Acuerdo de Encargado del tratamiento de datos (DPA) de LanSchool Air

Este Acuerdo de Encargado del tratamiento de datos (Data Processor Agreement, "**DPA**") de LanSchool Air, que aborda tanto los requisitos de privacidad como los de seguridad, y sus anexos, forma parte del Acuerdo de Compraventa de Stoneware u otro acuerdo escrito o electrónico celebrado entre Stoneware, Inc. y el Cliente (el "**Acuerdo**") para la adquisición de servicios de LanSchool Air de Stoneware, Inc. con el objeto de reflejar el acuerdo de las partes en relación con el tratamiento de Datos personales.

Este DPA complementa cualquier acuerdo entre las partes con respecto al objeto del presente; y entrará en vigor desde el momento en que el Cliente acepte los Términos de Servicio de LanSchool Air (**"Fecha de entrada en vigor").**

Una vez firmado el Acuerdo y aceptados los Términos de Servicio de LanSchool Air, este DPA será legalmente vinculante; y usted (Cliente) celebrará este DPA en nombre del Cliente, en la medida que lo requieran las leyes y regulaciones de protección de datos y de seguridad y privacidad aplicables, incluidas aquellas leyes y regulaciones de seguridad y privacidad aplicables en materia de educación y estudiantes, en nombre de sus Afiliados autorizados en la medida en que Stoneware procese Datos personales para los cuales dichos Afiliados autorizados califican como el Responsable. El Cliente comprende que este DPA es aplicable a todos los usuarios y garantiza que tiene las facultades necesarias para celebrar este DPA en nombre de dichos usuarios.

Es probable que actualicemos estos términos para cumplir con los nuevos requisitos legales o según sea necesario para reflejar las actualizaciones operativas. Si tiene una suscripción activa a LanSchool Air, se lo haremos saber por correo electrónico o mediante una notificación en el producto. Puede encontrar versiones archivadas del DPA aquí.

Celebración del DPA:

a) Este DPA consta de dos partes: el cuerpo principal del DPA, y los Anexos A, B, C, D y E
Este DPA, incluidas las Cláusulas Contractuales Estándar de la Unión Europea (UE) que se encuentran en el Anexo D, se firmó previamente en nombre de Stoneware, Inc. como importador de datos. (Nota: El Anexo D, por lo general, se aplica solo a las actividades de tratamiento que puedan implicar la transferencia de Datos personales desde la Unión Europea, el Espacio Económico Europeo, el Reino Unido u otros países con estándares similares de adecuación o equivalencia relacionados con las transferencias de datos transfronterizas). Además, representa disposiciones contractuales que actúan como salvaguardias para transferencias de datos de carácter personal que exigen las leyes de protección de datos vigentes.

Para evitar dudas, debe firmar este DPA en la página 5. Si corresponde, el Anexo D se aplicará como referencia.

Protección de datos

Definiciones: en la presente Cláusula, los siguientes términos tendrán los siguientes significados:

a) "**Responsable**", "**Encargado**", **"Subencargado",** "**Tratamiento de datos**" y "**Tratamiento**" (y "**Proceso**") tendrán los significados indicados en la Ley de Protección de Datos de la UE y términos equivalentes en la Ley de Protección de Datos Aplicable.

   a. "**Ley de Protección de Datos Aplicable**" significa todas las leyes, las normas, los reglamentos, las órdenes y todas sus modificaciones relacionadas, en cualquier jurisdicción en la que el Proveedor provea los Servicios de LanSchool, incluidas las leyes relativas a la privacidad, la seguridad de los datos, la protección de los datos, las violaciones de datos y la confidencialidad, como la Ley de Privacidad del Consumidor de California de 2018 (California Consumer Privacy Act, "CCPA") y la Ley de Derechos de Privacidad de California (California Privacy Rights Act, "CPRA"), el Reglamento General de Protección de Datos ("RGPD") 2016/279 de la Unión Europea, con sus modificaciones, reemplazos y sustituciones eventuales; la Ley de Protección de Datos del Reino Unido de 2018, con sus respectivas enmiendas; la Ley General de Protección de Datos Personales de Brasil n.º 13.709/18 con sus modificaciones ("LGPD") y las reglamentaciones implementadas (o que se deben implementar); y cualquiera de las leyes aplicables, incluidas las leyes de privacidad nacionales, estatales o locales en materia de educación y estudiantes.

b) Los **"Datos personales"** son información que se relaciona con una persona identificada o identificable, incluidos, entre otros, estudiantes, padres, madres y empleados escolares.

c) El **"Interesado"** es una persona individual que puede ser identificada directa o indirectamente, incluidos, entre otros, estudiantes, padres, madres y empleados escolares.

d) **"Cliente"** es el Responsable. A los efectos de este DPA exclusivamente, el término "Cliente" incluirá el Cliente y los Afiliados autorizados.

e) **"Proveedor"** significa Stoneware, Inc., que actúa como Encargado del tratamiento.

   a. "Exportador de datos" significa una parte que transfiere Datos personales a otra Parte de conformidad con el Acuerdo.

   b. "Importador de datos" significa una parte que recibe Datos personales del cliente de otra Parte de conformidad con este Acuerdo.

Relación de las partes: el Cliente reconoce al Proveedor como el Encargado del tratamiento de los Datos personales que son objeto del Contrato de Compraventa de Stoneware, los Términos de Servicios de LanSchool Air y el Acuerdo de licencia para el usuario final (End User License Agreement, EULA) con el Proveedor. Cada parte cumplirá con las obligaciones que le correspondan en virtud de la Ley de Protección de Datos Aplicable.

Limitación del propósito: el Proveedor tratará los Datos personales como Encargado y estrictamente de acuerdo con las instrucciones documentadas por el Responsable (el "Propósito permitido") tal

como se documenta en el Anexo A "Detalles del tratamiento", excepto cuando exija lo contrario cualquier Ley de Protección de Datos Aplicable. El Proveedor informará inmediatamente al Responsable si tiene conocimiento de que las instrucciones de Tratamiento del Responsable infringen la Ley de Protección de Datos Aplicable. En ningún caso el Proveedor tratará los Datos personales para sus propios fines o los de terceros, incluidos los propósitos de mercadotecnia. Para evitar dudas, el Proveedor no enviará comunicaciones de mercadotecnia o promocionales de otro tipo a usuarios de Lenovo LanSchool Air. Para hacerlo, hará uso de los Datos personales obtenidos del uso de Lenovo Lan School Air. Esto último no impedirá a una persona recibir comunicaciones de mercadotecnia o promocionales si se originan en el contexto de canales estándares como, por ejemplo, el sitio web de Stoneware o Lenovo y otros canales relacionados con ventas.

Transferencias internacionales: el Proveedor puede transferir los Datos personales a cualquier país fuera del país desde el cual se recopilaron Datos personales de conformidad con las Leyes de Protección de Datos y de localización de datos aplicables. Para evitar dudas, los datos deberán ser alojados según lo especificado más adelante en el presente Contrato (es decir, conforme a un enfoque o ubicación específica por región), y:

a) Las transferencias de Datos personales fuera del Espacio Económico Europeo ("**EEE**") y el Reino Unido se permiten: (i) si la transferencia de Datos personales se hace a un destinatario en un país que la Comisión Europea, el Secretario de Estado del Reino Unido o la Oficina del Comisionado de la Información del Reino Unido han decidido que proporciona protección adecuada a los Datos personales; y (ii) a un destinatario que haya celebrado cláusulas contractuales tipo adoptadas o aprobadas por la Comisión Europea, el Secretario de Estado del Reino Unido o la Oficina del Comisionado de la Información del Reino Unido.

   El Proveedor puede transferir los Datos personales fuera de Brasil si: (i) la transferencia de Datos es a un destinatario en un país que la Autoridad nacional ha decidido que proporciona una protección adecuada para los Datos personales; (ii) a un destinatario que haya celebrado cláusulas contractuales estándar adoptadas o aprobadas por la Autoridad nacional; o (iii) cuando el destinatario pueda proporcionar y demostrar que implementa otras salvaguardias de acuerdo con la Ley de Protección de Datos Brasileña y la transferencia internacional sea aprobada por el Responsable.

b) En general, la aceptación del presente DPA da lugar a la aprobación por parte del Cliente de que Stoneware, Inc. puede transferir Datos personales a través de las fronteras, en la medida en que Stoneware cumpla con las Leyes de Protección de Datos aplicables. A este respecto, el Anexo D "Transferencias Internacionales de Datos" se aplica entre el Responsable y el Proveedor cuando corresponda.

Los Subencargados podrán acceder a los Datos del Cliente conforme al Anexo B del presente Contrato en terceros países, por ejemplo, en los Estados Unidos, lo que se lleva a cabo con las garantías adecuadas exigidas para las transferencias a terceros países, como las Cláusulas Contractuales Tipo. Cada transferencia de datos intragrupo se realiza con base en el Acuerdo de Transferencia de Datos Intragrupo del Proveedor, que incorpora Cláusulas Contractuales Tipo para garantizar transferencias internacionales de datos seguras.

Confidencialidad del tratamiento: el Proveedor se asegurará de que cualquier persona a la que autorice a procesar los Datos personales (incluido el personal, los agentes y el Subencargado del Proveedor) (una "Persona autorizada") esté sujeta a un estricto deber de confidencialidad (ya sea un deber contractual o un deber legal), y no permitirá que ninguna persona que no esté bajo dicho deber de confidencialidad procese los Datos personales. El Proveedor se asegurará de que todas las Personas autorizadas procesen los Datos personales solo cuando sea necesario para el Propósito permitido. Además, el Proveedor no explotará comercialmente los Datos personales.

Uso de inteligencia artificial: el Proveedor utiliza tecnología de inteligencia artificial (la "IA") relacionada con alguna de sus ofertas (Por ejemplo, Monitoreo de tareas de LanSchool). La IA se emplea para interpretar el significado del objetivo de la clase y para analizar los datos de los alumnos. No se recopilará ninguna información adicional de los usuarios que no se relacione con los requerimientos habituales del producto. No se debe activar ninguna toma de decisiones automática que no se relacione con la simple identificación. **La IA no proporcionará ninguna salida que constituya un acto de discriminación penado por la ley, sesgos o infracción de los derechos de propiedad intelectual. El Proveedor cuenta con un proceso para abordar los inconvenientes relacionados con la calidad y seguridad de las salidas de los Sistemas de IA, lo que incluye cualquier acto de discriminación penado por la ley o sesgo contenido en dichas salidas**. El Proveedor cumple **con** la Legislación de Protección de Datos aplicable y demás normativa vigente **con respecto a la IA**.

Seguridad: el Encargado implementará las medidas técnicas y organizativas apropiadas para proteger los Datos personales (i) de la destrucción accidental o ilegal, y (ii) la pérdida, alteración, divulgación no autorizada o acceso a los Datos personales (un "Incidente de seguridad"). El Anexo C contiene Medidas Técnicas y Organizativas de LanSchool Air (Technical and Organizational Measures, TOM).

Subtratamiento: el Proveedor acepta que cualquier Subencargado externo que designe estará vinculado a estándares de protección de datos sustancialmente similares a los previstos en este Acuerdo y que el Proveedor celebrará acuerdos con los Subencargados correspondientes para cumplir con los requisitos incluidos en este DPA. El Responsable acepta que el Proveedor puede utilizar a cualquier Subencargado mencionado en el Anexo B. No obstante esto, el Responsable acepta que el Proveedor contrate a nuevos Subencargados (incluida la sustitución de los existentes) para procesar los Datos personales**,** siempre que: (i) el Proveedor dé aviso con al menos 30 días de anticipación del agregado o la sustitución de cualquier Subencargado (incluidos los detalles del tratamiento que realice o realizará), que podrán facilitarse mediante la provisión de detalles respecto a tal agregado o sustitución al Responsable; y (ii) el Proveedor imponga términos de protección de datos a cualquier Subencargado que designe que proteja los Datos personales con estándares sustancialmente similares a los previstos por el presente DPA. Si el Responsable se niega a dar su consentimiento al nombramiento de parte del Proveedor de un nuevo Subencargado externo, consentimiento que no debe ser retenido de manera irrazonable, entonces el Proveedor no nombrará al Subencargado o el Responsable podrá optar por rescindir el Acuerdo, siempre que el Responsable tenga razones importantes y documentadas para objetar el cambio.

Cooperación y derechos de los Interesados: el Proveedor proporcionará asistencia razonable y oportuna al Responsable para permitir al Responsable responder a: (i) cualquier solicitud de un

Interesado para ejercer cualquiera de sus derechos en virtud de la Ley de Protección de Datos Aplicable (incluidos sus derechos de acceso a Datos personales, corrección, objeción, supresión y portabilidad de estos, según corresponda); y (ii) cualquier otra correspondencia, consulta o denuncia recibida de un Interesado, regulador u otro tercero en relación con el Tratamiento de los Datos personales. Para evitar cualquier duda, las Solicitudes de Interesados (Data Subject Requests, DSR) serán presentadas por el Responsable mediante el envío de una solicitud formal en el Formulario web de privacidad DSR de Stoneware.

Incidentes de seguridad: al tener conocimiento de un Incidente de seguridad, el Proveedor informará al Responsable sin demora injustificada. Además, deberá proporcionar toda la información y cooperación oportunas que el Responsable pueda necesitar para cumplir con sus obligaciones de notificación de violación de los Datos personales en virtud de la Ley de Protección de Datos Aplicable (y de acuerdo con los plazos requeridos por ella). El Proveedor adoptará además las medidas y acciones necesarias para remediar o mitigar los efectos del Incidente de seguridad y mantendrá informado al Responsable de todos los acontecimientos en relación con el Incidente de seguridad.

Eliminación o devolución de Datos: tras la rescisión o el vencimiento del Contrato de Venta de Stoneware, el Proveedor, a solicitud de los Responsables, destruirá o devolverá al Responsable todos los Datos personales (incluidas todas las copias de los Datos personales) en su posesión o control (incluidos los Datos personales subcontratados a un tercero para su Tratamiento). Si el Responsable no brinda más instrucciones al Proveedor, se aplicará el calendario de retención de datos del Proveedor, tal como se establece en el Anexo A. Este requisito no se aplicará en la medida en que el Proveedor esté obligado por cualquier Ley de Protección de Datos aplicable a conservar algunos de los Datos personales o todos ellos, en cuyo caso el Proveedor aislará y protegerá los Datos personales de cualquier otro Tratamiento, excepto en la medida requerida por dicha ley.

Auditorías: durante la vigencia del presente Acuerdo y durante tres años después de la rescisión o el vencimiento, el Proveedor deberá proporcionar al Responsable, previa solicitud razonable y con un preaviso razonable: (i) acceso a resúmenes de: (1) las prácticas del Proveedor (incluidos sus protocolos y procedimientos de seguridad); (2) políticas internas; y (3) registros relacionados con la privacidad y seguridad de la Información Personal y el Tratamiento de la Información Personal disponibles para su revisión, excluyendo aquellos registros protegidos por el privilegio abogado-cliente o que constituyan producto del trabajo legal; (ii) la asistencia y cooperación del personal relevante del Proveedor; y (iii) respuestas a cuestionarios con el fin de determinar el cumplimiento por parte del Proveedor de sus obligaciones en virtud del presente Acuerdo ("Auditoría"). Dichas Auditorías estarán limitadas a una vez por año, salvo en los siguientes casos: (i) cuando la Auditoría sea requerida por las Leyes Aplicables de Protección de Datos o para satisfacer solicitudes o requerimientos de cualquier autoridad reguladora o proceso legal o administrativo; (ii) cuando la Auditoría sea solicitada debido a que el Responsable tenga preocupaciones legítimas sobre la privacidad y seguridad de los Datos Personales tratados por el Proveedor; o (iii) cuando haya ocurrido un Incidente de Seguridad confirmado. No obstante lo anterior, si los resúmenes de prácticas, políticas y registros, o las respuestas al cuestionario proporcionadas por el Proveedor se consideran insuficientes para satisfacer los requisitos o solicitudes de una autoridad reguladora o de un proceso legal o administrativo, las partes acuerdan negociar de buena fe los términos y el alcance de una Auditoría adicional que permita satisfacer dicha solicitud o

requerimiento. El Proveedor deberá proporcionar al Responsable la información razonablemente necesaria para que este pueda llevar a cabo y documentar evaluaciones de protección de datos.

EN TESTIMONIO DE LO CUAL, Stoneware y el Cliente firmaron este Acuerdo en la fecha indicada anteriormente.

Stoneware, Inc.

Firma: _____

Nombre en letra de imprenta: Kimberly Page

Cargo: gerenta de operaciones estratégicas

Cliente

Firma: _____

Nombre en letra de imprenta:
_____

Cargo: _____

ANEXO A – DETALLES DE TRATAMIENTO

Tipo de datos e Interesados	Período de retención	Naturaleza, propósito y objeto
Datos relacionados con la interfaz de estudiante: • El identificador único global (Globally Unique Identifier, GUID) único generado automáticamente del estudiante. • La identificación (ID) del estudiante según fuera proporcionada. • El primer nombre del estudiante. • El apellido del estudiante. • La dirección de correo electrónico del estudiante. • El nombre de inicio de sesión del estudiante. • La fecha en que se creó este objeto de estudiante. • La fecha en que se actualizó este objeto de estudiante.	Tras la petición del usuario de su eliminación o después de 1 año de no tener una licencia o prueba activa, los datos se archivarán. Los datos archivados se purgan después de 90 días.	*Almacenamiento de datos* (grabar, alojar, registrar, archivar o almacenar de otro modo los Datos del cliente). *Acceso a datos* (recuperar, copiar, examinar, modificar, transportar, escanear los Datos del cliente o acceder de otro modo a estos).
Datos relacionados con la Interfaz de empleado escolar: • El GUID único generado automáticamente del profesor. • La identificación del empleado escolar. • El nombre del empleado escolar. • El apellido el empleado escolar. • La dirección de correo electrónico del empleado escolar. • La ID de MongoDB del usuario en la nube que corresponde a este objeto de profesor. • Acceso a tokens. • La fecha en que se creó este objeto de empleado escolar. • La fecha en que se actualizo este objeto de empleado escolar.	Tras la petición del usuario de su eliminación o después de 1 año de no tener una licencia o prueba activa, los datos se archivarán. Los datos archivados se purgan después de 90 días.	*Almacenamiento de datos* (grabar, alojar, registrar, archivar o almacenar de otro modo los Datos del cliente). *Acceso a datos* (recuperar, copiar, examinar, modificar, transportar, escanear los Datos del cliente o acceder de otro modo a estos). *Análisis de datos* (encuestar, probar, estudiar, interpretar, organizar, informar o de otra forma analizar los Datos del cliente).
Datos relacionados con la interfaz de cliente: • El GUID único generado automáticamente del cliente. • El nombre de inicio de sesión del estudiante actual. Podría ser una dirección de correo electrónico o un nombre de usuario.	Tras la petición del usuario de su eliminación o después de 1 año de no tener una licencia o prueba activa, los datos se archivarán. Los datos archivados se purgan después de 90 días.	*Almacenamiento de datos* (grabar, alojar, registrar, archivar o almacenar de otro modo los Datos del cliente). *Acceso a datos* (recuperar, copiar, examinar, modificar, transportar, escanear los Datos del

• La ID de MongoDB del dispositivo correspondiente de la base de datos principal. • La fecha en que se creó este objeto de cliente. • La fecha en que se actualizó este objeto de cliente.		cliente o acceder de otro modo a estos). *Análisis de datos* (encuestar, probar, estudiar, interpretar, organizar, informar o de otra forma analizar los Datos del cliente).
Datos relacionados con la lista de clases • El GUID único generado automáticamente de la clase. • El nombre de esta clase. Esto es obligatorio. • La ID de la clase proporcionada por el Sistema de Información Estudiantil. • La ID de la escuela proporcionada por el Sistema de Información Estudiantil. • El período de clase u otra designación que distingue a esta clase de otras clases del mismo tipo. • El propietario de esta lista de clases. • El profesor se opone a que los profesores tengan acceso a esta lista de clases. La Interfaz del profesor se define a continuación. • Los objetos de estudiante para los estudiantes que pertenezcan a esta lista de clases. • Los objetos de cliente para los dispositivos que pertenezcan a esta lista de clases. • La ID del usuario que cambió por última vez esta lista de clases. • La fecha en que se creó esta lista de clases. • La fecha en que se actualizó esta lista de clases. •	Tras la petición del usuario de su eliminación o después de 1 año de no tener una licencia o prueba activa, los datos se archivarán. Los datos archivados se purgan después de 90 días.	*Almacenamiento de datos* (grabar, alojar, registrar, archivar o almacenar de otro modo los Datos del cliente). *Acceso a datos* (recuperar, copiar, examinar, modificar, transportar, escanear los Datos del cliente o acceder de otro modo a estos). *Análisis de datos* (encuestar, probar, estudiar, interpretar, organizar, informar o de otra forma analizar los Datos del cliente).
Datos relacionados con la organización • El GUID único generado automáticamente de la organización. • El nombre de la organización. • La ID asignada a esta organización. • La dirección principal. • Información sobre la dirección secundaria.	Tras la petición del usuario de su eliminación o después de 1 año de no tener una licencia o prueba activa, los datos se archivarán. Los datos archivados se purgan después de 90 días.	*Almacenamiento de datos* (grabar, alojar, registrar, archivar o almacenar de otro modo los Datos del cliente). *Acceso a datos* (recuperar, copiar, examinar, modificar, transportar, escanear los Datos del

• La ciudad de la organización. • El estado o la provincia de la organización. • El código postal de la organización. • El país de la organización. • La información administrativa de contacto. • La información técnica de contacto. • La información de contacto de facturación. • Una marca que indica si esta organización tiene un agente del sitio. • La fecha en que se creó esta organización. • La directiva de seguridad predeterminada para la organización. • Datos de contacto de la organización: primer nombre, apellido, número de teléfono, dirección de correo electrónico.		cliente o acceder de otro modo a estos). *Análisis de datos* (encuestar, probar, estudiar, interpretar, organizar, informar o de otra forma analizar los Datos del cliente).
Datos del usuario • El GUID único generado automáticamente del usuario. • Un conjunto de pares clave-valor de todas las ID actuales de usuario. • El primer nombre del usuario. • El apellido del usuario. • La dirección de correo electrónico del usuario. • Permisos asignados directamente a este usuario. • Una referencia a la organización a la que pertenece este usuario. • Un subconjunto de ID de usuario que un usuario puede usar para un inicio de sesión. • Un registro de tiempo de la última vez que el usuario inició sesión correctamente en el sistema. • Un registro de tiempo de la primera vez en que el usuario falló la autenticación en la última hora. • La dirección IP de donde tuvo lugar el último inicio de sesión exitoso. • La dirección IP de donde tuvo lugar el último inicio de sesión fallido.	Tras la petición del usuario de su eliminación o después de 1 año de no tener una licencia o prueba activa, los datos se archivarán. Los datos archivados se purgan después de 90 días.	*Almacenamiento de datos* (grabar, alojar, registrar, archivar o almacenar de otro modo los Datos del cliente). *Acceso a datos* (recuperar, copiar, examinar, modificar, transportar, escanear los Datos del cliente o acceder de otro modo a estos). *Análisis de datos* (encuestar, probar, estudiar, interpretar, organizar, informar o de otra forma analizar los Datos del cliente).

• Un registro de tiempo del último intento de inicio de sesión fallido. • Un contador para el número de intentos de inicio de sesión fallidos consecutivos. • Los permisos concedidos al usuario. Se genera mediante la combinación de todos los permisos de los grupos del usuario. • La fecha en que se creó este usuario. • La fecha en que se actualizó este usuario.		
Datos relacionados con el registro de actividades • Historial de navegación web del estudiante (URL, registro de tiempo). • Historial de aplicaciones del estudiante (nombre de la aplicación, registro de tiempo). • Historial de mensajes de chat de la clase (remitente, destinatario, contenido del mensaje, registro de tiempo). • Registro de actividades administrativas (ID de usuario, tipo de actividad, registro de tiempo).	A pedido del usuario, para su eliminación o luego del transcurso de 45 días.	*Almacenamiento de datos* (grabación, registro, almacenamiento, archivo o cualquier otra manera de conservar los Datos del cliente); *Acceso a los datos* (obtención, copia, examen, modificación, transferencia, escaneo o cualquier otra manera de acceder a los Datos del cliente); *Análisis de datos* (encuesta, prueba, estudio, interpretación, organización, registro o cualquier otro análisis de los Datos del cliente).
Datos de la licencia (excluye los Datos personales)	Estos datos se conservan el tiempo que sea necesario para cumplir con las obligaciones legales, con el objeto de hacer cumplir nuestros acuerdos, etc. Esto no incluye los Datos personales.	*Almacenamiento de datos* (grabar, alojar, registrar, archivar o almacenar de otro modo los Datos del cliente). *Acceso a datos* (recuperar, copiar, examinar, modificar, transportar, escanear los Datos del cliente o acceder de otro modo a estos). *Análisis de datos* (encuestar, probar, estudiar, interpretar, organizar, informar o de otra forma analizar los Datos del cliente).

Duración del tratamiento
La duración del tratamiento corresponde a la duración del Acuerdo. Se aplicarán las políticas de retención de datos que se han descrito anteriormente.
Categorías de Interesados
Estudiantes, Profesores, contactos de la Organización y Usuarios en general

ANEXO B – SUBENCARGADOS

Nombre	Datos	Ubicación de almacenamiento	Propósito
Amazon Web Services	Todos los datos de usuario descritos en el Anexo A	AU, EE. UU., Reino Unido *(se aplican restricciones a las transferencias regionales, lo que significa, por ejemplo, que los datos de Europa se almacenan de manera exclusiva en el Reino Unido):*	Proveedor de servicios en la nube para la infraestructura de la aplicación. Todos los datos son procesados por la aplicación.
Datadog	Datos de la aplicación, dirección IP y nombre de usuario.	EE. UU.	Herramienta de recopilación de registros.
Hubspot	Primer nombre, Apellido, Correo electrónico, Teléfono, Nombre de la empresa, Título, Etiqueta geográfica (por ejemplo, estado), Industria.	EE. UU, UE	Incorporación.
MongoDB Atlas	Todos los datos de usuario descritos en el Anexo A	AU, EE. UU., Reino Unido *(se aplican restricciones a las transferencias regionales, lo que significa, por ejemplo, que los datos de Europa se almacenan de manera exclusiva en el Reino Unido):*	Para que la aplicación funcione correctamente.
Pendo	Estadísticas de uso de la aplicación; comentarios proporcionados por los usuarios; nombre, apellido, correo electrónico y nombre de la organización del usuario final.	EE. UU.	Mejorar la funcionalidad y usabilidad del producto.

ANEXO C – MEDIDAS TÉCNICAS Y ORGANIZATIVAS (TOM)

El Proveedor ha implementado un programa de seguridad integral escrito con controles físicos, técnicos, procedimentales y administrativos que reflejan los estándares prevalecientes de la industria para la protección y el uso responsable de Datos personales, incluidos, entre otros, los siguientes controles:

Técnicas	Alcance	Controles
Acceso	Inicio de sesión (sistema y aplicación).	Políticas de contraseñas basadas en NIST (autenticación de varios factores para acceso e interfaces a nivel de administrador).
Cifrado	Almacenamiento de datos en archivo y en tránsito.	AES 256-GCM (en reposo), TLS 1.2, 1.3 (en tránsito)
Pruebas de seguridad de aplicaciones estáticas	Todas las imágenes de servidor y microservicio. Todos los clientes binarios y extensiones/plugins.	Análisis y monitoreo habituales de vulnerabilidades.
Pruebas dinámicas de seguridad de aplicaciones	API de aplicaciones externas.	Escaneos de aplicaciones en la web. Pruebas de penetración (pruebas internas periódicas).
CIS benchmark hardening	Proveedor de plataforma en la nube. Instancias de servidor.	Comprobaciones de cumplimiento de CIS en la nube, monitoreo de seguridad en la nube. Evaluaciones periódicas de referencia de servidores CIS L2.
Análisis de composición del software	Dependencias de código abierto de terceros.	Llevar a cabo auditorías periódicas de vulnerabilidades, monitoreo de repositorios.
Evaluación de la infraestructura	Proveedor de plataforma en la nube.	Revisiones periódicas de todas las redes definidas por software (software-defined networks, SDN) (identificar la segmentación de la red, la configuración del firewall y las configuraciones erróneas de acceso a los recursos).
Firewall de aplicaciones en la web (Web application firewall, WAF)	Aplicaciones web de producción.	Protección WAF (reglas básicas para ataques comunes).
Análisis de código estático	Código propio.	Se lleva a cabo el análisis de código periódico mediante la utilización de una herramienta comercial, las revisiones seguras del código se llevan a

		cabo durante las fusiones de código.
Recopilación de registros	Proveedor de plataforma en la nube. Aplicación.	Transacciones de API de plataforma en la nube (los registros de más de 360 días son purgados, se puede acceder a ellos mediante ingeniería). Registro WAF para la detección de bordes (los registros de más de 90 días son purgados, se puede acceder a ellos mediante ingeniería). Subencargados, ver el Anexo B, a efectos de la aplicación.
Infraestructura como código	Proveedor de plataforma en la nube.	La infraestructura como código se utiliza para automatizar las implementaciones de infraestructura y mejorar la inmutabilidad, la configuración incorrecta de la infraestructura.

Organizativas	Alcance	Controles
Respuesta a incidentes (incluida la violación de datos)	Eventos de seguridad relacionados con productos en producción.	Plan de respuesta a incidentes del producto de acuerdo con los procesos NIST 800-61 y el equipo interno de respuesta a incidentes de seguridad de productos (Product Security Incident Response Team, PSIRT) de Lenovo.
Lista de proveedores de confianza	Todos los Subencargados que se integran directamente con los productos en producción.	Evaluaciones de seguridad estándar de los proveedores integrados, los DPA para proveedores de tratamiento de Datos personales.
Gestión de vulnerabilidades	Sistemas operativos (OSes) de servidor. Contenedores Docker. Clientes. Productos en producción.	Un programa que emplea diversas herramientas para ayudar a identificar vulnerabilidades en todos los sistemas informáticos.
Junta de revisión de seguridad de software (Software Security Review Board, SSRB)	Productos en producción.	Las revisiones de la SSRB se llevan a cabo regularmente. Durante las revisiones, se evalúan todas las medidas técnicas y organizativas para el producto en cuestión.
Política de retención de datos	Información de identificación personal,	Tras la petición del usuario de su eliminación o después de un

	datos de la aplicación, productos en producción.	año de no tener una licencia o prueba activa, los datos se archivarán. Los datos archivados se purgan después de 90 días.
Conciencia sobre la seguridad y privacidad	Todos los empleados (cursos Fundamentos básicos de privacidad y Fundamentos esenciales de seguridad).	Capacitación semestral para equipos especializados de TI y productos sobre temas de seguridad avanzados, como OWASP Top 10.
Seguridad continua	Productos en producción.	Aplicación habitual de Medidas Técnicas.
Revisiones de cumplimiento de código abierto	Productos en producción.	Las evaluaciones realizadas para garantizar que se provean las licencias y atribuciones adecuadas en el software distribuido.
Recuperación ante desastres	Productos en producción.	Siguiendo el NIST-800-34 como guía para maximizar el objetivo de tiempo de recuperación (Recovery Time Objective, RTO) y el objetivo de punto de recuperación (Recovery Point Objective, RPO).
Política de copia de seguridad	Bases de datos, código, registros.	La política general requiere varias copias de seguridad, una de las cuales debe estar fuera del sitio de la ubicación de almacenamiento principal. Se producen copias de seguridad regulares de la base de datos diariamente (2 veces por día), semanal y mensualmente. Las copias de seguridad diarias se conservan durante 7 días. Las copias de seguridad semanales se conservan durante 4 semanas. Las copias de seguridad mensuales se conservan durante 13 meses. La ventana de restauración es de 12 horas. Las copias de seguridad del código fuente de la aplicación

		se realizan diariamente y se conservan durante 360 días. Registros de producción: Datadog: los registros están activos durante 7 días. Luego, los registros pasan a almacenamiento a largo plazo por 180 días y posteriormente se purgan. Load Balancer: los registros se conservan durante 360 días y luego se purgan. Firewall de aplicaciones en la web: los registros se conservan durante 90 días y luego se purgan. Cloud Trail: los registros se conservan durante 90 días y luego se purgan. Cloud Watch: los registros se conservan durante 360 días y luego se purgan. MongoDB: los registros se conservan mientras dure el proyecto.

ANEXO D – ACUERDO DE TRANSFERENCIAS INTERNACIONALES DE DATOS

Este anexo establece los requisitos de protección de datos (incluidos los requisitos de las Leyes de Privacidad Aplicables) que se aplican: (i) al Exportador de datos (Responsable) cuando transfiere Datos personales al Importador de datos (Stoneware, Inc.), sus afiliadas o los Subencargados del Tratamiento de datos; y (ii) al Importador de datos cuando recibe Datos personales de un Exportador de datos para el Tratamiento de datos.

El Importador de datos garantiza y se compromete a que en todo momento:

a) tratará los Datos transferidos de acuerdo con las Leyes de Privacidad Aplicables y proporcionará asistencia razonable y oportuna al Exportador de datos según sea necesario para ayudar al Exportador de datos a cumplir con sus obligaciones en virtud de las Leyes de Privacidad Aplicables;

b) no cumplirá intencionadamente con sus obligaciones en virtud de este Acuerdo de tal forma que cause que el Exportador de datos incumpla cualquiera de sus obligaciones de conformidad con las Leyes de Privacidad Aplicables.

El Exportador de datos confirma que ha tomado las medidas necesarias para garantizar el cumplimiento de la legislación aplicable en materia de Protección de datos, incluidos los requisitos de transferencia transfronteriza de Datos personales, como haber obtenido el consentimiento explícito de los Interesados para que sus Datos personales se transfieran al extranjero, haber notificado a las autoridades pertinentes o haber solicitado su aprobación para la transferencia u otras obligaciones subyacentes, según corresponda.

1. Espacio Económico Europeo (EEE)

Si los servicios del Proveedor se suministran al Responsable dentro del Espacio Económico Europeo ("EEE") o la otra jurisdicción sujeta a la Ley de Protección de Datos de la UE, se aplicarán las siguientes disposiciones:

(A) "Ley de Protección de Datos de la UE" hace referencia (a) al Reglamento 2016/679 del Parlamento Europeo y del Consejo sobre la protección de personas naturales respecto al Tratamiento de Datos personales y sobre el libre movimiento de dichos datos (Reglamento General de Protección de Datos) (el "RGPD"); (b) la Directiva sobre la privacidad electrónica de la UE (Directiva 2002/58/EC; y (c) todas y cada una de las leyes nacionales correspondientes sobre protección de datos.

(B) El proveedor deberá informar de inmediato al Responsable (a) sobre cualquier requisito en virtud de la Ley de Protección de Datos de la UE que exigiría el Tratamiento de Datos personales de una forma diferente a las instrucciones emitidas por el Responsable, o (b) si, a consideración del Proveedor, las instrucciones del Responsable podrían infringir o violar la Ley de Protección de Datos de la UE.

(C) ***Transferencias de datos:*** si el Proveedor o sus Subcontratistas se encuentran fuera del EEE, el Proveedor y el Responsable, por medio del presente, formalizan las cláusulas contractuales tipo del

responsable al Encargado del tratamiento según se establece en el MÓDULO DOS en la Decisión de Implementación de la Comisión (UE) 2021/914 del 4 de junio de 2021 sobre cláusulas contractuales tipo para la transferencia de Datos personales a países terceros de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la UE conforme sea remplazado o enmendado al momento correspondiente (las "Cláusulas Contractuales Tipo de Responsable a Encargado") y, por medio del presente, las incorpora a este Anexo mediante esta referencia. Las partes reconocen y acuerdan que:

a. el Proveedor y el Responsable cumplirán con sus respectivas obligaciones en virtud de las Cláusulas Contractuales Tipo de Responsable a Encargado;

b. si hubiese algún conflicto o incoherencia entre las Cláusulas Contractuales Tipo de Responsable a Encargado y este Anexo o el contrato base, prevalecerán las Cláusulas Contractuales Tipo de Responsable a Encargado en la medida del conflicto;

c. la información en las siguientes tablas se incorpora en las Cláusulas Contractuales Tipo de Responsable a Encargado entre las partes:

Información que se incorporará en las Cláusulas Contractuales Tipo de Responsable a Encargado entre el Responsable y el Proveedor:

Cláusula 9. Uso de Subencargados	Se selecciona la Opción 2: AUTORIZACIÓN ESCRITA GENERAL. El importador de datos suministrará información con mínimo 30 días de antelación conforme a la cláusula de "Subtratamiento".
Cláusula 17. Derecho aplicable	Estas cláusulas se interpretarán de conformidad con el derecho aplicable establecido en el contrato base de las Partes, a menos que el derecho aplicable no sea el de un Estado Miembro de la UE que permita derechos de terceros beneficiarios. En tal caso, las Partes aceptan que estas Cláusula se regirán por el derecho de IRLANDA.
Cláusula 18 (b). Elección de fuero y jurisdicción	Las Partes aceptan que toda controversia que surja a partir de estas Cláusula se resolverá ante los tribunales de IRLANDA.

Información que se incorporará al Anexo 1, Parte A de las Cláusulas Contractuales Tipo de Responsable a Encargado:

Nombre del exportador de datos	El Responsable, y cualquiera de las filiales de las que sea propietario mayoritario o que controle.
Dirección del exportador de datos	Esta información debe ser completada por el exportador de datos.

Nombre, cargo e información de contacto de la persona de contacto del exportador de datos	Esta información debe ser completada por el exportador de datos.
Actividades del exportador de datos pertinentes para los datos transferidos en virtud de estas Cláusulas	Esta información debe ser completada por el exportador de datos.
Firma y fecha del exportador de datos	Esta información debe ser completada por el exportador de datos.
Función del exportador de datos	Responsable.
Nombre del Importador de datos	El proveedor (Stoneware, Inc.) y sus subcontratistas.
Dirección del Importador de datos	Stoneware, Inc. 8001 Development Drive, Morrisville, NC 27560 Estados Unidos de América
Nombre, cargo e información de contacto de la persona de contacto del importador de datos	Dan Verwolf, Director privacy@lanschool.com
Actividades del importador de datos pertinentes para los datos transferidos en virtud de estas Cláusulas	Según la información establecida en la Parte B del Anexo 1.
Firma y fecha del Importador de datos	Esta información debe ser completada por el importador de datos.
Función del importador de datos	Encargado.

Información que se incorporará al Anexo 1, Partes B y C de las Cláusulas Contractuales Tipo de Responsable a Encargado:

Categorías de Interesados	Según se establece en el Anexo A anterior.
Categorías de Datos personales	Según se establece en el Anexo A anterior.
Datos sensibles	Según se establece en el Anexo A anterior.
Frecuencia de la transferencia	Frecuencia continua, siempre y cuando la licencia LSA esté activa.
Naturaleza del tratamiento	Según se establece en el Anexo A anterior.
Propósito del tratamiento	Según se establece en el Anexo A anterior.
Período durante el cual se retendrán los Datos personales	Según se establece en el Anexo A anterior.
Asunto, naturaleza y duración del tratamiento llevado a cabo por los Subencargados	Según se establece en el Anexo B anterior.
Autoridad supervisora competente con responsabilidad de verificar que el exportador de datos cumpla con el Reglamento (UE) 2016/679 ty	La autoridad supervisora que actuará como autoridad supervisora competente será la del Estado miembro de la UE donde está ubicado el Exportador de datos en la UE. Si el Exportador de datos (es decir, la entidad legal contratante)

	no está ubicado en la UE, entonces la autoridad supervisora competente será la del Estado Miembro de la UE en la que esté ubicado el representante para la UE del Exportador de Datos dentro del significado del artículo 27(1) del Reglamento (UE) 2016/679. Si el Exportador de datos no está ubicado en la UE pero no necesita nombrar a un representante para la UE, entonces la autoridad supervisora competente será la del Estado Miembro de la UE en el que están ubicados los Interesados cuyos Datos personales se transfieren en virtud de estas Cláusulas en relación con la oferta de bienes o servicios extendida a ellos, o cuyo comportamiento es supervisado.

Información que se incorporará al Anexo 2 de las Cláusulas Contractuales Tipo de Responsable a Encargado:

Descripción de las medidas técnicas y organizativas implementadas por el importador de datos (incluida cualquier certificación pertinente) para garantizar un nivel de seguridad adecuado, teniendo en cuenta la naturaleza, el alcance, el contexto y el propósito del tratamiento, y los riesgos para los derechos y las libertades de personas naturales.	Según se establece en el Anexo C anterior.

Información que se incorporará al Anexo 3 de las Cláusulas Contractuales Tipo de Responsable a Encargado:

Lista de Subencargados del tratamiento de datos autorizados	Según se establece en el Anexo B anterior.

2. Reino Unido (R. U.)

Si los servicios del Proveedor se proporcionan al Responsable dentro del Reino Unido, o la naturaleza de los Datos personales activa la aplicación de la Ley 2018 (Ley del Retiro) de la Unión Europea (el "RGPD del R. U.") y la Ley de Protección de Datos de 2018 (la "DPA 2018"), se aplicarán las siguientes disposiciones adicionales:

(A) Las transferencias de Datos personales a un destinatario en un país considerado por el secretario de Estado del R. U. como un país que brinda protección adecuada a los

Datos personales (una “Decisión de adecuación”) estarán permitidas en virtud del (de los) Acuerdo(s) sin la necesidad de Cláusulas Contractuales Tipo del R. U.

(B) Se considerará que los países del EEE están sujetos a una Decisión de adecuación para fines de transferencias de Datos personales desde el R. U. al EEE.

(C) En caso de que no haya una Decisión de adecuación, el Responsable y el Proveedor aceptan formalizar una adenda aprobada de transferencia de datos Reino Unido Internacional a las cláusulas contractuales tipo de la Comisión Europea para transferencias de datos internacionales (https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf).

Parte 1: Tablas/Tabla 1: Partes

Información que se incorporará en la “Parte 1: Tablas” de la Adenda a transferencia de datos internacionales a las Cláusulas contractuales tipo de la Comisión de la UE:		
Fecha de inicio	Conforme a lo anterior	
Las Partes	**Exportador (que envía la Transferencia restringida)**	**Importador (que recibe la Transferencia restringida)**
Datos de las Partes	Nombre legal completo, dirección principal (si es el domicilio oficial de una compañía): conforme a la información en la 2.ª tabla en el art. 1. Espacio Económico Europeo (EEE) en el Anexo D Número de registro oficial (si lo hubiera) (número de compañía o identificador similar): Conforme al cliente identificado en virtud del Contrato de compraventa	Nombre legal completo, dirección principal (si es el domicilio oficial de una compañía): conforme a la información en la 2.ª tabla en el art. 1. Espacio Económico Europeo (EEE) en el Anexo D Número de registro oficial (si lo tuviera) (número de compañía o identificador similar): 35-2097171 registrada en el estado de Indiana
Contacto clave	Nombre completo (opcional), cargo, información de contacto, incluido el correo electrónico: conforme a la información en la 2.ª tabla en el art. 1. Espacio Económico Europeo (EEE) en el Anexo D	Nombre completo (opcional), cargo, información de contacto, incluido el correo electrónico: conforme a la información en la 2.ª tabla en el art. 1. Espacio Económico Europeo (EEE) en el Anexo D

Tabla 2: Cláusulas Contractuales Tipo (Standard Contractual Clauses, SCC) seleccionadas, módulos y cláusulas seleccionadas

Adenda a las SCC de la UE	Véase el Anexo D, art. 1 anterior

Tabla 3: Información del apéndice

Anexo 1A: Lista de Partes conforme se indica en el art. 1. Espacio Económico Europeo (EEE) en el Anexo D
Anexo 1B: Descripción de la transferencia: según se establece en el Anexo A anterior
Anexo II: medidas técnicas y organizativas incluidas las medidas técnicas y organizativas para asegurar la seguridad de los datos: Descripción de la transferencia: según se establece en el Anexo C anterior
Anexo III: Lista de Subencargados (solo módulos 2 y 3): Descripción de la transferencia: según se establece en el Anexo B anterior

Tabla 4: Finalización de esta Adenda cuando cambia la adenda aprobada

Finalización de esta Adenda cuando cambia la adenda aprobada	Qué partes pueden finalizar esta adenda conforme se establece en la sección **Error! Reference source not found.**: ☒ Importador ☐ Exportador ☐ ninguna parte

Información que se incorporará en la "Parte 2: Cláusulas obligatorias" de la Adenda de transferencia internacional de datos a las Cláusulas contractuales tipo de la Comisión de la UE:
Parte 2: Cláusulas obligatorias de la Adenda aprobada; que es la plantilla de Adenda B.1.0 emitida por la Oficina el Comisionado de Información (Information Commissioner's Office, ICO) y presentada ante el Parlamento de conformidad con s119A de la Ley de Protección de Datos de 2018, el 2 de febrero de 2022, conforme sea revisada en virtud de la sección **Error! Reference source not found.** de dichas cláusulas obligatorias.

3. Suiza

En la medida en que la transferencia de Datos personales esté sujeta a la Ley Federal Suiza de Protección de Datos, las partes acuerdan cumplir las Cláusulas del Estándar Contractual de la UE y se aplicarán las siguientes disposiciones: (i) el Comisionado Federal de Protección de Datos e Información (Federal Data Protection and Information Commissioner, FDPIC) será la autoridad de supervisión competente en virtud de la Cláusula 13 de las Cláusulas Contractuales Estándares de la UE; (ii) las Partes acuerdan cumplir el RGPD en relación con todo el Tratamiento de los Datos Personales que se rija por la Ley Federal Suiza de Protección de Datos; (iii) las Cláusulas Contractuales Estándares de la UE se regirán por las leyes de Suiza, de conformidad con la Cláusula 17 (Opción 1), en la medida en que las transferencias de datos se rijan por la Ley Federal Suiza de Protección de Datos; (iv) el término "Estado miembro" utilizado en las Cláusulas Contractuales Estándares de la UE no se interpretará de manera que excluya a los Interesados en Suiza de la posibilidad de iniciar acciones legales por sus derechos en su lugar de residencia habitual (Suiza), de conformidad con la Cláusula 18(c) de las Cláusulas Contractuales Estándares de la UE; (v) las referencias al "RGPD" en las Cláusulas Contractuales Estándares de la UE se entenderán como referencias a la Ley Federal Suiza sobre Protección de Datos en la medida en que la transferencia de datos del Responsable se encuentre sujeta a la Ley Federal Suiza sobre Protección de Datos.

4. Brasil

En caso de una transferencia de Datos personales sujeta a la Ley General de Protección de Datos Personales de Brasil (modificada por la Ley n.º 13.853 de 8 de julio de 2019) ("LGPD"), y Lenovo, el Proveedor, o ambos, estén ubicados en Países No Adecuados, se aplicarán las Cláusulas Contractuales Estándares de C2P a las que se hace referencia en el presente documento con las siguientes modificaciones:

(i) la autoridad de control de las Cláusulas Contractuales Estándares de C2P será la Autoridad Nacional de Protección de Datos (ANPD) de Brasil;

(ii) la ley aplicable de conformidad con la Cláusula 17 de las Cláusulas Contractuales Estándares de C2P será la LGPD;

(iii) la elección del foro y jurisdicción de conformidad con la Cláusula 18 de las Cláusulas Contractuales Estándares de C2P será la legislación brasileña en caso de que la transferencia de datos esté sujeta exclusivamente a la LGPD; y

(iv) cualquier referencia al RGPD en las Cláusulas Contractuales Estándares de C2P incluirá también la referencia a las disposiciones equivalentes de la LGPD (en su versión modificada o sustituida).

5. Sudáfrica

Si los servicios del Proveedor se suministran al Responsable dentro de Sudáfrica u otra jurisdicción sujeta a la Ley de Protección de la Información Personal (Protection of Personal Information Act, POPIA), se aplicarán las siguientes disposiciones adicionales:

(A) El término "Interesado" hace referencia a una persona natural que pueda ser identificada por referencia a un nombre, número único, datos de ubicación, identificador en línea o a uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de esa persona natural, así como de una persona jurídica o entidad legal identificable.

6. Australia

Las partes acuerdan usar y proteger los Datos personales aplicables de conformidad con la Ley de Privacidad de Datos de Australia y sus enmiendas.

ANEXO E – DISPOSICIONES ADICIONALES

1. Ley de Privacidad del Consumidor de California (California Consumer Privacy Act, "CCPA").

Stoneware, Inc. es una empresa. Además, el Proveedor es el Proveedor de Servicios del Cliente y procesará Datos Personales en nombre del Cliente.

a. El Proveedor no venderá los Datos Personales ni la Información de Propiedad. "Vender" significa vender, alquilar, facilitar, divulgar, difundir, poner a disposición, transferir o de otra forma comunicar la información para una contraprestación en dinero u otra cosa de valor.

b. El Proveedor no conservará, utilizará ni divulgará los Datos personales: (a) para ningún propósito que no sea el propósito específico de realizar los servicios establecidos en el Acuerdo para Stoneware, Inc. o según lo permita la CCPA y sus reglamentos de implementación, (b) para un propósito comercial que no sea proveer los servicios especificados en el contrato con la empresa, o (c) fuera de la relación comercial directa entre la persona y Stoneware Inc.

c. Este DPA servirá como la certificación del Proveedor de que el Proveedor comprende los requisitos de la CCPA aplicables a las empresas y a los proveedores de servicios, incluidas las restricciones en California en virtud de su Código Civil, art. 1798.140(w)(2)(A), y los cumplirá.