales que recopila como Responsable del Tratamiento mientras VTEX tenga un fin comercial para ello o durante el período más largo permitido por la ley aplicable.

2.SCC

2.1. A los efectos de las Cláusulas Contractuales Tipo:

Cláusula 7, Módulo 1: Las partes acuerdan que la cláusula de atraque (*docking clause*) no será aplicable.
Cláusula 11(a), Módulo 1: Las partes no seleccionan la opción de resolución independiente de disputas.
Cláusula 17, Módulo 1: Las partes seleccionan la Opción 1. El Estado Miembro se indica en la cláusula de foro del Contrato.
Cláusula 18(b), Módulo 1: Las Partes acuerdan que estos serán los tribunales como se indica en la cláusula de competencia del Contrato.

Anexo I (A): El exportador de datos es el Cliente. El importador de datos es VTEX. Los datos de contacto del Cliente son las direcciones de correo electrónico designadas por el Cliente en su cuenta VTEX. El contacto VTEX es dpo@vtex.com, o como se establece en el Contrato.

Anexo I (B): Las partes acuerdan que el Schedule 1 describe la transferencia.

Anexo I (C): La autoridad de control competente es la Autoridad supervisora del ICO.

Anexo II: Las Partes acuerdan que el Schedule 3, Sección 3.3. describe las medidas técnicas y organizativas aplicables a la transferencia.

2.2. A los efectos del Anexo del Reino Unido:

Tabla 1: El exportador de datos es el Cliente. El importador de los datos es la Entidad VTEX indicada en el Contrato. Los datos de contacto del Cliente son las direcciones de correo electrónico designadas por el Cliente en su cuenta VTEX. El contacto VTEX es dpo@vtex.com, o como se establece en el Contrato.

Tabla 2: Las Partes seleccionan la casilla de verificación que dice: “SCC de la UE aprobadas, incluida la Información del Apéndice y solo con los siguientes módulos, cláusulas o disposiciones opcionales de las SCC de la UE aprobadas y vigentes para los fines de este Anexo”, y la tabla adjunta será se

considerará completado de acuerdo con las preferencias de las Partes descritas en el Schedule 2, Sección 2.1 anterior.

Tabla 3: La Tabla 3 deberá completarse con la información establecida en el Schedule 2, Sección 2.1 anterior, refiriéndose al Anexo I(A), Anexo I(B) y Anexo II.

Tabla 4: Las Partes acuerdan que el importador de datos puede rescindir el Anexo del Reino Unido según lo establecido en la Sección 19 del Anexo del Reino Unido.

Se agregará IDTA del Reino Unido

Tabla 1: Ver el Contrato.

Tabla 2: Ley del país del Reino Unido que rige el IDTA y jurisdicción principal para las reclamaciones legales que deben presentar las Partes: Inglaterra y Gales. Estado de exportador e importador: consulte el Schedule 1. Si el RGPD del Reino Unido se aplica al importador: consulte el contrato. Contrato y Plazo Vinculados: Ver Contrato. Terminación del IDTA antes del final del Plazo: Las Partes no podrán rescindir el IDTA antes del final del Plazo a menos que exista una violación del IDTA o las Partes acuerden por escrito. Terminación del IDTA cuando cambia el IDTA aprobado: Importador. El importador podrá realizar transferencias adicionales de los Datos Transferidos: Ver Schedule 1. Restricciones específicas cuando el Importador podrá transferir los Datos Transferidos: Ver Schedule 1. Fechas de revisión: siempre que haya un cambio en los Datos Transferidos, Propósitos, Información del Importador, TRA o Evaluación de riesgos.

Tabla 3: Ver Schedule 1.

Tabla 4: Ver sección 3.3. Medidas técnicas y organizativas para garantizar la seguridad de los datos ("TOM")

Schedule 3: Información para SCC - Módulo 2

1. Sub-Encargados

VTEX utiliza Sub-Encargados cuando actúa como Encargado. El Cliente autoriza a VTEX a utilizar estos Sub-Encargados de acuerdo con la Sección 5.3. Los Sub-Encargados están disponibles en nuestra **Lista de Sub-Encargados**.

2. Plazos de conservación

VTEX conserva los datos personales que recopila o recibe del Cliente como Encargado durante la vigencia del Contrato y es consistente con sus obligaciones bajo este DPA.

3. Información para Transferencias Internacionales

3.1. A los efectos de las Cláusulas Contractuales Tipo o CEC:

Cláusula 9, Módulo 2(a): Las partes seleccionan la Opción 2. El plazo es de 30 (treinta) días.
Cláusula 11(a): Las partes no seleccionan la opción de resolución independiente de disputas.
Cláusula 17, Módulo 2: Las partes seleccionan la Opción 2. El Estado miembro del exportador de datos es el Estado miembro de la UE en el que se encuentra el Cliente.

Cláusula 18 (b), Módulo 2: Las Partes acuerdan que estos serán los tribunales del Estado miembro de la UE nombrado en el Contrato.

Anexo I (A): El exportador de datos es el Cliente. El importador de los datos es la Entidad VTEX indicada en el Contrato. Los datos de contacto del Cliente son las direcciones de correo electrónico designadas por el Cliente en su cuenta VTEX. El contacto VTEX es dpo@vtex.com, o como se establece en el Contrato.

Anexo I (B): Las partes acuerdan que **Schedule 1** describe la transferencia.

Anexo I (C): La autoridad de control competente es la autoridad de control designada por el Cliente que actúa como exportador de datos.

Anexo II: Las partes acuerdan que el Schedule 3, Sección 3.3 describe las medidas técnicas y organizativas aplicables a la transferencia.

3.2. A los efectos del Anexo del Reino Unido:

Tabla 1: El exportador de datos es el Cliente. El importador de los datos es la Entidad VTEX indicada en el Contrato. Los datos de contacto del Cliente son las direcciones de correo electrónico designadas por el Cliente en su cuenta VTEX. El contacto VTEX es dpo@vtex.com o según lo dispuesto en el Contrato.

Tabla 2: Las Partes seleccionan la casilla que dice: “SCC de la UE aprobadas, incluida la Información del Apéndice y solo con los siguientes módulos, cláusulas o disposiciones opcionales de las SCC de la UE aprobadas y vigentes para los fines de este Adendo”, y se considerará la tabla adjunta. celebrado de conformidad con las preferencias de las Partes descritas en **Schedule 3, Sección 3.1 anterior**.

Tabla 3: La Tabla 3 debe completarse con la información proporcionada en (i) **Schedule 3, Sección 3.1 anterior** en relación con el Anexo I(A), el Anexo I(B), el Anexo II y (ii) el Schedule 3, Sección 1 anterior en relación con el Anexo III.

Tabla 4: Las Partes acuerdan que el importador de datos puede rescindir el Anexo del Reino Unido según lo establecido en la Sección 19 del Anexo del Reino Unido.

Se agregará IDTA del Reino Unido

Tabla 1: Ver el Contrato.

Tabla 2: Ley del país del Reino Unido que rige el IDTA y jurisdicción principal para las reclamaciones legales que deben presentar las Partes: Inglaterra y Gales. Estado de exportador e importador: consulte el Schedule 1. Si el RGPD del Reino Unido se aplica al importador: consulte el contrato. Contrato y Plazo Vinculados: Ver Contrato. Terminación del IDTA antes del final del Plazo: Las Partes no podrán rescindir el IDTA antes del final del Plazo a menos que exista una violación del IDTA o las Partes acuerden por escrito. Terminación del IDTA cuando cambia el IDTA aprobado: Importador. El importador puede hacer más transferencias de Datos Transferidos: Ver Schedule 1. Restricciones específicas sobre cuándo el Importador puede transferir los Datos Transferidos: Ver Schedule 1. Fechas de revisión: siempre que haya un cambio en los Datos Transferidos, Propósitos, Información del Importador, TRA o evaluación de riesgos.

Tabla 3: Ver Schedule 1.

Tabla 4: Ver sección 3.3. Medidas técnicas y organizativas para garantizar la seguridad de los datos ("TOM")

3.3. Medidas técnicas y organizativas para garantizar la seguridad de los datos ("TOM")

El Importador de Datos ha implementado y mantendrá medidas técnicas y organizativas apropiadas para proteger los datos personales contra el mal uso y la pérdida o destrucción accidental según lo establecido en las Políticas de Privacidad y Seguridad de VTEX.

Las medidas técnicas y organizativas actuales del Importador de datos se detallan a continuación.

Como se mencionó anteriormente, a continuación se presenta una lista no exhaustiva de los puntos que actualmente se implementan en VTEX con enfoque en la protección y seguridad de datos considerando la tríada: TI, Seguridad y Privacidad.

1. Concientización y Capacitación
    a. VTEX ofrece ciclos de capacitación recurrentes, que incluyen sesiones generales y específicas de roles, con fuerte énfasis en privacidad y seguridad. VTEX ofrece capacitación especializada en prácticas de desarrollo seguro, alineadas con nuestras certificaciones de seguridad.

2. Protección con contraseña
    a. Las contraseñas se cifran mediante PBKDF2 basado en SHA-256. Durante este proceso, solo se almacena el valor hash resultante, lo que garantiza que las contraseñas originales permanezcan seguras y no sean accesibles directamente.
    b. Los comerciantes pueden optar por imponer la caducidad de la contraseña después de un período específico para los usuarios administradores.
    c. Los comerciantes también pueden optar por integrar un proveedor de identidad externo, lo que les permite establecer sus propias políticas de contraseña personalizadas.

3. Autorización y control de acceso

VTEX gestiona eficientemente el acceso lógico, asegurando un control y monitoreo preciso de los permisos de acceso a sistemas y datos. Nuestras prácticas siguen políticas de seguridad, incluidas medidas como el principio de privilegio mínimo y la segregación de funciones. Los usuarios sólo tienen acceso a lo estrictamente necesario para sus funciones, reduciendo el riesgo de exposición de información confidencial y reforzando la seguridad de los sistemas y datos.

4. Seguridad de terminales
    a. VTEX adopta un enfoque integral para mitigar los ciberataques, empleando medidas como antivirus avanzados, firewalls y filtros de contenido para bloquear el malware. Nuestra plataforma incluye protección contra ataques DDoS (Denegación de Servicio Distribuido) y otras amenazas.
    b. VTEX también utiliza herramientas de monitoreo para garantizar la seguridad integral de los endpoints.

5. Clasificación de datos
    a. VTEX cuenta con una política de clasificación de la información para determinar el nivel adecuado de protección requerido para cada tipo de datos.

6. Registros de registro

Todas las operaciones en la plataforma se registran automáticamente. Los errores de la plataforma se registran en el software de Gestión de Eventos e Información de Seguridad, accesible al equipo de VTEX para análisis y mejora del producto.

7. Gestión de vulnerabilidades
    a. VTEX realiza evaluaciones periódicas de amenazas y vulnerabilidades en nuestra plataforma y procesos operativos. Los riesgos identificados conducen a mejoras en nuestros sistemas de monitoreo y presentación de informes, lo que nos permite gestionar problemas potenciales de manera efectiva, ya sea alertando al personal relevante o iniciando acciones automatizadas para mitigarlos o eliminarlos. Para obtener una explicación detallada de nuestros procedimientos de pruebas de penetración, consulte el punto 14 del apéndice.

8. Certificaciones
    a. Según los estándares de la industria, las certificaciones de las empresas generalmente cubren el período de enero a diciembre, siendo diciembre el inicio del proceso de renovación para el próximo año. Por lo tanto, cuando nos referimos a nuestras certificaciones actuales, nos referimos a aquellas que se mantuvieron durante el período de aplicación más reciente. Las certificaciones que VTEX mantuvo durante este período son las siguientes:"
        i. ISO 27001: Estándar internacional para sistemas de gestión de seguridad de la información.
        ii. SOC 1 - Tipo 2: Un informe que cubre los controles internos de los sistemas de información financiera.
        iii. SOC 2 - Tipo 2: Informe que cubre seguridad, disponibilidad, integridad, confidencialidad y privacidad.
        iv. PCI: una validación de los controles sobre los datos de los Interesados de tarjetas para reducir el fraude con tarjetas de crédito.

Todas estas certificaciones pueden solicitarse a VTEX en cualquier momento y están disponibles en el enlace de la Sección Cumplimiento en VTEX Trust Hub (https://vtex.com/pt-br/trust/).

9. Cómo VTEX aborda el Backup y la Redundancia de Datos
    a. Los datos manejados por VTEX se almacenan en servicios de AWS utilizando servicios administrados como S3, RDS y DynamoDB. Todos estos servicios brindan una infraestructura de respaldo administrada por AWS que es utilizada por VTEX. La plataforma AWS es referencia en el sector de la computación en la nube y cuenta con importantes certificaciones como: ISO 27001, PCI DSS, CSA, NIST y muchas otras. (Para ver una lista de certificaciones detalladas, visite: https://aws.amazon.com/en/compliance/programs/).

10. Plan de continuidad del negocio y plan de recuperación ante desastres
    a. VTEX cuenta con un Plan integral de Recuperación de Desastres, que incluye políticas y procedimientos internos diseñados para manejar las interrupciones del servicio. Este plan tiene como objetivo restaurar los componentes afectados lo más rápido posible. Para garantizar su efectividad, VTEX realiza pruebas periódicas de este plan.
    b. El alcance de este plan es la Plataforma VTEX Cloud Commerce, incluyendo: (i) todos los servicios que constituyen la solución; (ii) todos los procesos de negocio que lo respaldan o su operación; (iii) todos los procesos de negocio que soportan a los clientes de VTEX que dependen de la Plataforma VTEX Cloud Commerce;

c. El Plan de Recuperación de Desastres de VTEX está soportado e implementado por procesos automatizados que se activan con base en herramientas automatizadas de monitoreo y notificación. Además, un equipo especializado supervisa estos procesos y monitorea su desempeño para garantizar la efectividad y capacidad de respuesta del plan.
d. Las partes interesadas externas son notificadas a través de la página de estado (https://estado.vtex.com): La página de estado está disponible públicamente para cualquier persona interesada en ver el estado de salud actual de la plataforma VTEX True Cloud CommerceTM.

11. Cifrado de datos privados
    a. VTEX garantiza el cifrado de acuerdo con las normas de privacidad y cumplimiento de la información de identificación personal. Los módulos de pago cumplen con PCI e implementan cifrado de datos y rotación de claves de acuerdo con los estándares PCI-DSS. VTEX tiene en marcha proyectos de ingeniería para implementar cifrado y aislamiento de información de identificación personal, así como implementar registro de auditoría en multitud de aplicaciones más allá de las que ya lo ofrecen.

12. Almacenamiento de datos en VTEX
    a. El proveedor de hosting de VTEX es AWS, el proveedor líder mundial de servicios de computación en la nube, y los datos se almacenan en la Región AWS del Norte de Virginia en Estados Unidos.

13. Transmisión de datos
    a. Todo el tráfico que ingresa a la red VTEX está protegido por tecnología TLS 1.2 (o superior) vía http.

14. Políticas de Pentest
    a. Debido a la naturaleza del negocio de VTEX, hemos establecido como política la realización de pruebas de penetración, o *pentest*, al menos cada seis meses. Además, nuestra plataforma es evaluada periódicamente por clientes, socios y auditores independientes, lo que garantiza un escrutinio externo e interno continuo.
    b. Se anima a los minoristas a compartir informes de pruebas de penetración y notificaciones de vulnerabilidad con VTEX, lo que permitirá a nuestro equipo de Seguridad resolver rápidamente cualquier problema potencial identificado. Las pruebas de penetración deben programarse previamente con VTEX. Cualquier prueba realizada de forma autónoma sin previo aviso a VTEX será considerada un intento de acción no autorizada.

15. Evaluación de riesgos de terceros

VTEX cuenta con un proceso integral de evaluación de nuestros proveedores para garantizar que cumplan con nuestros estándares de seguridad y gestión de riesgos. Utilizamos un cuestionario detallado de evaluación de Sub-Encargados, que incluye preguntas relacionadas con la seguridad para evaluar los riesgos potenciales asociados con cada relación con el proveedor. Los proveedores que se considera que presentan riesgos inaceptables están excluidos de ser miembros de nuestro ecosistema o están obligados contractualmente a implementar un plan de acción correctiva si es necesario. Por ejemplo, AWS, que figura como Sub-Encargado en el Schedule 1, mantiene las certificaciones de seguridad y privacidad ISO 27017:2015 e ISO 27018:2014, que son subconjuntos de ISO 27001:2013, el estándar de seguridad más estricto disponible.

16. Respuesta a incidentes de seguridad

VTEX cuenta con un protocolo formal de respuesta a incidentes de seguridad que cubre los pasos esenciales del proceso: preparación, identificación de incidentes, contención, erradicación, recuperación y post incidente. Este procedimiento también incluye un plan de comunicación integrado que se aplica en todas las fases de la respuesta.

***