Accord de traitement de données (ATD) de LanSchool Air

Le présent Accord relatif au traitement des données de LanSchool Air (répondant aux exigences de confidentialité et de sécurité) et ses annexes (« **ATD** ») font partie de l'Accord de vente de Stoneware ou de tout autre accord écrit ou électronique entre Stoneware, Inc. et le client (l'« **Accord** ») concernant l'achat de services LanSchool Air auprès de Stoneware, Inc. afin de traduire l'accord convenu entre les parties en ce qui concerne le traitement des données à caractère personnel.

Le présent ATD accompagne tout accord entre les parties en ce qui concerne l'objet des présentes ; et prendra effet dès lors que le Client accepte les Conditions de service de LanSchool Air (« **Date d'entrée en vigueur** »).

Dès la signature de l'Accord et l'acceptation des Conditions de service de LanSchool Air, cet ATD devient juridiquement contraignant ; et vous (le Client) concluez cet ATD au nom du Client, dans la mesure requise par le droit et les réglementations applicables en matière de confidentialité, de sécurité et de protection des données, au nom et pour le compte de ses Affiliés autorisés dans la mesure où Stoneware traite des données à caractère personnel pour lesquelles ces Affiliés autorisés ont la qualité de Responsable. Le Client comprend que cet ATD est applicable à tous les utilisateurs et garantit qu'il dispose des pouvoirs nécessaires pour conclure cet ATD au nom desdits utilisateurs.

Nous pouvons mettre à jour ces conditions pour les adapter à de nouvelles exigences légales ou, le cas échéant, pour tenir compte de mises à jour opérationnelles. Si vous avez un abonnement actif à LanSchool Air, nous vous en informerons par e-mail ou par une notification sur les produits. Vous pouvez consulter les versions archivées de l'ATD ici

Exécution de l'ATD :

a) Cet ATD se compose de deux parties : le texte principal de l'ATD et les annexes A, B, C, D et E Le présent ATD a été présigné au nom de Stoneware, Inc., incluant les clauses contractuelles types de l'annexe D qui ont été présignées par Stoneware en tant qu'Importateur de données. (Remarque : l'Annexe D est généralement applicable aux seules activités de traitement qui peuvent impliquer le transfert de Données à caractère personnel depuis l'Union européenne, l'Espace économique européen, le Royaume-Uni et/ou vers d'autres pays ayant des normes d'adéquation ou d'équivalence similaires relatives aux transferts transfrontaliers de données). En outre, il contient des dispositions contractuelles servant de garanties pour assurer des transferts sécurisés de données personnelles, conformément aux exigences des lois applicables en matière de protection des données.

Pour éviter tout doute, vous devez signer cet ATD à la page 5. Le cas échéant, l'annexe D sera appliquée par renvoi.

Protection des données

Définitions : Dans cette Clause, les termes suivants ont les significations suivantes :

a) « **Responsable du traitement** », « **Sous-traitant** », « **Sous-traitant ultérieur** » « **Traitement des données** », « **Traitement** » (et « **Traiter »**) ont les significations qu'ils revêtent dans la législation de l'UE sur la protection des données et aux termes équivalents dans le Droit applicable à la protection des données.

(a) « **Droit applicable à la protection des données** » désigne toutes les lois, règles, réglementations, ordonnances en vigueur et toutes les modifications y afférentes, dans toute juridiction où le fournisseur propose des services LanSchool, y compris toutes les lois concernant la vie privée, la sécurité des données, la protection des données, les atteintes à la sécurité des données et à la confidentialité, notamment la loi sur la protection du consommateur de Californie (California Consumer Privacy Act, « CCPA ») de 2018 et la loi californienne sur la protection de la vie privée (California Privacy Rights Act, « CPRA »), le Règlement général sur la protection des données de l'Union européenne 2016/279, tel que modifié, tel que remplacé ou abrogé de temps à autre (« RGPD »), la Loi de protection des données du Royaume-Uni de 2018 telle qu'amendée ; la loi n° 13.709/18 du Brésil telle que modifiée (« LGPD ») et les réglementations mises en œuvre (ou à mettre en œuvre), ainsi que de telles lois en vigueur, y compris les lois nationales, d'état, et/ou locales en matière d'éducation et de confidentialité des étudiants.

b) **Les « Données à caractère personnel »** sont des informations qui concernent une personne identifiée ou identifiable, y compris, mais sans s'y limiter, les élèves, les parents et les employés de l'école.

c) **Une « Personne concernée »** est une personne individuelle qui peut être identifiée directement ou indirectement, y compris, mais sans s'y limiter, les élèves, les parents et les employés de l'école.

d) **Un « Client »** est le Responsable du traitement. Aux fins du présent ATD uniquement, le terme « client » inclut le Client et les Affiliés autorisés.

e) **« Fournisseur »** désigne Stoneware, Inc., qui agit en tant que Sous-traitant.

(b) Un **« Exportateur de données »** désigne une partie qui transfère des Données à caractère personnel à une autre Partie conformément à l'Accord.

(c) Un **« Importateur de données »** désigne une partie qui reçoit des Données à caractère personnel du Client d'une autre Partie conformément au présent Accord.

Relations entre les parties : le Client reconnaît le Fournisseur comme Sous-traitant pour traiter les Données à caractère personnel dans le cadre du Contrat de vente Stoneware, des Conditions d'utilisation de LanSchool Air et du Contrat de licence utilisateur final (CLUF) conclus avec le

Fournisseur. Chaque partie doit se conformer aux obligations qui lui incombent en vertu de la Loi sur la protection des données applicable.

Limitation de la finalité : Le Fournisseur doit traiter les Données à caractère personnel en tant que Sous-traitant conformément aux instructions documentées du Responsable du traitement (la « Finalité autorisée ») figurant à l'annexe A « Informations relatives au traitement », sauf disposition contraire de tout Droit applicable à la protection des données. Le Fournisseur doit informer immédiatement le Responsable du traitement s'il se rend compte que les Instructions de traitement du Responsable du traitement enfreignent le Droit applicable à la protection des données. En aucun cas le Fournisseur ne doit traiter les Données à caractère personnel à ses propres fins ou à celles d'un tiers, y compris à des fins de marketing. Pour éviter tout doute, le Fournisseur ne doit pas envoyer de messages marketing ou autrement promotionnels aux utilisateurs de Lenovo LanSchool Air en exploitant les données à caractère personnel obtenues par l'utilisation de Lenovo LanSchool Air. Cette dernière n'empêchera pas un individu de recevoir des messages marketing ou promotionnels si ceux-ci proviennent du contexte des canaux standard tels que le site Web de Stoneware ou de Lenovo et d'autres canaux liés aux ventes.

Transferts internationaux : le Fournisseur est autorisé à transférer les Données à caractère personnel vers tout pays situé en dehors du territoire d'origine de la collecte desdites Données à caractère personnel. Ces transferts doivent être effectués en conformité avec les Lois applicables en matière de protection et de localisation des données. Pour éviter toute ambiguïté, les données doivent être hébergées conformément aux dispositions énoncées ultérieurement dans le présent Accord, à savoir selon une approche ou un lieu spécifique à une région, et :

a) Les transferts de Données à caractère personnel en dehors de l'Espace économique européen (« **EEE** ») et le Royaume-Uni sont autorisés : (i) si les Données à caractère personnel sont transférées vers un destinataire dans un pays qui, selon la Commission européenne, le Secrétaire d'État du Royaume-Uni et/ou le Bureau du Commissaire à l'information du Royaume-Uni assure un niveau de protection adéquat des Données à caractère personnel ; et (ii) à un destinataire qui a signé des clauses contractuelles types adoptées ou approuvées par la Commission européenne, le Secrétaire d'État du Royaume-Uni et/ou le Bureau du Commissaire à l'information du Royaume-Uni.

   Le Fournisseur peut transférer les Données à caractère personnel en dehors du Brésil si : (i) le Transfert de données est effectué vers un destinataire situé dans un pays dont l'Autorité nationale a décidé qu'il assurait une protection adéquate des Données à caractère personnel ; (ii) vers un destinataire qui a signé des Clauses contractuelles types adoptées ou approuvées par l'Autorité nationale ; ou (iii) lorsque le destinataire est en mesure de fournir et de démontrer la mise en œuvre d'autres garanties conformément à la Loi brésilienne sur la protection des données et que le transfert international est approuvé par le Responsable du traitement.

b. En acceptant le présent Accord de Traitement des Données (ATD), le Client consent expressément à ce que Stoneware, Inc. procède au transfert transfrontalier de Données à caractère personnel, sous réserve du respect par Stoneware des Lois applicables en matière

de protection des données. À cet égard, l'Annexe D « Transferts internationaux de données » s'applique entre le Responsable du traitement et le Prestataire le cas échéant.

Les Données des clients sont susceptibles d'être consultées par des sous-traitants ultérieurs, conformément aux dispositions de l'Annexe B du présent Accord, dans des pays tiers, tels que les États-Unis. Ce traitement s'effectue avec les garanties appropriées exigées pour les transferts vers des pays tiers, notamment via des Clauses contractuelles types. Chaque transfert de données au sein du groupe est réalisé conformément à l'Accord de transfert de données intragroupe du Fournisseur, lequel intègre des Clauses contractuelles types destinées à assurer la sécurité des transferts internationaux de données.

Confidentialité du traitement : Le Fournisseur doit s'assurer que toute personne qu'il autorise à traiter les Données à caractère personnel (y compris le personnel, les agents et le sous-traitant ultérieur du Fournisseur) (une « Personne autorisée ») est tenue à une obligation stricte de confidentialité (qu'il s'agisse d'une obligation contractuelle ou d'une obligation juridique) et qu'il ne permet pas à toute personne qui n'est pas tenue à cette obligation de confidentialité de traiter les Données à caractère personnel. Le Fournisseur doit s'assurer que toutes les Personnes autorisées traitent les Données à caractère personnel uniquement aux fins nécessaires à la Finalité autorisée. En outre, le Fournisseur ne doit pas exploiter commercialement les Données à caractère personnel.

c. *Utilisation de l'intelligence artificielle :* le Fournisseur utilise la technologie de l'intelligence artificielle (l'« IA ») en relation avec certaines de ses offres, telles que LanSchool On-Task Monitoring. L'IA est utilisée pour interpréter la signification de l'objectif de la classe et analyser les données déjà capturées sur les étudiants. Elle ne collecte pas d'informations supplémentaires auprès des utilisateurs au-delà des exigences normales liées au produit. Aucune prise de décision automatisée, outre la simple identification, ne doit être déclenchée. **L'IA s'abstiendra de produire toute sortie constituant une discrimination illégale, un biais ou une atteinte aux droits de propriété intellectuelle. Le Fournisseur a mis en place un processus qui permet de traiter** des **résultats générés par le système d'IA, y compris toute discrimination illégale ou tout préjugé présent dans ces résultats.** Le Fournisseur s'engage à **respecter** la Loi applicable en matière de protection des données ainsi que toute autre réglementation **pertinente relative à l'IA.**

Sécurité : Le Sous-traitant doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour protéger les Données à caractère personnel (i) contre la destruction fortuite ou illicite, et (ii) la perte, la modification, la divulgation non autorisée ou l'accès aux Données à caractère personnel (un « Incident de sécurité »). L'annexe C contient les mesures techniques et organisationnelles (MTO) de LanSchool Air.

Sous-traitance ultérieure : le Fournisseur accepte que tout sous-traitant ultérieur tiers qu'il désigne soit soumis à des normes de protection des données substantiellement similaires à celles stipulées par le présent Accord ; et qu'il conclura des accords appropriés avec ses sous-traitants ultérieurs concernés afin de donner un effet approprié aux exigences du présent ATD. Le Responsable du traitement accepte que le Fournisseur puisse utiliser tout sous-traitant ultérieur indiqué à l'Annexe B. Nonobstant cette disposition, le Responsable du traitement autorise le Fournisseur à

engager de nouveaux sous-traitants ultérieurs (y compris le remplacement de sous-traitants existants) pour le traitement des Données à caractère personnel, à condition que : (i) le Fournisseur fournisse un préavis d'au moins 30 jours de l'ajout ou du remplacement de tout sous-traitant ultérieur (y compris les détails du traitement qu'il effectue ou effectuera), qui peut être donné en fournissant les détails de cet ajout ou de ce remplacement au Responsable du traitement ; et (ii) que le Fournisseur impose des conditions de protection des données à tout sous-traitant ultérieur qu'il désigne pour protéger les Données à caractère personnel selon des normes substantiellement similaires à celles prévues par le présent ATD. Si le Responsable du traitement refuse d'accepter la nomination par le Fournisseur d'un nouveau sous-traitant ultérieur tiers, étant entendu que ce refus ne saurait être déraisonnable, le Fournisseur s'abstiendra de procéder à ladite nomination. En outre, le Responsable du traitement pourra choisir de résilier l'Accord, à condition qu'il ait des raisons substantielles et dûment documentées justifiant son opposition à la modification proposée.

Coopération et droits des Personnes concernées : le Fournisseur doit fournir une assistance raisonnable et en temps opportun au Responsable du traitement pour permettre à celui-ci de répondre à : (i) toute demande d'une Personne concernée souhaitant exercer l'un de ses droits en vertu de la Loi sur la protection des données applicable (y compris ses droits d'accès, de correction, d'opposition, d'effacement et de portabilité des Données à caractère personnel, le cas échéant) ; et (ii) toute autre correspondance, demande ou réclamation reçue d'une Personne concernée, d'un organisme de réglementation ou d'un autre tiers dans le cadre du Traitement des Données à caractère personnel. Afin d'éviter toute ambiguïté, les Demandes de Personnes concernées doivent être soumises au Responsable du traitement par l'intermédiaire d'une demande officielle via le Formulaire Web Stoneware pour les Demandes de personnes concernées.

Incidents de sécurité : Dès lors qu'il constate un Incident de sécurité, le Fournisseur doit en informer le Responsable du traitement dans les meilleurs délais et doit fournir les informations et la coopération en temps utile dont le Responsable du traitement peut avoir besoin pour s'acquitter de ses obligations en matière de signalement des atteintes à la sécurité des Données à caractère personnel en vertu du Droit applicable à la protection des données (et conformément aux délais prescrits). Le Fournisseur doit en outre prendre les mesures et les dispositions nécessaires pour atténuer ou remédier aux effets de l'Incident de sécurité et tenir le Responsable du traitement informé de l'évolution de la situation en ce qui concerne ledit Incident de sécurité.

Suppression ou restitution des données : à la résiliation ou à l'expiration du Contrat de vente Stoneware, le Fournisseur doit, à la demande du Responsable du traitement, détruire ou retourner au Responsable du traitement toutes les Données à caractère personnel (y compris toutes les copies de celles-ci) en sa possession ou sous son contrôle (y compris les Données à caractère personnel sous-traitées ultérieurement à un tiers pour Traitement). Si le Responsable du traitement ne donne pas d'autres instructions au Prestataire, le calendrier de conservation des données du Prestataire, comme défini à l'Annexe A, s'appliquera. Cette exigence ne s'applique pas dans la mesure où le Fournisseur est tenu par toute Loi applicable sur la protection des données de conserver tout ou partie des Données à caractère personnel, auquel cas le Fournisseur doit isoler et protéger les Données à caractère personnel de tout Traitement ultérieur, sauf dans la mesure requise par ladite loi.

Audit : durant la validité du présent Accord et pendant une durée de trois ans suivant sa résiliation ou son expiration, le Fournisseur s'engage à fournir au Responsable du traitement, sur demande raisonnable et moyennant un préavis adéquat, les éléments suivants : (i) l'accès aux résumés des : (1) pratiques du Fournisseur, y compris ses protocoles et procédures de sécurité ; (2) politiques internes ; et (3) dossiers relatifs à la confidentialité et à la sécurité des Informations personnelles ainsi qu'au Traitement des Informations personnelles disponibles pour examen, à l'exclusion des dossiers protégés par le secret professionnel ou constituant un produit du travail ; (ii) l'assistance et la coopération du personnel concerné du Fournisseur ; et (iii) les réponses aux questionnaires visant à évaluer le respect par le Fournisseur de ses obligations en vertu du présent Accord (« Audit »). Ces audits seront limités à une fois par an, sauf dans les cas suivants : (i) cet audit est requis par les Lois applicables en matière de protection des données, ou pour satisfaire à toute demande ou exigence d'une autorité de régulation ou de toute procédure juridique ou administrative ; (ii) cet audit est sollicité en raison de préoccupations légitimes du Responsable du traitement quant à la confidentialité et à la sécurité des Données à caractère personnel traitées par le Fournisseur ; ou (iii) un incident de sécurité avéré s'est produit. Nonobstant ce qui précède, si le résumé des pratiques, des politiques et des dossiers ou les réponses au questionnaire fournies par le Fournisseur sont jugés insuffisants pour répondre aux exigences ou demandes d'une autorité de régulation ou d'une procédure juridique ou administrative, les parties s'engagent à négocier de bonne foi les modalités et l'étendue d'un audit complémentaire afin de satisfaire à ladite demande ou requête. Le Fournisseur s'engage à transmettre au Responsable du traitement les informations raisonnablement nécessaires afin de lui permettre de mener à bien et de documenter les évaluations relatives à la protection des données.

EN FOI DE QUOI, Stoneware et le Client ont signé le présent Accord à la date indiquée ci-dessus.

Stoneware, Inc.	**Client**
Signature : _____	Signature : _____
Nom en caractères d'imprimerie : Kimberly Page	Nom en caractères d'imprimerie : _____
Titre : Directeur des opérations stratégiques	Titre : _____

ANNEXE A : INFORMATIONS RELATIVES AU TRAITEMENT

Type de données et personnes concernées	Durée de conservation	Nature, finalité et objet
Données relatives à l'interface apprenant : • L'identificateur unique universel (GUID) de l'apprenant généré automatiquement • L'identifiant apprenant tel que fourni. • Le prénom de l'apprenant. • Le nom de l'apprenant. • L'adresse e-mail de l'apprenant. • Le nom de connexion de l'apprenant. • La date de création de cet objet apprenant. • La date de mise à jour de cet objet apprenant.	Sur demande de suppression de l'utilisateur ou après 1 année de non-activation de la licence ou d'un essai, les données seront archivées. Les données archivées sont purgées après 90 jours.	*Stockage de données* (enregistrement, hébergement, journal, archive ou tout autre mode de stockage des données du Client) ; *Accès aux données* (récupération, copie, examen, modification, transport, numérisation ou tout autre mode d'accès aux Données du Client)
Données relatives à l'interface employé de l'école : • Le GUID unique de l'enseignant généré automatiquement • L'identifiant de l'employé de l'école. • Le prénom de l'employé de l'école. • Le nom de famille de l'employé de l'école. • L'adresse e-mail de l'employé de l'école. • L'identifiant MongoDB de l'utilisateur du cloud qui correspond à cet objet enseignant. • Les jetons d'accès • La date de création de cet objet employé de l'école. • La date de mise à jour de cet objet employé de l'école.	Sur demande de suppression de l'utilisateur ou après 1 année de non-activation de la licence ou d'un essai, les données seront archivées. Les données archivées sont purgées après 90 jours.	*Stockage de données* (enregistrement, hébergement, journal, archive ou tout autre mode de stockage des données du Client) ; *Accès aux données* (récupération, copie, examen, modification, transport, numérisation ou tout autre mode d'accès aux Données du Client) *Analyse des données* (sondage, test, étude, interprétation, organisation, rapport ou tout autre mode d'analyse des Données du Client).
Données relatives à l'interface client : • Le GUID unique du client généré automatiquement • Le nom de connexion de l'apprenant actuel. Il peut s'agir d'une adresse e-mail ou d'un nom d'utilisateur. • L'identifiant MongoDB de l'appareil correspondant depuis la base de données centrale. • La date de création de cet objet client.	Sur demande de suppression de l'utilisateur ou après 1 année de non-activation de la licence ou d'un essai, les données seront archivées. Les données archivées sont purgées après 90 jours.	*Stockage de données* (enregistrement, hébergement, journal, archive ou tout autre mode de stockage des données du Client) ; *Accès aux données* (récupération, copie, examen, modification, transport, numérisation ou tout autre mode

• La date de mise à jour de cet objet client.		d'accès aux Données du Client) *Analyse des données* (sondage, test, étude, interprétation, organisation, rapport ou tout autre mode d'analyse des Données du Client).
Données relatives aux listes de classes • Le GUID unique de la classe généré automatiquement • Le nom de cette classe. Cette information est obligatoire. • L'identifiant de la classe fourni par le Système d'information des apprenants. • L'identifiant de l'établissement d'enseignement fourni par le Système informatisé d'information sur les apprenants. • L'heure de cours ou toute autre désignation qui distingue cette classe des autres classes du même type. • Le propriétaire de cette liste de classes. • Des objets enseignant pour les enseignants qui ont accès à cette liste de classes. L'interface enseignant est définie ci-dessous. • Des objets apprenant pour les apprenants qui appartiennent à cette liste de classes. • Des objets client pour les appareils qui appartiennent à cette liste de classes. • L'identifiant de l'utilisateur qui a modifié cette liste de classes pour la dernière fois. • La date de création de cette liste de classes. • La date de mise à jour de cette liste de classes.	Sur demande de suppression de l'utilisateur ou après 1 année de non-activation de la licence ou d'un essai, les données seront archivées. Les données archivées sont purgées après 90 jours.	*Stockage de données* (enregistrement, hébergement, journal, archive ou tout autre mode de stockage des données du Client) ; *Accès aux données* (récupération, copie, examen, modification, transport, numérisation ou tout autre mode d'accès aux Données du Client) *Analyse des données* (sondage, test, étude, interprétation, organisation, rapport ou tout autre mode d'analyse des Données du Client).
Données relatives à l'organisation • Le GUID unique de l'organisation généré automatiquement • Le nom de l'organisation. • L'identifiant attribué à cette organisation.	Sur demande de suppression de l'utilisateur ou après 1 année de non-activation de la licence ou d'un essai, les données seront	*Stockage de données* (enregistrement, hébergement, journal, archive ou tout autre mode de stockage des données du Client) ;

• L'adresse postale principale. • Les coordonnées de l'adresse postale secondaire. • La ville d'attache de l'organisation. • L'État ou la province d'attache de l'organisation. • Le code postal de l'organisation. • Le pays d'attache de l'organisation. • Les coordonnées administratives. • Les coordonnées techniques. • Les coordonnées de facturation. • Un drapeau indiquant si cette organisation a un agent de site. • La date de création de cette organisation. • La stratégie de sécurité par défaut de l'organisation. • Les coordonnées de l'organisation : nom, prénom, numéro de téléphone, adresse e-mail.	archivées. Les données archivées sont purgées après 90 jours.	*Accès aux données* (récupération, copie, examen, modification, transport, numérisation ou tout autre mode d'accès aux données du Client) ; *Analyse des données* (sondage, test, étude, interprétation, organisation, rapport ou tout autre mode d'analyse des Données du Client).
Données utilisateur • Le GUID unique de l'utilisateur généré automatiquement • Un ensemble de paires clé-valeur de tous les identifiants actuels de l'utilisateur. • Le prénom de l'utilisateur. • Le nom de l'utilisateur. • L'adresse e-mail de l'utilisateur. • Les autorisations directement attribuées à cet utilisateur. • Une référence à l'organisation à laquelle appartient cet utilisateur. • Un sous-ensemble d'identifiants d'utilisateur dont un utilisateur est autorisé à se servir pour une connexion. • Un horodatage de la dernière fois où l'utilisateur s'est connecté avec succès au système. • Un horodatage de la première fois où l'utilisateur n'a pas pu être authentifié au cours de la dernière heure. • L'adresse IP de l'endroit où la dernière connexion réussie a eu lieu. • L'adresse IP de l'endroit où la dernière connexion infructueuse a eu lieu.	Sur demande de suppression de l'utilisateur ou après 1 année de non-activation de la licence ou d'un essai, les données seront archivées. Les données archivées sont purgées après 90 jours.	*Stockage de données* (enregistrement, hébergement, journal, archive ou tout autre mode de stockage des données du Client) ; *Accès aux données* (récupération, copie, examen, modification, transport, numérisation ou tout autre mode d'accès aux Données du Client) *Analyse des données* (sondage, test, étude, interprétation, organisation, rapport ou tout autre mode d'analyse des Données du Client).

• L'horodatage du dernier échec de la tentative de connexion. • Un compteur indiquant le nombre de tentatives de connexion infructueuses consécutives. • Les autorisations accordées à l'utilisateur. Générées en combinant toutes les autorisations des groupes de l'utilisateur. • La date de création de cet utilisateur. • La date de mise à jour de cet utilisateur.		
Données relatives au Journal d'activité • L'historique de navigation Web des étudiants (URL, horodatage) • L'historique des applications des étudiants (nom de l'application, horodatage) • L'historique des messages de chat en classe (expéditeur, réception, contenu du message, horodatage) • Le journal des activités administratives (identifiant utilisateur, type d'activité, horodatage) • Captures d'écran des étudiants, métadonnées de l'onglet, contenu de la page d'onglet active • Objectifs de classe des enseignants.	Sur demande de suppression de l'utilisateur ou après 45 jours.	*Stockage de données* (enregistrement, hébergement, consignation, archivage ou autre stockage des Données du Client) ; *Accès aux données* (récupération, copie, examen, modification, transport, numérisation ou accès de toute autre manière aux Données du Client) ; *Analyse des données* (enquête, test, étude, interprétation, organisation, rapport ou autre analyse des Données du Client).
Données de licence (excluent les données à caractère personnel)	Ces données sont conservées aussi longtemps que nécessaire pour se conformer aux obligations légales, pour faire appliquer nos accords, etc. Elles n'incluent pas les données à caractère personnel.	*Stockage de données* (enregistrement, hébergement, journal, archive ou tout autre mode de stockage des données du Client) ; *Accès aux données* (récupération, copie, examen, modification, transport, numérisation ou tout autre mode d'accès aux données du Client) ; *Analyse des données* (sondage, test, étude, interprétation, organisation, rapport ou tout autre mode d'analyse des Données du Client).

Durée du traitement
La durée du traitement correspond à la durée de l'Accord. Les stratégies de conservation décrites ci-dessus s'appliqueront.
Catégories de personnes concernées
Apprenants, enseignants, contacts de l'organisation et utilisateurs en général

ANNEXE B – SOUS-TRAITANTS ULTÉRIEURS

Nom	Données	Lieu de stockage	Finalité
Amazon Web Services	Toutes les données utilisateur décrites à l'annexe A	Australie, États-Unis ou Royaume-Uni *(des restrictions de transfert régionales sont appliquées, par exemple pour des données européennes stockées exclusivement au Royaume-Uni).*	Prestataire de services cloud pour l'infrastructure d'application. Toutes les données sont traitées par l'application.
Datadog	Données d'application, adresse IP et nom d'utilisateur	US	Outil de collecte de journaux.
Hubspot	Prénom, Nom, Adresse e-mail, Téléphone, Raison sociale, Titre, Balise géographique (par exemple, État), Secteur	États-Unis, UE	Embarquement.
Atlas MongoDB	Toutes les données utilisateur décrites à l'annexe A	Australie, États-Unis ou Royaume-Uni *(des restrictions de transfert régionales sont appliquées, par exemple pour des données européennes stockées exclusivement au Royaume-Uni).*	Pour le bon fonctionnement de l'application.
Pendo	Analyse d'utilisation de l'application, commentaires fournis par l'utilisateur, prénom de l'utilisateur final, nom de famille, e-mail, et nom de l'organisation.	US	Permet d'améliorer la fonctionnalité et la facilité d'utilisation du produit.

ANNEXE C – MESURES TECHNIQUES ET ORGANISATIONNELLES (MTO)

Le Fournisseur a mis en œuvre un programme de sécurité complet et écrit avec des contrôles physiques, techniques, procéduraux et administratifs qui reflètent les normes du secteur en vigueur pour la protection et l'utilisation responsable des Données à caractère personnel, y compris, mais sans s'y limiter, les contrôles suivants :

Technique	Périmètre	Contrôles
Accès	Connexions (système et application).	Stratégies de mot de passe basées sur le NIST (authentification multifacteurs pour l'accès au niveau administrateur et les interfaces).
Chiffrement	Stockage de données au repos et en transit.	AES 256-GCM (au repos), TLS 1.2, 1.3 (en transit)
Tests statiques de sécurité des applications	Toutes les images de serveur et de micro-service, Tous les clients binaires et les extensions/plug-ins.	Analyses et suivi réguliers des vulnérabilités.
Tests dynamiques de sécurité des applications	API des applications externes.	Analyses d'applications Web, Tests de pénétration (Tests internes réguliers.)
Durcissement des critères de référence CIS	Fournisseur de plateformes cloud, Instances serveur.	Contrôles de conformité cloud CIS, surveillance de la sécurité cloud, Évaluations de référence régulières du serveur CIS L2.
Analyse de composition logicielle	dépendances à l'égard de logiciels tiers en open source.	Exécution régulière d'audits de vulnérabilité, surveillance du répertoire.
Évaluation de l'infrastructure	Fournisseur de plateformes cloud.	Examens réguliers de tous les réseaux définis par logiciel (SDN) (identifier la segmentation du réseau, la configuration du pare-feu et les erreurs de configuration de l'accès aux ressources).
Pare-feu d'application Web (WAF)	Applications Web de production.	Protection WAF (règles de base pour les attaques courantes).
Analyse statique du code	Code propriétaire.	L'analyse régulière du code est effectuée à l'aide d'un outil commercial, des révisions de code sécurisées sont effectuées lors des fusions de code.
Collection de journaux	Fournisseur de plateformes cloud, Application.	Transactions API de la plateforme cloud (les journaux de plus de 360 jours sont purgés, accessibles par ingénierie), Journalisation WAF pour la détection des bords (les journaux

		de plus de 90 jours sont purgés, accessibles par ingénierie), Sous-traitants ultérieurs, voir annexe B, aux fins de l'application.
Infrastructure en tant que code	Fournisseur de plateformes cloud.	L'infrastructure en tant que code sert à automatiser les déploiements d'infrastructure et à améliorer l'immuabilité et la mauvaise configuration de l'infrastructure.

Organisationnel	Périmètre	Contrôles
Réponse aux incidents (y compris les violations de données)	Événements de sécurité liés aux produits en production.	Plan d'intervention en cas d'incident conformément au NIST 800-61 et les processus internes de l'équipe d'intervention en cas d'incident de sécurité des produits (PSIRT) de Lenovo.
Liste des prestataires de confiance	Tous les sous-traitants ultérieurs qui s'intègrent directement aux produits en production.	Évaluations de sécurité standard des fournisseurs intégrés, des autorités de protection des données (APD) pour les prestataires de traitement des Données à caractère personnel.
Gestion des vulnérabilités	OSes serveur, Conteneurs Docker, Clients, Produits en production.	Un programme qui utilise divers outils pour aider à identifier les vulnérabilités dans tous les systèmes de calcul.
Conseil d'examen de la sécurité logicielle (Software Security Review Board, SSRB)	Produits en production.	Des examens du SSRB sont effectués régulièrement. Au cours des examens, toutes les mesures techniques et organisationnelles sont évaluées pour le produit en question.
Stratégie de conservation des données	Informations identifiables personnellement, Données d'application, Produits en production.	Sur demande de suppression de l'utilisateur ou après 1 année de non-activation de la licence ou de l'essai, les données à caractère personnel seront archivées. Les données archivées sont purgées après 90 jours.

Sensibilisation à la sécurité et à la confidentialité	Tous les employés (cours sur les fondamentaux de la confidentialité et les fondamentaux de la sécurité)	Formation semi-annuelle pour les équipes spécialisées en informatique et en produits sur des sujets de sécurité avancés, tels que le Top 10 OWASP.
Sécurité continue	Produits en production.	Application régulière des mesures techniques.
Examens de conformité Open source.	Produits en production.	Évaluations effectuées pour s'assurer que les licences et les attributions appropriées sont fournies dans les logiciels distribués.
Reprise après sinistre	Produits en production	Suivre NIST-800-34 comme guide pour maximiser la DMIA et la PDMA.
Stratégie de sauvegarde	Bases de données, Code, Journaux.	La stratégie générale nécessite plusieurs sauvegardes, dont l'une doit être effectuée hors du site de stockage principal, Des sauvegardes régulières des bases de données sont effectuées quotidiennement (2 fois par jour), hebdomadairement et mensuellement. Les sauvegardes quotidiennes sont conservées pendant 7 jours. Les sauvegardes hebdomadaires sont conservées pendant 4 semaines. Les sauvegardes mensuelles sont conservées pendant 13 mois. La fenêtre de restauration est de 12 heures, Les sauvegardes du code source des applications sont effectuées quotidiennement et sont conservées pendant 360 jours. Journaux de production : Datadog – les journaux sont actifs pendant 7 jours. Les journaux sont ensuite placés dans un système de stockage à

		long terme pendant 180 jours, puis purgés. Équilibreur de charge – les journaux sont conservés pendant 360 jours, puis purgés. Pare-feu d'application Web – les journaux sont conservés pendant 90 jours, puis purgés. CloudTrail – les journaux sont conservés pendant 90 jours, puis purgés. CloudWatch – les journaux sont conservés pendant 360 jours, puis purgés. MongoDB – les journaux sont conservés pendant toute la durée du projet.

ANNEXE D – ACCORD DE TRANSFERTS INTERNATIONAUX DE DONNÉES

La présente Annexe énonce les exigences en matière de protection des données (y compris les exigences prévues par le droit applicable en matière de protection de la vie privée) qui s'appliquent : (i) à l'Exportateur de données (Responsable du traitement) lorsqu'il transfère des données à caractère personnel à l'Importateur de données (Stoneware, Inc.), à ses affiliés et/ou à ses sous-traitants ultérieurs, à des fins de traitement de données ; et (ii) à l'Importateur de données lorsqu'il reçoit des données à caractère personnel de la part d'un Exportateur de données à des fins de traitement de données.

L'importateur de données déclare et garantit :

a) toujours traiter les Données transférées conformément au droit applicable en matière de protection de la vie privée et apporter une assistance raisonnable et en temps opportun à l'Exportateur de données, selon les besoins, pour l'aider à respecter ses obligations en vertu du droit applicable en matière de protection de la vie privée ; et

b) ne jamais remplir sciemment ses obligations au titre du présent Accord de manière à amener l'Exportateur de données à enfreindre l'une de ses obligations en vertu du droit applicable en matière de protection de la vie privée.

L'Exportateur de données confirme avoir pris les mesures nécessaires afin d'assurer la conformité aux lois applicables en matière de Protection des données, y compris en ce qui concerne les exigences en matière de transfert transfrontalier des données à caractère personnel, telles que l'obtention du consentement explicite des Personnes concernées au transfert de leurs données à caractère personnel à l'étranger, la notification aux autorités compétentes, la demande de leur approbation du transfert ou d'autres obligations sous-jacentes, le cas échéant.

1. Espace économique européen (EEE)

Si les services du Fournisseur sont fournis au Responsable du traitement au sein de l'Espace économique européen (« EEE ») ou de toute autre juridiction soumise à la loi européenne sur la protection des données, les dispositions suivantes s'appliquent :

(A) « Loi européenne sur la protection des données » désigne (a) le règlement 2016/679 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des Données à caractère personnel et à la libre circulation de ces données (Règlement général sur la protection des données) (le « RGPD ») ; (b) la directive européenne relative à la vie privée en ligne (directive 2002/58/CE) ; et (c) toutes les lois nationales applicables en matière de protection des données.

(B) Le Fournisseur informera rapidement le Responsable du traitement (a) de toute exigence en vertu de la loi européenne sur la protection des données qui nécessiterait de traiter les Données à caractère personnel d'une manière autre que selon les instructions du Responsable du traitement, ou (b) si, de l'avis du Fournisseur, les instructions du Responsable du traitement peuvent enfreindre ou violer toute loi européenne applicable sur la protection des données.

(C) ***Transferts de données :*** Si le Fournisseur ou ses sous-traitants ultérieurs sont situés en dehors de l'EEE, le Fournisseur et le Responsable du traitement conviennent de signer les clauses contractuelles types opposables au responsable du traitement et au sous-traitant énoncées dans le MODULE DEUX de la décision d'exécution (UE) 2021/914 de la Commission du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de Données à caractère personnel vers des pays tiers conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil telle que modifiée ou remplacée de temps à autre (les « Clauses contractuelles types C2P ») et de les incorporer par les présentes au présent Addendum par renvoi. Les parties reconnaissent et conviennent que :

a. Le Fournisseur et le Responsable du traitement doivent chacun se conformer à leurs obligations respectives visées dans les clauses contractuelles types C2P ;

b. En cas de conflit ou de divergence entre les clauses contractuelles types C2P et le présent Addenda ou l'accord-cadre, les Clauses contractuelles types C2P prévaudront dans la mesure du conflit, et

c. Les informations figurant sur les tableaux suivants sont par les présentes intégrées dans clauses contractuelles types entre les parties :

Informations à intégrer dans les
Clauses contractuelles types C2P entre le Responsable du traitement et le Fournisseur :

Clause 9. Recours à des sous-traitants secondaires	L'option 2 AUTORISATION ÉCRITE GÉNÉRALE est sélectionnée. L'importateur de données doit fournir des informations au moins 30 jours à l'avance, conformément à la clause « Sous-traitance secondaire ».
Clause 17. Droit applicable	Ces clauses seront interprétées conformément à la loi applicable énoncée dans l'accord-cadre des Parties, sauf si cette loi applicable n'est pas celle d'un État membre de l'UE qui autorise les droits des tiers bénéficiaires. Dans ce cas, les parties conviennent que les présentes clauses seront régies par les lois de l'IRLANDE.
Clause 18 (b). Choix du lieu de jugement et compétence juridique	Les parties conviennent que tout litige découlant des présentes clauses sera résolu par les tribunaux d'IRLANDE.

Informations à intégrer dans l'annexe 1, partie A, des clauses contractuelles types C2P :

Nom de l'exportateur de données	Responsable du traitement, et toute société affiliée qu'il possède ou contrôle en commun
Adresse de l'exportateur de données	À remplir par l'exportateur de données

Nom, fonction et coordonnées de la personne de contact de l'exportateur de données	À remplir par l'exportateur de données
Activités de l'exportateur de données relatives aux données transférées en vertu des présentes clauses.	À remplir par l'exportateur de données
Date et signature de l'exportateur de données	À remplir par l'exportateur de données
Rôle de l'exportateur de données	Responsable du traitement
Nom de l'importateur de données	Fournisseur (Stoneware, Inc.) et ses sous-traitants
Adresse de l'importateur de données	Stoneware, Inc. 8001 Development Drive, Morrisville, NC 27560 United States of America
Nom, fonction et coordonnées de la personne de contact de l'importateur de données	Dan Verwolf, Directeur privacy@lanschool.com
Activités de l'importateur de données relatives aux données transférées en vertu des présentes clauses.	Comme indiqué dans la partie B de l'annexe 1
Date et signature de l'importateur de données	À remplir par l'importateur de données
Rôle de l'importateur de données	Sous-traitant

Informations à intégrer à l'annexe 1, parties B et C, des clauses contractuelles types C2P :

Catégories de personnes concernées	Comme indiqué à l'annexe A ci-dessus
Catégories de données à caractère personnel	Comme indiqué à l'annexe A ci-dessus
Données sensibles	Comme indiqué à l'annexe A ci-dessus
Fréquence du transfert	Fréquence continue, tant que la licence LSA est active
Nature du traitement	Comme indiqué à l'annexe A ci-dessus
Finalité du traitement	Comme indiqué à l'annexe A ci-dessus
Période pendant laquelle les données à caractère personnel seront conservées	Comme indiqué à l'annexe A ci-dessus
Finalité, nature et durée du traitement effectué par les sous-traitants ultérieurs	Comme indiqué à l'annexe B ci-dessus
Autorité de contrôle compétente chargée de veiller au respect par l'exportateur de données du Règlement (UE) 2016/679	L'autorité de contrôle qui agira en tant qu'autorité de contrôle compétente sera celle de l'État membre de l'UE dans lequel

	l'Exportateur de données est établi dans l'UE. Si l'Exportateur de données (c'est-à-dire l'entité juridique contractante) n'est pas établi dans l'UE, l'autorité de surveillance compétente sera celle de l'État membre de l'UE dans lequel le représentant de l'UE de l'Exportateur de données au sens de l'article 27, paragraphe 1, du règlement (UE) 2016/679 est établi. Si l'Exportateur de données n'est pas établi dans l'UE mais n'a pas besoin de désigner un représentant de l'UE, alors l'Autorité de contrôle compétente sera celle de l'État membre de l'UE dans lequel se trouvent les personnes concernées dont les données à caractère personnel sont transférées en vertu des présentes Clauses en relation avec l'offre de biens ou de services qui leur est faite, ou dont le comportement est surveillé.

Informations à intégrer dans l'annexe 2 des clauses contractuelles types C2P :

Description des mesures techniques et organisationnelles mises en œuvre par le ou les importateurs de données (y compris toute certification pertinente) pour garantir un niveau de sécurité approprié, compte tenu de la nature, de la portée, du contexte et de la finalité du traitement, ainsi que des risques pour les droits et libertés des personnes physiques.	Comme indiqué à l'annexe C ci-dessus

Informations à intégrer dans l'annexe 3 des clauses contractuelles types C2P :

Liste des sous-traitants ultérieurs autorisés	Comme indiqué à l'annexe B ci-dessus

2. Royaume-Uni (RU)

Si les services du Fournisseur sont fournis au Responsable du traitement au Royaume-Uni, ou si la nature des Données à caractère personnel déclenche l'application de la Loi de 2018 sur l'Union européenne (retrait) (le « RGPD britannique ») et de la Loi de 2018 sur la

protection des données (le « DPA 2018 »), les dispositions supplémentaires suivantes s'appliquent :

(A) Les transferts de Données à caractère personnel vers un destinataire situé dans un pays considéré par le Secrétaire d'État du Royaume-Uni comme offrant une protection adéquate des Données à caractère personnel (une « Décision d'adéquation ») seront autorisés en vertu du ou des accords sans qu'il soit nécessaire d'approuver des clauses contractuelles types britanniques.
(B) Les pays de l'EEE sont réputés être soumis à une Décision d'adéquation aux fins des transferts de Données à caractère personnel du Royaume-Uni vers l'EEE.
(C) En l'absence d'une Décision d'adéquation, le Responsable du traitement et le Fournisseur conviennent de signer l'addendum britannique approuvé pour le transfert de données international aux clauses contractuelles types de la Commission européenne pour les transferts de données internationaux(https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf).

Partie 1 : Tableaux / Tableau 1 : Parties

Informations à intégrer dans la « Partie 1 : Tableaux » de l'addendum sur le transfert international de Données aux clauses contractuelles types de la Commission européenne :		
Date d'entrée en vigueur	Conformément à ce qui précède	
Les parties	**Exportateur (qui envoie le transfert restreint)**	**Importateur (qui reçoit le transfert restreint)**
Détails des parties	Nom légal complet, adresse principale (s'il s'agit d'une société) : Selon les informations figurant dans le 2ème tableau de l'art. 1. Espace économique européen (EEE) dans l'annexe D Numéro d'enregistrement officiel (le cas échéant) (numéro d'entreprise ou identifiant similaire) : Selon le client identifié dans le Contrat de vente	Nom légal complet, adresse principale (s'il s'agit d'une société) : Selon les informations figurant dans le 2ème tableau de l'art. 1. Espace économique européen (EEE) dans l'annexe D Numéro d'enregistrement officiel (le cas échéant) (numéro d'entreprise ou identifiant similaire) : 35-2097171 enregistré dans l'État d'Indiana
Contact clé	Nom complet (facultatif), intitulé du poste, coordonnées, y compris l'adresse électronique : Selon les informations figurant dans le 2ème tableau de l'art. 1. Espace	Nom complet (facultatif), intitulé du poste, coordonnées, y compris l'adresse électronique : Selon les informations figurant dans le 2ème tableau de l'art. 1. Espace économique européen (EEE) dans l'annexe D

	économique européen (EEE) dans l'annexe D	

Tableau 2 : CCT, modules et clauses sélectionnées

Addendum des CCT de l'UE	Voir l'annexe D, art. 1 ci-dessus

Tableau 3 : Informations sur l'annexe

Annexe 1A : Liste des Parties comme indiqué dans l'Art. 1. Espace économique européen (EEE) dans l'annexe D
Annexe 1B : Description du transfert : Comme indiqué à l'annexe A ci-dessus
Annexe II : Mesures techniques et organisationnelles, y compris les mesures techniques et organisationnelles visant à garantir la sécurité des données : Description du transfert : Comme indiqué à l'annexe C ci-dessus
Annexe III : Liste des sous-traitants ultérieurs (modules 2 et 3 uniquement) : Description du transfert : Comme indiqué à l'annexe B ci-dessus

Tableau 4 : Fin du présent addendum lorsque l'addendum approuvé est modifié

Mettre fin au présent addendum lorsque l'addendum approuvé change	Les Parties peuvent mettre fin au présent addendum comme indiqué à l'article **Error! Reference source not found.** : ☒ Importateur ☐ Exportateur ☐ aucune des Parties

Informations à intégrer dans la « Partie 2 : Clauses obligatoires » de l'addendum sur le transfert international de Données aux clauses contractuelles types de la Commission européenne :
Partie 2 : Clauses obligatoires de l'addendum approuvé, qui est le modèle d'addendum B.1.0 publié par l'OIC et déposé devant le Parlement conformément à l'article 119A de la loi sur la protection des données 2018 le 2 février 2022, tel qu'il est révisé en vertu de la section**Error! Reference source not found.** de ces Clauses obligatoires.

3. Suisse

Dans la mesure où le transfert de Données à caractère personnel est soumis à la Loi fédérale suisse sur la protection des données, les parties conviennent de se conformer aux Clauses contractuelles types de l'UE et les dispositions suivantes s'appliquent : (i) le Préposé fédéral à la protection des données et à la transparence (PFPDT) sera l'autorité de contrôle compétente en vertu de la Clause 13 des Clauses contractuelles types de l'UE ; (ii) les Parties conviennent de respecter la norme RGPD en ce qui concerne tout Traitement des Données à caractère personnel régi par la Loi fédérale suisse sur la protection des données ; (iii) les Clauses contractuelles types de l'UE seront régies par les lois suisses conformément à la Clause 17 (Option 1) dans la mesure où les transferts de données sont régis par la Loi fédérale suisse sur la protection des données ; (iv) l'expression « État membre » dans les Clauses contractuelles types de l'UE ne sera pas interprétée de manière à exclure les Personnes concernées situées en Suisse de la possibilité de défendre leurs droits en justice dans leur lieu de résidence habituelle (Suisse) conformément à la Clause 18(c) des Clauses contractuelles types de l'UE ; (v) les références au « RGPD » dans les Clauses contractuelles types de l'UE s'entendront comme des références à la Loi fédérale suisse sur la protection des données dans la mesure où le transfert des Données du Responsable du traitement est soumis à la Loi fédérale suisse sur la protection des données.

4. Brésil

Dans le cas d'un transfert de données à caractère personnel soumis à la loi brésilienne sur la protection des données à caractère personnel (telle qu'amendée par la loi nº 13.853 du 8 juillet 2019) (« LGPD »), et si Lenovo, le Fournisseur, ou les deux, sont situés dans des pays n'offrant pas un niveau de protection adéquat, les Clauses contractuelles types C2P référencées aux présentes s'appliquent, avec les modifications suivantes :

(i) l'autorité de contrôle des Clauses contractuelles types C2P est l'autorité nationale brésilienne de la protection des données (Autoridade Nacional de Proteção de Dados, ANPD) ;

(ii) le droit applicable au sens de la Clause 17 des Clauses contractuelles types C2P est la loi LGPD ;

(iii) l'élection de forum et de juridiction au sens de la Clause 18 des Clauses contractuelles types C2P est le droit brésilien si le transfert des données est exclusivement soumis à la loi LGPD ; et

(iv) toutes les références au RGPD dans les Clauses contractuelles types C2P comprennent également les références aux dispositions équivalentes de la loi LGPD (telle qu'amendée ou remplacée).

5. Afrique du Sud

Si les services du Fournisseur sont proposés au Responsable du traitement en Afrique du Sud ou dans une autre juridiction soumise à la loi sur la protection des données à caractère personnel (POPIA), les dispositions supplémentaires suivantes s'appliquent :

(A) A. « Personne concernée » désigne une personne physique qui peut être identifiée par un nom, un numéro unique, des données de localisation, un identifiant en ligne, ou par un ou

plusieurs facteurs propres à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne physique, ainsi qu'une personne morale ou entité juridique identifiable.

6. Australie

Les parties conviennent d'utiliser et de protéger les Données à caractère personnel applicables conformément à la Loi australienne sur la confidentialité des données telle que modifiée.

ANNEXE E – DISPOSITIONS SUPPLÉMENTAIRES

1. Loi sur la protection du consommateur de Californie (California Consumer Privacy Act, « CCPA »).

Stoneware, Inc. est une entreprise. En outre, le Fournisseur est le prestataire de services du Client et traitera des Données à caractère personnel pour le compte du Client.

d. Le Fournisseur ne doit pas vendre les Données à caractère personnel ou les informations exclusives. « Vendre » signifie commercialiser, louer, publier, divulguer, diffuser, rendre disponible, transférer ou communiquer autrement l'information à des fins pécuniaires ou moyennant valable contrepartie.

e. Le Fournisseur ne doit pas conserver, utiliser ou divulguer les Données à caractère personnel : (a) à d'autres fins que dans le but précis d'exécuter les services énoncés dans l'Accord avec Stoneware, Inc. ou que celui autorisé par le CCPA et ses règlements d'application, (b) dans un but commercial autre que la fourniture des services prévus dans le contrat avec l'entreprise, ou (c) en dehors de la relation commerciale directe entre la personne et Stoneware, Inc.

f. Cet ATD vaut attestation du Fournisseur qu'il comprend les exigences de la loi CCPA applicables aux entreprises et aux prestataires de services, y compris les restrictions visées dans Cal. Civ. Code § 1798.140(w)(2)(A), et s'engage à les respecter.