Contrato do Processador de Dados do LanSchool Air (DPA)

Este Contrato do Processador de Dados do LanSchool Air (que aborda exigências de privacidade e segurança) e seus anexos (Data Processor Agreement, "**DPA**") fazem parte do Contrato de Vendas da Stoneware ou de outro contrato por escrito ou eletrônico celebrado entre a Stoneware, Inc. e o Cliente ("**Contrato**") para a aquisição de serviços do LanSchool Air da Stoneware, Inc. para refletir o acordo das partes em relação ao Processamento de Dados Pessoais.

Este DPA complementa qualquer contrato entre as partes em relação ao objeto deste documento; e entrará em vigor a partir do momento em que o Cliente aceitar os Termos de Serviço do LanSchool Air ("**Data de entrada em vigor**").

Após a assinatura do Contrato e aceitação dos Termos de serviço do LanSchool Air, este DPA passará a vincular legalmente as partes; e você (Cliente) está celebrando este DPA em nome do Cliente, na medida exigida pelas Leis e Regulamentos de proteção de dados, privacidade e segurança aplicáveis, incluindo leis e regulamentos de privacidade e segurança de ensino e estudantes, em nome de suas Afiliadas Autorizadas, na medida em que a Stoneware processa Dados Pessoais em relação aos quais essas Afiliadas Autorizadas se qualificam como a Controladora. O Cliente entende que este DPA é aplicável a todos os usuários e garante que tem os poderes necessários para celebrar este DPA em nome desses usuários.

Poderemos atualizar estes termos para atender a novas exigências legais ou conforme necessário para refletir atualizações operacionais. Se você tiver uma assinatura ativa do LanSchool Air, informaremos por e-mail ou por notificação no próprio produto. As versões arquivadas do DPA estão disponíveis aqui.

Assinatura do DPA:

a) Este DPA é composto por duas partes: o corpo principal do DPA e os Anexos A, B, C, D e E. Este DPA foi pré-assinado em nome da Stoneware, Inc., incluindo as Cláusulas contratuais padronizadas da União Europeia (UE) no Anexo D, como importadora de dados. (Observação: o Anexo D é geralmente aplicável apenas a atividades de processamento que possam envolver a transferência de Dados Pessoais da União Europeia, Espaço Econômico Europeu, Reino Unido e/ou outros países com normas de adequação ou equivalência semelhantes relativas a transferências internacionais de dados). Além disso, representa provisões contratuais que servem como proteção para transferências seguras de dados pessoais pelas leis de proteção de dados aplicáveis.

Para evitar dúvidas, você precisa assinar este DPA na página 5. Se aplicável, o Anexo D será aplicado por referência.

Proteção de dados

Definições: nesta Cláusula, os termos a seguir terão os seguintes significados:

a) "**Controlador**", "**Processador**", "**Subprocessador**", "**Processamento de dados**" e "**Processamento**" (e "**Processar**") terão os significados dispostos na Lei de Proteção de Dados da UE e termos equivalentes na Lei de Proteção de Dados aplicável.

(a) "**Lei de Proteção de Dados aplicável**" refere-se a todas as leis, regras, regulamentos e ordens aplicáveis, bem como a todas as alterações relacionadas, em qualquer jurisdição em que o Fornecedor preste os Serviços LanSchool, inclusive qualquer lei relativa à privacidade, segurança de dados, proteção de dados, violações de dados e confidencialidade, como a Lei de Privacidade do Consumidor da Califórnia (California Consumer Privacy Act, "CCPA") de 2018, a Lei de Direitos de Privacidade da Califórnia (California Privacy Rights Act, "CPRA"), o Regulamento Geral de Proteção de Dados 2016/279 da União Europeia, e suas alterações, substituições ou revogações ao longo do tempo ("RGPD"), a Lei de Proteção de Dados do Reino Unido, de 2018, e suas alterações, a Lei n.º 13.709/18 e suas alterações (Lei Geral de Proteção de Dados, "LGPD"), e os regulamentos implementados (ou a serem implementados) e qualquer lei aplicável, inclusive leis de privacidade de ensino e estudantes nacionais, estaduais e/ou municipais.

b) **"Dados pessoais"** refere-se a informações relacionadas a um indivíduo identificado ou identificável, incluindo, entre outros, alunos, pais e funcionários da escola.

c) **"Titular dos dados"** refere-se a uma pessoa que pode ser identificada direta ou indiretamente, incluindo, entre outros, alunos, pais e funcionários da escola.

d) **"Cliente"** é o Controlador. Apenas para os fins deste DPA, o termo "Cliente" incluirá o Cliente e as Afiliadas Autorizadas.

e) **"Fornecedor"** significa a Stoneware, Inc., que atua como Processador.

(b) **"Exportador dos Dados"** significa uma parte que transfere Dados Pessoais para outra Parte de acordo com o Contrato.

(c) **"Importador de Dados"** refere-se à parte que, conforme este Contrato, recebe os Dados Pessoais do Cliente de outra Parte.

Relacionamento das partes: o Cliente reconhece o Fornecedor como um Processador para processar os Dados Pessoais que estão sujeitos ao Contrato de Vendas da Stoneware, aos Termos de Serviços do LanSchool Air e ao EULA com o Fornecedor. Cada parte cumprirá as obrigações aplicáveis a ela de acordo com a Lei de Proteção de Dados Aplicável.

Limitação do propósito: o Fornecedor processará os Dados Pessoais como um Processador e estritamente de acordo com as instruções documentadas do Controlador ("Propósito permitido") conforme documentado em "Detalhes de processamento", no Anexo A, salvo exigência contrária

estabelecida por Lei de proteção de dados aplicável. O Fornecedor informará imediatamente ao Controlador se tomar conhecimento de que as instruções de Processamento do Controlador infringem a Lei de Proteção de Dados aplicável. Sob nenhuma circunstância o Fornecedor processará os Dados Pessoais para seus propósitos particulares ou de qualquer terceiro, inclusive para fins de marketing. Para fins de esclarecimento, o Fornecedor não enviará comunicações de marketing ou promocionais de qualquer forma aos usuários do Lenovo LanSchool Air aproveitando os dados pessoais obtidos com o uso do Lenovo LanSchool Air. Isso não impedirá que as pessoas recebam comunicações de marketing ou promocionais se estas comunicações se originarem no contexto de canais padrão, como o site da Stoneware ou da Lenovo e outros canais relacionados a vendas.

Transferências internacionais: o Fornecedor poderá transferir os Dados Pessoais para qualquer local fora do país do qual os Dados Pessoais foram coletados em conformidade com as Leis de Proteção de Dados aplicáveis e leis de localização de dados. Com o objetivo de evitar ambiguidades, os dados deverão ser armazenados conforme estabelecido neste Contrato (isto é, seguindo a abordagem/localização determinada para cada região) e:

a) As transferências de Dados pessoais para fora do Espaço Econômico Europeu ("**EEE**") e do Reino Unido são permitidas: (i) se a transferência de Dados pessoais for para um destinatário em um país ao qual a Comissão Europeia, o Secretário de Estado do Reino Unido e/ou o Gabinete do Comissário de Informação do Reino Unido decidiu fornecer proteção adequada aos Dados pessoais; e (ii) a um destinatário que tenha assinado cláusulas contratuais padronizadas adotadas ou aprovadas pela Comissão Europeia, pelo Secretário de Estado do Reino Unido e/ou pelo Gabinete do Comissário de Informação do Reino Unido.

   O Fornecedor poderá transferir os Dados Pessoais para fora do Brasil se: (i) a transferência dos Dados for para um destinatário em um país que a Autoridade Nacional decidiu que fornece proteção adequada para Dados Pessoais; (ii) para um destinatário que assinou cláusulas contratuais padrão adotadas ou aprovadas pela Autoridade Nacional; ou (iii) quando o destinatário conseguir fornecer e demonstrar a implementação de outras proteções de acordo com a Lei de Proteção de Dados do Brasil e a transferência internacional for aprovada pelo Controlador.

b. Em geral, a aceitação deste DPA resulta na aprovação pelo Cliente de que a Stoneware, Inc. poderá transferir Dados Pessoais para outros países se a Stoneware cumprir todas as Leis de Proteção de Dados Aplicáveis. A este respeito, o Anexo D "Transferências de Dados Internacionais" é aplicável entre o Controlador e o Fornecedor quando pertinente.

Os Dados do Cliente poderão ser acessados por subprocessadores, conforme estabelecido no Anexo B deste Contrato, inclusive em países terceiros — como os Estados Unidos —, sendo tais acessos realizados mediante as salvaguardas adequadas exigidas para transferências internacionais, como, por exemplo, as Cláusulas Contratuais Padrão. Todas as transferências de dados entre as partes do grupo são realizadas conforme o Contrato de Transferência de Dados Intragrupo do Fornecedor, o qual inclui as Cláusulas Contratuais Padrão, assegurando a realização segura das transferências internacionais de dados.

Confidencialidade do processamento: o Fornecedor garantirá que qualquer pessoa à qual autorize o processamento dos Dados Pessoais (incluindo funcionários, representantes e subprocessadores do Fornecedor) (uma "Pessoa autorizada") estará sujeita a um dever estrito de confidencialidade (seja um dever contratual ou legal) e não permitirá que qualquer pessoa que não esteja vinculada a esse dever de confidencialidade processe os Dados Pessoais. O Fornecedor garantirá que todas as Pessoas autorizadas processem os Dados Pessoais apenas conforme necessário para o Propósito permitido. Além disso, o Fornecedor não explorará comercialmente os Dados Pessoais.

c. *Uso de Inteligência Artificial:* o Fornecedor usa a tecnologia de Inteligência Artificial ("IA") em relação a algumas de suas ofertas (por exemplo, Monitoramento na tarefa do LanSchool). A IA é utilizada para interpretar o significado do objetivo da sala de aula e para analisar os dados já capturados dos alunos. Ela não coleta nenhuma informação adicional dos usuários além dos requisitos normais do produto. Não deve ser acionada nenhuma tomada de decisões automatizada, além da simples identificação. **A IA não fornecerá nenhum resultado que constitua discriminação ou viés ilegal tampouco violação de direitos de propriedade intelectual**. **O Fornecedor tem um processo implementado para tratar questões relacionadas à qualidade e à segurança dos resultados do sistema de IA, incluindo qualquer discriminação ou viés ilegal nesses resultados**. O Fornecedor cumpre **com a** Lei de Proteção de Dados Aplicável e outras legislações aplicáveis **em relação à IA**.

Segurança: o Processador implementará medidas técnicas e organizacionais adequadas para proteger os Dados Pessoais (i) de destruição acidental ou ilegal; e (ii) de perda, alteração, divulgação ou acesso não autorizado aos Dados Pessoais (um "Incidente de segurança"). O Anexo C contém Medidas Técnicas e Organizacionais (Technical and Organisational Measures, TOMs) do LanSchool Air.

Subprocessamento: o Fornecedor concorda que qualquer subprocessador terceirizado que venha a nomear estará sujeito a padrões de proteção de dados substancialmente semelhantes aos estabelecidos neste Contrato; além disso, o Fornecedor se compromete a firmar acordos com seus subprocessadores aplicáveis, conforme necessário, para garantir a implementação adequada dos requisitos deste DPA. O Controlador concorda que o Fornecedor pode utilizar qualquer subprocessador informado no Anexo B. No entanto, o Controlador autoriza o Fornecedor a contratar novos subprocessadores (inclusive substituindo os existentes) para o processamento dos Dados Pessoais, desde que: (i) o Fornecedor forneça um aviso prévio de pelo menos 30 dias sobre a adição ou substituição de qualquer subprocessador (incluindo detalhes sobre o processamento realizado ou a ser realizado), sendo esse aviso feito por meio da comunicação dos detalhes dessa adição ou substituição ao Controlador; e (ii) o Fornecedor imponha termos de proteção de dados a qualquer subprocessador nomeado, que assegurem a proteção dos Dados Pessoais de acordo com padrões substancialmente semelhantes aos previstos neste DPA. Se o Controlador se recusar a consentir com a indicação por parte do Fornecedor de um novo subprocessador de terceiros, o que não pode ser negado sem motivos razoáveis, o Fornecedor não indicará o subprocessador ou o Controlador poderá optar por rescindir o Contrato, desde que o Controlador tenha motivos substanciais e documentados para opor-se à alteração.

Cooperação e direitos dos Titulares dos Dados: o Fornecedor prestará assistência razoável e pontual ao Controlador para permitir que este responda a: (i) qualquer solicitação de um Titular dos Dados

para exercer qualquer um de seus direitos previstos na Lei de Proteção de Dados Aplicável (incluindo seus direitos de acesso, correção, objeção, apagamento e portabilidade dos Dados Pessoais, conforme aplicável); e (ii) qualquer outra correspondência, consulta ou queixa recebida de um Titular dos Dados, regulador ou outro terceiro em conexão com o Processamento dos Dados Pessoais. Para evitar dúvidas, as Solicitações de Titulares dos Dados (DSRs) deverão ser realizadas pelo Controlador por meio de uma solicitação formal no Formulário da Web de Privacidade de DSR da Stoneware.

Incidentes de segurança: ao tomar conhecimento de um Incidente de segurança, o Fornecedor informará o ocorrido ao Controlador sem atrasos indevidos e fornecerá todas essas informações e cooperação sem atrasos conforme o Controlador possa exigir para o cumprimento de suas obrigações de relato de violação de Dados Pessoais nos termos da Lei de proteção de dados aplicável (e de acordo com os respectivos prazos exigidos). O fornecedor tomará ainda medidas e ações necessárias para remediar ou diminuir os efeitos do Incidente de segurança e manterá o Controlador informado de todos os desdobramentos relacionados ao Incidente de segurança.

Exclusão ou Devolução dos Dados: na rescisão ou no término do Contrato de Vendas da Stoneware, o Fornecedor, mediante solicitação do Controlador, destruirá ou devolverá para o Controlador todos os Dados Pessoais (incluindo todas as cópias dos Dados Pessoais) em seu poder ou controle (incluindo quaisquer Dados Pessoais subcontratados a um terceiro para Processamento). Se o Controlador não fornecer instruções adicionais ao Fornecedor, o cronograma de retenção de dados do Fornecedor, conforme indicado no Anexo A, será aplicável. Esse requisito não será aplicável se o Fornecedor for obrigado por qualquer Lei de Proteção de Dados Aplicável a reter alguns ou todos os Dados Pessoais, caso em que o Fornecedor deverá isolar e proteger os Dados Pessoais de qualquer Processamento adicional se exigido por tal lei.

Auditoria: durante a vigência deste Contrato e por um período de três anos após sua rescisão ou expiração, o Fornecedor se compromete a fornecer ao Controlador, mediante solicitação razoável e com aviso prévio adequado: (i) acesso a resumos de: (1) práticas do Fornecedor (incluindo seus protocolos e procedimentos de segurança); (2) políticas internas; e (3) registros relacionados à privacidade e segurança das Informações Pessoais e ao Processamento de Informações Pessoais, disponíveis para revisão, exceto os registros protegidos pelo privilégio advogado-cliente ou que constituam produto de trabalho; (ii) assistência e cooperação da equipe pertinente do Fornecedor; e (iii) respostas a questionários que visem avaliar a conformidade do Fornecedor com suas obrigações estabelecidas neste Contrato ("Auditoria"). Essas Auditorias serão limitadas a uma vez por ano, salvo nas seguintes situações: (i) quando a Auditoria for exigida pelas Leis de Proteção de Dados Aplicáveis, ou para atender a qualquer solicitação ou demanda de reguladores, ou a um processo legal ou administrativo; (ii) quando a Auditoria for solicitada devido a preocupações legítimas do Controlador sobre a privacidade e segurança dos Dados Pessoais Processados pelo Fornecedor; ou (iii) no caso de um Incidente de Segurança confirmado. Não obstante o exposto acima, caso o resumo das práticas, políticas e registros ou as respostas ao questionário fornecidas pelo Fornecedor sejam consideradas insuficientes para atender aos requisitos ou demandas de um regulador, ou de um processo legal ou administrativo, as partes concordam em negociar, de boa-fé, os termos e o escopo de uma Auditoria adicional, a fim de atender a tais solicitações ou demandas. O Fornecedor deverá fornecer ao

Controlador as informações necessárias de forma razoável para permitir a condução das avaliações de proteção de dados pelo Controlador, bem como documentar tais avaliações.

ESTANDO JUSTAS E CONTRATADAS, a Stoneware e o Cliente assinaram este Contrato na data escrita acima.

Stoneware, Inc.	**Cliente**
Assinatura: _____	Assinatura: _____
Nome em letra de forma: Kimberly Page	Nome em letra de forma: _____
Cargo: Gerente de operações estratégicas	Cargo: _____

ANEXO A – DETALHES DE PROCESSAMENTO

Tipo de dados e Titular de dados	Período de retenção	Natureza, propósito e assunto
Dados relacionados à interface do aluno: • O Identificador global exclusivo (Globally Unique Identifier, GUID) do aluno gerado automaticamente • A ID do aluno conforme previsto. • O nome do aluno • O sobrenome do aluno • O endereço de e-mail do aluno. • O nome de login do aluno. • A data em que esse objeto do aluno foi criado. • A data em que este objeto do aluno foi atualizado.	Após o usuário solicitar exclusão ou após 1 ano sem haver uma licença ou teste ativo, os dados serão arquivados. Os dados arquivados são apagados após 90 dias.	*Armazenamento de dados* (registrar, hospedar, fazer log, arquivar ou armazenar os Dados do cliente); *Acesso aos dados* (recuperar, copiar, analisar, modificar, transportar, digitalizar ou acessar os Dados do cliente)
Dados relacionados à interface do funcionário da escola: • O GUID exclusivo do professor gerado automaticamente • A identificação (ID) do funcionário da escola. • O nome do funcionário da escola. • O sobrenome do funcionário da escola. • O endereço de e-mail do funcionário da escola. • A ID MongoDB do usuário de nuvem que corresponde a este objeto do professor. • Tokens de acesso • A data de criação deste objeto do funcionário da escola. • A data de atualização deste objeto do funcionário da escola.	Após o usuário solicitar exclusão ou após 1 ano sem haver uma licença ou teste ativo, os dados serão arquivados. Os dados arquivados são apagados após 90 dias.	*Armazenamento de dados* (registrar, hospedar, fazer log, arquivar ou armazenar os Dados do cliente); *Acesso aos dados* (recuperar, copiar, analisar, modificar, transportar, digitalizar ou acessar os Dados do cliente) *Análise dos dados* (pesquisar, testar, estudar, interpretar, organizar, criar relatório ou analisar os Dados do cliente).
Dados relacionados à interface do cliente: • O GUID exclusivo do cliente gerado automaticamente • O nome de login do aluno atual. Pode ser um endereço de e-mail ou um nome de usuário. • A ID MongoDB do dispositivo correspondente do banco de dados principal. • A data em que este objeto do cliente foi criado.	Após o usuário solicitar exclusão ou após 1 ano sem haver uma licença ou teste ativo, os dados serão arquivados. Os dados arquivados são apagados após 90 dias.	*Armazenamento de dados* (registrar, hospedar, fazer log, arquivar ou armazenar os Dados do cliente); *Acesso aos dados* (recuperar, copiar, analisar, modificar, transportar, digitalizar ou acessar os Dados do cliente)

• A data em que este objeto do cliente foi atualizado.		*Análise dos dados* (pesquisar, testar, estudar, interpretar, organizar, criar relatório ou analisar os Dados do cliente).
Dados relacionados à lista de aulas • O GUID exclusivo da aula gerado automaticamente • O nome desta aula. Esse item é obrigatório. • A ID da aula, conforme fornecida pelo Sistema de informações do aluno. • A ID da escola, conforme fornecida pelo Sistema de informações do aluno. • O período de aula ou outra designação que possa distinguir esta aula de outras aulas do mesmo tipo. • O responsável desta lista de aulas. • Os objetos do professor para os professores que têm acesso a esta lista de aulas. A Interface do professor é definida abaixo. • Os objetos do aluno para os alunos que pertencem a esta lista de aulas. • Os objetos do cliente para os dispositivos que pertencem a esta lista de aulas. • A ID do último usuário que alterou esta lista de aulas. • A data em que esta lista de aulas foi criada. • A data em que esta lista de aulas foi atualizada. •	Após o usuário solicitar exclusão ou após 1 ano sem haver uma licença ou teste ativo, os dados serão arquivados. Os dados arquivados são apagados após 90 dias.	*Armazenamento de dados* (registrar, hospedar, fazer log, arquivar ou armazenar os Dados do cliente); *Acesso aos dados* (recuperar, copiar, analisar, modificar, transportar, digitalizar ou acessar os Dados do cliente) *Análise dos dados* (pesquisar, testar, estudar, interpretar, organizar, criar relatório ou analisar os Dados do cliente).
Dados relacionados à organização • O GUID exclusivo da organização gerado automaticamente • O nome da organização. • A ID atribuída a esta organização. • O endereço principal. • As informações do endereço secundário. • A cidade da organização. • O estado ou a província da organização. • O código postal da organização.	Após o usuário solicitar exclusão ou após 1 ano sem haver uma licença ou teste ativo, os dados serão arquivados. Os dados arquivados são apagados após 90 dias.	*Armazenamento de dados* (registrar, hospedar, fazer log, arquivar ou armazenar os Dados do cliente); *Acesso aos dados* (recuperar, copiar, analisar, modificar, transportar, digitalizar ou acessar os Dados do cliente);

• O país da organização. • As informações de contato administrativo. • As informações técnicas de contato. • As informações de contato de faturamento. • Uma bandeira indicando se esta organização tem um representante local. • A data em que essa organização foi criada. • A política de segurança padronizada para a organização. • Dados de contato da organização: nome, sobrenome, número de telefone, endereço de e-mail.		*Análise dos dados* (pesquisar, testar, estudar, interpretar, organizar, criar relatório ou analisar os Dados do cliente).
Dados do usuário • O GUID exclusivo do usuário gerado automaticamente. • Um conjunto de pares de valor-chave de todas as IDs atuais do usuário. • O nome do usuário. • O sobrenome do usuário. • O endereço de e-mail do usuário. • Permissões diretamente atribuídas a este usuário. • Uma referência à organização à qual esse usuário pertence. • Um subconjunto de IDs de usuário que um usuário pode usar para um login. • Data/hora da última vez em que o usuário fez login com sucesso no sistema. • Data/hora da primeira vez em que o usuário obteve erro na autenticação dentro período de uma hora antes da verificação. • O endereço de IP onde ocorreu o último login bem-sucedido. • O endereço de IP onde ocorreu o último erro de login. • Data/hora da última falha na tentativa de login. • Um contador para o número de falhas nas tentativas de login consecutivas.	Após o usuário solicitar exclusão ou após 1 ano sem haver uma licença ou teste ativo, os dados serão arquivados. Os dados arquivados são apagados após 90 dias.	*Armazenamento de dados* (registrar, hospedar, fazer log, arquivar ou armazenar os Dados do cliente); *Acesso aos dados* (recuperar, copiar, analisar, modificar, transportar, digitalizar ou acessar os Dados do cliente) *Análise dos dados* (pesquisar, testar, estudar, interpretar, organizar, criar relatório ou analisar os Dados do cliente).

• As permissões concedidas ao usuário. Geradas pela combinação de todas as permissões dos grupos de usuários. • A data em que este usuário foi criado. • A data em que este usuário foi atualizado.		
Dados relacionados a registro de atividades • Histórico de navegação na web do aluno (URL, registro de data/horário) • Histórico de matrícula do aluno (nome na matrícula, registro de data/horário) • Histórico de mensagens de bate-papo em sala de aula (remetente, recebimento, conteúdo da mensagem, registro de data/horário) • Registro de atividades administrativas (ID de usuário, tipo de atividade, registro de data/horário) • Capturas de tela dos alunos, metadados da guia, conteúdo da página da guia ativa • Objetivos de sala de aula dos professores.	Mediante solicitação do usuário para exclusão ou depois de 45 dias.	*Armazenamento de Dados* (registrar, hospedar, arquivar ou de outra forma armazenar Dados do Cliente); *Acesso aos Dados* (recuperar, copiar, examinar, modificar, transportar, verificar ou de outra forma acessar Dados do Cliente); *Análise de Dados* (pesquisar, testar, estudar, interpretar, organizar, relatar ou de outra forma analisar Dados do Cliente).
Dados de licença (Exclui dados pessoais)	Esses dados são mantidos pelo tempo necessário para cumprir com as obrigações legais, exigir o cumprimento de nossos contratos etc. Esses dados não incluem dados pessoais.	*Armazenamento de dados* (registrar, hospedar, fazer log, arquivar ou armazenar os Dados do cliente); *Acesso aos dados* (recuperar, copiar, analisar, modificar, transportar, digitalizar ou acessar os Dados do cliente); *Análise dos dados* (pesquisar, testar, estudar, interpretar, organizar, criar relatório ou analisar os Dados do cliente).

Duração do processamento
A duração do processamento corresponde à duração do Contrato. As políticas de retenção de dados descritas acima serão aplicadas.
Categorias de Titulares dos dados
Alunos, professores, contatos da organização e usuários em geral

ANEXO B – SUBPROCESSADORES

Nome	Dados	Localização de armazenamento	Propósito
Amazon Web Services	Todos os dados do usuário descritos no anexo A	AU, EUA ou REINO UNIDO *(restrições regionais de transferência são aplicadas, o que significa, por exemplo, que dados europeus são armazenados exclusivamente no Reino Unido).*	Provedor de serviços de nuvem para a infraestrutura de aplicativos. Todos os Dados são processados pelo aplicativo.
Datalog	Dados do aplicativo, endereço IP e nome de usuário	EUA	Ferramenta de coleta de registros (log).
Hubspot	Nome, sobrenome, e-mail, telefone, nome da empresa, cargo, marcação geográfica (p. ex., estado), setor	EUA, UE	Integração.
MongoDB Atlas	Todos os dados do usuário descritos no anexo A	AU, EUA ou REINO UNIDO *(restrições regionais de transferência são aplicadas, o que significa, por exemplo, que dados europeus são armazenados exclusivamente no Reino Unido).*	Para que o aplicativo seja executado corretamente.
Pendo	Análise de uso do aplicativo, feedback enviado pelos usuários, nome, sobrenome e e-mail do usuário final e nome da organização.	EUA	Para melhorar a funcionalidade e a usabilidade do produto.

ANEXO C – MEDIDAS TÉCNICAS E ORGANIZACIONAIS (TOMs)

O Fornecedor implementou um programa de segurança abrangente e por escrito com controles físicos, técnicos, processuais e administrativos que refletem as normas predominantes do setor para a proteção e uso responsável de Dados Pessoais, incluindo, entre outros, os seguintes controles:

Técnicas	Escopo	Controles
Acesso	Logins (sistema e aplicativo).	Políticas de senha baseadas conforme orientações do Instituto nacional de padrões e tecnologia (National Institute of Standards and Technology, NIST) (autenticação multifatorial para acesso e interfaces em nível de administração).
Criptografia	Armazenamento de dados em repouso e em trânsito.	AES 256-GCM (em repouso), TLS 1.2, 1.3 (em trânsito)
Teste de segurança de aplicativos estáticos	Todas as imagens de servidor e microatendimento, Todos os clientes binários e extensões/plugins.	Varreduras e monitoramento regulares de vulnerabilidades.
Testes dinâmicos de segurança de aplicativos	Interface de Programação de Aplicativos (Application Programming Interfaces, APIs) de aplicativos externos.	Varreduras de aplicativos web, Teste de penetração (Testes internos regulares.)
Fortalecimento dos parâmetros do Centro de segurança na Internet (Center for Internet Security, CIS)	Provedor de plataformas em nuvem, instâncias do servidor.	Verificações de conformidade com CIS na nuvem, monitoramento de segurança na nuvem, Avaliações regulares de parâmetro de servidores CIS L2.
Análise de composição de software	Dependências de código aberto de terceiro.	Realizar auditorias regulares de vulnerabilidade, monitoramento de repositórios.
Avaliação de infraestrutura	Provedor de plataforma em nuvem.	Avaliações regulares de todas as redes definidas por software (software-defined networks, SDNs) (identificar segmentação de rede, configuração de firewall e configurações de acesso de recursos).
Firewall de aplicativos web (Web application firewall, WAF)	Aplicativos web de produção.	Proteção de WAF (regras fundamentais para ataques comuns).
Análise de código estático	Código proprietário.	A análise regular de código é realizada por uma ferramenta comercial e, durante as

		mesclagens de código, são realizadas revisões de código seguras.
Coleta de log	Provedor de plataformas em nuvem, aplicativo.	Transações de API da plataforma em nuvem (os registros com mais de 360 dias são removidos, acessíveis pela engenharia), Registro WAF para detecção de borda (os registros com mais de 90 dias são removidos, acessíveis pela engenharia), Subprocessadores, consulte o anexo B, para fins de aplicativos.
Infraestrutura como código	Provedor de plataforma em nuvem.	A infraestrutura como código é usada para automatizar implantações de infraestrutura e melhorar a imutabilidade, a configuração incorreta da infraestrutura.

Organizacionais	Escopo	Controles
Resposta a incidentes (incluindo violação de dados)	Eventos de segurança relacionados aos produtos em produção.	Plano de resposta a incidentes do produto de acordo com os processos NIST 800-61 e da Equipe interna de resposta a incidentes de segurança de produtos (Product Security Incident Response Team, PSIRT) da Lenovo.
Lista de provedores confiáveis	Todos os subprocessadores que se integram diretamente aos produtos na produção.	Avaliações de segurança padronizadas de provedores integrados, DPAs para provedores que processam Dados Pessoais.
Gerenciamento de vulnerabilidades	Ambientes de sistema operacional (Operating System Environment, OSEs) do servidor, contêineres do Docker, clientes, produtos em produção.	Um programa que emprega várias ferramentas para ajudar na identificação de vulnerabilidades em todos os sistemas de computação.
Conselho de revisão de segurança de software (Software Security Review Board, SSRB)	produtos em produção.	As revisões do SSRB são realizadas regularmente. Durante as revisões, todas as medidas técnicas e organizacionais são avaliadas para o produto em questão.

Política de retenção de dados	Informações de identificação pessoal, dados do aplicativo, produtos em produção.	Caso o usuário solicite exclusão ou após um ano sem ter uma licença ou teste ativo, os dados pessoais serão arquivados. Os dados arquivados são apagados após 90 dias.
Conscientização sobre segurança e privacidade	Todos os funcionários (cursos Fundamentos de privacidade e Fundamentos de segurança)	Treinamento semestral para equipes especializadas de TI e produtos sobre tópicos avançados de segurança, como OWASP Top 10.
Segurança contínua	produtos em produção.	Aplicação regular de medidas técnicas.
Avaliações de conformidade de código aberto.	produtos em produção.	Avaliações são realizadas para garantir o licenciamento adequado, e as atribuições são fornecidas no software distribuído.
Recuperação de desastres	Produtos em produção.	Seguindo o NIST-800-34 como um guia para maximizar o objetivo de tempo de recuperação (Recovery Time Objective, RTO) e o objetivo do ponto de recuperação (Recovery Point Objective, RPO).
Política de backup	Bancos de dados, código logs.	A política geral requer vários backups, um dos quais deve ser externo ao local de armazenamento principal; Backups de bancos de dados regulares realizados diariamente (2 vezes ao dia), semanalmente e mensalmente. Os backups realizados diariamente são armazenados por 7 dias. Os backups realizados semanalmente são armazenados por 4 semanas. Os backups mensais ficam retidos por 13 meses. A janela de restauração é de 12 horas. Os backups de código-fonte do aplicativo são realizados

		diariamente e são armazenados por 360 dias. Registros de produção: Datalog – Os registros são mantidos disponíveis para acesso em tempo real por 7 dias. Os registros são então transferidos para armazenamento de longo prazo por 180 dias, então são apagados. Load Balancer – Os registros são retidos por 360 dias, então são apagados. Firewall do aplicativo da web – Os registros são retidos por 90 dias, então são apagados. Cloud Trail – Os registros são retidos por 90 dias, então são apagados. Cloud Watch – Os registros são retidos por 360 dias, então são apagados. MongoDB – Os registros são retidos durante a existência do projeto.

ANEXO D – CONTRATO DE TRANSFERÊNCIAS INTERNACIONAIS DE DADOS

Este Anexo estabelece os requisitos de proteção de dados (incluindo os requisitos determinados nas Leis de Privacidade Aplicáveis) que se aplicam: (i) ao Exportador de Dados (Controlador) quando ele transfere Dados Pessoais para o Importador de Dados (Stoneware, Inc.), suas afiliadas e/ou seus Subprocessadores para Processamento de Dados; e (ii) ao Importador de Dados quando ele recebe Dados Pessoais de um Exportador de Dados para Processamento de dados.

O Importador de Dados garante e compromete-se a:

a) processar os Dados Transferidos de acordo com as Leis de Privacidade Aplicáveis e prestar assistência razoável e oportuna ao Exportador de Dados, conforme necessário, para ajudar o Exportador de Dados a cumprir suas obrigações de acordo com as Leis de Privacidade Aplicáveis; e

b) não cumprir conscientemente suas obrigações nos termos deste Contrato de forma a fazer com que o Exportador de Dados viole qualquer uma de suas obrigações nos termos das Leis de Privacidade Aplicáveis.

O Exportador de Dados confirma que tomou todas as medidas necessárias para assegurar a conformidade com as leis de Proteção de Dados aplicáveis, inclusive com os requisitos para a transferência transfronteiriça de dados pessoais, por exemplo, obteve os consentimentos explícitos dos Titulares dos Dados para a transferência de seus dados pessoais para o exterior, notificou as autoridades competentes, solicitou a aprovação da transferência, e cumpriu outras obrigações subjacentes, conforme aplicável.

1. Espaço Econômico Europeu (EEE)

Se os serviços do Fornecedor forem fornecidos ao Controlador dentro do Espaço Econômico Europeu ("EEE") ou de outra jurisdição sujeita à Lei de proteção de dados da UE, as seguintes disposições serão aplicadas:

(A) "Lei de proteção de dados da UE" se refere (a) ao Regulamento 2016/679 do Parlamento Europeu e do Conselho sobre a proteção de pessoas físicas no que diz respeito ao Processamento de Dados pessoais e sobre a livre circulação desses dados (Regulamento Geral de Proteção de Dados) ("RGPD"); (b) à Diretiva de privacidade eletrônica da UE (Diretiva 2002/58/CE); e (c) a toda e qualquer lei nacional de proteção de dados aplicável.

(B) O Fornecedor informará imediatamente o Controlador (a) sobre qualquer exigência nos termos da Lei de proteção de dados da UE que exigiria o Processamento de Dados pessoais de qualquer forma diferente das instruções do Controlador ou (b) se, na opinião do Fornecedor, as instruções do Controlador infringirem ou violarem qualquer Lei de proteção de dados da UE aplicável.

(C) ***Transferências de dados:*** se o Fornecedor ou seus respectivos Subcontratados estiverem localizados fora do EEE, por meio deste instrumento, o Fornecedor e o Controlador assinam as cláusulas contratuais padronizadas de controlador para processador, conforme estabelecido no

MÓDULO DOIS da Decisão de Execução (UE) 2021/914 da Comissão, de 4 de junho de 2021, sobre as cláusulas contratuais padronizadas para a transferência de dados pessoais para países terceiros nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, e suas alterações ou substituições ao longo do tempo ("Cláusulas contratuais padronizadas C2P") e, por meio deste instrumento, as incorporam neste Adendo por referência. As partes reconhecem e concordam que:

a. o Fornecedor e o Controlador cumprirão suas respectivas obrigações nas Cláusulas contratuais padronizadas C2P;

b. se houver algum conflito ou inconsistência entre as Cláusulas contratuais padronizadas C2P e este Adendo, ou o contrato base, as Cláusulas contratuais padronizadas C2P terão precedência, na medida do conflito; e

c. por meio deste instrumento, as informações nas tabelas abaixo são incorporadas nas Cláusulas contratuais padronizadas C2P entre as Partes:

Informações a serem incorporadas às
Cláusulas contratuais padronizadas C2P entre Controlador e Fornecedor:

Cláusula 9. Uso de subprocessadores	A Opção 2, AUTORIZAÇÃO GERAL POR ESCRITO, está selecionada. O importador de dados fornecerá informações com, no mínimo, 30 dias de antecedência de acordo com a Cláusula "Subprocessamento"
Cláusula 17. Legislação aplicável	Estas Cláusulas serão interpretadas de acordo com a legislação aplicável estabelecida no contrato base das Partes, salvo se a legislação aplicável não pertencer a algum Estado Membro da UE que permita direitos de terceiros beneficiários. Nesse caso, as partes concordam que estas cláusulas serão regidas pela legislação da IRLANDA.
Cláusula 18 (b). Eleição de foro	As partes elegem os tribunais da IRLANDA para dirimir disputas, controvérsias ou demandas decorrentes destas Cláusulas.

Informações a serem incorporadas ao Anexo 1, Parte A, das Cláusulas contratuais padronizadas C2P:

Nome do exportador de dados	Controlador e qualquer uma das suas respectivas afiliadas de propriedade ou controle comum
Endereço do exportador de dados	A ser preenchido pelo exportador de dados
Nome, cargo e informações de contato da pessoa de contato do exportador de dados	A ser preenchido pelo exportador de dados

Atividades do exportador de dados relevantes para os dados transferidos de acordo com estas Cláusulas	A ser preenchido pelo exportador de dados
Assinatura do exportador de dados e data	A ser preenchido pelo exportador de dados
Função do exportador de dados	Controlador
Nome do importador de dados	Fornecedor (Stoneware, Inc.) e seus respectivos Subcontratados
Endereço do importador de dados	Stoneware, Inc. 8001 Development Drive, Morrisville, NC 27560 United States of America
Nome, cargo e informações de contato da pessoa de contato do importador de dados	Dan Verwolf, Diretor privacy@lanschool.com
Atividades do importador de dados referentes aos dados transferidos de acordo com estas Cláusulas	Conforme estabelecido na Parte B do Anexo 1
Assinatura do importador de dados e data	A ser preenchido pelo importador de dados
Função do importador de dados	Processador

Informações a serem incorporadas ao Anexo 1, Partes B e C, das Cláusulas contratuais padronizadas C2P:

Categorias de titulares de dados	Conforme estabelecido no Anexo A, acima
Categorias de dados pessoais	Conforme estabelecido no Anexo A, acima
Dados sigilosos	Conforme estabelecido no Anexo A, acima
Frequência da transferência	Frequência contínua, enquanto a licença LSA estiver ativa
Natureza do processamento	Conforme estabelecido no Anexo A, acima
Objetivo do processamento	Conforme estabelecido no Anexo A, acima
Período durante o qual os dados pessoais serão preservados	Conforme estabelecido no Anexo A, acima
Objeto, natureza e duração do processamento realizado pelos subprocessadores	Conforme estabelecido no Anexo B, acima
Autoridade supervisora competente responsável por assegurar a conformidade do exportador de dados com o Regulamento (UE) 2016/679	A autoridade supervisora que atuará como autoridade supervisora competente será a do Estado Membro da UE no qual o Exportador de dados está estabelecido na UE. Se o Exportador de dados (ou seja, a pessoa jurídica parte no contrato) não estiver estabelecido na UE, a Autoridade supervisora competente será a do Estado Membro da UE no qual o representante da UE do Exportador de dados, na acepção do

	Artigo 27(1) do Regulamento (UE) 2016/679, estiver estabelecido. Se o Exportador de dados não estiver estabelecido na UE, e não precisar nomear um representante da UE, a Autoridade supervisora competente será a do Estado Membro da UE em que estejam localizados os titulares dos dados cujos dados pessoais estejam sendo transferidos de acordo com estas Cláusulas, em relação à oferta de bens ou serviços, ou cujo comportamento esteja sendo monitorado.

Informações a serem incorporadas ao Anexo 2 das Cláusulas contratuais padronizadas C2P:

Descrição das medidas técnicas e organizacionais implementadas pelos importadores de dados (inclusive as certificações pertinentes) para assegurar um nível adequado de segurança, levando em consideração a natureza, o escopo, o contexto e a finalidade do processamento, bem como os riscos para os direitos e liberdades das pessoas físicas.	Conforme estabelecido no Anexo C, acima

Informações a serem incorporadas ao Anexo 3 das Cláusulas contratuais padronizadas C2P:

Lista de subprocessadores autorizados	Conforme estabelecido no Anexo B, acima

2. Reino Unido

Se os serviços do Fornecedor forem fornecidos ao Controlador dentro do Reino Unido, ou a natureza dos Dados pessoais requerer a aplicação da Lei da União Europeia (Retirada), de 2018 (o "RGPD do Reino Unido"), e da Lei de Proteção de Dados, de 2018 (a "DPA de 2018"), as seguintes disposições adicionais serão aplicadas:

(A) Transferências de Dados pessoais para um destinatário em um país considerado pelo Secretário de Estado do Reino Unido como tendo proteção adequada para os Dados pessoais ("Decisão de adequação") serão permitidas nos termos dos Contratos sem a necessidade das Cláusulas contratuais padronizadas do Reino Unido aprovadas.
(B) Os países do EEE serão considerados sujeitos à Decisão de adequação para fins de transferência de Dados pessoais do Reino Unido para o EEE.
(C) Na ausência de uma Decisão de adequação, o Controlador e o Fornecedor concordam em assinar o adendo aprovado de transferência internacional de dados do Reino Unido às cláusulas contratuais padronizadas da Comissão Europeia para

transferências internacionais de dados (https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf).

Parte 1: Tabelas / Tabela 1: Partes

Informações a serem incorporadas à "Parte 1: Tabelas" do Adendo de transferência internacional de dados às Cláusulas contratuais padronizadas da Comissão da UE:		
Data de início	Conforme especificado acima	
As Partes	**Exportador (quem envia a Transferência restrita)**	**Importador (quem recebe a Transferência restrita)**
Informações das Partes	Razão social completa, endereço principal (se for um endereço registrado da empresa): Conforme as informações da 2.ª tabela do Art. 1.º. Espaço Econômico Europeu (EEE) no Anexo D Número de registro oficial (se houver) (número da empresa ou identificador semelhante): De acordo com o cliente identificado no Contrato de vendas	Razão social completa, endereço principal (se for um endereço registrado da empresa): Conforme as informações da 2.ª tabela do Art. 1.º. Espaço Econômico Europeu (EEE) no Anexo D Número de registro oficial (se houver) (número da empresa ou identificador semelhante): 35-2097171, registrado no estado de Indiana, EUA
Contato principal	Nome completo (opcional), cargo, informações de contato, inclusive e-mail: Conforme as informações da 2.ª tabela do Art. 1.º. Espaço Econômico Europeu (EEE) no Anexo D	Nome completo (opcional), cargo, informações de contato, inclusive e-mail: Conforme as informações da 2.ª tabela do Art. 1.º. Espaço Econômico Europeu (EEE) no Anexo D

Tabela 2: SCCs, módulos e cláusulas selecionadas

Cláusulas contratuais padronizadas (Standard Contractual Clauses, SCCs) do Adendo da UE	Consulte o Anexo D, Art. 1.º, acima

Tabela 3: Informações do Apêndice

Anexo 1A: Lista de Partes conforme estabelecido no Art. 1.º. Espaço Econômico Europeu (EEE) no Anexo D
Anexo 1B: Descrição da transferência: Conforme estabelecido no Anexo A, acima
Anexo II: Medidas técnicas e organizacionais, inclusive medidas técnicas e organizacionais para assegurar a segurança dos dados: Descrição da transferência: Conforme estabelecido no Anexo C, acima
Anexo III: Lista de subprocessadores (Módulos 2 e 3 apenas): Descrição da transferência: Conforme estabelecido no Anexo B, acima

Tabela 4: Rescisão deste Adendo mediante alteração do Adendo aprovado

Rescisão deste Adendo mediante alteração do Adendo aprovado	Partes que podem rescindir este Adendo conforme estabelecido na Seção **Error! Reference source not found.**: ☒ Importador ☐ Exportador ☐ Nenhuma das Partes

Informações a serem incorporadas à "Parte 2: Cláusulas obrigatórias" do Adendo de transferência internacional de dados às Cláusulas contratuais padronizadas da Comissão da UE:
Parte 2: Cláusulas obrigatórias do Adendo aprovado, sendo o modelo do Adendo B.1.0 emitido pela OIC e apresentado ao Parlamento de acordo com a seção 119A da Lei de Proteção de Dados de 2018 em 2 de fevereiro de 2022, conforme revisado na Seção **Error! Reference source not found.** dessas Cláusulas obrigatórias.

3. Suíça

Na medida em que a transferência de Dados Pessoais estiver sujeita à Lei Federal Suíça sobre Proteção de Dados, as partes concordam em estar em conformidade com as Cláusulas Contratuais Padrão da UE e as seguintes disposições se aplicarão: (i) o Comissário Federal de Proteção de Dados e Informação (Federal Data Protection and Information Commissioner, FDPIC) será a autoridade supervisora competente nos termos da Cláusula 13 das Cláusulas Contratuais Padrão da UE; (ii) as Partes concordam em cumprir o padrão do RGPD em relação a todo Processamento de Dados Pessoais que seja regido pela Lei Federal Suíça sobre Proteção de Dados; (iii) as Cláusulas Contratuais Padrão da UE serão regidas pelas leis da Suíça de acordo com a Cláusula 17 (Opção 1) na medida em que as

transferências de dados sejam regidas pela Lei Federal da Suíça sobre Proteção de Dados; (iv) o termo "Estado membro" nas Cláusulas contratuais padrão da UE não será interpretado de forma a excluir os Titulares de dados na Suíça da possibilidade de processar seus direitos em seu local de residência habitual (Suíça) de acordo com a Cláusula 18(c) das Cláusulas contratuais padrão da UE; (v) as referências ao "RGPD" nas Cláusulas Contratuais Padrão da UE serão entendidas como referências à Lei Federal Suíça sobre Proteção de Dados, na medida em que a transferência de Dados do Controlador esteja sujeita à Lei Federal Suíça sobre Proteção de Dados.

4. Brasil

No caso de uma transferência de Dados Pessoais sujeitos à Lei Geral de Proteção de Dados Pessoais ("LGPD") do Brasil (conforme alterada pela Lei nº 13.853 de 8 de julho de 2019), e a Lenovo, o Fornecedor ou ambos estiverem localizados em Países Não Adequados, as Cláusulas Contratuais Padrão C2P conforme referenciadas neste instrumento se aplicarão, com as seguintes alterações:

(i) a autoridade supervisora das Cláusulas Contratuais Padrão C2P será a Autoridade Nacional de Proteção de Dados (ANPD);

(ii) a lei regente, de acordo com a Cláusula 17 das Cláusulas Contratuais Padrão C2P, será a LGPD;

(iii) a escolha do foro e da jurisdição de acordo com a Cláusula 18 das Cláusulas Contratuais Padrão C2P será a legislação brasileira caso a transferência de dados esteja exclusivamente sujeita à LGPD; e

(iv) referências ao RGPD nas Cláusulas Contratuais Padrão C2P também incluirão a referência às disposições equivalentes da LGPD (conforme alterada ou substituída).

5. África do Sul

Se os serviços do Fornecedor forem fornecidos ao Controlador na África do Sul ou em outra jurisdição sujeita à Lei de proteção de Informações pessoais (Protection of Personal Information Act , POPIA), as seguintes disposições adicionais serão aplicadas:

(A) Titular de dados refere-se a uma pessoa física que pode ser identificada por referência a um nome, número exclusivo, dados de localização, identificador on-line ou um ou mais fatores específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa física, bem como uma pessoa jurídica ou entidade legal identificável.

6. Austrália

As partes concordam em usar e proteger os Dados Pessoais aplicáveis em conformidade com a Lei de Privacidade de Dados da Austrália e suas alterações.

ANEXO E – DISPOSIÇÕES ADICIONAIS

1. Lei de Privacidade do Consumidor da Califórnia (California Consumer Privacy Act, "CCPA").

A Stoneware, Inc. é uma empresa. Além disso, o Fornecedor é o Prestador de Serviços do Cliente e processará dados pessoais em nome do Cliente.

d. O Fornecedor não venderá os Dados pessoais ou as Informações exclusivas. "Vender" significa vender, alugar, liberar, divulgar, disseminar, disponibilizar, transferir ou comunicar as informações em troca de consideração monetária ou outra consideração valiosa.

e. O fornecedor não reterá, usará ou divulgará os Dados pessoais: (a) para qualquer finalidade que não seja para a finalidade específica de prestar os serviços estabelecidos no Contrato para a Stoneware, Inc. ou conforme permitido pela CCPA e suas regulamentações de implantação; (b) para uma finalidade comercial que não seja a prestação dos serviços especificados no contrato com a empresa; ou (c) fora da relação comercial direta entre a pessoa e a Stoneware Inc.

f. Este DPA servirá como confirmação do Fornecedor de que o Fornecedor compreende as exigências da CCPA aplicáveis às empresas e aos prestadores de serviços, inclusive as restrições constantes no Código Civil da Califórnia, § 1798.140(w)(2)(A), e cumprirá essas exigências.