

Contrat de sous-traitant des données (CSTD) de LanSchool Air

Le présent Contrat de sous-traitant des données de LanSchool Air (qui aborde les exigences en matière de confidentialité et de sécurité) et ses annexes (le « **CSTD** ») font partie du Contrat de vente de Stoneware ou d'un autre contrat écrit ou électronique entre Stoneware, Inc. et le Client (le « **Contrat** ») pour l'achat des services LanSchool Air auprès de Stoneware, Inc. afin de refléter le contrat des parties concernant le traitement des Données personnelles.

Le présent CSTD complète toute entente entre les parties en ce qui concerne l'objet des présentes; et entrera en vigueur dès que le Client acceptera les Conditions générales de services de LanSchool Air (la « **Date d'entrée en vigueur** »).

Dès la signature du Contrat et l'acceptation des Conditions de services de LanSchool Air, ce CSTD deviendra juridiquement contraignant; et vous (Client) concluez ce CSTD au nom du Client, dans la mesure requise par les Lois et règlements applicables en matière de confidentialité, de sécurité et de protection des données, y compris les lois et règlements applicables en matière d'éducation et de sécurité des apprenants, au nom et pour le compte de ses Sociétés affiliées autorisées dans la mesure où Stoneware traite des Données personnelles pour lesquelles ces Sociétés affiliées autorisées sont qualifiées de Responsable du traitement. Le Client comprend que le présent CSTD s'applique à tous les utilisateurs et garantit qu'il a les pouvoirs nécessaires pour conclure le présent CSTD au nom de ces utilisateurs.

Nous pouvons mettre à jour ces conditions pour répondre à de nouvelles exigences légales ou au besoin pour refléter les mises à jour opérationnelles. Si vous avez un abonnement LanSchool Air actif, nous vous en informerons par courriel ou par notification intégrée au produit. Vous pouvez trouver des versions archivées du CSTD [ici](#).

Exécution du CSTD :

- a) Ce CSTD comprend deux parties : le corps principal du CSTD et les annexes A, B, C, D et E. Le présent CSTD a été présigné au nom de Stoneware, Inc., y compris les clauses contractuelles types de l'UE à l'annexe D, en tant qu'importateur de données. (Remarque : L'annexe D s'applique généralement aux activités de traitement qui peuvent impliquer le transfert de données personnelles de l'Union européenne, de l'Espace économique européen, du Royaume-Uni et/ou d'autres pays ayant des normes d'adéquation ou d'équivalence similaires relatives aux transferts transfrontaliers de données.) En outre, il représente les dispositions contractuelles servant de mesures de protection pour les transferts sécuritaires de données personnelles requis par les lois applicables en matière de protection des données.

Pour éviter toute ambiguïté, vous devez signer ce CSTD à la page 5. Le cas échéant, l'annexe D s'appliquera par référence.

Protection des données

Définitions : Dans la présente clause, les termes suivants ont les significations suivantes :

- a) « **Responsable du traitement** », « **Sous-traitant** », « **Sous-traitant ultérieur** », « **Traitement des données** », « **Traitement** » (et « **Traiter** ») ont le sens donné dans la Législation sur la protection des données de l'UE et des termes équivalents dans la Loi applicable sur la protection des données.
 - (a) « **Législation applicable sur la protection des données** » désigne l'ensemble des lois applicables, règles, règlements, ordonnances et modifications connexes dans toute juridiction où le Fournisseur fournit les Services LanSchool, y compris toute loi concernant la confidentialité, la sécurité des données, la protection des données, les violations de données et la confidentialité comme la California Consumer Privacy Act de 2018 (« CCPA ») et la California Privacy Rights Act (« CPRA »); le Règlement général sur la protection des données 2016/279 de l'Union européenne, tel que modifié ou remplacé de temps à autre (le « RGPD »); la Data Protection Act 2018 du Royaume-Uni telle que modifiée; la loi brésilienne n° 13.709/18 telle que modifiée (« LGPD ») et les règlements mis en œuvre (ou à mettre en œuvre); et toute autre loi applicable, y compris les lois nationales, étatiques et/ou locales sur l'éducation et la confidentialité des apprenants.
- b) Les « **Données personnelles** » désignent les renseignements qui concernent une personne identifiée ou identifiable, y compris, mais sans s'y limiter, les apprenants, les parents et les employés de l'établissement d'enseignement.
- c) La « **Personne concernée** » est une personne qui peut être identifiée directement ou indirectement, y compris, mais sans s'y limiter, les apprenants, les parents et les employés de l'établissement d'enseignement.
- d) Le « **Client** » désigne le Responsable du traitement. Aux fins du présent CSTD seulement, le terme « Client » comprend le Client et les Sociétés affiliées autorisées.
- e) Le « **Fournisseur** » désigne Stoneware, Inc., qui agit comme Sous-traitant.
 - (b) Un « **Exportateur de données** » désigne une partie qui transfère des Données personnelles à une autre Partie conformément à l'Accord.
 - (c) Un « **Importateur de données** » désigne une partie qui reçoit des Données personnelles du Client d'une autre Partie conformément au présent Accord.

Relations entre les parties : le Client reconnaît le Prestataire comme Sous-traitant pour traiter les Données personnelles faisant l'objet du Contrat de vente Stoneware, des Conditions d'utilisation de LanSchool Air et du Contrat de licence utilisateur final (CLUF) conclus avec le Prestataire. Chaque partie doit se conformer aux obligations qui lui sont applicables en vertu de la loi en vigueur en matière de protection des données.

Limitation de l'objectif : Le Fournisseur doit traiter les Données personnelles en tant que Sous-traitant et strictement conformément aux instructions documentées du Responsable du traitement

(l'« Objectif autorisé ») telles que documentées à l'Annexe A « Détails du traitement », sauf si une Législation applicable sur la protection des données l'exige. Le Fournisseur doit immédiatement informer le Responsable du traitement s'il apprend que les instructions de Traitement du Contrôleur enfreignent la Législation applicable sur la protection des données. En aucun cas le Fournisseur ne doit traiter les Données personnelles à ses propres fins ou celles d'un tiers, y compris à des fins de marketing. Pour éviter tout doute, le Fournisseur ne doit pas envoyer de communications marketing ou promotionnelles aux utilisateurs de Lenovo LanSchool Air en tirant parti des données personnelles obtenues grâce à l'utilisation de Lenovo Lan School Air. Ce dernier point n'empêchera pas une personne de recevoir des communications marketing ou promotionnelles si celles-ci proviennent de canaux standard tels que le site Web de Stoneware ou de Lenovo et d'autres canaux liés aux ventes.

Transferts internationaux : le Prestataire est autorisé à transférer les Données personnelles vers tout pays situé en dehors du territoire d'origine de la collecte desdites Données personnelles. Ces transferts doivent être effectués en conformité avec les Lois applicables en matière de protection des données 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 la région, et :

- a) Les transferts de données personnelles en dehors de l'Espace économique européen (« EEE ») et du Royaume-Uni sont autorisés : (i) si le transfert de données personnelles est destiné à un destinataire situé dans un pays dont la Commission européenne, le Secrétaire d'État britannique et/ou le Bureau du Commissaire à l'information du Royaume-Uni ont décidé qu'il offrait une protection adéquate des données personnelles; et (ii) à un destinataire qui a signé des clauses contractuelles types adoptées ou approuvées par la Commission européenne, le Secrétaire d'État britannique et/ou le Bureau du Commissaire à l'information du Royaume-Uni.

Le Prestataire peut transférer les Données personnelles 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 personnelles; (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. De manière générale, en acceptant le présent ATD, le Client donne son autorisation pour que Stoneware, Inc. puisse transférer des Données personnelles au-delà des frontières dans la mesure où Stoneware respecte les Lois applicables sur la protection des données. À cet égard, l'annexe D « Transferts internationaux de données » s'applique entre le responsable du traitement et le fournisseur, le cas échéant.

Les Données des clients sont susceptibles d'être consultées par des sous-traitants secondaires, conformément aux dispositions de l'Annexe B du présent Accord, dans des pays tiers comme les États-Unis. Ce traitement s'effectue avec les garanties appropriées exigées pour les transferts vers des pays tiers, notamment par des Clauses contractuelles types. Chaque transfert de données au sein du groupe est réalisé conformément à l'Accord de transfert de données intragroupe du Prestataire,

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 personnelles (y compris le personnel, les agents et le sous-traitant du Fournisseur) (une « Personne autorisée ») est soumise à une obligation stricte de confidentialité (qu'il s'agisse d'une obligation contractuelle ou d'une obligation légale) et ne doit permettre à aucune personne de traiter les Données personnelles qui ne relève pas d'une telle obligation de confidentialité. Le Fournisseur doit s'assurer que toutes les Personnes autorisées traitent les Données personnelles uniquement si cela est nécessaire aux fins autorisées. De plus, le Fournisseur ne doit pas exploiter commercialement les Données personnelles.

- c. **Utilisation de l'intelligence artificielle** : Le Prestataire utilise la technologie de l'intelligence artificielle (l'« IA ») en relation avec certaines de ses offres, notamment LanSchool On-Task Monitoring. L'IA est utilisée pour interpréter la signification de l'objectif de la classe et d'analyser les données déjà capturées sur les étudiants. Elle ne recueille aucun renseignement supplémentaire à propos des utilisateurs outre ceux concernant les exigences standard relatives au produit. Aucune prise de décision automatique, hormis une simple identification, ne devrait 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 Prestataire 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 Prestataire 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 des mesures techniques et organisationnelles appropriées pour protéger les Données personnelles (i) contre la destruction accidentelle ou illégale, et (ii) la perte, l'altération, la divulgation non autorisée ou l'accès aux Données personnelles (un « Incident de sécurité »). L'annexe C contient les mesures techniques et organisationnelles (TOM) de LanSchool Air.

Sous-traitance ultérieure : Le Prestataire accepte que tout sous-traitant 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 énuméré à l'Annexe B. Nonobstant cette disposition, le Responsable du traitement autorise le Prestataire à engager de nouveaux sous-traitants ultérieurs (y compris le remplacement de sous-traitants existants) pour le traitement des Données personnelles, à condition que : (i) le Prestataire 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 Prestataire impose des conditions de protection des données à tout sous-traitant ultérieur qu'il désigne pour protéger les Données personnelles selon des normes substantiellement similaires à celles prévues par le présent ATD. Si le responsable du traitement refuse de consentir à la nomination par le fournisseur d'un nouveau sous-processeur tiers, ce qui ne doit pas être refusé de manière déraisonnable, alors soit le

fournisseur ne nommera pas le sous-traitant ultérieur, soit le responsable du traitement peut décider de résilier le contrat, à condition que le responsable du traitement ait des motifs substantiels et documentés pour s'opposer au changement.

Coopération et droits des personnes concernées : Le fournisseur doit fournir une assistance raisonnable et sans tarder au responsable du traitement pour permettre au responsable du traitement de répondre : i) à toute demande d'une personne concernée d'exercer l'un de ses droits en vertu de la loi en vigueur sur la protection des données (y compris ses droits d'accès, de correction, d'opposition, effacement et portabilité des données personnelles, le cas échéant); ii) toute autre correspondance, demande ou plainte reçue d'une personne concernée, d'un régulateur ou d'un autre tiers en relation avec le traitement des données personnelles. Pour éviter tout doute, les demandes des personnes concernées (DPC) doivent être présentées par le responsable du traitement en soumettant une [demande formelle au moyen du formulaire Web de confidentialité des DPC de Stoneware](#).

Incidents de sécurité : Dès qu'il a connaissance d'un Incident de sécurité, le Fournisseur informe le Responsable du traitement sans retard excessif et fournit toutes les informations et la coopération opportunes que le Responsable du traitement peut exiger pour remplir ses obligations de notification de violation des Données personnelles en vertu de la Législation sur la protection des données (et conformément aux délais requis par celle-ci). Le Fournisseur doit également prendre les mesures et les mesures nécessaires pour remédier ou atténuer les effets de l'Incident de sécurité et doit tenir le Responsable du traitement informé de tous les développements liés à l'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 restituer au responsable du traitement toutes les données personnelles (y compris toutes les copies des données personnelles) en sa possession ou sous son contrôle (y compris les données personnelles sous-traitées à un tiers pour le traitement). Si le responsable du traitement ne donne pas d'autres instructions au fournisseur, le calendrier de conservation des données du fournisseur, tel qu'énoncé à l'annexe A, s'appliquera. Cette exigence ne s'applique pas dans la mesure où le fournisseur est tenu par une loi en vigueur sur la protection des données de conserver tout ou partie des données personnelles, auquel cas le fournisseur doit isoler et protéger les données personnelles de tout traitement ultérieur, sauf dans la mesure requise par une telle loi.

Audit : durant la validité du présent Accord et pendant une durée de trois ans suivant sa résiliation ou son expiration, le Prestataire 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 Prestataire, 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 Prestataire; et (iii) les réponses aux questionnaires visant à évaluer le respect par le Prestataire 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 réglementation 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 personnelles traitées par le prestataire; 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 Prestataire 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 Prestataire 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 Contrat à la date indiquée ci-dessus.

Stoneware, Inc.

Signature : _____

Nom en caractères d'imprimerie : Kimberly Page

Titre : Directeur des opérations stratégiques

Client

Signature : _____

Nom en caractères d'imprimerie : _____

Titre : _____

ANNEXE A – DÉTAILS DU TRAITEMENT

Type de données et personnes concernées	Période de conservation	Nature, objectif et sujet
Données relatives à l'interface des apprenants : <ul style="list-style-type: none"> • L'identificateur global unique (GUID) généré automatiquement unique de l'apprenant • La pièce d'identité de l'apprenant telle que fournie. • Le prénom de l'apprenant. • Le nom de famille de l'apprenant. • L'adresse courriel de l'apprenant. • Le nom de connexion de l'apprenant. • La date à laquelle cet objet apprenant a été créé. • La date à laquelle cet objet apprenant a été mis à jour. 	<p>Les données seront archivées à la demande de l'utilisateur ou après un an d'inactivité de la licence ou de la période d'essai. Les données archivées sont éliminées après 90 jours.</p>	<p><i>Stockage des données</i> (enregistrer, héberger, consigner, archiver ou stocker de toute autre manière les données des clients);</p> <p><i>Accès aux données</i> (récupérer, copier, examiner, modifier, transporter, numériser ou autrement accéder aux données du client);</p>
Données relatives à l'interface des employés de l'établissement d'enseignement : <ul style="list-style-type: none"> • Le GUID unique généré automatiquement de l'enseignant • La pièce d'identité de l'employé de l'établissement d'enseignement. • Le prénom de l'employé de l'établissement d'enseignement. • Le nom de famille de l'employé de l'établissement d'enseignement. • L'adresse courriel de l'employé de l'établissement d'enseignement. • L'ID MongoDB de l'utilisateur infonuagique qui correspond à cet objet d'enseignant. • Jetons d'accès • La date à laquelle cet objet d'employé d'établissement d'enseignement a été créé. • La date à laquelle cet objet d'employé d'établissement d'enseignement a été mis à jour. 	<p>Les données seront archivées à la demande de l'utilisateur ou après un an d'inactivité de la licence ou de la période d'essai. Les données archivées sont éliminées après 90 jours.</p>	<p><i>Stockage des données</i> (enregistrer, héberger, consigner, archiver ou stocker de toute autre manière les données des clients);</p> <p><i>Accès aux données</i> (récupérer, copier, examiner, modifier, transporter, numériser ou autrement accéder aux données du client);</p> <p><i>Analyse des données</i> (enquête, test, étude, interprétation, organisation, rapport ou autre analyse des données client.)</p>
Données relatives à l'interface client : <ul style="list-style-type: none"> • Le GUID unique généré automatiquement du client • L'identifiant de connexion de l'apprenant actuel. Il peut s'agir d'une adresse courriel ou d'un nom d'utilisateur. 	<p>Les données seront archivées à la demande de l'utilisateur ou après un an d'inactivité de la licence ou de la période d'essai. Les données archivées sont éliminées après 90 jours.</p>	<p><i>Stockage des données</i> (enregistrer, héberger, consigner, archiver ou stocker de toute autre manière les données des clients);</p> <p><i>Accès aux données</i> (récupérer, copier,</p>

<ul style="list-style-type: none"> • L'ID MongoDB du dispositif correspondant de la base de données principale. • La date à laquelle cet objet client a été créé. • La date à laquelle cet objet client a été mis à jour. 		<p>examiner, modifier, transporter, numériser ou autrement accéder aux données du client);</p> <p><i>Analyse des données</i> (enquête, test, étude, interprétation, organisation, rapport ou autre analyse des données client.)</p>
<p>Données relatives à la liste de classes</p> <ul style="list-style-type: none"> • Le GUID unique généré automatiquement de la classe • Le nom de cette classe. Ceci est obligatoire. • L'identifiant de la classe fourni par le système d'information pour apprenants. • L'identifiant de l'établissement d'enseignement fourni par le système d'information pour apprenants. • La période de classe ou autre désignation qui distingue cette classe des autres classes du même type. • Le responsable de cette liste de cours. • Les objets enseignants pour les enseignants qui ont accès à cette liste de classes. L'interface de l'enseignant est définie ci-dessous. • Les objets des apprenants pour les apprenants qui appartiennent à cette liste de classes. • Les objets clients pour les dispositifs qui appartiennent à cette liste de classes. • L'ID de l'utilisateur qui a modifié cette liste de cours pour la dernière fois. • La date à laquelle cette liste de classes a été créée. • La date à laquelle cette liste de classes a été mise à jour. • 	<p>Les données seront archivées à la demande de l'utilisateur ou après un an d'inactivité de la licence ou de la période d'essai. Les données archivées sont éliminées après 90 jours.</p>	<p><i>Stockage des données</i> (enregistrer, héberger, consigner, archiver ou stocker de toute autre manière les données des clients);</p> <p><i>Accès aux données</i> (récupérer, copier, examiner, modifier, transporter, numériser ou autrement accéder aux données du client);</p> <p><i>Analyse des données</i> (enquête, test, étude, interprétation, organisation, rapport ou autre analyse des données client.)</p>
<p>Données relatives à l'organisation</p> <ul style="list-style-type: none"> • Le GUID unique généré automatiquement de l'organisation • Le nom de l'organisation. 	<p>Les données seront archivées à la demande de l'utilisateur ou après un an d'inactivité de la licence ou de la période</p>	<p><i>Stockage des données</i> (enregistrer, héberger, consigner, archiver ou stocker de toute autre</p>

<ul style="list-style-type: none"> • L'identifiant attribué à cette organisation. • L'adresse municipale principale. • Les renseignements sur l'adresse municipale secondaire. • La ville de l'organisation. • L'État ou la province de l'organisation. • Le code postal de l'organisation. • Le pays de l'organisation. • Les coordonnées administratives. • Les coordonnées techniques. • Les coordonnées de facturation. • Un indicateur précisant si cette organisation dispose d'un agent de site. • La date à laquelle cette organisation a été créée. • La politique de sécurité par défaut pour l'organisation. • Coordonnées de l'organisation : prénom, nom de famille, numéro de téléphone, adresse courriel. 	<p>d'essai. Les données archivées sont éliminées après 90 jours.</p>	<p>manière les données des clients); <i>Accès aux données</i> (récupérer, copier, examiner, modifier, transporter, numériser ou autrement accéder aux données du client); <i>Analyse des données</i> (enquête, test, étude, interprétation, organisation, rapport ou autre analyse des données client.)</p>
<p>Données de l'utilisateur</p> <ul style="list-style-type: none"> • Le GUID unique généré automatiquement de l'utilisateur • Un ensemble de paires de valeurs clés de tous les ID actuels de l'utilisateur, • Le prénom de l'utilisateur. • Le nom de famille de l'utilisateur. • L'adresse courriel de l'utilisateur. • Autorisations directement attribuées à cet utilisateur. • Une référence à l'organisation dont cet utilisateur appartient. • Un sous-ensemble d'identifiants d'utilisateur qu'un utilisateur peut utiliser pour une connexion. • Horodatage de la dernière connexion réussie de l'utilisateur au système. • Horodatage de la première fois que l'utilisateur a échoué l'authentification au cours de la dernière heure. • L'adresse IP de l'endroit où la dernière connexion a eu lieu. • L'adresse IP de l'endroit où la dernière connexion a échoué. 	<p>Les données seront archivées à la demande de l'utilisateur ou après un an d'inactivité de la licence ou de la période d'essai. Les données archivées sont éliminées après 90 jours.</p>	<p><i>Stockage des données</i> (enregistrer, héberger, consigner, archiver ou stocker de toute autre manière les données des clients); <i>Accès aux données</i> (récupérer, copier, examiner, modifier, transporter, numériser ou autrement accéder aux données du client); <i>Analyse des données</i> (enquête, test, étude, interprétation, organisation, rapport ou autre analyse des données client.)</p>

<ul style="list-style-type: none"> • L'horodatage de la dernière tentative de connexion échouée. • Un compteur pour le nombre de tentatives de connexion échouées consécutives. • Les autorisations accordées à l'utilisateur. Généré en combinant toutes les autorisations des groupes de l'utilisateur. • La date à laquelle cet utilisateur a été créé. • La date à laquelle cet utilisateur a été mis à jour. 		
Données relatives au journal d'activités <ul style="list-style-type: none"> • Historique de navigation Web des étudiants (URL, horodatage) • Historique des applications des étudiants (nom de l'application, horodatage) • Historique des messages de clavardage en classe (expéditeur, réception, contenu du message, horodatage) • Journal des activités administratives (identifiants d'utilisateur, type d'activités, horodatage) • Captures d'écran des étudiants, métadonnées de l'onglet, contenu de la page d'onglet active • Objectifs de classe des enseignants. 	<p>À la demande de l'utilisateur pour suppression ou après 45 jours.</p>	<p><i>Stockage des données</i> (enregistrement, hébergement, journalisation, archivage ou autre forme de stockage des données des clients); <i>accès aux données</i> (récupération, copie, examen, modification, numérisation ou autre moyen d'accès aux données des clients); <i>analyse des données</i> (enquête, test, étude, interprétation, organisation, production de rapports ou autre moyen d'analyse des données des clients).</p>
Données de licence (exclut les données personnelles)	<p>Ces données sont conservées aussi longtemps que nécessaire pour se conformer aux obligations légales, pour faire respecter nos contrats, etc. Elles ne comprennent pas les données personnelles.</p>	<p><i>Stockage des données</i> (enregistrer, héberger, consigner, archiver ou stocker de toute autre manière les données des clients); <i>Accès aux données</i> (récupérer, copier, examiner, modifier, transporter, numériser ou autrement accéder aux données du client); <i>Analyse des données</i> (enquête, test, étude, interprétation, organisation, rapport ou autre analyse des données client.)</p>

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

ANNEXE B – SOUS-TRAITANTS

Nom	Données	Emplacement de stockage	Objectif
Amazon Web Services	Toutes les données de l'utilisateur comme décrit à l'annexe A	Australie, É.-U. ou R.-U. <i>(des restrictions de transfert régionales sont appliquées, ce qui signifie par exemple que les données européennes sont stockées exclusivement au R.-U.).</i>	Fournisseur de services informatiques pour l'infrastructure de l'application. Toutes les données sont traitées par l'application.
Datadog	Données d'application, adresse IP et nom d'utilisateur	États-Unis	Outil de collecte de journaux.
Hubspot	Prénom, nom de famille, courriel, téléphone, nom de l'entreprise, titre, étiquette géographique (p. ex., État), industrie	É.-U., UE.	Intégration.
MongoDB Atlas	Toutes les données de l'utilisateur comme décrit à l'annexe A	Australie, É.-U. ou R.-U. <i>(des restrictions de transfert régionales sont appliquées, ce qui signifie par exemple que les données européennes sont stockées exclusivement au R.-U.).</i>	Pour que l'application fonctionne correctement.
Pendo	Analyse de l'utilisation de l'application, commentaires soumis par les utilisateurs, prénom de l'utilisateur final, nom de famille, courriel et nom de l'organisation.	États-Unis	Améliorer la fonctionnalité et la convivialité 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 de l'industrie en vigueur pour la protection et l'utilisation responsable des Données personnelles, y compris, mais sans s'y limiter, les contrôles suivants :

Technique	Portée	Contrôles
Accès	Connexions (système et application).	Politiques de mot de passe basées sur NIST (authentification multifacteurs pour l'accès et les interfaces de niveau administrateur.)
Chiffrement	Stockage des données au repos et en transit.	AES 256-GCM (au repos) TLS 1.2, 1.3 (en transit)
Test de sécurité des applications statiques	Toutes les images du serveur et du microservice, Tous les clients binaires et les extensions/branchements.	Analyses et surveillance régulières des vulnérabilités.
Test dynamique de sécurité des applications	API d'applications externes.	Balayages d'applications Web, Essais de pénétration (Tests internes réguliers.)
Renforcement des bonnes pratiques CIS	Fournisseur de plateforme infonuagique, instances de serveur.	Vérifications de conformité infonuagique au CIS, surveillance de la sécurité infonuagique, Évaluations régulières des points de référence des serveurs L2 du CIS.
Analyse de la composition du logiciel	Dépendances à code source ouvert de tiers.	Effectuer régulièrement des vérifications de vulnérabilité, la surveillance des référentiels.
Évaluation des infrastructures	Fournisseur de plateforme infonuagique.	Examens réguliers de tous les réseaux définis par logiciel (SDN) (identifier la segmentation du réseau, la configuration du pare-feu et les mauvaises configurations d'accès aux ressources).
Pare-feu des applications Web (WAF)	Applications Web de production.	Protection WAF (règles de base pour les attaques courantes).
Analyse de code statique	Code exclusif.	Une analyse régulière du code est effectuée à l'aide d'un outil commercial, des revues de code sécurisées sont effectuées lors des fusions de code.
Collecte de journaux	Fournisseur de plateforme infonuagique, Application.	Transactions API de la plateforme infonuagique (les journaux datant de plus de 360 jours sont purgés et accessibles par l'ingénierie) Journalisation WAF pour la détection des bords (les journaux

		datant de plus de 90 jours sont purgés, accessibles par l'ingénierie) Sous-traitants ultérieurs, voir l'annexe B, pour les besoins de l'application.
Infrastructure comme code	Fournisseur de plateforme infonuagique.	L'infrastructure en tant que code est utilisée pour automatiser les déploiements d'infrastructure et améliorer l'immuabilité, la mauvaise configuration de l'infrastructure.

Organisationnel	Portée	Contrôles
Réponse aux incidents (y compris les violations de données)	Événements de sécurité liés aux produits en production.	Plan de réponse aux incidents liés aux produits, conformément à la norme NIST 800-61 et aux processus internes de l'équipe de réponse aux incidents de sécurité des produits (ERISP) de Lenovo.
Liste des fournisseurs de confiance	Tous les sous-traitants qui s'intègrent directement aux produits en production.	Évaluations de sécurité standard des fournisseurs intégrés, CSTD pour les fournisseurs de traitement des données personnelles.
Gestion des vulnérabilités	Systèmes d'exploitation du serveur, Contenants de station d'accueil, Clients, Produits en production.	Un programme qui utilise divers outils pour aider à identifier les vulnérabilités dans tous les systèmes informatiques.
Comité d'examen de la sécurité des logiciels (CESL)	Produits en production.	Les examens du CESL sont effectués régulièrement. Pendant les examens, toutes les mesures techniques et organisationnelles sont évaluées pour le produit en question.
Politique de conservation des données	Informations personnelles identifiables, Données d'application, Produits en production.	À la demande de l'utilisateur, ou après un an d'inactivité de la licence ou de la période d'essai, les données personnelles seront archivées. Les données archivées sont éliminées après 90 jours.
Sensibilisation à la sécurité et au respect de la vie privée	Tous les employés (cours Fondamentaux de la protection de la vie privée [Privacy Basics] et Essentiels de la sécurité [Security Essentials])	Formation semestrielle pour les équipes spécialisées en informatique et en produits sur des sujets de sécurité avancés, tels que les 10 premiers de l'OWASP.

Sécurité continue	Produits en production.	Application régulière des mesures techniques.
Examens de conformité Opensource.	Produits en production.	Des évaluations sont effectuées pour s'assurer que les licences et attributions appropriées sont fournies dans le logiciel distribué.
Reprise après sinistre	Produits en production.	Suivre le NIST-800-34 comme guide pour maximiser le RTO et le RPO.
Politique de sauvegarde	Bases de données, Code, Journaux.	<p>La politique générale exige plusieurs sauvegardes, dont l'une doit être hors site à partir de l'emplacement de stockage principal,</p> <p>Des sauvegardes régulières de la base de données ont lieu quotidiennement (deux fois par jour), hebdomadairement et mensuellement. Les sauvegardes quotidiennes sont conservées pendant sept jours. Les sauvegardes hebdomadaires sont conservées pendant quatre semaines. Les sauvegardes mensuelles sont conservées pendant 13 mois. La fenêtre de restauration est de 12 heures.</p> <p>Les sauvegardes du code source de l'application ont lieu quotidiennement et sont conservées pendant 360 jours.</p> <p>Journaux de production : Datadog – Les journaux sont en ligne pendant sept jours. Les journaux sont ensuite entreposés à long terme pendant 180 jours, puis purgés.</p> <p>Équilibreur de charge – Les journaux sont conservés pendant 360 jours, puis purgés.</p>

		<p>Pare-feu d'application Web – Les journaux sont conservés pendant 90 jours, puis éliminés.</p> <p>Cloud Trail – Les journaux sont conservés pendant 90 jours, puis purgés.</p> <p>Cloud Watch – Les journaux sont conservés pendant 360 jours et ensuite purgés.</p> <p>MongoDB – Les journaux sont conservés pendant toute la durée du projet.</p>
--	--	---

ANNEXE D – CONTRAT INTERNATIONAL DE TRANSFERT DE DONNÉES

La présente Annexe définit les exigences en matière de protection des données (y compris les exigences en vertu de la Législation applicable sur la protection de la vie privée) qui s'appliquent : (i) à l'Exportateur de données (Responsable du traitement) lorsqu'il transfère des Données personnelles à l'Importateur de données (Stoneware, Inc.), ses sociétés affiliées et/ou ses Sous-traitants, pour le Traitement des données; et (ii) à l'Importateur de données lorsqu'il reçoit des Données personnelles d'un Exportateur de données pour le Traitement des données.

L'Importateur de données garantit et s'engage à ce qu'à tout moment il :

- a) traitera les Données transférées conformément à la Législation applicable sur la protection de la vie privée et fournira une assistance raisonnable et opportune à l'exportateur de données si nécessaire pour l'aider à se conformer à ses obligations en vertu de la Législation applicable sur la protection de la vie privée; et
- b) n'exécutera pas sciemment ses obligations en vertu du présent Contrat de manière à amener l'Exportateur de données à violer l'une de ses obligations en vertu de la Législation applicable sur la protection de la vie privée applicables.

L'Exportateur de données confirme qu'il a pris les mesures nécessaires pour assurer la conformité aux lois applicables en matière de protection des données, y compris le transfert transfrontalier des exigences en matière de données personnelles, comme l'obtention des consentements explicites des Personnes concernées eu égard au transfert à l'étranger de leurs données personnelles, avoir informé les autorités compétentes du transfert ou avoir demandé leur approbation à cet égard, ou d'autres obligations sous-jacentes, selon le cas.

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 Législation sur la protection des données, les dispositions suivantes s'appliquent :

(A) « Législation sur la protection des données de l'UE » 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 sur la vie privée en ligne (directive 2002/58/CE); et (c) toute Législation nationale applicable sur la protection des données.

(B) Le Fournisseur informera rapidement le Responsable du traitement (a) de toute exigence en vertu de la Législation sur la protection des données européenne qui nécessiterait de traiter les données personnelles d'une manière autre que celle prévue par 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 Législation sur la protection des données européenne applicable.

(C) **Transferts de données** : Si le Fournisseur ou ses Sous-traitants sont situés en dehors de l'EEE, le Fournisseur et le Responsable du traitement exécutent par les présentes les clauses contractuelles

types de Responsable du traitement à sous-traitant telles que définies 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](#) tel que modifié ou remplacé de temps à autre (les « Clauses contractuelles types de responsable du traitement à sous-traitant ») et les intègrent par les présentes dans le présent Addenda par référence. Les parties reconnaissent et conviennent que :

- a. Le Fournisseur et le Responsable du traitement doivent chacun se conformer à leurs obligations respectives dans les Clauses contractuelles types de responsable du traitement à sous-traitant;
- b. En cas de conflit ou d'incohérence entre les Clauses contractuelles types de responsable du traitement à sous-traitant et le présent Addenda ou le contrat de base, les Clauses contractuelles types de responsable du traitement à sous-traitant prévaudront dans la mesure du conflit; et
- c. Les informations contenues dans les tableaux suivants sont par les présentes incorporées aux Clauses contractuelles types de responsable du traitement à sous-traitant entre les Parties :

***Renseignements à intégrer dans les
Clauses contractuelles types de responsable du traitement à sous-traitant entre le
Responsable du traitement et le Fournisseur :***

Clause 9. Utilisation de sous-traitants	L'option 2 AUTORISATION GÉNÉRALE ÉCRITE est sélectionnée. L'Importateur de données doit fournir des renseignements au moins 30 jours à l'avance, conformément à la clause « Sous-traitement »
Clause 17. Loi applicable	Ces Clauses doivent être interprétées conformément à la loi applicable énoncée dans le contrat de base des Parties, sauf si cette loi applicable n'est pas celle d'un État membre de l'UE qui permet des droits de bénéficiaire tiers. Dans un tel cas, les Parties conviennent que ces Clauses seront régies par la loi de l'IRLANDE.
Clause 18 (b). Choix du forum et de la juridiction	Les Parties conviennent que tout différend découlant des présentes Clauses sera résolu par les tribunaux de l'IRLANDE.

***Renseignements à intégrer à l'annexe 1, partie A des Clauses contractuelles types de responsable
du traitement à sous-traitant :***

Nom de l'exportateur de données	Le 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

<i>Nom, poste et coordonnées de la personne-ressource de l'exportateur de données</i>	À remplir par l'exportateur de données
<i>Activités de l'exportateur de données pertinentes aux données transférées en vertu des présentes Clauses</i>	À remplir par l'exportateur de données
<i>Signature et date de l'exportateur de données</i>	À remplir par l'exportateur de données
<i>Rôle de l'exportateur de données</i>	Responsable du traitement
<i>Nom de l'importateur de données</i>	Fournisseur (Stoneware, Inc.) et ses sous-traitants
<i>Adresse de l'importateur de données</i>	Stoneware, Inc. 8001 Development Drive, Morrisville, NC 27560 États-Unis d'Amérique
<i>Nom, poste et coordonnées de la personne-ressource de l'importateur de données</i>	Dan Verwolf, Directeur privacy@lanschool.com
<i>Activités de l'importateur de données pertinentes aux données transférées en vertu des présentes Clauses</i>	Comme indiqué dans la partie B de l'annexe 1
<i>Signature et date de l'importateur de données</i>	À remplir par l'importateur de données
<i>Rôle de l'importateur de données</i>	Processeur

Renseignements à intégrer à l'annexe 1, partie B et C des Clauses contractuelles types de responsable du traitement à sous-traitant :

<i>Catégories de personnes concernées</i>	Comme indiqué à l'annexe A ci-dessus
<i>Catégories de données personnelles</i>	Comme indiqué à l'annexe A ci-dessus
<i>Données sensibles</i>	Comme indiqué à l'annexe A ci-dessus
<i>Fréquence du transfert</i>	Fréquence continue, tant que la licence LSA est active
<i>Nature du traitement</i>	Comme indiqué à l'annexe A ci-dessus
<i>Objectif du traitement</i>	Comme indiqué à l'annexe A ci-dessus
<i>Période pendant laquelle les données personnelles seront conservées</i>	Comme indiqué à l'annexe A ci-dessus
<i>Sujet, nature et durée du traitement effectué par les sous-traitants</i>	Comme indiqué à l'annexe B ci-dessus
<i>Autorité de contrôle compétente chargée de veiller au respect par l'exportateur de données du règlement (UE) 2016/679 ty.</i>	L'autorité de contrôle qui agira en tant qu'autorité de contrôle compétente sera celle de l'État membre de l'UE où 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, alors l'autorité de contrôle 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 personnelles 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.
--	---

Renseignements à intégrer à l'annexe 2 des Clauses contractuelles types de responsable du traitement à sous-traitant :

<i>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.</i>	Comme indiqué à l'annexe C ci-dessus
--	--------------------------------------

Information à incorporer dans l'annexe 3 des clauses contractuelles types de responsable du traitement à sous-traitant :

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

2. Royaume-Uni (R.-U.)

Si les services du Fournisseur sont fournis au Responsable du traitement au sein du Royaume-Uni, ou si la nature des Données personnelles déclenche l'application de la Loi de 2018 sur l'Union européenne (retrait) (le « RGPD du Royaume-Uni ») et de la Data Protection Act de 2018 (la « DPA de 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 britannique comme offrant une protection adéquate des données à caractère personnel (une « Décision d'adéquation ») seront autorisés en vertu du ou des contrats sans qu'il soit nécessaire d'approuver les clauses contractuelles types du Royaume-Uni.
- (B) Les pays de l'EEE sont réputés être soumis à une décision d'adéquation aux fins de transferts de données personnelles du Royaume-Uni à l'EEE.
- (C) En l'absence d'une décision d'adéquation, le Responsable du traitement et le Fournisseur conviennent d'exécuter l'addenda approuvé pour le transfert international de données du Royaume-Uni aux clauses contractuelles types de la Commission européenne pour les transferts internationaux de données (<https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf>).

Partie 1 : Tableaux / Tableau 1 : Fêtes

Renseignements à intégrer dans « Partie 1 : Tableaux » de l'Addenda international sur le transfert de données aux Clauses contractuelles types de la Commission européenne :		
Date de début	Comme indiqué ci-dessus	
Les Parties	Exportateur (qui envoie le transfert restreint)	Importateur (qui reçoit le transfert restreint)
Détails des parties	<p>Nom légal complet, adresse principale (s'il s'agit d'une société) : Conformément aux informations du 2^e tableau de l'art. 1. Espace économique européen (EEE) à l'annexe D</p> <p>Numéro d'enregistrement officiel (le cas échéant) (numéro d'entreprise ou identifiant similaire) : Selon le client identifié dans le contrat de vente</p>	<p>Nom légal complet, adresse principale (s'il s'agit d'une société) : Conformément aux informations du 2^e tableau de l'art. 1. Espace économique européen (EEE) à l'annexe D</p> <p>Numéro d'enregistrement officiel (le cas échéant) (numéro d'entreprise ou identifiant similaire) : 35-2097171 enregistré dans l'État de l'Indiana</p>
Personne-ressource principale	Nom complet (facultatif), titre du poste, coordonnées, y compris le courriel : Conformément aux informations du 2 ^e tableau de l'art. 1. Espace économique européen (EEE) à l'annexe D	Nom complet (facultatif), titre du poste, coordonnées, y compris le courriel : Conformément aux informations du 2 ^e tableau de l'art. 1. Espace économique européen (EEE) à l'annexe D

Tableau 2 : SCC sélectionnés, modules et clauses sélectionnées

Addenda aux CCT de l'UE	Voir l'annexe D, art. 1 ci-dessus
--------------------------------	-----------------------------------

Tableau 3 : Renseignements sur l'annexe

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

Tableau 4 : Mettre fin à cet addenda lorsque l'addenda approuvé change

Mettre fin à cet addenda lorsque l'addenda approuvé change	Quelles parties peuvent mettre fin au présent addenda comme indiqué à l'article Error! Reference source not found. : <input checked="" type="checkbox"/> Importateur <input type="checkbox"/> Exportateur <input type="checkbox"/> ni l'une ni l'autre des parties
---	--

Renseignements à intégrer dans « Partie 2 : Clauses obligatoires » de l'Addenda international sur le transfert de données aux Clauses contractuelles types de la Commission européenne :

Partie 2 : Clauses obligatoires de l'addenda approuvé, qui est le modèle d'addenda B.1.0 publié par l'ICO 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 personnelles est assujéti 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 se conformer à la norme RGPD en ce qui concerne tout Traitement des Données personnelles régi par la Loi fédérale suisse sur la protection des données; (iii) les Clauses contractuelles types de l'UE seront régies par les lois de la Suisse 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) le terme « État membre » figurant dans les Clauses contractuelles types de l'UE ne sera pas interprété de manière à priver les Personnes concernées en Suisse de la possibilité d'exercer leurs droits dans leur lieu de résidence habituel (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 seront entendues 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

En cas de transfert de Données personnelles soumises à la loi générale sur la protection des données personnelles du Brésil (telle que modifiée par la Loi n° 13.853 du 8 juillet 2019) (« LGPD »), et si Lenovo, le Fournisseur ou les deux sont situés dans des Pays non adéquats, les Clauses contractuelles standard de responsable du traitement à sous-traitant telles que référencées dans le présent document s'appliqueront avec les modifications suivantes :

- (i) l'autorité de contrôle des clauses contractuelles types de responsable du traitement à sous-traitant est l'autorité nationale de protection des données du Brésil (ANPD);
- (ii) la loi applicable conformément à la clause 17 des clauses contractuelles types de responsable du traitement à sous-traitant est la LGPD;
- (iii) le choix du lieu du procès et de la juridiction conformément à la clause 18 des clauses contractuelles types de responsable du traitement à sous-traitant sera le droit brésilien dans le cas où le transfert de données est exclusivement soumis à la LGPD; et
- (iv) toute référence au RGPD dans les clauses contractuelles types de responsable du traitement à sous-traitant inclut également la référence aux dispositions équivalentes de la LGPD (telle que modifiée ou remplacée).

5. Afrique du Sud

Si les services du Fournisseur sont fournis au Responsable du traitement en Afrique du Sud ou dans une autre juridiction soumise à la Protection of Personal Information Act (POPIA), les dispositions supplémentaires suivantes s'appliquent :

- (A) **Personne concernée** : une personne physique qui peut être identifiée par référence à un nom, un numéro unique, des données de localisation, un identifiant en ligne, ou à un ou plusieurs facteurs spécifiques 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 personnelles applicables conformément à la Loi australienne sur la confidentialité des données dans sa version modifiée.

ANNEXE E – DISPOSITIONS SUPPLÉMENTAIRES

1. California Consumer Privacy Act (« CCPA »).

Stoneware, Inc. est une entreprise. De plus, le Fournisseur est le Fournisseur de services du Client et traitera les Données personnelles au nom du Client.

- d. Le Fournisseur ne doit pas vendre les Données personnelles ou les Renseignements exclusifs. « Vendre » désigne la vente, la location, la libération, la divulgation, la diffusion, la mise à disposition, le transfert ou la communication de toute autre façon de l'information à des fins monétaires ou autres contreparties de valeur.
- e. Le Fournisseur ne doit pas conserver, utiliser ou divulguer les Données personnelles : (a) à des fins autres que celles spécifiques de l'exécution des services énoncés dans le Contrat pour Stoneware, Inc. ou tel que permis par la CCPA et ses règlements d'application, (b) à des fins commerciales autres que la prestation des services spécifiés dans le contrat avec l'entreprise, ou (c) en dehors de la relation commerciale directe entre la personne et Stoneware, Inc.
- f. Le présent CSTD sert à certifier que le Fournisseur comprend les exigences de la CCPA applicables aux entreprises et aux fournisseurs de services, y compris les restrictions du Code civil de la Californie § 1798.140(w)(2)(A), et s'y conformera.