

## LanSchool Air データ処理契約（DPA）

この LanSchool Air データ処理契約（プライバシーおよびセキュリティ要件の両方を記載）およびその付属文書（「**DPA**」）は、Stoneware 売買契約書、または Stoneware, Inc.からの LanSchool Air サービスの購入に関して Stoneware, Inc.とお客様の間で締結されるその他の書面による契約もしくは電子契約（「**本契約**」）の一部を構成し、個人データの処理に関する両当事者の合意を反映するものです。

本 DPA は、本契約の主題に関する両当事者の合意を補足するものであり、お客様が LanSchool Air サービス規約を受諾した時点から有効となります（「**発効日**」）。

本契約に署名し、LanSchool Air サービス規約を受諾した時点で、本 DPA には法的な拘束力が生じます。お客様は、適用されるプライバシー、セキュリティおよびデータ保護法および規制（適用される教育および学生に関するプライバシーおよびセキュリティ法および規制を含む）において義務付けられる範囲で、許可を受けた関連会社が管理者としての資格を有する個人データを Stoneware が処理する範囲において、かかる許可を受けた関連会社の代表者としてその名義でお客様を代表して本 DPA を締結します。お客様は、本 DPA がすべてのユーザーに適用されることを理解し、当該ユーザーに代わって本 DPA を締結するために必要な権限を有することを保証します。

当社は、新たな法的要件に対応するため、または運用上のアップデートを反映するために必要に応じて、これらの規定を更新する場合があります。お客様の LanSchool Air サブスクリプションが有効である場合、メールまたは製品内の通知を使用してお知らせいたします。以前のバージョンの DPA は、[こちら](#)からご覧いただけます。

### DPA の締結：

- a) 本 DPA は、DPA 本文と付属文書 A、B、C、D および E の二部で構成されます。
- 本 DPA は、データ輸入者としての付属文書 D の EU 標準契約条項を含め、Stoneware, Inc.の代表者により署名済みです。（注：付属文書 D は、一般には欧州連合、欧州経済領域、英国および／または越境データ移転に関して類似の充分性標準または等価標準を持つその他の国からの個人データの移転を伴う処理活動にのみ適用されます。）本 DPA はさらに、適用データ保護法令が義務付けている、安全な個人データ移転を確保するための契約条項を示します。

誤解のないよう明記いたしますが、お客様は本 DPA の 5 ページに署名する必要があります。該当する場合は、参照により付属文書 D が適用されます。

### データ保護

定義：本条項において、以下の用語は以下の意味を持つものとします。

- a) 「**管理者**」、「**処理者**」、「**サブプロセッサー**」、「**データ処理**」、および「**処理中**」（および「**処理**」）の各用語は、EU データ保護法、および適用されるデータ保護法における同等の用語に定められる意味を持つものとします。
  - (a) 「**適用されるデータ保護法**」とは、本件サプライヤーが LanSchool サービスを提供する管轄区において適用されるすべての法律、規則、規制、命令、およびこれらに関連するすべての修正を意味します。これには、2018 年カリフォルニア州消費者プライバシー法（「CCPA」）およびカリフォルニア州プライバシー権法（「CPRA」）、EU 一般データ保護規則 2016/279（「GDPR」）およびその随時の修正、置き換え、差し替え、英国の 2018 年データ保護法改正法、ブラジルの一般データ保護法 No.13.709/18（「LGPD」）などの、施行された（またはこれから施行される）プライバシー、データセキュリティ、データ保護、データ漏洩、機密保持に関する法律および規制、ならびにかかる適用法（国内、州および／または現地の教育および学生に関するプライバシー法を含む）が含まれます。
- b) 「**個人データ**」は、学生、両親、学校職員を含むがこれらに限定されない、特定されたまたは特定可能な個人に関連する情報をいいます。
- c) 「**データ主体**」は、学生、両親、学校職員を含むがこれらに限定されない、直接的または間接的に特定できる個人をいいます。
- d) 「**お客様**」とは、管理者をいいます。本 DPA においてのみ、「お客様」にはお客様と許可を受けた関連会社を含むものとします。
- e) 「**本件サプライヤー**」とは、処理者として行為する Stoneware, Inc.を意味します。
  - (b) 「**データ輸出者**」とは、本契約に基づいて個人データを他の当事者に移転する当事者を意味します。
  - (c) 「**データ輸入者**」とは、本契約に基づいて個人データを他の当事者から受領する当事者を意味します。

当事者の関係：お客様にとってサプライヤーは、サプライヤーとの Stoneware 販売契約、LanSchool Air サービス利用条件、および EULA の対象である個人データを処理する処理者です。各当事者は、適用データ保護法令に基づいて適用される義務を遵守するものとします。

目的の制限：本件サプライヤーは、処理者として、付属文書 A「処理の詳細」に記載される管理者の指示文書に厳密に従い（「許容される目的」）、個人データを処理するものとします。ただし、適用されるデータ保護法で別途義務付けられている場合を除きます。本件サプライヤーは、管理者の処理の指示が適用されるデータ保護法に違反することを知り得た場合、直ちに管理者に知らせるものとします。いかなる場合においても、本件サプライヤーは、自己または第三者の目的（マーケティングの目的を含む）で個人データを処理しないものとします。誤解を避けるために記すと、本件サプライヤーは、Lenovo LanSchool Air の使用によ

り取得した個人データを利用して Lenovo LanSchool Air ユーザーにマーケティングや販売促進コミュニケーションのお知らせを送ってはなりません。ただし、こうしたマーケティングや販売促進コミュニケーションが、Stoneware または Lenovo のウェブサイトなどの正式なチャネルや販売関連チャネルを介して発信される場合には、個人が受け取ることを妨害することはありません。

**国際的な移転:** サプライヤーは、適用されるデータ保護法およびデータ・ローカライズ法に準拠して、個人データが収集された国以外の国に個人データを移転できます。疑義を避けるため、データは本契約でさらに指定される方法 (すなわち、地域別のアプローチ/ロケーション) でホストされるものとし、および:

- a) 欧州経済領域 (「EEA」) および英国の域外への個人データの移転は、(i) 個人データの移転先の受領者が、欧州委員会、英国国務大臣および/または英国個人情報保護監督機関が個人データに適切な保護を提供すると判断した国内に所在する場合、ならびに (ii) 受領者が、欧州委員会、英国国務大臣および/または英国個人情報保護監督機関が採択または承認した標準契約条項を締結している場合に許可されます。

サプライヤーは、以下の場合に、ブラジル国外に個人データを移転することができます。(i) 当該データ移転が、国家機関が決定した、個人データの適切な保護を提供する国の受領者宛てである場合、(ii) 国家機関の採用または承認する標準契約条項を実行した受領者宛ての場合、または (iii) 受領者が、ブラジル・データ保護法令に従って他の保護手段を実施してそれを実証でき、かつ当該国際的な移転が管理者によって承認されている場合。

- b. 一般に、本 DPA に同意することにより、お客様は、Stoneware, Inc. が適用されるデータ保護法を遵守する限りにおいて、Stoneware が個人データを国境を越えて移転することを承認したものとみなされます。これに関連して、該当する場合、附属書 D「国際的なデータ移転」が管理者とサプライヤーの間で適用されます。

お客様データは、本契約の附属書 B に基づいて、第三国 (米国など) において、標準契約条項などの第三国移転に必要な適切な保護措置を講じて、復処理者によってアクセスされる場合があります。各グループ内データ転送は、安全な国際データ転送を確保するための標準契約条項を含むサプライヤーのグループ内データ転送契約に基づいて行われます。

**処理における機密保持:** 本件サプライヤーは、自らが個人データの処理を許可する者 (本件サプライヤーのスタッフ、代理人、サブプロセッサーを含む) (「許可を受けた者」) が厳密な守秘義務 (契約上の義務または法定義務を問わない) を負うよう徹底するものとし、かかる守秘義務に服さない者に個人データの処理を許容しないものとします。本件サプライヤーは、すべての許可を受けた者が許容される目的に必要な限りにおいて個人データを処理するよう徹底するものとします。さらに、本件サプライヤーは個人データを商業的に活用しないものとします。

- c. **人工知能の使用:** サプライヤーは、提供するサービスの一部 (LanSchool On-Task Monitoring など) に関連して人工知能技術 (以下「AI」) を使用します。AI は、授業目標の意味を解釈し、事前に取得済みの学生データを分析するために利用されます。

通常の製品要件を超えた追加情報をユーザーから収集することはありません。単純な識別を超えた自動意思決定が作動することはありません。AI は、違法な差別や偏見、または知的財産権の侵害となるような出力を提供しません。サプライヤーは、AI システムの出力に存在する違法な差別や偏見を含め、AI システムの出力の品質と安全性に関する問題に対処する手順を定めています。サプライヤーは、AI に関する適用されるデータ保護法およびその他の適用可能な法制を遵守します。

セキュリティ：処理者は、(i) 偶発的または違法な破壊、および (ii) 喪失、変更、不正な開示、アクセス（「セキュリティインシデント」）から個人データを保護するための適切な技術的、組織的対策を講じるものとします。付属文書 C に、LanSchool Air 技術的・組織的対策（TOM）が記載されています。

復処理：サプライヤーは、自らが任命する第三者の復処理者が、本契約で規定されているデータ保護と同一の基準に拘束されることに同意し、サプライヤーが当該復処理者との間で、本 DPA の要件を適切に実現するための契約を締結することに同意します。管理者は、サプライヤーが附属書 B に記載されている種類の復処理者を使用することに同意します。これにかかわらず、管理者は、以下の条件で、サプライヤーが個人データを処理するために新しい復処理者（既存の復処理者からの交代を含む）に従事させることに同意します。(i) サプライヤーが、30 営業日前までに、復処理者の追加または交代（実行するまたは実行予定の処理の詳細を含む）を通知すること、および (ii) サプライヤーが、自らが任命したすべての復処理者に対し、本 DPA で規定されているのと同じ基準で個人データを保護するためのデータ保護条件を課すこと。サプライヤーによる新たな第三者復処理者の任命に管理者が同意しない場合、管理者の決定を不当に抑えるべきではないため、サプライヤーが復処理者の任命を取りやめるか、そうでなければ、管理者は本契約を終了できます。ただし、管理者がその変更に関する異議を唱えることに重要な理由があり、その理由が文書化されていることを条件とします。

協力およびデータ主体の権利：サプライヤーは、管理者が以下に対応できるよう、管理者に合理的かつ適時的な支援を提供するものとします。(i) データ主体が適用されるデータ保護法に基づく権利（該当する場合、アクセス、訂正、異議申し立て、消去、個人データのポータビリティの権利を含む）を行使するための要求、および (ii) 個人データの処理に関連してデータ主体、規制当局、またはその他の第三者から受け取ったその他の通信、問い合わせ、または苦情。疑義を避けるために付記すると、データ主体の要求（DSR）を行うには、管理者が [Stoneware DSR プライバシー Web フォーム](#) で正式な要求を提出する必要があります。

セキュリティインシデント：本件サプライヤーは、セキュリティインシデントを知り得た時点で不当な遅延なく管理者に知らせるものとし、管理者が適用されるデータ保護法に基づき個人データ漏洩報告に関する自らの義務を（同法により義務付けられる期限に従って）果たすために要請するすべての情報と協力を適時に提供するものとします。本件サプライヤーはさらに、セキュリティインシデントの影響を是正または軽減するために必要な対策と措置を講じるものとし、セキュリティインシデントに関連するすべての進展を常にデータ管理者に報告するものとします。

データの削除または返却：Stoneware 販売契約の終了または満了に伴い、サプライヤーは、管理者の要求に応じて、その保有または管理下にあるすべての個人データ（個人データのすべ

てのコピーを含む)を破棄または管理者に返却するものとします(処理のために第三者に委託された個人データを含む)。管理者がサプライヤーに追加の指示をしない限り、附属書 A に記載されたサプライヤーのデータ保持スケジュールが適用されます。この要件は、適用されるデータ保護法によってサプライヤーが個人データの一部または全部を保持することが義務付けられている場合には適用されないものとし、その場合、サプライヤーは、かかる法令によって義務付けられている範囲を除き、個人データをそれ以上の処理から分離し保護するものとします。

**監査:** 本契約の期間中、および終了または満了後 3 年間、サプライヤーは、合理的な要求および合理的な事前通知に基づいて、管理者に以下を提供するものとします。(i) 以下の概要へのアクセス: (1) サプライヤーの慣行(そのセキュリティ・プロトコルおよび手順を含む)、(2) 社内方針、(3) 個人情報のプライバシーとセキュリティ、およびレビュー可能な個人情報の処理に関連する記録 (弁護士と依頼人の特権の対象となる記録、または作業成果物を構成する記録を除く)、(ii) サプライヤーの関連スタッフの支援と協力、および (iii) サプライヤーが本契約の義務を遵守しているかどうかを判断するための質問票への回答 (以下「監査」といいます)。このような監査は、以下の場合を除き、年 1 回に制限されるものとします: (i) 適用されるデータ保護法によって監査が義務付けられている場合、または規制当局または法的あるいは行政手続きによる要請や要求に応じる場合、(ii) 管理者が、サプライヤーが処理する個人データのプライバシーおよびセキュリティに関して正当な懸念を有する場合、または (iii) セキュリティ・インシデントが確認された場合。上記にかかわらず、サプライヤーが提供する慣行、方針、記録の要約、またはサプライヤーが提供する質問票への回答が、規制当局または法的または行政的プロセスの要件または要求を満たすには不十分であると判断された場合、両当事者は、そのような要求/要求を満たすための追加監査の条件と範囲について誠意を持って交渉することに同意します。サプライヤーは、管理者がデータ保護評価を実施し、文書化するために合理的に必要な情報を管理者に提供するものとします。

上記を証するため、Stoneware とお客様は上記の日付で本契約を締結しました。

**Stoneware, Inc.**

**お客様**

署名 : \_\_\_\_\_

署名 : \_\_\_\_\_

氏名 (活字体) : Kimberly Page

氏名 (活字体) : \_\_\_\_\_

役職 : 戦略オペレーションマネージャー

役職 : \_\_\_\_\_

付属文書 A - 処理の詳細

データの種別およびデータ主体	保持期間	性質、目的、主題
<b>学生インターフェース関連データ：</b> <ul style="list-style-type: none"> <li>自動生成された学生の一意の GUID</li> <li>提供された学生 ID</li> <li>学生の名前（名）</li> <li>学生の名前（姓）</li> <li>学生のメールアドレス</li> <li>学生のログイン名</li> <li>学生オブジェクトの作成日</li> <li>学生オブジェクトの更新日</li> </ul>	<p>ユーザーが削除を要請した場合、または有効なライセンスもしくはトライアルがなく1年が経過した場合、データはアーカイブに移されます。アーカイブされたデータは90日後にパージされます。</p>	<p>データストレージ（レコード、ホスト、ログ、アーカイブ、または顧客データのその他ストレージ）</p> <p>データアクセス（検索、コピー、検証、変更、移動、スキャン、または顧客データへのその他アクセス）</p>
<b>学校職員のインターフェースに関連するデータ：</b> <ul style="list-style-type: none"> <li>自動生成された教師の一意の GUID</li> <li>学校職員の ID</li> <li>学校職員の名前（姓）</li> <li>学校職員の名前（名）</li> <li>学校職員のメールアドレス</li> <li>当該教師オブジェクトに対応するクラウドユーザーの MongoDB ID</li> <li>アクセストークン</li> <li>学校職員オブジェクトの作成日</li> <li>学校職員オブジェクトの更新日</li> </ul>	<p>ユーザーが削除を要請した場合、または有効なライセンスもしくはトライアルがなく1年が経過した場合、データはアーカイブに移されます。アーカイブされたデータは90日後にパージされます。</p>	<p>データストレージ（レコード、ホスト、ログ、アーカイブ、または顧客データのその他ストレージ）</p> <p>データアクセス（検索、コピー、検証、変更、移動、スキャン、または顧客データへのその他アクセス）</p> <p>データ分析（調査、テスト、研究、解釈、整理、報告、または顧客データのその他分析）</p>
<b>顧客インターフェース関連データ：</b> <ul style="list-style-type: none"> <li>自動生成された顧客の一意の GUID</li> <li>現在の学生のログイン名（メールアドレスまたはユーザー名の場合あり）</li> <li>コアデータベースで対応するデバイスの MongoDB ID</li> <li>顧客オブジェクトの作成日</li> <li>顧客オブジェクトの更新日</li> </ul>	<p>ユーザーが削除を要請した場合、または有効なライセンスもしくはトライアルがなく1年が経過した場合、データはアーカイブに移されます。アーカイブされたデータは90日後にパージされます。</p>	<p>データストレージ（レコード、ホスト、ログ、アーカイブ、または顧客データのその他ストレージ）</p> <p>データアクセス（検索、コピー、検証、変更、移動、スキャン、または顧客データへのその他アクセス）</p> <p>データ分析（調査、テスト、研究、解釈、整理、報告、または顧客データのその他分析）</p>
<b>クラスリスト関連データ</b> <ul style="list-style-type: none"> <li>自動生成されたクラスの一意の GUID</li> <li>クラスの名前（必須）</li> <li>学生情報システムから提供されたクラス ID</li> </ul>	<p>ユーザーが削除を要請した場合、または有効なライセンスもしくはトライアルがなく1年が経過した場合、データはアーカイブに移されます。アーカイブさ</p>	<p>データストレージ（レコード、ホスト、ログ、アーカイブ、または顧客データのその他ストレージ）</p> <p>データアクセス（検索、コピー、検証、変</p>

<ul style="list-style-type: none"> <li>学生情報システムから提供された学校 ID</li> <li>クラスの期間、または当該クラスと他の同種のクラスを区別するその他の指示</li> <li>クラスリストの所有者</li> <li>当該クラスリストにアクセスできる教師の教師オブジェクト（教師インターフェースは以下に定義）</li> <li>当該クラスリストに掲載される学生の学生オブジェクト</li> <li>当該クラスリストに掲載されるデバイスの顧客オブジェクト</li> <li>当該クラスリストを最後に変更したユーザーの ID</li> <li>当該クラスリストの作成日</li> <li>当該クラスリストの更新日</li> </ul>	<p>れたデータは 90 日後にパージされます。</p>	<p>更、移動、スキャン、または顧客データへのその他アクセス） データ分析（調査、テスト、研究、解釈、整理、報告、または顧客データのその他分析）</p>
<p><b>組織関連データ</b></p> <ul style="list-style-type: none"> <li>自動生成された組織の一意の GUID</li> <li>組織の名称</li> <li>組織に割り当てられた ID</li> <li>所在地（町名、番地）</li> <li>所在地（番地以降の情報）</li> <li>組織が所在する都市名</li> <li>組織が所在する都道府県名</li> <li>組織の郵便番号</li> <li>組織が所在する国</li> <li>事務担当者の連絡先情報</li> <li>技術担当者の連絡先情報</li> <li>請求先情報</li> <li>組織に現場代理人がいるかどうかを示すフラグ</li> <li>組織の創設日</li> <li>組織のデフォルトのセキュリティポリシー</li> <li>組織の担当者の情報：姓名、電話番号、メールアドレス</li> </ul>	<p>ユーザーが削除を要請した場合、または有効なライセンスもしくはトライアルがなく 1 年が経過した場合、データはアーカイブに移されます。アーカイブされたデータは 90 日後にパージされます。</p>	<p>データストレージ（レコード、ホスト、ログ、アーカイブ、または顧客データのその他ストレージ） データアクセス（検索、コピー、検証、変更、移動、スキャン、または顧客データへのその他アクセス） データ分析（調査、テスト、研究、解釈、整理、報告、または顧客データのその他分析）</p>
<p><b>ユーザーデータ</b></p> <ul style="list-style-type: none"> <li>自動生成されたユーザーの一意の GUID</li> <li>ユーザーのすべての現行 ID のキーと値のペア</li> <li>ユーザーの名前（名）</li> <li>ユーザーの名前（姓）</li> <li>ユーザーのメールアドレス</li> </ul>	<p>ユーザーが削除を要請した場合、または有効なライセンスもしくはトライアルがなく 1 年が経過した場合、データはアーカイブに移されます。アーカイブさ</p>	<p>データストレージ（レコード、ホスト、ログ、アーカイブ、または顧客データのその他ストレージ） データアクセス（検索、コピー、検証、変更、移動、スキャン、</p>

<ul style="list-style-type: none"> <li>• 当該ユーザーに直接割り当てられているパーミッション</li> <li>• 当該ユーザーが所属する組織への参照</li> <li>• ユーザーがログインに使用できるユーザーIDのサブセット</li> <li>• ユーザーがシステムのログインに最後に成功した時のタイムスタンプ</li> <li>• 過去1時間においてユーザーが認証に失敗した初回のタイムスタンプ</li> <li>• 最後のログイン成功時のIPアドレス</li> <li>• 最後のログイン失敗時のIPアドレス</li> <li>• 最後のログイン失敗時のタイムスタンプ</li> <li>• 連続ログイン失敗回数のカウンター</li> <li>• ユーザーに付与されたパーミッション（ユーザーのグループのすべてのパーミッションを組み合わせて生成）</li> <li>• 当該ユーザーの作成日</li> <li>• 当該ユーザーの更新日</li> </ul>	<p>れたデータは90日後にパージされます。</p>	<p>または顧客データへのその他アクセス) データ分析（調査、テスト、研究、解釈、整理、報告、または顧客データのその他分析）</p>
<p><b>データに関するアクティビティログ</b></p> <ul style="list-style-type: none"> <li>• 学生のウェブ閲覧履歴（URL、タイムスタンプ）</li> <li>• 学生の申請履歴（申請名、タイムスタンプ）</li> <li>• 教室でのチャットメッセージ履歴（送信者、受信者、メッセージ内容、タイムスタンプ）</li> <li>• 管理アクティビティログ（ユーザーID、アクティビティタイプ、タイムスタンプ）</li> <li>• 学生のスクリーンショット、タブのメタデータ、アクティブなタブ・ページのコンテンツ</li> <li>• 教員の授業目標。</li> </ul>	<p>ユーザーからの削除要求があり次第、または45日後まで。</p>	<p>データ保存（お客様データの記録、ホスト、アーカイブ、またはその他の方法での保存）、データ・アクセス（お客様データの取得、コピー、精査、修正、移動、スキャン、またはその他の方法でのアクセス）、データ分析（お客様データの調査、テスト、検討、解釈、整理、報告、またはその他の方法での分析）。</p>
<p><b>ライセンスデータ（個人データを除く）</b></p>	<p>このデータは、法的義務の遵守、当社契約の執行等に必要な限り保持されます。これには個人データは含まれません。</p>	<p>データストレージ（レコード、ホスト、ログ、アーカイブ、または顧客データのその他ストレージ）</p>

		データアクセス（検索、コピー、検証、変更、移動、スキャン、または顧客データへのその他アクセス） データ分析（調査、テスト、研究、解釈、整理、報告、または顧客データのその他分析）
--	--	---

処理の期間

処理の期間は本契約の期間に相当します。上記に示すデータ保持ポリシーが適用されます。

データ主体のカテゴリ

学生、教師、組織の連絡先とユーザー全般

付属文書 B - サブプロセッサー

名前	データ	保存場所	目的
Amazon Web Services	付属文書 A に記載するすべてのユーザーデータ	AU、US、または UK (地域的な移転制限が適用されます。たとえば、欧州のデータは、英国 (UK) にのみ保存されます)。	アプリケーションインフラストラクチャのクラウドサービスプロバイダー。すべての本件データはアプリケーションで処理されます。
Datadog	アプリケーションデータ、IP アドレス、ユーザー名	米国	ログ収集ツール
HubSpot	姓名、メールアドレス、電話番号、会社名、役職、地理的タグ（州など）、業種	US、EU	オンボーディング
MongoDB Atlas	付属文書 A に記載するすべてのユーザーデータ	AU、US、または UK (地域的な移転制限が適用されます。たとえば、欧州のデータは、英国 (UK) にのみ保存されます)。	アプリケーションを正しく実行するため。
Pendo	アプリケーションの使用状況アナリティクス、ユーザーが送信したフィードバック、エンド・ユーザーの名、姓、メール・アドレス、組織名。	米国	製品の機能とユーザビリティの向上

付属文書 C - 技術的・組織的対策 (TOM)

本件サプライヤーは、個人データの保護および責任ある使用に関する一般的な業界基準を反映した、物理的、技術的、手順および事務管理的な管理策により総合的な書面でのセキュリティプログラムを実施しています。これには以下の管理策が含まれますが、これらに限定されません：

技術的対策	範囲	管理策
アクセス	ログイン (システムおよびアプリケーション)	NIST ベースのパスワードポリシー (管理者レベルのアクセスとインターフェースの多要素認証)
暗号化	保存中および送信中のデータストレージ	AES 256-GCM (静止時)、 TLS 1.2、1.3 (移転時)
静的アプリケーションセキュリティテスト	すべてのサーバーとマイクロサービスイメージ、 すべてのバイナリクライアントとエクステンション/プラグイン	定期的な脆弱性スキャンとモニタリング
動的アプリケーションセキュリティテスト	外部アプリケーション API	ウェブアプリケーションスキャン、 侵入テスト (定期的な内部テスト)
CIS ベンチマークのハードニング	クラウドプラットフォームプロバイダー、 サーバーインスタンス	クラウドの CIS コンプライアンスチェック、クラウドのセキュリティモニタリング、 定期的な CIS L2 サーバーのベンチマーク評価
ソフトウェア構成分析	第三者オープンソースへの依存	定期的な脆弱性監査、レポートのモニタリングの実施
インフラアセスメント	クラウドプラットフォームプロバイダー	すべてのソフトウェア定義ネットワーク (SDN) の定期的レビュー (ネットワークセグメント、ファイアウォール設定、リソースアクセスのミスコンフィギュレーションの特定)
ウェブアプリケーションファイアウォール (WAF)	本番環境のウェブアプリケーション	WAF 保護 (一般的な攻撃に対するコア規則)
静的コード解析	プロプライエタリコード	商用ツールを使用して定期的なコード分析を実施し、 コードマージ中にセキュアコードレビューを実施します。
ログ収集	クラウドプラットフォームプロバイダー、	クラウドプラットフォームの API トランザクション (360 日以上経過したログはパージ)

	アプリケーション	れ、エンジニアリング部門はアクセス可能)、 エッジ検出のための WAF ログ (90 日以上経過したログはパージされ、エンジニアリング部門はアクセス可能)、 サブプロセッサ、アプリケーションの目的については付属文書 B を参照してください。
コードとしてのインフラストラクチャ (IaC)	クラウドプラットフォームプロバイダー	IaC は、インフラストラクチャのデプロイを自動化し、不変性の向上とインフラのミスコンフィギュレーションの改良のために使用されます。

組織的対策	範囲	管理策
インシデント（データ違反を含む）への対応	本番環境にある製品に関するセキュリティイベント	NIST 800-61 と Lenovo の製品セキュリティインシデント対応チーム (PSIRT) の社内プロセスに従った製品のインシデント対応計画
信頼プロバイダーリスト	本番環境にある製品を直接統合するすべてのサブプロセッサ	統合プロバイダーの標準セキュリティアセスメント、個人データを処理するプロバイダー向けの DPA
脆弱性管理	サーバーOS、 Docker コンテナ、 顧客、 本番環境にある製品	すべてのコンピューターシステムに渡る脆弱性の特定を支援するための各種ツールを採用したプログラム
ソフトウェアセキュリティ審査委員会 (SSRB)	本番環境にある製品	SSRB の審査は定期的実施されます。審査では、問題の製品について、すべての技術的対策と組織的対策が評価されます。
データ保持ポリシー	個人を特定できる情報、 アプリケーションデータ、 本番環境にある製品	ユーザーが削除を要請した場合、または有効なライセンスもしくはトライアルがなく 1 年が経過した場合、個人データはアーカイブに移されます。アーカイブされたデータは 90 日後にパージされます。
セキュリティおよびプライバシーに対する認識	全従業員（プライバシー基本コースおよびセキュリティ必須コース）	特別 IT および製品チーム向けの高度セキュリティトピック (OWASP トップ 10 な

		ど)に関する半年ごとのトレーニング
継続的セキュリティ	本番環境にある製品	技術的対策の定期的な適用
オープンソースコンプライアンスレビュー	本番環境にある製品	配布されたソフトウェアに適切なライセンスと属性が提供されていることを確認するために実施するアセスメント
ディザスターリカバリー	本番環境にある製品	手引きとして NIST-800-34 に従い、RTO と RPO を最適化します。
バックアップポリシー	データベース、 コード、 ログ	<p>一般的なポリシーでは多重バックアップを要求しており、その 1 つは主記憶位置から離れた場所である必要があります。</p> <p>毎日（1 日に 2 回）、毎週、毎月実施される定期的なデータベースバックアップ。毎日のバックアップは 7 日間保持されます。毎週のバックアップは 4 週間保持されます。毎月のバックアップは 13 か月間保持されます。リストアの時間枠は 12 時間です。</p> <p>アプリケーションのソースコードのバックアップは毎日行われ、360 日間保持されます。本番環境のログ： Datadog - ログは 7 日間保持されます。その後ログは 180 日間長期ストレージに保存された後、パージされます。</p> <p>ロードバランサー - ログは 360 日間保持され、その後パージされます。</p> <p>ウェブアプリケーションファイアウォール - ログは 90 日間保持され、その後パージされます。</p>

		<p>Cloud Trail - ログは 90 日間保持され、その後パージされます。</p> <p>Cloud Watch - ログは 360 日間保持され、その後パージされます。</p> <p>MongoDB - ログはプロジェクトの存続期間中保持されます。</p>
--	--	--

## 付属文書 D - 国際データ移転契約

本付属文書はデータ保護要件（適用されるプライバシー法に基づく要件を含む）を定めるものです。このデータ保護要件は、(i) データ輸出者（管理者）がデータ輸入者

（Stoneware, Inc.）、その関連会社および／またはそのサブプロセッサーにデータ処理のために個人データを移転する場合にデータ輸出者（管理者）、ならびに (ii) データ輸入者がデータ輸出者からデータ処理のために個人データを受領する場合にデータ輸入者に適用されます。

データ輸入者は、常に以下に従うことを保証し、約束します。

- a) 適用されるプライバシー法に従って移転されたデータを処理し、必要に応じて適切な支援を適時にデータ輸出者に提供し、データ輸出者が適用されるプライバシー法に基づく自身の義務を遵守できるようにします。
- b) データ輸出者が適用されるプライバシー法に基づく自身の義務に違反することになるような方法で、本契約に基づく自身の義務を故意に履行しません。

データ輸出者は、適用されるデータ保護法（個人データの国境を越えた移転のために必要な要件を含みます）を遵守するために必要な措置を講じたことを確認します。かかる措置には、個人データが海外に移転されることについてデータ主体の明示的な同意を得たこと、関連当局へ通知・移転承認申請を行ったこと、該当するその他の義務を履行したことなどが含まれます。

### 1. 欧州経済領域（EEA）

本件サプライヤーのサービスが欧州経済領域（「EEA」）内、またはその他の EU データ保護法の対象となる法域内の管理者に提供される場合、以下の規定が適用されるものとします。

(A) 「EU データ保護法」とは、(a) 欧州議会および欧州理事会による個人データの処理とかかるデータの自由な移動に関する自然人の保護についての規則 2016/679（一般データ保護規則）（「GDPR」）、(b) EU の e プライバシー指令（指令 2002/58/EC）ならびに (c) 国家において適用されるあらゆるデータ保護法を意味します。

(B) 本件サプライヤーは、(a) 管理者の指示とは異なる形による個人データの処理を求める EU データ保護法に基づく要件、または (b) 本件サプライヤーの意見において管理者の指示が適用される EU データ保護法に違反または反する場合はそのことを、管理者に速やかに通知するものとします。

(C) **データの移転**：本件サプライヤーまたはその下請業者が EEA 域外に所在する場合、本件サプライヤーと管理者は、[欧州議会および欧州理事会規則（EU）2016/679 に従った第三国への個人データ移転のための標準契約条項に関する 2021 年 6 月 4 日付欧州委員会実施決定（EU）2021/914](#) のモジュール 2 に規定され、随時改正、置き換えられる、管理者から処理者への移転に関する標準契約条項（「C2P 標準契約条項」）をこれにより締結し、参照により本補遺へ組み込みます。両当事者は以下を認め、これに同意します。

- a. 本件サプライヤーと管理者は、C2P 標準契約条項における各自の義務を遵守するものとします。
- b. 本補遺または基本契約と C2P 標準契約条項との間に矛盾または不一致が存在する場合、その不一致の範囲に関しては C2P 標準契約条項の規定が優先するものとします。
- c. 下表の情報はこれにより両当事者間の C2P 標準契約条項に組み込まれます。

**管理者と本件サプライヤー間の  
C2P 標準契約条項へ組み込まれる情報：**

第 9 条 サブプロセッサの使用	オプション 2「包括的な書面による承諾」を選択します。データ輸入者は「サブ処理」の条項に従い 30 日以上前に情報を提供するものとします。
第 17 条 準拠法	本条項は、準拠法が第三者受益権を許可する EU 加盟国のものではない限り、両当事者の基本契約に定める準拠法に従って解釈されるものとします。そのような場合、両当事者は本条項にアイルランドの法律が適用されるものとするに合意します。
第 18 条(b) 裁判地と裁判管轄	両当事者は本条項に起因する紛争はアイルランドの法廷にて解決されるものとするに合意します。

**C2P 標準契約条項、付属文書 1 パート A に組み込まれる情報：**

データ輸出者の名称	管理者、およびその共同所有／支配する関連会社
データ輸出者の住所	データ輸出者が記入
データ輸出者の担当者の氏名、役職、連絡先	データ輸出者が記入
本条項に従って移転されるデータに関するデータ輸出者の活動	データ輸出者が記入
データ輸出者の署名と日付	データ輸出者が記入
データ輸出者の役割	管理者
データ輸入者の名称	本件サプライヤー（Stoneware, Inc.）およびその下請業者
データ輸入者の住所	Stoneware, Inc. 8001 Development Drive, Morrisville, NC 27560 United States of America
データ輸入者の担当者の氏名、役職、連絡先	Dan Verwolf、ディレクター privacy@lanschool.com

本条項に従って移転されるデータに関するデータ輸入者の活動	付属文書 1 パート B に定めるとおり
データ輸入者の署名と日付	データ輸入者が記入
データ輸入者の役割	処理者

**C2P 標準契約条項の付属文書 1 パート B と C に組み込まれる情報：**

データ主体のカテゴリ	上記の付属文書 A に定めるとおり
個人データのカテゴリ	上記の付属文書 A に定めるとおり
センシティブデータ	上記の付属文書 A に定めるとおり
移転の頻度	LSA ライセンスが有効である限り、継続的
処理の性質	上記の付属文書 A に定めるとおり
処理の目的	上記の付属文書 A に定めるとおり
個人データの保管期間	上記の付属文書 A に定めるとおり
サブプロセッサーが実行する処理の主題、性質および期間	上記の付属文書 B に定めるとおり
データ輸出者による EU 一般データ保護規則（規則 2016/679）の遵守確保に責任を負う管轄権を有する監督機関	データ輸出者が EU で設立されている場合は、その EU 加盟国の監督機関が、管轄権を有する監督機関としての役割を果たします。データ輸出者（契約を締結する法人）が EU 内で設立されていない場合は、EU 一般データ保護規則（規則 2016/679）第 27 条（1）の意味によるデータ輸出者の EU 代理人が設立された EU 加盟国の監督機関が管轄権を有する監督機関となります。データ輸出者が EU 内で設立されておらず、EU 代理人を任命する必要もない場合は、物品またはサービスの提供に関連し本条項に基づいて個人データが移転される、またはその行動が監視されるデータ主体が所在する EU 加盟国の監督機関が、管轄権を有する監督機関となります。

**C2P 標準契約条項の付属文書 2 に組み込まれる情報：**

データ輸入者が、処理の性質、範囲、文脈、目的と、自然人の権利と自由に与えるリスクを考慮した上で、適切な水準のセキュリティを確保するために実装する技術的・組織的対策の記述（該当する証明を含む）	上記の付属文書 C に定めるとおり
---	-------------------

**C2P 標準契約条項の付属文書 3 に組み込まれる情報：**

認定されたサブプロセッサのリスト	上記の付属文書 B に定めるとおり
------------------	-------------------

## 2. 英国

本件サプライヤーのサービスが英国内で管理者に提供される場合、または個人データの性質上、2018 年欧州連合離脱法（「英国 GDPR」）および 2018 年データ保護法（「2018 年 DPA」）が適用される場合は、以下の追加規定が適用されるものとします。

- (A) 英国国務大臣が個人データに対して適切な保護を提供すると判断（「十分性認定」）した国内の受領者に対する個人データの移転は、承認された英国標準契約条項を必要としない契約に基づき許可されます。
- (B) EEA 加盟国は、英国から EEA への個人データの移転において十分性認定の対象であるとみなされるものとします。
- (C) 十分性認定が欠如している場合、管理者と本件サプライヤーは、国際データ移転について、「欧州委員会の標準契約条項」に関する承認済みの英国国際データ移転補遺（<https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf>）を締結することに合意するものとします。

パート 1：表／表 1：当事者

「欧州委員会の標準契約条項」に対する「国際データ移転補遺」の「パート 1：表」に組み込まれる情報		
開始日	上記を参照	
当事者	輸出者（制限付きのデータ移転を行う者）	輸入者（制限付きのデータ移転を受け取る者）
当事者の説明	<p>正式名称、主たる事業所の住所（会社の場合には、登記されている住所）：第 1 条の第 2 表の情報による。付属文書 D の欧州経済領域（EEA）</p> <p>正式な登録番号（該当する場合）（会社番号または同様の識別子）：売買契約書に記載されている顧客に基づく</p>	<p>正式名称、主たる事業所の住所（会社の場合には、登記されている住所）：第 1 条の第 2 表の情報による。付属文書 D の欧州経済領域（EEA）</p> <p>正式な登録番号（該当する場合）（会社番号または同様の識別子）：インディアナ州で登録されている 35-2097171</p>
主要連絡先	氏名（任意）、役職名、メールアドレスを含む連絡先：第 1 条の第 2 表の情報による。付属文書 D の欧州経済領域（EEA）	氏名（任意）、役職名、メールアドレスを含む連絡先：第 1 条の第 2 表の情報による。付属文書 D の欧州経済地域（EEA）

表 2：選択された SCC、モジュール、および選択された条項

EU SCC 補遺	上記の付属文書 D 第 1 条を参照
-----------	--------------------

表 3：添付文書の情報

付属文書 1A：第 1 条に定める当事者リスト 付属文書 D の欧州経済領域（EEA）
付属文書 1B：データ移転の内容：上記の付属文書 A に定めるとおり
付属文書 II：技術的・組織的対策（データのセキュリティを確保するための対策を含む） データ移転の内容：上記の付属文書 C に定めるとおり
付属文書 III：サブプロセッサのリスト（モジュール 2 と 3 のみ）：データ移転の内容：上記の付属文書 B に定めるとおり

表 4：承認済みの補遺が変更された時点で本補遺を終了する

承認済みの補遺が変更された時点で本補遺を終了する	<p>第 <b>Error! Reference source not found.</b>条に基づき本補遺を終了する当事者</p> <p><input checked="" type="checkbox"/> 輸入者</p> <p><input type="checkbox"/> 輸出者</p> <p><input type="checkbox"/> 上記以外の者</p>
--------------------------	--

**「欧州委員会の標準契約条項」に対する「国際データ移転補遺」の「パート 2：必須条項」に組み込まれる情報**

パート 2：承認済補遺の必須条項（2018 年データ保護法第 119A 条に基づき、2022 年 2 月 2 日に ICO が発行し、議会に提出され、後に必須条項第 **Error! Reference source not found.**条に基づき修正された補遺 B.1.0 テンプレート）

### 3. スイス

個人データの移転にスイス連邦の連邦データ保護法が適用される限りにおいて、両当事者は EU 標準契約条項を遵守することに合意し、また以下の条項が適用されるものとします。(i) 連邦データ保護情報コミッショナー（FDPIC）が、EU 標準契約条項第 13 条に定める管轄権を有する監督当局となる、(ii) 両当事者は、スイス連邦の連邦データ保護法が適用される個人データに関するすべての処理に関連して、GDPR 基準を遵守することに合意する、(iii) スイス連邦の連邦データ保護法がデータ移転に適用される限り、第 17 条（オプション 1）に従い、EU 標準契約条項はスイス法を準拠法とする、(iv) EU 標準契約条項における「加盟国」という用語は、スイス国内のデータ主体から、かかるデータ主体の常居所地（スイス）における権利を EU 標準契約条項第 18 条(c)に従って行使するために訴訟する可能性を奪うような方法で解釈しない、(v) EU 標準契約条項が「GDPR」について言及する場合、管理者データの移転がスイス連邦の連邦データ保護法の適用を受ける限りにおいて、スイス連邦の連邦データ保護法に言及していると理解する。

#### 4. ブラジル

ブラジルの一般個人データ保護法（2019 年 7 月 8 日付法律第 13.853 号により改正）（「LGPD」）の対象となる個人データの移転が行われ、Lenovo、本件サプライヤー、またはその両方が非適格国に所在する場合、本契約で言及されている C2P 標準契約条項が、以下の修正を加えた上で適用されるものとします。

- (i) C2P 標準契約条項の監督当局は、ブラジルの国家データ保護局（ANPD）とする。
- (ii) C2P 標準契約条項第 17 条に基づく準拠法は、LGPD とする。
- (iii) C2P 標準契約条項第 18 条に基づく裁判地および裁判管轄の選択は、データ移転に LGPD だけが適用される場合、ブラジル法に従うものとする。
- (iv) C2P 標準契約条項で GDPR に言及している場合、LGPD（改正または置換されたもの）における同等の条項も含めて言及しているものとする。

#### 5. 南アフリカ

南アフリカ国内または個人情報保護法（POPIA）が適用される法域内で本件サプライヤーのサービスが管理者に提供される場合、以下の追加の規定が適用されるものとします。

- (A) データ主体とは、氏名、一意な番号、位置データ、オンライン識別子、またはその自然人の身体的、生理的、遺伝子的、精神的、経済的、文化的もしくは社会的なアイデンティティに固有な 1 つ以上の要素を参照することにより特定可能な自然人および特定可能な法人を意味します。

#### 6. オーストラリア

両当事者は、オーストラリアのデータプライバシー法（その後の改正を含む）に従い、該当する個人データを使用し、保護することに同意します。

## 付属文書 E - その他の規定

### 1. カリフォルニア州消費者プライバシー法（「CCPA」）

Stoneware, Inc.は事業体に該当します。さらに、本件サプライヤーは、お客様のサービスプロバイダーであり、お客様に代わり個人データを処理します。

- d. 本件サプライヤーは、個人データまたは専有情報を売却しないものとします。「売却」とは、金銭その他の価値ある対価と引き換えに情報を販売、賃貸、リリース、開示、普及、供用、譲渡、その他伝達することを意味します。
- e. 本件サプライヤーは、次の目的で個人データを保持、使用、開示しないものとします。（a）Stoneware, Inc.のために本契約に定めるサービスを履行する特定の目的、もしくは CCPA およびその施行規則で別途認められた目的以外の目的、（b）事業者との契約に定めるサービスを提供する以外の商業的目的、または（c）本人と Stoneware, Inc.との直接の取引関係以外。
- f. 本 DPA は、本件サプライヤーが事業およびサービスプロバイダーに適用される CCPA の要件（Cal. Civ. Code § 1798.140(w)(2)(A)における制限を含む）を理解していること、およびこれを遵守することを証する認定書となるものとします。