

**LanSchool Air Data Processor Agreement
(DPA)**

**Perjanjian Pemrosesan Data LanSchool Air
(DPA)**

This LanSchool Air Data Processor Agreement (which addresses both privacy and security requirements) and its annexes, (“DPA”) form part of the Stoneware Sales Agreement or other written or electronic agreement between Stoneware, Inc., and Customer (the “Agreement”) for the purchase of LanSchool Air services from Stoneware, Inc. to reflect the parties’ agreement in relation to the Processing of Personal Data.

Perjanjian Pemrosesan Data LanSchool Air ini (yang membahas persyaratan-persyaratan privasi dan keamanan) dan lampiran-lampirannya (“DPA”) menjadi bagian dari Perjanjian Penjualan Stoneware atau perjanjian tertulis atau elektronik lainnya antara Stoneware, Inc., dan Pelanggan (“Perjanjian”) untuk pembelian layanan LanSchool Air dari Stoneware, Inc. untuk mencerminkan kesepakatan para pihak sehubungan dengan Pemrosesan Data Pribadi.

This DPA supplements any agreement between the parties with respect to the subject matter hereof; and will be effective from the moment that Customer accepts LanSchool Air Terms of Services (“Effective Date”).

DPA ini melengkapi perjanjian apa pun antara para pihak sehubungan dengan pokok bahasan di sini, dan akan berlaku efektif sejak Pelanggan menerima Ketentuan Layanan LanSchool Air (“Tanggal Efektif”).

Upon signature of the Agreement and acceptance of the LanSchool Air Terms of Services, this DPA will become legally binding; and you (Customer) are entering into this DPA on behalf of Customer, to the extent required under applicable privacy, security and data protection Laws and Regulations, including applicable education and student privacy and security laws and regulations, in the name and on behalf of its Authorized Affiliates to the extent Stoneware processes Personal Data for which such Authorized Affiliates qualify as the Controller. Customer understands that this DPA is applicable to all users and warrants that it has the necessary powers to enter into this DPA on behalf of such users.

Setelah penandatanganan Perjanjian dan penerimaan Ketentuan Layanan LanSchool Air, DPA ini akan mengikat secara sah; dan Anda (Pelanggan) mengikatkan diri pada DPA ini atas nama Pelanggan, sejauh diwajibkan berdasarkan Peraturan Perundang-Undangan privasi, keamanan, dan perlindungan data yang berlaku, termasuk peraturan perundang-undangan pendidikan dan privasi siswa serta keamanan, atas nama Afiliasi Resminya sejauh Stoneware memproses Data Pribadi yang Afiliasi Resmi tersebut memenuhi syarat sebagai Pengendali. Pelanggan memahami bahwa DPA ini berlaku bagi semua pengguna dan menjamin bahwa Pelanggan memiliki wewenang yang diperlukan

untuk mengikatkan diri pada DPA ini atas nama para pengguna.

We may update these terms to accommodate new legal requirements or as necessary to reflect operational updates. If you have an active LanSchool Air subscription, we will let you know via email or via in-product notification. You can find archived versions of the DPA [here](#).

Kami dapat memperbarui ketentuan-ketentuan ini untuk mengakomodasi persyaratan hukum baru atau sebagaimana yang dibutuhkan untuk mencerminkan pembaruan-pembaruan operasi. Jika Anda memiliki langganan LanSchool Air yang aktif, kami akan memberitahukan Anda melalui email atau pemberitahuan dalam produk. Anda dapat menemukan versi DPA terarsip [di sini](#).

DPA execution:

- a) This DPA consists of two parts: the main body of the DPA, and Annexes A, B, C, D and E.
- b) This DPA has been pre-signed on behalf of Stoneware, Inc., including the EU Standard Contractual Clauses in Annex D, as the data importer. (Note: Annex D is generally applicable to only processing activities that may involve the transfer of Personal Data from the European Union, European Economic Area, United Kingdom and/or other countries with similar adequacy or equivalency standards pertaining to cross-border data transfers).

Pelaksanaan DPA:

- a) *DPA ini terdiri dari dua bagian: bagian utama DPA, dan Lampiran A, B, C, D, dan E.*
- b) *DPA ini telah ditandatangani sebelumnya atas nama Stoneware, Inc., termasuk Klausul Kontraktual Standar EU dalam Lampiran D, sebagai penerima data. (Catatan: Lampiran D umumnya berlaku hanya terhadap kegiatan pemrosesan yang mungkin melibatkan pengalihan Data Pribadi dari Uni Eropa, Wilayah Ekonomi Eropa, Inggris Raya, dan/atau negara lain dengan standar yang memadai atau kesetaraan serupa terkait pengalihan data lintas batas).*

For the avoidance of doubt, you need to sign this DPA on page 5. If applicable, Annex D will apply by reference.

Demi menghindari keraguan, Anda perlu menandatangani DPA ini di halaman 5. Jika berlaku, Lampiran D berlaku sebagai acuan.

Data Protection

Definitions: In this Clause, the following terms shall have the following meanings:

Perlindungan Data

Definisi: Pada Klausul ini, istilah-istilah berikut memiliki makna-makna sebagai berikut:

- a) **"Controller", "Processor", "Subprocessor", "Data Processing", and "Processing"** (and **"Process"**) shall have the meanings given in EU Data Protection Law and equivalent terms in Applicable Data Protection Law.
- b) **"Applicable Data Protection Law"** means all applicable laws, rules, regulations, orders, and all related amendments thereto, in any jurisdiction in which Supplier provides LanSchool Services, including any laws concerning privacy, data security, data protection, data breaches, and confidentiality such as the California Consumer Privacy Act of 2018 ("CCPA") and the California Privacy Rights Act ("CPRA"); the European Union's General Data Protection Regulation 2016/279, as amended, replaced or superseded from time to time ("GDPR"); the United Kingdom's Data Protection Act 2018 as amended; The Brazil Law No. 13.709/18 as amended ("LGPD") and the regulations implemented (or to be implemented); and any such applicable laws, including national, state and/or local education and student privacy laws.
- c) **"Personal Data"** is information that relates to an identified or identifiable individual including, but not limited to, students, parents, and school employees.
- a) **"Pengendali", "Pemroses", "Pemroses lanjutan", "Pemrosesan Data", dan "Pemrosesan"** (dan **"Proses"**) harus memiliki makna yang diberikan dalam Undang-Undang Perlindungan Data EU dan ketentuan setara dalam Undang-Undang Perlindungan Data yang Berlaku.
- b) **"Undang-Undang Perlindungan Data yang Berlaku"** berarti semua undang-undang, peraturan, regulasi, putusan, dan semua perubahan terkait yang berlaku, di yurisdiksi mana pun tempat Pemasok menyediakan Layanan LanSchool, termasuk undang-undang tentang privasi, keamanan data, pelanggaran data, perlindungan data, pelanggaran data, dan kerahasiaan seperti Undang-Undang Privasi Pelanggan California tahun 2018 ("CCPA") dan Undang-Undang Hak Privasi California ("CPRA"); Regulasi Perlindungan Data Umum Uni Eropa 2016/279, sebagaimana diubah, diganti atau disubstitusikan dari waktu ke waktu ("GDPR"); Undang-Undang Perlindungan Data Inggris Raya 2018 sebagaimana diubah; Undang-Undang Brazil No.13.709/18 sebagaimana di ubah ("LGPD") dan peraturan pelaksana (atau yang akan dilaksanakan); dan undang-undang yang berlaku, termasuk undang-undang privasi pendidikan dan siswa nasional, negara bagian dan/atau lokal.
- c) **"Data Pribadi"** berarti informasi yang berhubungan dengan individu yang teridentifikasi atau dapat diidentifikasi, termasuk namun tidak terbatas pada siswa, orang tua, dan pegawai sekolah.

- d) **“Data Subject”** is an individual person who can be identified directly or indirectly including, but not limited to, students, parents, and school employees.
- e) **“Customer”** is the Controller. For the purposes of this DPA only, the term “Customer” shall include Customer and Authorized Affiliates.
- f) **“Supplier”** means Stoneware, Inc., which acts as Processor.
- g) **“Data Exporter”** means a party that transfers Personal Data (acting as a Controller) to another Party in accordance with the Agreement.
- h) **“Data Importer”** means a party that receives Customer Personal Data (acting as a Processor or Subprocessor) from another Party (Controller) in accordance with this Agreement.
- d) **“Subyek Data”** berarti seseorang yang dapat diidentifikasi secara langsung maupun tidak langsung, termasuk namun tidak terbatas pada siswa, orang tua, dan pegawai sekolah.
- e) **“Pelanggan”** adalah Pengendali. Untuk tujuan hanya DPA ini, istilah “Pelanggan” harus meliputi Pelanggan dan Afiliasi Resmi.
- f) **“Pemasok”** berarti Stoneware, Inc. Yang bertindak sebagai Pemroses.
- g) **“ Pengirim Data”** berarti pihak yang mengirim Data Pribadi (bertindak sebagai Pengendali) ke Pihak lain sesuai dengan Perjanjian.
- h) **“Penerima Data”** berarti pihak yang menerima Data Pribadi Pelanggan (bertindak sebagai Pemroses atau Pemroses lanjutan) dari Pihak (Pengendali) sesuai dengan Perjanjian ini.

Relationship of the parties: The Controller acknowledges Supplier as a Processor to process the Personal Data that is the subject of Stoneware Sales Agreement, LanSchool Air Terms of Services and EULA with Supplier. Each party shall comply with the obligations that apply to it under Applicable Data Protection Law.

Hubungan para pihak: Pengendali mengakui Pemasok sebagai Pemroses untuk memproses Data Pribadi yang tunduk pada Perjanjian Penjualan Stoneware, Ketentuan Layanan LanSchool Air dan EULA dengan Pemasok. Tiap pihak harus mematuhi kewajiban yang berlaku padanya berdasarkan Undang-Undang Perlindungan Data yang Berlaku.

Purpose limitation: Supplier shall process the Personal Data as a Processor and strictly in accordance with the documented instructions of Controller (the "Permitted Purpose") as documented in Annex A "Processing details," except where otherwise required by any Applicable Data Protection Law. Supplier shall immediately inform Controller if it becomes aware that Controller's Processing instructions infringe Applicable Data Protection Law. In no event shall Supplier process the Personal Data for its own purposes or those of any third-party, including for marketing purposes. For the avoidance of doubt, Supplier shall not send marketing or otherwise promotional communications to Lenovo LanSchool Air users leveraging personal data obtained from the use of Lenovo Lan School Air. The latter will not prevent any individual from receiving marketing or promotional communications if those originate in the context of standard channels such as Stoneware or Lenovo website and other sales related channels.

Batasan Tujuan: Pemasok akan memproses Data Pribadi sebagai suatu Pemroses dan secara ketat mengikuti instruksi Pengendali yang terdokumentasi ("Tujuan yang Diizinkan") sebagaimana didokumentasi dalam Lampiran A "Rincian Pemrosesan," kecuali diwajibkan lain oleh Undang-Undang Perlindungan Data yang Berlaku. Pemasok harus segera memberitahu Pengendali jika pihaknya menjadi sadar bahwa instruksi Pemrosesan Pengendali melanggar Undang-undang Perlindungan Data yang berlaku. Dalam keadaan apapun, Pemasok tidak boleh memproses Data Pribadi demi tujuannya sendiri atau pihak ketiga, termasuk untuk tujuan pemasaran. Untuk menghindari keraguan, Pemasok tidak akan mengirimkan komunikasi yang bersifat promosi pemasaran ataupun promosi lainnya kepada Pengguna LanSchool Air Lenovo yang memanfaatkan data pribadi yang diperoleh dari penggunaan Lan School Air Lenovo. Yang tersebut terakhir tidak akan menghalangi seseorang pun untuk menerima komunikasi pemasaran atau promosi jika hal tersebut berasal dari konteks jaringan standar seperti Stoneware atau situs web Lenovo dan jaringan penjualan terkait lainnya.

International transfers: Supplier may transfer the Personal Data to any country outside of the country from which Personal Data was collected in compliance with applicable Data Protection and data localization laws. For the avoidance of doubt:

Pengalihan Internasional: Pemasok dapat mengalihkan Data Pribadi ke negara mana pun di luar negara tempat Data Pribadi dikumpulkan berdasarkan undang-Undang Perlindungan Data dan lokalisasi data yang berlaku. Untuk menghindari keraguan:

- a) Personal Data transfers outside of the European Economic Area ("EEA") and the United Kingdom are allowed: (i) if the Personal Data transfer is to a recipient in a country that the European Commission, United

- a) Data Pribadi yang dikirim ke luar Wilayah Ekonomi Eropa ("EEA") dan Inggris Raya diperbolehkan: (i) jika pengalihan Data Pribadi dilakukan untuk penerima dalam sebuah negara yang diputuskan Komisi

Kingdom Secretary of State, and/or the United Kingdom's Information Commissioner's Office have decided provides adequate protection for Personal Data; and (ii) to a recipient that has executed standard contractual clauses adopted or approved by the European Commission, United Kingdom Secretary of State, and/or the United Kingdom's Information Commissioner's Office.

Eropa, Menteri Dalam Negeri Inggris Raya, dan/atau Kantor Komisioner Informasi Inggris Raya menerima perlindungan yang cukup atas Data Pribadi; dan (ii) untuk penerima yang telah menjalankan klausul kontraktual standar yang diambil atau disetujui oleh Komisi Eropa, Menteri Dalam Negeri Inggris Raya, dan/atau Kantor Komisioner Informasi Inggris Raya.

Supplier may transfer the Personal Data outside of Brazil if: (i) the Data transfer is to a recipient in a country that the National Authority has decided provides adequate protection for Personal Data; (ii) to a recipient that has executed standard contractual clauses adopted or approved by the National Authority; or (iii) when the recipient is able to provide and demonstrate the implementation other safeguards in accordance to the Brazilian Data Protection Law and the international transfer is approved by the Controller.

Pemasok dapat mengalihkan Data Pribadi ke luar Brazil jika: (i) Pengalihan Data ke penerima di suatu negara yang Otoritas Nasional telah memutuskan menyediakan perlindungan yang memadai untuk Data Pribadi; (ii) ke penerima yang telah menjalankan klausul kontraktual standar yang diambil atau disetujui oleh Otoritas Nasional; atau (iii) ketika penerima mampu menyediakan dan mendemonstrasikan penerapan keamanan lain berdasarkan Undang-Undang Perlindungan Data Brazil dan pengalihan internasional disetujui oleh Pengendali.

b) Generally, the acceptance of this DPA results in approval by the Customer that Stoneware, Inc. may transfer Personal Data across borders to the extent that Stoneware complies with any applicable Data Protection Laws. In this regard, Annex D "International Data Transfers" applies between Controller and Supplier where relevant.

b) Secara umum, penerimaan DPA ini berarti persetujuan oleh Pengguna bahwa Stoneware, Inc. dapat mengalihkan Data Pribadi secara lintas batas sejauh Stoneware mematuhi Undang-Undang Perlindungan Data yang berlaku. Dalam hal ini, Lampiran D "Pengalihan Data Internasional" berlaku antara Pengendali dan Pemasok jika relevan.

Confidentiality of Processing: Supplier shall ensure that any person that it authorizes to process the Personal Data (including Supplier's staff, agents and subprocessor) (an "Authorized Person") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty) and shall not permit any person to process the Personal Data who is not under such a duty of confidentiality. Supplier shall ensure that all Authorized Persons process the Personal Data only as necessary for the Permitted Purpose. Furthermore, Supplier shall not commercially exploit the Personal Data.

Kerahasiaan Pemrosesan: Pemasok harus memastikan bahwa siapa pun yang ia beri wewenang untuk memproses Data Pribadi (termasuk staf, agen, dan pemroses lanjutan dari Pemasok) ("Orang yang Berwenang") harus tunduk pada kewajiban kerahasiaan secara ketat (baik kewajiban kontraktual atau pun kewajiban yang timbul dari undang-undang) dan tidak akan mengizinkan siapa pun memproses Data Pribadi jika ia tidak tunduk pada kewajiban kerahasiaan tersebut. Pemasok harus memastikan bahwa semua Orang yang Berwenang memproses Data Pribadi hanya jika diperlukan untuk Tujuan yang Diizinkan. Lebih lanjut, Pemasok tidak akan memanfaatkan Data Pribadi secara komersial.

Security: The Processor shall implement appropriate technical and organizational measures to protect the Personal Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorized disclosure of, or access to the Personal Data (a "Security Incident"). Annex C contains LanSchool Air Technical and Organisational Measures (TOMs).

Keamanan: Pemroses harus melaksanakan upaya-upaya teknis dan organisasi yang sesuai untuk melindungi Data Pribadi (i) dari penghancuran yang disengaja atau melanggar hukum, dan (ii) kehilangan, perubahan, pengungkapan atau akses ke Data Pribadi secara tidak sah ("Insiden Keamanan"). Lampiran C memuat Upaya-upaya Teknis dan Organisasi LanSchool Air (TOM).

Subprocessing: Supplier agrees that any third-party Subprocessor it appoints shall be bound to the same standard of data protection provided for by this Agreement; and that Supplier will enter into agreements accordingly with its applicable subprocessors to give appropriate effect to the requirements in this DPA Controller agrees that Supplier may use any subprocessor listed in Annex B. Notwithstanding this, Controller consents to Supplier engaging new subprocessors (including the replacement of existing ones) to process the Personal Data, **provided that:** (i)

Pemrosesan Lanjutan: Pemasok setuju bahwa Pemroses lanjutan pihak ketiga mana pun yang ditunjuknya harus terikat standar perlindungan data yang sama yang diatur di dalam Perjanjian ini; dan bahwa Pemasok akan mengikatkan diri ke dalam perjanjian-perjanjian sebagaimana mestinya dengan pemroses lanjutan yang berlaku untuk memberikan efek yang sesuai terhadap persyaratan dalam DPA ini, Pengendali setuju bahwa Pemasok dapat menggunakan pemroses lanjutannya sebagaimana tercantum dalam Lampiran B. Terlepas dari hal ini, Pengendali mengizinkan Pemasok melibatkan pemroses

Supplier provides at least 30 business days prior notice of the addition or replacement of any subprocessor (including details of the processing it performs or will perform), which may be given by provided details of such addition or replacement to Controller; and (ii) Supplier imposes data protection terms on any subprocessor it appoints that protect the Personal Data to the same standard provided for by this DPA. If Controller refuses to consent to Supplier's appointment of a new third-party subprocessor, which should not be withheld unreasonably, then either Supplier will not appoint the subprocessor or Controller may elect to terminate the Agreement, provided that the Controller has substantial and documented reasons for objection to the change.

lanjutan baru (termasuk penggantian Pemroses lanjutan yang sudah ada) untuk memproses Data Pribadi, **dengan ketentuan bahwa:** (i) Pemasok memberikan pemberitahuan penambahan atau penggantian pemroses lanjutan (termasuk rincian pemrosesan yang dilakukan atau akan dilakukan olehnya) selambat-lambatnya 30 hari kerja sebelumnya, yang dapat diberikan dengan menyediakan rincian penambahan atau penggantian tersebut kepada Pengendali; dan (ii) Pemasok menerapkan ketentuan perlindungan data kepada pemroses lanjutan yang ditunjuknya bahwa perlindungan Data Pribadi dilakukan sama seperti standar yang disediakan oleh DPA ini. Jika Pengendali menolak memberikan izin terhadap penunjukan pemroses lanjutan pihak ketiga yang baru oleh Pemasok, yang tidak boleh tidak diberikan dengan alasan yang tidak wajar, maka Pemasok tidak akan menunjuk pemroses lanjutan tersebut atau Pengendali dapat memilih mengakhiri Perjanjian, dengan ketentuan bahwa Pengendali memiliki alasan-alasan substansial dan terdokumentasi atas keberatan perubahan tersebut.

Cooperation and Data Subjects' rights:

Supplier shall provide reasonable and timely assistance to Controller to enable Controller to respond to: (i) any request from a Data Subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and Personal Data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a Data Subject, regulator or other third-party in connection with the Processing of the Personal Data. For the avoidance of doubt, Data Subject Requests (DSRs) shall be requested by Controller by

Hak Perusahaan dan Subyek Data:

Pemasok akan menyediakan bantuan yang wajar dan tepat waktu kepada Pengendali untuk memungkinkan Pengendali menanggapi: (i) permintaan apa pun dari Subyek Data untuk menjalankan hak-haknya berdasarkan Undang-Undang Perlindungan Data yang Berlaku (termasuk hak akses, perbaikan, keberatan, penghapusan, dan Portabilitas Data Pribadi, jika berlaku); dan (ii) korespondensi lain, pertanyaan atau komplain yang diterima dari Subyek Data, pengatur atau pihak ketiga lain sehubungan dengan Pemrosesan Data Pribadi. Untuk menghindari keraguan, Permintaan Subyek Data (DSRs) akan dimintakan oleh Pengendali

submitting a formal request in the [Stoneware DSR Privacy Webform](#).

Security incidents: Upon becoming aware of a Security Incident, Supplier shall inform Controller without undue delay and shall provide all such timely information and cooperation as Controller may require to fulfil its Personal Data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. Supplier shall further take measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep Controller informed of all developments in connection with the Security Incident.

Deletion or return of Data: Upon termination or expiry of the Stoneware Sales Agreement, Supplier shall, upon Controller's request, destroy or return to Controller all Personal Data (including all copies of the Personal Data) in its possession or control (including any Personal Data subcontracted to a third-party for Processing). If Controller does not give further instructions to Supplier, Supplier's data retention schedule, as laid out in Annex A, will apply. This requirement shall not apply to the extent that Supplier is required by any applicable Data Protection Law to retain some or all of the Personal Data, in which event Supplier shall isolate and protect the Personal Data from any further Processing except to the extent required by such law.

dengan mengajukan suatu permohonan resmi dalam [Stoneware DSR Privacy Webform](#).

Insiden Keamanan: Setelah menyadari adanya Insiden Keamanan, Pemasok harus memberitahukan kepada Pengendali tanpa penundaan dan harus memberikan semua informasi dan kerja sama dengan tepat waktu sebagaimana dibutuhkan Pengendali untuk memenuhi kewajiban pelaporan pelanggaran Data Pribadi berdasarkan (dan sesuai dengan rentang waktu yang disyaratkan oleh) Undang-Undang Perlindungan Data yang Berlaku. Pemasok harus mengambil langkah dan tindakan lebih lanjut yang dibutuhkan untuk memulihkan atau mengurangi dampak Insiden Keamanan dan harus terus memberitahukan kepada Pengendali tentang semua perkembangan sehubungan dengan Insiden Keamanan.

Penghapusan atau pengembalian Data: Setelah pengakhiran atau berakhirnya Perjanjian Penjualan Stoneware, Pemasok harus, atas permintaan Pengendali, menghancurkan atau mengembalikan kepada Pengendali semua Data Pribadi (termasuk semua salinan Data Pribadi) dalam kepemilikan atau kendalinya (termasuk Data Pribadi apa pun yang dibuat kontrak lanjutan dengan pihak ketiga untuk Pemrosesan). Jika Pengendali tidak memberikan instruksi lebih lanjut kepada Pemasok, jadwal retensi data Pemasok, sebagaimana tercantum dalam Lampiran A, akan berlaku. Persyaratan ini tidak berlaku sejauh Pemasok diwajibkan oleh Undang-Undang Perlindungan Data yang berlaku untuk menyimpan beberapa atau semua Data Pribadi, maka Pemasok harus memisahkan dan melindungi Data Pribadi dari pemrosesan lebih

lanjut kecuali sejauh diwajibkan oleh undang-undang tersebut.

Audit: During the term of this Agreement and for three years after termination or expiration, Supplier shall permit Controller (or its third-party auditors) to audit Supplier's compliance at its own expense and shall make available to Controller information necessary for Controller (or its third-party auditors) to conduct such audit, provided that such audit request is reasonable in scope and that Controller gives it reasonable prior notice of its intention to audit. Controller will not exercise its audit rights more than once in any twelve (12) calendar month period, except if and when required by instruction of a competent data protection authority.

Audit: Selama masa Perjanjian ini dan untuk tiga tahun setelah pengakhiran atau berakhirnya Perjanjian, Pemasok harus mengizinkan Pengendali (atau auditor pihak ketiganya) untuk mengaudit kepatuhan Pemasok dengan biayanya sendiri dan harus menyediakan kepada Pengendali informasi yang dibutuhkan Pengendali (atau auditor pihak ketiganya) untuk melaksanakan audit tersebut, dengan ketentuan bahwa permintaan audit tersebut bersifat wajar dan dalam ruang lingkup dan Pengendali memberikan pemberitahuan wajar sebelumnya mengenai niatnya untuk mengadakan audit. Pengendali tidak akan menjalankan hak auditnya lebih dari sekali dalam dua belas (12) bulan kalender, kecuali jika dan saat dibutuhkan oleh petunjuk otoritas perlindungan data yang kompeten.

IN WITNESS WHEREOF, Stoneware and Customer have executed this Agreement as of the date written above.

DEMIKIAN, Stoneware dan Pelanggan telah menandatangani Perjanjian ini pada tanggal yang tertulis di atas.

Stoneware, Inc.

Customer/Pelanggan

Signature/

Signature/

Tanda Tangan:

Tanda Tangan: _____

Print Name/

Print Name/

Nama Dengan Huruf Cetak : Kimberly Page

Nama Dengan Huruf Cetak: Kimberly Page

Title/Jabatan: Strategic Operations Manager

Title/Jabatan: Manajer Operasi Strategis

ANNEX A/LAMPIRAN A – PROCESSING DETAILS/RINCIAN PEMROSESAN

Type of data & data subjects/ <i>Jenis data & subyek data</i>	Retention Period/ <i>Periode Retensi</i>	Nature, purpose, and subject matter/ <i>Sifat, tujuan, dan pokok bahasan</i>
<p>Student Interface related data:/Data terkait Antarmuka Siswa:</p> <ul style="list-style-type: none"> • The auto-generated unique GUID of the student/<i>GUID unik siswa yang dijalankan secara otomatis</i> • The student ID as provided. /<i>ID siswa yang disediakan.</i> • The first name of the student. /<i>Nama depan siswa.</i> • The last name of the student. /<i>Nama belakang siswa.</i> • The e-mail address of the student. /<i>Alamat email siswa.</i> • The student’s login name. /<i>Nama login siswa.</i> • The date that this student object was created. /<i>Tanggal obyek siswa ini dibuat.</i> • The date that this student object was updated. /<i>Tanggal obyek siswa ini diperbarui</i> 	<p>Upon user’s request for deletion or after 1 year of not having an active license or trial, data will be archived. Archived data is purged after 90 days. /</p> <p><i>Atas permintaan pengguna untuk penghapusan atau setelah 1 tahun tidak memiliki lisensi atau masa percobaan yang aktif, data akan diarsipkan. Data terarsip akan dibersihkan setelah 90 hari.</i></p>	<p><i>Data Storage (record, host, log, archive or otherwise store Customer Data);</i></p> <p><i>Data Access (retrieve, copy, examine, modify, transport, scan, or otherwise access Customer Data)/</i></p> <p><i>Penyimpanan Data (menyimpan, melakukan host, mencatat, mengarsipkan atau secara lain menyimpan Data Pelanggan);</i></p> <p><i>Akses Data (mengambil, menyalin, memeriksa, memodifikasi, memindahkan, memindai, atau secara lain mengakses Data Pelanggan)</i></p>
<p>School Employee Interface related data:/Data terkait Antarmuka Pegawai Sekolah:</p> <ul style="list-style-type: none"> • The auto-generated unique GUID of the teacher/<i>GUID unik guru yang dijalankan secara otomatis</i> • The school employee’s ID. /<i>ID pegawai sekolah.</i> 	<p>Upon user’s request for deletion or after 1 year of not having an active license or trial, data will be archived. Archived data is purged after 90 days. /</p> <p><i>Atas permintaan pengguna untuk</i></p>	<p><i>Data Storage (record, host, log, archive or otherwise store Customer Data);</i></p> <p><i>Data Access (retrieve, copy, examine, modify, transport, scan, or otherwise access Customer Data)</i></p>

<ul style="list-style-type: none"> • The first name of the school employee./Nama depan pegawai sekolah. • The last name of the school employee./Nama belakang pegawai sekolah. • The e-mail address of the school employee./Alamat surat elektronik (e-mail) pegawai sekolah. • The MongoDB ID of the cloud user that corresponds to this teacher object. /IDMongoDB pengguna cloud yang terhubung dengan obyek guru ini. • Access tokens / Token akses • The date that this school employee object was created. /Tanggal obyek pegawai sekolah ini dibuat. • The date that this school employee object was updated. /Tanggal obyek pegawai sekolah ini diperbarui. 	<p><i>penghapusan atau setelah 1 tahun tidak memiliki lisensi atau masa percobaan yang aktif, data akan diarsipkan. Data terarsip akan dibersihkan setelah 90 hari.</i></p>	<p><i>Data Analysis (survey, test, study, interpret, organize, report, or otherwise analyse Customer Data)./</i></p> <p><i>Penyimpanan Data (menyimpan, melakukan host, mencatat, mengarsipkan atau secara lain menyimpan Data Pelanggan);</i></p> <p><i>Akses Data (mengambil, menyalin, memeriksa, memodifikasi, memindahkan, memindai, atau secara lain mengakses Data Pelanggan)</i></p> <p><i>Analisis Data (menyurvei, menguji, mempelajari, menginterpretasikan, menyusun, melaporkan, atau secara lain menganalisis Data Pelanggan).</i></p>
<p>Client Interface related data:/Data terkait Antarmuka Klien:</p> <ul style="list-style-type: none"> • The auto-generated unique GUID of the client/GUID unik klien yang dijalankan secara otomatis • The login name of the current student. It could be an e-mail address or a username. /Nama login siswa saat ini. Bisa menggunakan alamat email atau nama pengguna. • The MongoDB ID of the corresponding device from the core database. /IDMongoDB dari perangkat terkait dari database inti. 	<p>Upon user’s request for deletion or after 1 year of not having an active license or trial, data will be archived. Archived data is purged after 90 days. /</p> <p><i>Atas permintaan pengguna untuk penghapusan atau setelah 1 tahun tidak memiliki lisensi atau masa percobaan yang</i></p>	<p><i>Data Storage (record, host, log, archive or otherwise store Customer Data);</i></p> <p><i>Data Access (retrieve, copy, examine, modify, transport, scan, or otherwise access Customer Data)</i></p> <p><i>Data Analysis (survey, test, study, interpret, organize, report, or</i></p>

<ul style="list-style-type: none"> • The date that this client object was created. / <i>Tanggal obyek klien ini dibuat.</i> • The date that this client object was updated. / <i>Tanggal obyek klien ini diperbarui.</i> 	<p><i>aktif, data akan diarsipkan. Data terarsip akan dibersihkan setelah 90 hari.</i></p>	<p>otherwise analyse Customer Data)./ <i>Penyimpanan Data (menyimpan, melakukan host, mencatat, mengarsipkan atau secara lain menyimpan Data Pelanggan);</i> <i>Akses Data (mengambil, menyalin, memeriksa, memodifikasi, memindahkan, memindai, atau secara lain mengakses Data Pelanggan)</i> <i>Analisis Data (menyurvei, menguji, mempelajari, menginterpretasikan, menyusun, melaporkan, atau secara lain menganalisis Data Pelanggan).</i></p>
<p>Class list related data/ <i>Data terkait daftar kelas</i></p> <ul style="list-style-type: none"> • The auto-generated unique GUID of the class/<i>GUID unik kelas yang dijalankan secara otomatis</i> • The name of this class. This is required. /<i>Nama kelas ini diperlukan.</i> • The class ID as provided by the Student Information System. /<i>ID kelas yang disediakan oleh Sistem Informasi Siswa.</i> • The school ID as provided by the Student Information System. /<i>ID sekolah yang disediakan oleh Sistem Informasi Siswa.</i> • The class period or other designation that distinguishes this 	<p>Upon user’s request for deletion or after 1 year of not having an active license or trial, data will be archived. Archived data is purged after 90 days. /</p> <p><i>Atas permintaan pengguna untuk penghapusan atau setelah 1 tahun tidak memiliki lisensi atau masa percobaan yang aktif, data akan diarsipkan. Data terarsip</i></p>	<p><i>Data Storage (record, host, log, archive or otherwise store Customer Data);</i> <i>Data Access (retrieve, copy, examine, modify, transport, scan, or otherwise access Customer Data)</i> <i>Data Analysis (survey, test, study, interpret, organize, report, or otherwise analyse Customer Data)./</i></p>

<p>class from other classes of the same type. /Periode kelas atau tujuan lain yang membedakan kelas ini dari kelas lain dalam jenis yang sama.</p> <ul style="list-style-type: none"> • The owner of this class list. /Pemilik daftar kelas ini. • The teacher objects for the teachers that have access to this class list. The Teacher Interface is defined below. /Obyek guru untuk guru yang memiliki akses ke daftar kelas ini. Antarmuka guru dijelaskan di bawah ini. • The student objects for the students that belong to this class list. /Obyek siswa untuk siswa yang termasuk dalam daftar kelas ini. • The client objects for the devices that belong to this class list. /Obyek klien untuk perangkat yang termasuk dalam daftar kelas ini. • The ID of the user that last changed this class list. /ID pelanggan yang terakhir mengubah daftar kelas ini. • The date that this class list was created. /Tanggal kelas ini dibuat. • The date that this class list was updated. /Tanggal kelas ini diperbarui. 	<p>akan dibersihkan setelah 90 hari.</p>	<p>Penyimpanan Data (menyimpan, melakukan host, mencatat, mengarsipkan atau secara lain menyimpan Data Pelanggan);</p> <p>Akses Data (mengambil, menyalin, memeriksa, memodifikasi, memindahkan, memindai, atau secara lain mengakses Data Pelanggan)</p> <p>Analisis Data (menyurvei, menguji, mempelajari, menginterpretasikan, menyusun, melaporkan, atau secara lain menganalisis Data Pelanggan).</p>
<p>Organization related data/ Data terkait organisasi</p> <ul style="list-style-type: none"> • The auto-generated unique GUID of the organization /GUID unik organisasi yang dijalankan secara otomatis • The name of the organization. /Nama organisasi. • The ID assigned to this organization. /ID yang ditetapkan ke organisasi ini. • The primary street addresses. /Alamat jalan utama. • The secondary street address information. / Informasi alamat jalan sekunder. 	<p>Upon user's request for deletion or after 1 year of not having an active license or trial, data will be archived. Archived data is purged after 90 days. /</p> <p>Atas permintaan pengguna untuk penghapusan atau setelah 1 tahun tidak memiliki lisensi atau masa percobaan yang aktif, data akan diarsipkan. Data tersip</p>	<p>Data Storage (record, host, log, archive or otherwise store Customer Data);</p> <p>Data Access (retrieve, copy, examine, modify, transport, scan, or otherwise access Customer Data);</p> <p>Data Analysis (survey, test, study, interpret, organize, report, or otherwise analyse Customer Data). /</p>

<ul style="list-style-type: none"> • The city of the organization. /Kota Organisasi • The state or province of the organization. /Negara bagian atau provinsi organisasi. • The postal code of the organization. /Kode pos organisasi. • The country of the organization. /Negara organisasi. • The administrative contact information. /Informasi kontak administratif. • The technical contact information. /Informasi kontak teknis. • The billing contact information. /Informasi kontak tagihan. • A flag indicating if this organization has a site agent. /Bendera (penanda) yang menandakan jika organisasi ini memiliki agen situs. • The date that this organization was created. /Tanggal organisasi ini dibuat. • The default security policy for the organization. /Kebijakan keamanan bawaan untuk organisasi. • Organization's contact data: first name, last name, phone number, e-mail address. /Data kontak organisasi: nama depan, nama belakang, nomor telepon, alamat email. 	<p>akan dibersihkan setelah 90 hari.</p>	<p>Penyimpanan Data (menyimpan, melakukan host, mencatat, mengarsipkan atau secara lain menyimpan Data Pelanggan);</p> <p>Akses Data (mengambil, menyalin, memeriksa, memodifikasi, memindahkan, memindai, atau secara lain mengakses Data Pelanggan)</p> <p>Analisis Data (menyurvei, menguji, mempelajari, menginterpretasikan, menyusun, melaporkan, atau secara lain menganalisis Data Pelanggan).</p>
<p>User data / Data pengguna</p> <ul style="list-style-type: none"> • The auto-generated unique GUID of the user / GUID unik pengguna yang dijalankan secara otomatis • A set of key-value pairs of all current IDs of user, /Kumpulan sepasang nilai kunci dari semua ID pengguna terkini. • The first name of the user. /Nama depan pengguna. • The last name of the user. /Nama belakang pengguna. 	<p>Upon user's request for deletion or after 1 year of not having an active license or trial, data will be archived. Archived data is purged after 90 days. /</p> <p>Atas permintaan pengguna untuk penghapusan atau setelah 1 tahun tidak memiliki lisensi atau masa percobaan yang</p>	<p>Data Storage (record, host, log, archive or otherwise store Customer Data);</p> <p>Data Access (retrieve, copy, examine, modify, transport, scan, or otherwise access Customer Data)</p> <p>Data Analysis (survey, test, study, interpret, organize, report, or</p>

<ul style="list-style-type: none"> • The e-mail address of the user. / <i>Alamat surat elektronik (e-mail) pengguna.</i> • Permissions directly assigned to this user. / <i>Izin yang secara langsung diberikan kepada pengguna ini.</i> • A reference to the organization of which this user belongs. / <i>Acuan terhadap organisasi tempat pengguna ini berada.</i> • A subset of user IDs that a user is allowed to use for a login. / <i>SubsetID pengguna yang diperbolehkan untuk digunakan saat login.</i> • A timestamp of the last time the user successfully logged into the system. / <i>Tanda waktu terakhir kali pengguna berhasil masuk ke sistem.</i> • A timestamp of the first time the user failed authentication within the past hour. / <i>Tanda waktu pertama kali pengguna gagal mengautentikasi dalam sejam terakhir.</i> • The IP address of where the last successful login took place. / <i>Alamat IP tempat login berhasil terakhir kali dilakukan.</i> • The IP address of where the last failed login took place. / <i>Alamat IP tempat login gagal terakhir kali dilakukan.</i> • The timestamp of the last failed login attempt. / <i>Alamat IP tempat login gagal terakhir kali diupayakan.</i> • A counter for the number of consecutive failed login attempts. / <i>Penghitung jumlah upaya login yang gagal secara berturut-turut.</i> • The permissions granted to the user. Generated by combining all permissions from the user's groups. / <i>Izin yang diberikan kepada pengguna. Dijalankan dengan menggabungkan semua izin dari grup pengguna.</i> 	<p><i>aktif, data akan diarsipkan. Data terarsip akan dibersihkan setelah 90 hari.</i></p>	<p>otherwise analyse Customer Data)./</p> <p><i>Penyimpanan Data (menyimpan, melakukan host, mencatat, mengarsipkan atau secara lain menyimpan Data Pelanggan);</i></p> <p><i>Akses Data (mengambil, menyalin, memeriksa, memodifikasi, memindahkan, memindai, atau secara lain mengakses Data Pelanggan)</i></p> <p><i>Analisis Data (menyurvei, menguji, mempelajari, menginterpretasikan, menyusun, melaporkan, atau secara lain menganalisis Data Pelanggan).</i></p>
---	--	---

<ul style="list-style-type: none"> • The date that this user was created. /Tanggal pengguna ini dibuat. • The date that this user was updated. /Tanggal pengguna ini diperbarui. 		
<p>Activity Log related data/ Data terkait Aktivitas Log</p> <ul style="list-style-type: none"> • Student web browsing history (URL, timestamp). /Riwayat penjelajahan web siswa (URL, tanda waktu). • Student application history (application name, timestamp). /Riwayat aplikasi siswa (nama aplikasi, tanda waktu). • Classroom chat message history (sender, receive, message content, timestamp). /Riwayat pesan obrolan kelas (pengirim, penerima, isi pesan, tanda waktu). • Administrative activity log (user ID, activity type, timestamp). / Aktivitas administratif log (ID pengguna, jenis aktivitas, tanda waktu). 	<p>Upon user's request for deletion or after 45 days. / Atas permintaan pengguna untuk penghapusan atau setelah 45 hari.</p>	<p><i>Data Storage</i> (record, host, log, archive or otherwise store Customer Data);</p> <p><i>Data Access</i> (retrieve, copy, examine, modify, transport, scan, or otherwise access Customer Data);</p> <p><i>Data Analysis</i> (survey, test, study, interpret, organize, report, or otherwise analyse Customer Data)./</p> <p><i>Penyimpanan Data</i> (menyimpan, melakukan host, mencatat, mengarsipkan atau secara lain menyimpan Data Pelanggan);</p> <p><i>Akses Data</i> (mengambil, menyalin, memeriksa, memodifikasi, memindahkan, memindai, atau secara lain mengakses Data Pelanggan);</p> <p><i>Analisis Data</i> (menyurvei, menguji, mempelajari, menginterpretasikan, menyusun, melaporkan, atau secara lain menganalisis Data Pelanggan).</p>

<p>License data (Excludes personal data)/Data lisensi (Tidak termasuk data pribadi)</p>	<p>This data is kept as long as necessary to comply with legal obligations, to enforce our agreements, etc. This does not include personal data. /</p> <p><i>Data ini disimpan selama diperlukan untuk memenuhi kewajiban hukum, melaksanakan perjanjian, dll. Tidak termasuk data pribadi.</i></p>	<p><i>Data Storage</i> (record, host, log, archive or otherwise store Customer Data);</p> <p><i>Data Access</i> (retrieve, copy, examine, modify, transport, scan, or otherwise access Customer Data);</p> <p><i>Data Analysis</i> (survey, test, study, interpret, organize, report, or otherwise analyse Customer Data). /</p> <p><i>Penyimpanan Data</i> (menyimpan, melakukan host, mencatat, mengarsipkan atau secara lain menyimpan Data Pelanggan);</p> <p><i>Akses Data</i> (mengambil, menyalin, memeriksa, memodifikasi, memindahkan, memindai, atau secara lain mengakses Data Pelanggan)</p> <p><i>Analisis Data</i> (menyurvei, menguji, mempelajari, menginterpretasikan, menyusun, melaporkan, atau secara lain menganalisis Data Pelanggan).</p>
---	---	--

Duration of the Processing/Jangka Waktu Pemrosesan

The duration of the processing corresponds to the duration of the Agreement. Data retention policies as described above will apply./*Jangka waktu pemrosesan sesuai dengan jangka waktu Perjanjian. Kebijakan retensi data sebagaimana dijelaskan di atas akan berlaku.*

Categories of Data Subjects/Kategori Subjek Data

Students, Teachers, Organization contacts and Users in general./*Kontak Siswa, Guru, Organisasi dan Pengguna secara umum.*

ANNEX B/LAMPIRAN B – SUBPROCESSORS/PEMROSES LANJUTAN

Name/Name	Data	Storage Location/Lokasi Penyimpanan	Purpose/Tujuan
Amazon Web Services/ <i>Layanan Web Amazon</i>	All user data as described in Annex A/ <i>Semua data pengguna sebagaimana dijelaskan dalam Lampiran A</i>	AU, US, UK (<i>regional transfer restrictions are applied, meaning e.g. European data stored exclusively in the UK.</i>) / AU, AS, Inggris (<i>pembatasan transfer regional diberlakukan, misalnya data Eropa disimpan secara eksklusif di Inggris.</i>)	Cloud service provider for the application infrastructure. All Data is processed by the application. / <i>Penyedia layanan cloud untuk infrastruktur aplikasi. Semua Data diproses oleh aplikasi.</i>
Canny	Feedback sent by customers, email addresses and hashes of the user first name, last name, and user id / <i>Masukan yang dikirim oleh pelanggan, alamat email, dan hash nama depan pengguna, nama belakang, dan id pengguna</i>	US / AS	Help users provide enhancement requests. / <i>Membantu pengguna menyediakan permintaan peningkatan.</i>
Datadog	Application data, IP address and username / <i>Data aplikasi, alamat IP, dan nama pengguna</i>	US / AS	Log collection tool. / <i>Perangkat pengumpulan log.</i>
Hubspot	First name, Last name, Email, Phone, Company Name, Title, Geographic tag (e.g., state), Industry / <i>Nama depan, Nama belakang, Email, Nomor Telepon, Nama Perusahaan, Jabatan, Tanda Geografis (misalnya negara bagian), Industri</i>	Hubspot's product infrastructure is hosted on Amazon Web Services (AWS) in the United States East region. HubSpot leverages the Google Cloud Platform (GCP) in the EU (Frankfurt, Germany region) to support the	On-boarding. / <i>masa pengenalan.</i>

		<p>processing of local customer data that is critical to our customers' businesses. This includes leads, email events, and analytics.</p> <p><i>/ Infrastruktur produk Hubspot dihost pada Layanan Web Amazon (AWS) di wilayah Amerika Timur. HubSpot memanfaatkan Platform Google Cloud (GCP) di EU (wilayah Frankfurt, Jerman) untuk mendukung pemrosesan data pelanggan lokal yang penting untuk bisnis pelanggan. Ini meliputi petunjuk, acara email, dan analitik.</i></p>	
Loggly	<p>Application data, IP address and username / <i>Data aplikasi, alamat IP, dan nama pengguna</i></p>	US / AS	<p>Log collection tool. / <i>Perangkat pengumpulan log</i></p>
MongoDB Atlas	<p>All user data as described in Annex A/</p>	<p>AU, US, UK (<i>regional transfer restrictions are applied, meaning e.g. European data stored exclusively in the UK</i>). / <i>AU, AS, Inggris</i></p>	<p>For the application to run correctly. / <i>Agar aplikasi berjalan secara benar.</i></p>

	<i>Semua data pengguna sebagaimana dijelaskan dalam Lampiran A</i>	<i>(pembatasan transfer regional diberlakukan, misalnya data Eropa disimpan secara eksklusif di Inggris).</i>	
Pendo	<p>Application usage analytics, visitor (first name, last name, email)</p> <p>Organization Name/</p> <p><i>Analitis penggunaan aplikasi pengunjung (nama depan, nama belakang, email)</i></p> <p><i>Nama Organisasi</i></p>	US / AS	<p>To improve the functionality and usability of the product. /</p> <p><i>Untuk meningkatkan fungsionalitas dan kegunaan produk.</i></p>
Twilio	Customers IP/IP Pelanggan	<p>US, data is only processed, not stored. /</p> <p><i>AS, data hanya diproses, tidak disimpan.</i></p>	<p>Provides STUN/TURN based traversal services for establishing live event streaming and telephony connectivity./</p> <p><i>Menyediakan layanan traversal berbasis STUN/TURN untuk membuat streaming acara langsung dan konektivitas teleponi.</i></p>

**ANNEX C/LAMPIRAN C – TECHNICAL AND ORGANIZATIONAL MEASURES (TOMs)/ UPAYA-UPAYA
TEKNIS DAN ORGANISASI (TOM)**

Supplier has implemented a comprehensive and written security program with physical, technical, procedural, and administrative controls that reflect prevailing industry standards for the protection and responsible use of Personal Data including, but not limited to, the following controls:

/
Pemasok telah menjalankan program keamanan yang menyeluruh dan tertulis dengan kendali fisik, teknis, prosedural, dan administratif yang mencerminkan standar industri yang berlaku untuk perlindungan dan tanggung jawab penggunaan Data Pribadi, termasuk namun tidak terbatas pada pengendalian-pengendalian berikut ini:

Technical/Teknis	Scope/Lingkup	Controls/Kendali
Access/Akses	Logins (system & application). /Login (sistem & aplikasi).	NIST-based password policies (multi-factor authentication for admin-level access and interfaces). / <i>Kebijakan kata sandi berbasis NIST</i> (otentikasi multi faktor untuk akses dan antarmuka tingkat admin).
Encryption/Enkripsi	Data storage at rest & in transit. / <i>Penyimpanan data saat tidak aktif & transit.</i>	AES 256-GCM (at rest), TLS 1.2 (in transit) Protocol TLS 1.3 (in transit) Supported TLS Ciphers TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256

		<p>ECDHE-ECDSA-AES256-GCM-SHA384</p> <p>ECDHE-RSA-AES256-GCM-SHA384</p> <p>(server preferred cipher suites). /</p> <p><i>AES 256-GCM (tidak aktif),</i></p> <p><i>TLS 1.2 (dalam transit)</i></p> <p>Protocol TLS 1.3 (dalam transit)</p> <p>Cipher TLS yang didukung</p> <p>TLS_AES_128_GCM_SHA256</p> <p>TLS_AES_256_GCM_SHA384</p> <p>TLS_CHACHA20_POLY1305_SHA256</p> <p>ECDHE-ECDSA-AES128-GCM-SHA256</p> <p>ECDHE-RSA-AES128-GCM-SHA256</p> <p>ECDHE-ECDSA-AES256-GCM-SHA384</p> <p>ECDHE-RSA-AES256-GCM-SHA384</p> <p>(cipher suites pilihan server).</p>
<p>Static application security testing/ <i>Pengujian keamanan aplikasi statik</i></p>	<p>All server and micro-service images, All binary clients and extensions/plugins. / <i>Semua server dan gambar mikro-service,</i></p>	<p>Regular vulnerability scans and monitoring. / <i>Pemindaian dan pengawasan kerentanan secara berkala.</i></p>

	<i>Semua klien biner dan ekstensi/plugin.</i>	
Dynamic application security testing/ <i>Pengujian keamanan aplikasi Dinamis</i>	External applications APIs. / <i>API aplikasi eksternal.</i>	Web application scans, Penetration testing (Regular internal tests). / <i>Pemindaian aplikasi web,</i> <i>Pengujian penetrasi</i> (<i>Pengujian internal secara berkala.</i>)
CIS benchmark hardening / Penguatan Tolok Ukur CIS	Cloud platform provider, Server instances. / <i>Penyedia platform cloud,</i> <i>Instances server.</i>	Cloud CIS compliance checks, Cloud security monitoring, Regular CIS L2 server benchmark assessments. / <i>Pengecekan kepatuhan CIS cloud, Pengawasan keamanan cloud,</i> <i>Penilaian tolok ukur server CIS L2 reguler.</i>
Software compositional analysis/ <i>Analisis komposisional perangkat lunak</i>	3 rd party opensource dependencies. / <i>Dependensi opensource pihak ke-3.</i>	Conduct regular vulnerability audits, repository monitoring. / <i>Menjalankan audit kerentanan secara berkala, pengawasan penyimpanan.</i>
Infrastructure assessment/ <i>Penilaian infrastruktur</i>	Cloud platform provider. / <i>Penyedia platform cloud.</i>	Regular reviews of all software-defined networks (SDNs) (identify network segmentation, firewall configuration, and resource access misconfigurations). / <i>Peninjauan reguler terhadap semua jaringan yang ditentukan perangkat lunak (SDN)</i> (<i>mengidentifikasi segmentasi jaringan, konfigurasi firewall, dan kesalahan konfigurasi akses sumber daya.</i>)

<p>Web application firewall (WAF)/ <i>Firewall aplikasi web (WAF)</i></p>	<p>Production web applications. / <i>Aplikasi web produksi.</i></p>	<p>WAF protection (core rules for common attacks). / <i>Perlindungan WAF</i> (peraturan inti untuk serangan umum).</p>
<p>Static code analysis/ <i>Analisis kode statik</i></p>	<p>Proprietary code. / <i>Kode kepemilikan.</i></p>	<p>Regular code analysis is conducted using a commercial tool, secure code reviews are conducted during code merges. / <i>Analisis kode secara berkala dilakukan menggunakan alat komersial, peninjauan kode keamanan dilakukan selama penggabungan kode.</i></p>
<p>Log collection/ <i>Koleksi log</i></p>	<p>Cloud platform provider, Application. / <i>Penyedia platform cloud, Aplikasi.</i></p>	<p>Cloud platform API transactions (logs older than 360-days are purged, accessible by engineering), WAF logging for edge detection (logs older than 90-days are purged, accessible by engineering), Subprocessors, see Annex B, for application purposes. / <i>Transaksi API platform cloud (log berusia lebih dari 360 hari akan dibersihkan, dapat diakses oleh teknisi),</i> <i>Pengelogan WAF untuk deteksi tepi (log berusia lebih dari 90 hari dibersihkan, dapat diakses oleh teknisi),</i> <i>Pemroses lanjutan, lihat lampiran B untuk tujuan aplikasi.</i></p>

<p>Infrastructure as code/ <i>Infrastruktur sebagai kode</i></p>	<p>Cloud platform provider. / <i>Penyedia platform cloud.</i></p>	<p>Infrastructure as code is used to automate infrastructure deployments and improve the immutability, misconfiguration of infrastructure. / <i>Infrastruktur sebagai kode digunakan untuk mengotomatisasi penerapan infrastruktur dan meningkatkan kekekalan, kesalahan konfigurasi infrastruktur.</i></p>
--	---	--

Organizational/Organisasi	Scope/Lingkup	Controls/Kendali
<p>Incident (including data breach) response/ <i>Respon insiden (termasuk pelanggaran data)</i></p>	<p>Security events related to products in production. / <i>Peristiwa keamanan terkait produk-produk dalam produksi.</i></p>	<p>Product incident response plan in accordance with NIST 800-61 and Lenovo’s internal Product Security Incident Response Team (PSIRT) processes. / <i>Rencana respon insiden produk berdasarkan NIST 800-61 dan proses Tim Respon Insiden Keamanan Produk (PSIRT) internal Lenovo.</i></p>
<p>Trusted providers list/ <i>Daftar penyedia yang dipercaya</i></p>	<p>All subprocessors that directly integrate with products in production. /<i>Semua pemroses lanjutan yang secara langsung terintegrasi dengan produk-produk dalam produksi.</i></p>	<p>Standard security assessments of integrated providers, DPAs for Personal Data processing providers. / <i>Penilaian keamanan standar penyedia yang terintegrasi, DPA untuk penyedia pemrosesan Data Pribadi.</i></p>

<p>Vulnerability management/ <i>Pengelolaan terhadap kerentanan</i></p>	<p>Server OSes, Docker containers, Clients, Products in production. / OSes server, Kontainer docker, Klien, Produk-produk dalam produksi.</p>	<p>A program that employs various tools to aid in identifying vulnerabilities across all compute systems. / <i>Program yang menggunakan berbagai alat untuk membantu mengidentifikasi kerentanan di seluruh sistem komputasi.</i></p>
<p>Software Security Review Board (SSRB)/ <i>Dewan Peninjau Keamanan Perangkat Lunak (SSRB)</i></p>	<p>Products in production. / <i>Produk-produk dalam produksi.</i></p>	<p>SSRB reviews are conducted regularly. During reviews all technical and organizational measures are assessed for the product in question. / <i>Peninjauan SSRB dijalankan secara berkala. Selama peninjauan, semua tindakan teknis dan organisasi dinilai untuk produk terkait.</i></p>
<p>Data retention policy/ <i>Kebijakan retensi data</i></p>	<p>Personal identifiable information, Application data, Products in production. /<i>Informasi pribadi yang dapat diidentifikasi,</i> <i>Data aplikasi,</i> <i>Produk-produk dalam produksi.</i></p>	<p>Upon user's request for deletion or after one year of not having an active license or trial, personal data will be archived. Archived data is purged after 90 days. / <i>Atas permintaan pengguna untuk penghapusan atau setelah satu tahun tidak memiliki lisensi aktif atau masa percobaan, data pribadi akan diarsipkan. Data terarsip akan dibersihkan setelah 90 hari.</i></p>

<p>Security and privacy awareness/ <i>Kesadaran keamanan dan privasi</i></p>	<p>All employees (Privacy Basics and Security Essentials courses)/ <i>Semua pegawai (dalam hal Dasar-Dasar Privasi dan Dasar-Dasar Keamanan)</i></p>	<p>Semi-annual training for specialized IT and product teams on advanced security topics, such as OWASP Top 10. / <i>Pelatihan semi tahunan tim TI khusus dan produk tentang topik keamanan lebih lanjut, seperti OWASP Top 10.</i></p>
<p>Continuous security/ <i>Keamanan berkelanjutan</i></p>	<p>Products in production. / <i>Produk-produk dalam produksi.</i></p>	<p>Regular application of Technical Measures. / <i>Penerapan secara berkala Tindakan Teknis.</i></p>
<p>Opensource compliance reviews. / <i>Peninjauan kepatuhan opensource.</i></p>	<p>Products in production. / <i>Produk-produk dalam produksi.</i></p>	<p>Assessments conducted to ensure proper licensing and attributions are provided in distributed software. / <i>Penilaian dilaksanakan untuk memastikan pemberian lisensi dan data yang memuat informasi yang pantas disediakan dalam perangkat lunak yang terdistribusi.</i></p>
<p>Disaster Recovery/ <i>Pemulihan Bencana</i></p>	<p>Products in production/ <i>Produk-produk dalam produksi</i></p>	<p>Following NIST-800-34 as a guide to maximize RTO and RPO. / <i>Mengikuti NIST-800-34 sebagai panduan untuk memaksimalkan RTO dan RPO.</i></p>

<p>Backup policy/ <i>Kebijakan cadangan</i></p>	<p>Databases/<i>Kumpulan Data,</i> <i>Code/Kode,</i> <i>Logs/Catatan-catatan.</i></p>	<p>The general policy requires multiple backups, one of which must be offsite from the primary storage location. Regular database backups occurring daily (2 times per</p>
---	---	---

		<p>day), weekly, and monthly. Daily backups are retained for 7 days. Weekly backups are retained for 4 weeks. Monthly backups are retained for 13 months. The restore window is 12 hours.</p> <p>Application source code backups occur daily and are retained for 360 days.</p> <p>Production logs: Datadog – Logs are live for 7 days. Logs are then put in long-term storage for 180 days and then purged.</p> <p>Load Balancer – Logs are retained for 360 days and then purged.</p> <p>Web Application Firewall – Logs are retained for 90 days and then purged.</p> <p>Cloud Trail – Logs are retained for 90 days and then purged.</p> <p>Cloud Watch – Logs are retained for 360 days and then purged.</p> <p>MongoDB – Logs are retained for the life of the project. /</p> <p><i>Kebijakan umum memerlukan cadangan berganda, yang salah satunya harus disimpan terpisah dari lokasi penyimpanan utama,</i></p> <p><i>Cadangan database secara berkala terjadi setiap hari (2 kali sehari), setiap minggu, dan</i></p>
--	--	---

		<p><i>setiap bulan. Cadangan harian disimpan selama 7 hari. Cadangan mingguan disimpan selama 4 minggu. Cadangan bulanan disimpan selama 13 bulan. Jendela pemulihan selama 12 jam,</i></p> <p><i>Cadangan kode sumber aplikasi terjadi setiap hari dan disimpan selama 360 hari.</i></p> <p><i>Log produksi :</i></p> <p><i>Datadog – Log aktif selama 7 hari. Log kemudian disimpan dalam penyimpanan jangka panjang selama 180 hari dan kemudian dibersihkan.</i></p> <p><i>Load Balancer – Log disimpan selama 360 hari dan kemudian dibersihkan.</i></p> <p><i>Firewall Aplikasi Web – Log disimpan selama 90 hari dan kemudian dibersihkan.</i></p> <p><i>Cloud Trail – Log disimpan selama 90 hari dan kemudian dibersihkan.</i></p> <p><i>Cloud Watch – Log disimpan selama 360 hari dan kemudian dibersihkan.</i></p> <p><i>MongoDB – Log disimpan selama proyek berlangsung.</i></p>
--	--	--

**ANNEX D/LAMPIRAN D – INTERNATIONAL DATA TRANSFER AGREEMENT/PERJANJIAN
PENGALIHAN DATA INTERNASIONAL**

This Annex sets out the data protection requirements (including requirements under Applicable Privacy Laws) that apply: (i) to the Data Exporter (Controller) when it transfers Personal Data to the Data Importer (Stoneware, Inc.), its affiliates and/or its Subprocessors, for Data Processing; and (ii) to the Data Importer when it receives Personal Data from a Data Exporter for Data Processing.

Lampiran ini mengatur persyaratan perlindungan data (termasuk persyaratan berdasarkan Undang-Undang Privasi yang Berlaku) yang berlaku: (i) terhadap Pengirim Data (Pengendali) saat pihaknya mengalihkan Data Pribadi ke Penerima Data (Stoneware, Inc.), afiliasi-afiliasinya dan/atau Pemroses lanjutan, untuk Pemrosesan Data; dan (ii) terhadap Penerima Data ketika pihaknya menerima Data Pribadi dari Pengirim Data untuk Pemrosesan Data.

The Data Importer warrants and undertakes that at all times it will:

Penerima Data menjamin dan berjanji bahwa setiap waktu pihaknya akan:

- a) Process the Transferred Data in accordance with Applicable Privacy Laws and will provide reasonable and timely assistance to the Data Exporter as needed to help the Data Exporter comply with its obligations under Applicable Privacy Laws; and
- b) not knowingly perform its obligations under this Agreement in such a way as to cause the Data Exporter to breach any of its obligations under Applicable Privacy Laws.

- a) *Memproses Data yang Dialihkan sesuai dengan Undang-Undang Privasi yang Berlaku dan akan menyediakan bantuan yang wajar dan tepat waktu kepada Pengirim Data jika dibutuhkan untuk membantu Pengirim Data mematuhi kewajibannya berdasarkan Undang-Undang Privasi yang Berlaku; dan*
- b) *tidak menjalankan kewajibannya berdasarkan Perjanjian ini dengan sengaja dan dalam cara apa pun mengakibatkan Pengirim Data melanggar salah satu kewajibannya berdasarkan Undang-Undang Privasi yang Berlaku.*

The Data Exporter confirms that it has taken necessary actions to ensure compliance with the applicable Data Protection laws, including the cross-border transfer of personal data requirements, such as having obtained explicit

Pengirim Data mengkonfirmasi bahwa pihaknya telah mengambil tindakan yang diperlukan untuk memastikan kepatuhan terhadap undang-undang Perlindungan Data yang berlaku, termasuk persyaratan

consents of the Data Subjects with their personal data being transferred abroad, notified relevant authorities or applied for their approval of the transfer or other underlying obligations, as applicable.

transfer data pribadi lintas batas negara, seperti misalnya telah memperoleh persetujuan eksplisit dari Subjek Data atas data pribadi mereka yang ditransfer ke luar negeri, telah memberitahukan otoritas terkait atau mengajukan permohonan persetujuan mereka atas pengalihan atau kewajiban mendasar lainnya, sebagaimana berlaku.

1. European Economic Area (EEA)

If Supplier's services are provided to Controller within the European Economic Area ("EEA") or such other jurisdiction subject to EU Data Protection Law, the following provisions shall apply:

(A) "EU Data Protection Law" means (a) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (the "GDPR"); (b) the EU e-Privacy Directive (Directive 2002/58/EC); and (c) any and all applicable national data protection laws.

(B) Supplier shall promptly inform Controller (a) of any requirement under EU Data Protection Law that would require Processing Personal Data in any way other than per Controller's instructions, or (b) if, in Supplier's opinion, Controller's instructions may infringe or violate any applicable EU Data Protection Law.

1. Wilayah Ekonomi Eropa (EEA)

Apabila layanan Pemasok disediakan kepada Pengendali di Wilayah Ekonomi Eropa ("EEA") atau yurisdiksi lain yang tunduk pada Undang-Undang Perlindungan Data UE, ketentuan berikut harus berlaku:

(A) "Undang-Undang Perlindungan Data UE" berarti (a) peraturan 2016/679 Parlemen Eropa dan Dewan perlindungan perorangan tentang Pemrosesan Data Pribadi dan pergerakan bebas data tersebut (Peraturan Perlindungan Data Umum) (General Data Protection Regulation atau "GDPR"); (b) Instruksi Privasi Elektronik (Instruksi 2002/58/EC); dan (c) setiap dan seluruh undang-undang perlindungan data nasional yang berlaku.

(B) Pemasok harus segera memberi tahu Pengendali (a) tentang persyaratan berdasarkan Undang-Undang Perlindungan Data UE yang mewajibkan Pemrosesan Data Pribadi dengan cara apa pun selain berdasarkan intruksi Pengendali, atau (b) jika menurut pendapat Pemasok, instruksi Pengendali dapat melanggar Undang-Undang Perlindungan Data UE.

(C) **Data Transfers:** If Supplier or its Subcontractors are located outside the EEA, Supplier and Controller hereby execute the controller to processor standard contractual clauses as set out in MODULE TWO in the [Commission Implementing Decision \(EU\) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation \(EU\) 2016/679 of the European Parliament and of the Council](#) as amended or superseded from time to time (the "C2P Standard Contractual Clauses") and hereby incorporate them into this Addendum by reference. The parties acknowledge and agree that:

- a) Supplier and Controller shall each comply with their respective obligations in the C2P Standard Contractual Clauses;
- b) If there is any conflict or inconsistency between the C2P Standard Contractual Clauses and this Addendum or the base agreement, the C2P Standard Contractual Clauses shall control to the extent of the conflict; and
- c) The information in the following tables is hereby incorporated into the C2P Standard Contractual Clauses between the Parties:

(C) **Pengalihan Data:** Jika Pemasok atau Kontraktor Lanjutannya berlokasi di luar EEA, Pemasok dan Pengendali dengan ini menandatangani klausul kontraktual standar pengendalian ke pemrosesan sebagaimana diatur dalam MODUL DUA dalam [Keputusan Pelaksanaan Komisi \(UE\) 2021/914 pada 4 Juni 2021 tentang klausul kontraktual standar untuk pengalihan data pribadi ke negara ketiga, sesuai dengan Peraturan \(UE\) 2016/679 Parlemen Eropa dan Dewan](#) sebagaimana diubah atau diganti dari waktu ke waktu ("Klausul Kontraktual Standar C2P") dan dengan ini menggabungkannya ke dalam Adendum ini dengan acuan. Para pihak mengakui dan menyetujui bahwa:

- a. Pemasok dan Pengendali masing-masing harus mematuhi kewajibannya masing-masing dalam Klausul Kontraktual Standar C2P;
- b. Jika terjadi pertentangan atau perbedaan antara Klausul Kontraktual Standar C2P dan Adendum ini atau perjanjian dasar, Klausul Kontraktual Standar C2P akan menentukan sepanjang mengenai pertentangan tersebut; dan
- c. Informasi di tabel berikut ini digabungkan dalam Klausul Kontraktual Standar C2P antara Para Pihak:

Information to be incorporated into the C2P Standard Contractual Clauses between Controller and Supplier:/ Informasi yang akan digabungkan ke dalam Klausul Kontraktual Standar C2P antara Pengendali dan Pemasok:	
<p>Clause 9. Use of sub-processors/ <i>Klausul 9. Penggunaan pemroses lanjutan</i></p>	<p>Option 2 GENERAL WRITTEN AUTHORISATION is selected. Data importer shall provide information at least 30 days in advance as per Clause "Subprocessing"/ <i>Opsi 2 OTORISASI TERTULIS UMUM dipilih. Penerima data akan menyediakan informasi selambat-lambatnya 30 hari sebelumnya sesuai dengan Klausul "Pemrosesan Lanjutan"</i></p>
<p>Clause 17. Governing law/ <i>Klausul 17. Hukum yang mengatur</i></p>	<p>These Clauses shall be construed in accordance with the governing law set forth in the Parties' base agreement unless that governing law is not that of an EU Member State that allows for third-party beneficiary rights. In such event, the Parties agree that these Clauses shall be governed by the law of IRELAND./ <i>Klausul ini akan ditafsirkan sesuai dengan hukum yang mengatur yang tercantum dalam perjanjian dasar Para Pihak kecuali jika hukum yang mengatur tersebut bukan hukum Negara Anggota UE yang mengizinkan hak penerima manfaat pihak ketiga. Dalam hal tersebut, Para Pihak setuju bahwa Klausul ini akan diatur oleh hukum IRLANDIA.</i></p>
<p>Clause 18 (b). Choice of forum and jurisdiction/ <i>Klausul 18 (b). Pilihan forum dan yurisdiksi</i></p>	<p>The Parties agree that any dispute arising from these Clauses shall be resolved by the courts of IRELAND./ <i>Para Pihak setuju bahwa setiap sengketa yang timbul dari Klausul ini harus diselesaikan di pengadilan IRLANDIA.</i></p>

Information to be incorporated into Annex 1, Part A of the C2P Standard Contractual Clauses:/ Informasi yang akan digabungkan ke dalam Lampiran 1, Bagian A Klausul Kontraktual Standar C2P	
<i>Data Exporter's Name/ Nama Pengirim Data</i>	Controller, and any of its commonly owned or controlled affiliates/ <i>Pengendali, dan setiap afiliasinya yang dimiliki atau dendalikan bersama</i>
<i>Data Exporter's Address/ Alamat Pengirim Data</i>	To be completed by data exporter/ <i>Diisi oleh pengirim data</i>
<i>Data Exporter's contact person's name, position, and contact details/ Nama, jabatan, dan informasi kontak narahubung Pengirim Data</i>	To be completed by data exporter/ <i>Diisi oleh pengirim data</i>
<i>Data Exporter's activities relevant to the data transferred under these Clauses/ Aktivitas Pengirim Data yang berkaitan dengan data yang dialihkan berdasarkan Klausul ini</i>	To be completed by data exporter/ <i>Diisi oleh pengirim data</i>
<i>Data Exporter's signature and date/ Tanda tangan Pengirim Data dan tanggal</i>	To be completed by data exporter/ <i>Diisi oleh pengirim data</i>
<i>Data Exporter's role/ Peran Pengirim Data</i>	Controller/ <i>Pengendali</i>
<i>Data Importer's name/ Nama Penerima Data</i>	Supplier (Stoneware, Inc.) and its Subcontractors/ <i>Pemasok (Stoneware, Inc.) dan Kontraktor Lanjutannya</i>
<i>Data Importer's address/ Alamat Penerima Data</i>	3400 E Coliseum Blvd, #310, Fort Wayne, IN 46805 United States of America/ <i>3400 E Coliseum Blvd, #310, Fort Wayne, IN 46805 Amerika Serikat</i>
<i>Data Importer's contact person's name, position and contact details/ Nama, jabatan, dan informasi kontak narahubung Penerima Data</i>	Kimberly Page, Strategic Operations Manager privacy@lanschool.com/ <i>Kimberly Page, Manajer Operasi Strategis</i> privacy@lanschool.com
<i>Data Importer's activities relevant to the data transferred under these Clauses/</i>	As set out in Part B of Annex 1/ <i>Sebagaimana ditetapkan di Bagian B Lampiran 1</i>

<i>Aktivitas Penerima Data yang berkaitan dengan data yang dialihkan berdasarkan Klausul ini</i>	
<i>Data Importer's signature and date/ Tanda tangan Penerima Data dan tanggal</i>	To be completed by data importer/ <i>Diisi oleh Penerima Data</i>
<i>Data Importer's Role/ Peran Penerima Data</i>	Processor/ <i>Pemroses</i>

Information to be incorporated into Annex 1, Parts B and C of the C2P Standard Contractual Clauses:/

Informasi yang akan digabungkan ke dalam Lampiran 1, Bagian B dan C Klausul Kontraktual Standar C2P:

<i>Categories of data subjects/ Kategori subjek data</i>	As set out in Annex A above/ <i>Sebagaimana tercantum dalam Lampiran A di atas</i>
<i>Categories of personal data/ Kategori data pribadi</i>	As set out in Annex A above/ <i>Sebagaimana tercantum dalam Lampiran A di atas</i>
<i>Sensitive data/ Data sensitive</i>	As set out in Annex A above/ <i>Sebagaimana tercantum dalam Lampiran A di atas</i>
<i>Frequency of the Transfer/ Frekuensi Pengalihan</i>	Ongoing frequency, as long as LSA license is active/ <i>Frekuensi berkelanjutan, selama lisensi LSA aktif</i>
<i>Nature of the processing/ Sifat pemrosesan</i>	As set out in Annex A above/ <i>Sebagaimana tercantum dalam Lampiran A di atas</i>
<i>Purpose of the processing/ Tujuan pemrosesan</i>	As set out in Annex A above/

	<i>Sebagaimana tercantum dalam Lampiran A di atas</i>
<i>Period for which personal data will be retained/ Periode penyimpanan data</i>	<i>As set out in Annex A above/ Sebagaimana tercantum dalam Lampiran A di atas</i>
<i>Subject matter, nature and duration of the processing carried out by subprocessors/ Pokok persoalan, sifat, dan jangka waktu pemrosesan yang dilaksanakan pemroses lanjutan</i>	<i>As set out in Annex B above/ Sebagaimana tercantum dalam Lampiran B di atas</i>
<i>Competent Supervisory Authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 ty/ Otoritas Pengawas yang Kompeten yang bertanggung jawab untuk memastikan kepatuhan pengirim data terhadap Peraturan (UE) 2016/679 ty</i>	<p>The supervisory authority that will act as competent supervisory authority will be that of the EU member State where Data Exporter is established in the EU. If Data Exporter (i.e., contracting legal entity) is not established in EU, then the Competent Supervisory Authority will be such of the EU Member State in which the Data Exporter’s EU representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established. If the Data Exporter is not established in the EU but does not need to appoint an EU representative, then the Competent Supervisory Authority will be that of the EU Member State in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located./</p> <p><i>Otoritas pengawas yang akan bertindak sebagai otoritas pengawas yang kompeten adalah otoritas pengawas Negara Anggota UE tempat Pengirim Data didirikan di UE. Apabila Pengirim Data (yakni badan hukum yang mengadakan kontrak) tidak didirikan di UE, maka Otoritas Pengawas yang Kompeten adalah otoritas pengawas Negara Anggota Negara UE tempat perwakilan UE Pengespor Data yang dimaksud dalam Pasal 27(1)</i></p>

	<p><i>Peraturan (UE) 2016/679 didirikan. Apabila Pengirim Data tidak didirikan di UE tetapi tidak perlu menunjuk perwakilan UE, maka Otoritas Pengawas yang Kompeten adalah otoritas pengawas Negara Anggota UE yang menjadi lokasi subjek data yang data pribadinya dialihkan berdasarkan Klausul ini sehubungan dengan penawaran barang atau layanan kepada mereka, atau yang perilakunya dipantau.</i></p>
--	---

Informasi yang akan digabungkan ke dalam Lampiran 2 Klausul Kontraktual StandarC2P:

<p><i>Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons. /</i></p> <p><i>Deskripsi langkah-langkah teknis dan organisasional yang diimplementasikan oleh penerima data (termasuk sertifikasi terkait) untuk memastikan tingkat keamanan yang tepat, dengan mempertimbangkan sifat, cakupan, konteks, dan tujuan pemrosesan, serta risiko hak dan kebebasan perorangan.</i></p>	<p><i>As set out in Annex C above/ Sebagaimana tercantum dalam Lampiran C di atas</i></p>
--	---

Information to be incorporated into Annex 3 of the C2P Standard Contract Clauses:/

Informasi yang akan digabungkan ke dalam Lampiran 3 Klausul Kontraktual Standar:

<p>List of authorized Sub-processors/ <i>Daftar Pemroses lanjutan resmi</i></p>	<p>As set out in Annex B above/ <i>Sebagaimana tercantum dalam Lampiran B di atas</i></p>
--	--

2. United Kingdom (UK)

2. Inggris Raya (UK)

If Supplier’s services are provided to Controller within the United Kingdom, or the nature of the Personal Data triggers the application of the European Union (Withdrawal) Act 2018 (the "UK GDPR") and the Data Protection Act 2018 (the "DPA 2018"), the following additional provisions shall apply:

Apabila layanan Pemasok disediakan untuk Pengendali di Inggris Raya, atau sifat dari Data Pribadi memicu penerapan Undang-undang (Penarikan) Uni Eropa 2018 (“UK GDPR”) dan Undang-undang Perlindungan Data 2018 (“DPA 2018”), ketentuan-ketentuan tambahan berikut akan berlaku:

(A) Transfers of Personal Data to a recipient in a country considered by the UK's Secretary of State, to provide adequate protection for Personal Data (an "Adequacy Decision") will be permitted under the Agreement(s) without the need for approved UK Standard Contractual Clauses.

(A) Pengalihan Data Pribadi ke penerima di negara yang dipertimbangkan oleh Menteri Dalam Negeri Inggris Raya, guna memberikan perlindungan yang memadai untuk Data Pribadi (“Keputusan yang Cukup”) akan diizinkan berdasarkan perjanjian(-perjanjian) tanpa memerlukan Klausul Kontraktual Standar Inggris Raya yang disetujui.

(B) EEA countries shall be deemed to be subject to an Adequacy Decision for the purpose of transfers of Personal Data from the UK to the EEA.

(B) Negara-negara Wilayah Ekonomi Eropa (EEA) akan dianggap tunduk pada Keputusan yang Cukup untuk tujuan pengalihan Data Pribadi dari Inggris Raya ke Wilayah Ekonomi Eropa (EEA).

- (C) In the absence of an Adequacy Decision, Controller and Supplier agree to execute approved UK International data transfer addendum to the European Commission’s standard contractual clauses for international data transfers (<https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf>).
- (C) Dengan tidak adanya Keputusan yang Cukup, Pengendali dan Pemasok setuju untuk menandatangani addendum pengalihan data Internasional Inggris Raya yang disetujui atas klausul kontraktual standar Komisi Eropa untuk transfer data internasional (<https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf>).

Part 1: Tables / Table 1: Parties

Bagian 1: Tabel/Tabel 1: Pihak-Pihak

Information to be incorporated into “Part 1: Tables” of the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses: / Informasi untuk digabungkan pada “Bagian 1: Tabel” dari Adendum Data Pengalihan pada Klausul Kontraktual Standar Komisi Uni Eropa:		
Start date / Tanggal dimulai	As per the above/Sebagaimana tersebut di atas	
The Parties / Pihak- Pihak	Exporter (who sends the Restricted Transfer)/Eksportir (pihak yang mengirimkan Transfer Terbatas)	Importer (who receives the Restricted Transfer) /Importir (pihak yang menerima Pengalihan Terbatas)
Parties’ details / Informasi Pihak- Pihak	Full legal name, main address (if a company registered address): As per the information in the 2 nd table of the Art. 1. European Economic Area (EEA) in the Annex D / Nama lengkap secara hukum, alamat Utama (jika perusahaan	Full legal name, main address (if a company registered address): As per the information in the 2 nd table of the Art. 1. European Economic Area (EEA) in the Annex D / Nama lengkap secara hukum, alamat Utama (jika perusahaan

	<p>alamat terdaftar): sesuai dengan informasi dalam tabel ke-2 dari Pasal 1 Wilayah Ekonomi Eropa (EEA) dalam Lampiran D</p> <p>Official registration number (if any) (company number or similar identifier): As per customer identified under the Sales Agreement / Nomor registrasi resmi (bila ada) (nomor perusahaan atau tanda pengenal lainnya yang serupa): sesuai dengan pengenal pelanggan berdasarkan Perjanjian Penjualan</p>	<p>Wilayah Ekonomi Eropa (EEA) dalam Lampiran D</p> <p>Official registration number (if any) (company number or similar identifier): 35-2097171 registered in State of Indiana / Nomor registrasi resmi (bila ada) (nomor perusahaan atau tanda pengenal lainnya yang serupa):35-2097171 terdaftar di Negara Bagian Indiana</p>
<p>Key Contact / Kontak Utama</p>	<p>Full Name (optional), job title, contact details including email: As per the information in the 2nd table of the Art. 1. European Economic Area (EEA) in the Annex D / Nama lengkap (pilihan), jabatan, detail kontak termasuk email: Sesuai dengan informasi dalam tabel ke-2 dari Pasal 1 Wilayah Ekonomi Eropa (EEA) dalam Lampiran D</p>	<p>Full Name (optional), job title, contact details including email:</p> <p>As per the information in the 2nd table of the Art. 1. European Economic Area (EEA) in the Annex D / Nama lengkap (pilihan), jabatan, detail kontak termasuk email: Sesuai dengan informasi dalam tabel ke-2 dari Pasal 1 Wilayah Ekonomi Eropa (EEA) dalam Lampiran D</p>

Table 2: Selected SCCs, Modules and Selected Clauses /

Tabel 2: SCCs Tertentu, Modul dan Klausula Tertentu

<p>Addendum EU SCCs / Adendum SCCs Uni Eropa</p>	<p>See Annex D, Art. 1 above / Lihat Lampiran D, Pasal 1 di atas</p>
---	--

Table 3: Appendix Information /

Tabel 3: Informasi Lampiran

Annex 1A: List of Parties As set out in in the Art. 1. European Economic Area (EEA) in the Annex D / <i>Lampiran 1A: Daftar Pihak-Pihak Sebagaimana ditetapkan dalam Pasal 1 Wilayah Ekonomi Eropa (EEA) dalam Lampiran D</i>
Annex 1B: Description of Transfer: As set out in Annex A above / <i>Lampiran 1B: Deskripsi Pengalihan: Sebagaimana ditetapkan dalam Lampiran A di atas</i>
Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data: Description of Transfer: As set out in Annex C above / <i>Lampiran II: Upaya-Upaya Teknis dan Organises untuk memastikan keamanan atas data: Deskripsi Pengalihan: Sebagaimana ditetapkan dalam Lampiran C di atas</i>
Annex III: List of Sub processors (Modules 2 and 3 only): Description of Transfer: As set out in Annex B above / <i>Lampiran III: Daftar Pemroses Lanjutan (hanya Modul 2 dan 3): Deskripsi Pengalihan: Sebagaimana ditetapkan dalam Lampiran B di atas</i>

Table 4: Ending this Addendum when the Approved Addendum Changes /

Tabel 4: Pengakhiran Adendum ini jika Adendum yang Disetujui Berubah

Ending this Addendum when the Approved Addendum changes/ <i>Pengakhiran Adendum ini jika Adendum yang Disetujui berubah</i>	Which Parties may end this Addendum as set out in Section 19: / <i>Pihak yang dapat mengakhiri Adendum ini sebagaimana diuraikan pada Bagian 19:</i> <input checked="" type="checkbox"/> Importer / <i>Importir</i> <input type="checkbox"/> Exporter / <i>Eksportir</i> <input type="checkbox"/> neither Party / <i>bukan Pihak Manapun</i>
--	---

Information to be incorporated into “Part 2: Mandatory Clauses” of the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses: /Informasi untuk digabungkan pada “Bagian 2: Klausul Wajib” dari Adendum Data Pengalihan Internasional pada Klausul Kontraktual Standar Komisi UE

Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses. / *Bagian 2: Klausul Wajib dari Adendum yang Disetujui, yang merupakan contoh (template) Adendum B.1.0 yang dikeluarkan oleh ICO dan disampaikan di hadapan Parlemen sesuai dengan s119A Undang-Undang Perlindungan Data 2018 tanggal 2 Februari 2022, sebagaimana diubah dengan Bagian 18 dari Klausul Wajib tersebut.*

3. Switzerland

Insofar as the transfer of Personal Data is subject to the Swiss Federal Act on Data Protection, the parties agree to comply with the EU Standard Contractual Clauses and the following provisions shall apply: (i) the Federal Data Protection and Information Commissioner (FDPIC) will be the competent supervisory authority under Clause 13 of the EU Standard Contractual Clauses; (ii) the Parties agree to abide by the GDPR standard in relation to all Processing of Personal Data that is governed by the Swiss Federal Act on Data Protection; (iii) the EU Standard Contractual Clauses will be governed by the laws of Switzerland in accordance with Clause 17 (Option 1) insofar as the data transfers are governed by the Swiss Federal Act on Data Protection; (iv) the term ‘Member State’ in the EU Standard Contractual Clauses will not be interpreted in such a way as to exclude Data Subjects in Switzerland from the

3. Switzerland

Sepanjang pengalihan Data Pribadi tunduk pada Undang-Undang Federal Swiss tentang Perlindungan Data, para pihak setuju untuk mematuhi Klausul Kontrak Standar UE dan ketentuan berikut akan berlaku: (i) Komisaris Perlindungan Data dan Informasi Federal (FDPIC) akan menjadi otoritas pengawas yang kompeten berdasarkan Klausul 13 Klausul Kontrak Standar UE; (ii) Para Pihak setuju untuk mematuhi standar GDPR sehubungan dengan semua Pemrosesan Data Pribadi yang diatur oleh Undang-Undang Federal Swiss tentang Perlindungan Data; (iii) Klausul Kontrak Standar UE akan diatur oleh hukum Swiss sesuai dengan Klausul 17 (Opsi 1) sepanjang transfer data diatur oleh Undang-Undang Federal Swiss tentang Perlindungan Data; (iv) istilah

possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU Standard Contractual Clauses; (v) references to the 'GDPR' in the EU Standard Contractual Clauses will be understood as references to the Swiss Federal Act on Data Protection insofar as the transfer of Controller Data is subject to the Swiss Federal Act on Data Protection.

'Negara Anggota' dalam Klausul Kontrak Standar UE tidak akan ditafsirkan sedemikian rupa sehingga mengecualikan Subjek Data di Swiss dari kemungkinan menggugat hak-hak mereka di tempat tinggal mereka (Swiss) sesuai dengan Klausul 18(c) Klausul Kontrak Standar UE; (v) referensi ke 'GDPR' dalam Klausul Kontrak Standar UE akan dipahami sebagai referensi ke Undang-Undang Federal Swiss tentang Perlindungan Data sepanjang transfer Data Pengontrol tunduk pada Undang-Undang Federal Swiss tentang Perlindungan Data.

4. Brazil

In case of a transfer of Personal Data subject to the Brazil's General Personal Data Protection Law (as amended by Law No. 13.853 of 8 July 2019) ("LGPD"), and Lenovo, Supplier, or both are located in Non-Adequate Countries, the C2P Standard Contractual Clauses as referenced herein shall apply with the following amendments:

- (i) the supervisory authority of the C2P Standard Contractual Clauses shall be the Brazil's National Data Protection Authority (ANPD);
- (ii) the governing law in accordance with Clause 17 of the C2P Standard Contractual Clauses shall be the LGPD;
- (iii) the choice of forum and jurisdiction in accordance with Clause 18 of the C2P Standard Contractual Clauses shall be Brazilian law in case the data transfer is exclusively subject to the LGPD; and
- (iv) any references to the GDPR in the C2P Standard Contractual Clauses shall also include the reference

4. Brazil

Dalam hal transfer Data Pribadi tunduk pada Undang-Undang Perlindungan Data Pribadi Umum Brasil (sebagaimana diubah dengan Undang-Undang No. 13.853 tanggal 8 Juli 2019) ("LGPD"), dan Lenovo, Pemasok, atau keduanya berlokasi di Negara yang Tidak Memadai, Klausul Kontrak Standar C2P sebagaimana dirujuk di sini akan berlaku dengan perubahan sebagai berikut:

- (i) otoritas pengawas Klausul Kontrak Standar C2P adalah Otoritas Perlindungan Data Nasional (ANPD) Brasil;*
- (ii) hukum yang mengatur sesuai dengan Klausul 17 Klausul Kontrak Standar C2P adalah LGPD;*
- (iii) pilihan forum dan yurisdiksi sesuai dengan Klausul 18 Klausul Kontrak Standar C2P adalah hukum Brasil dalam hal transfer data secara eksklusif tunduk pada LGPD; dan*
- (iv) referensi apa pun terhadap GDPR dalam Klausul Kontrak Standar C2P juga harus*

to the equivalent provisions of LGPD (as amended or replaced).

mencakup referensi terhadap ketentuan LGPD yang setara (sebagaimana diubah atau diganti).

5. South Africa

5. Afrika Selatan

If Supplier's services are provided to Controller within South Africa or such other jurisdiction subject to the Protection of Personal Information Act (POPIA), the following additional provisions shall apply:

Apabila layanan Pemasok disediakan untuk Pengendali di Afrika Selatan atau yurisdiksi lain yang tunduk pada Undang-Undang Perlindungan Informasi Pribadi (POPIA), ketentuan tambahan berikut harus berlaku:

(A) Data Subject means a natural person who can be identified by reference to a name, unique number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person as well as an identifiable juristic person or legal entity.

(A) Subjek Data berarti perorangan yang dapat diidentifikasi melalui penyebutan nama, nomor unik, data lokasi, pengidentifikasi online, atau satu faktor spesifik atau lebih terkait identitas fisik, fisiologis, genetik, mental, ekonomi, budaya, atau sosial perorangan tersebut, serta perorangan hukum atau badan hukum yang dapat diidentifikasi.

6. Australia

6. Australia

The parties agree to use and protect applicable Personal Data in compliance with Australia's Data Privacy Act as amended.

Para pihak setuju untuk menggunakan dan melindungi Data Pribadi yang berlaku sesuai dengan Undang-Undang Data Privasi Australia sebagaimana telah diubah.

ANNEX E/LAMPIRAN E – ADDITIONAL PROVISIONS/KETENTUAN-KETENTUAN TAMBAHAN

1. California Consumer Privacy Act (“CCPA”).

1. Undang-Undang Privasi Pelanggan California (“CCPA”).

Stoneware, Inc. is a Business. Additionally, Supplier is Customer’s Service Provider and will process Personal Data on behalf of Customer.

Stoneware, Inc. merupakan suatu Bisnis. Sebagai tambahan, Pemasok adalah Penyedia Layanan Pelanggan dan akan memproses Data Pribadi atas nama Pelanggan.

- a. Supplier shall not sell the Personal Data or Proprietary Information. “Sell” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating the information for monetary or other valuable consideration.
- a. Pemasok tidak boleh menjual Data Pribadi atau Informasi Hak Milik. “Menjual” berarti menjual, menyewa, merilis, mengungkapkan, menyebarkan, membuat tersedia, mengalihkan, atau mengkomunikasikan informasi untuk tujuan moneter atau pertimbangan lain yang memiliki nilai .
- b. Supplier shall not retain, use, or disclose the Personal Data: (a) for any purpose other than for the specific purpose of performing the services set forth in the Agreement for Stoneware, Inc. or as otherwise permitted by the CCPA and its implementing regulations, (b) for a commercial purpose other than providing the services specified in the contract with the business, or (c) outside the direct business relationship between the person and Stoneware, Inc.
- b. Pemasok tidak boleh menyimpan, menggunakan, atau mengungkapkan Data Pribadi: (a) untuk tujuan apa pun selain tujuan khusus dari layanan yang dilakukan dan diatur dalam Perjanjian Stoneware, Inc. atau diizinkan oleh CCPA dan peraturan pelaksanaannya, (b) untuk tujuan komersial selain menyediakan layanan yang diatur dalam kontrak dengan bisnis, atau (c) di luar hubungan bisnis langsung antara orang tersebut dan Stoneware, Inc.
- c. This DPA shall serve as Supplier’s certification that Supplier understands the CCPA requirements applicable to businesses and service
- c. DPA ini harus berlaku sebagai pernyataan Pemasok bahwa Pemasok memahami persyaratan CCPA yang berlaku terhadap penyedia layanan dan bisnis, termasuk

providers, including the restrictions in Cal. Civ. Code § 1798.140(w)(2)(A), and will comply with them.

batasan dalam Cal. Civ. Kode § 1798.140w)2)A), dan akan mematuhi.