

Lenovo NetFilter Data Processor Agreement (DPA)

This Lenovo NetFilter Data Processor Agreement (which addresses both privacy and security requirements) and its annexes, ("**DPA**") form part of the Lenovo Sales Agreement or other written or electronic agreement between Lenovo and Customer (the "**Agreement**") for the purchase of Lenovo NetFilter services from Lenovo, to reflect the parties' agreement in relation to the Processing of Personal Data.

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 Lenovo NetFilter Terms of Services ("**Effective Date**").

Upon signature of the Agreement and acceptance of the Lenovo NetFilter 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 Lenovo 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.

We may update these terms to accommodate new legal requirements or as necessary to reflect operational updates. If you have an active Lenovo NetFilter subscription, we will let you know via email or via in-product notification.

DPA execution:

Perjanjian Pemroses Data Lenovo NetFilter (DPA)

*Perjanjian Pemroses Data Lenovo NetFilter ini (yang membahas persyaratan privasi dan keamanan) beserta lampirannya, ("**DPA**") membentuk bagian dari Perjanjian Penjualan Lenovo atau perjanjian tertulis atau elektronik lainnya antara Lenovo dan Pelanggan ("**Perjanjian**") untuk pembelian layanan Lenovo NetFilter dari Lenovo, untuk mencerminkan kesepakatan para pihak dalam kaitannya dengan Pemrosesan Data Pribadi.*

*DPA ini melengkapi perjanjian apapun antara para pihak sehubungan dengan pokok bahasan di sini; dan akan berlaku dari saat Pelanggan menerima Syarat Layanan Lenovo NetFilter ("**Tanggal Efektif**").*

Setelah Perjanjian ditandatangani dan Syarat Layanan Lenovo NetFilter diterima, DPA ini akan mengikat secara hukum; dan Anda (Pelanggan) menyepakati DPA ini atas nama Pelanggan, sejauh diwajibkan oleh Undang-undang dan Peraturan privasi, keamanan, dan perlindungan data yang berlaku, termasuk undang-undang dan peraturan pendidikan dan privasi siswa dan keamanan yang berlaku, dalam nama dan atas nama Afiliasi Sah sejauh Lenovo memproses Data Pribadi yang Afiliasi Sah tersebut memenuhi kualifikasi sebagai Pengontrolnya. Pelanggan memahami bahwa DPA ini berlaku untuk semua pengguna, dan pelanggan menjamin mereka memiliki kuasa yang diperlukan untuk menyepakati DPA ini atas nama penggunaanya.

Kami dapat memperbarui syarat ini untuk mengakomodasi persyaratan hukum baru, atau sebagaimana diperlukan untuk mencerminkan pembaruan operasional. Jika Anda memiliki langganan Lenovo NetFilter yang aktif, kami akan memberi tahu Anda lewat e-mail atau notifikasi dalam produk.

Pelaksanaan DPA:

- 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 Lenovo., 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). Further, it represents contractual provisions serving as safeguards for safe personal data transfers required by applicable data protection laws.

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

Data Protection

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

- 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 NetFilter Services, including any laws

- a) *DPA ini terdiri dari dua bagian: bodi utama DPA, dan Lampiran A, B, C, D, dan E*
- b) *DPA ini telah ditandatangani di depan atas nama Lenovo, termasuk Klausul Kontrak Standar UE di Lampiran D, sebagai pengimpor data. (Perhatikan: Lampiran D umumnya hanya berlaku untuk aktivitas pemrosesan yang mungkin melibatkan pengalihan Data Pribadi dari Uni Eropa, Area Ekonomi Eropa, Britania Raya, dan/atau negara-negara lain dengan standar kecukupan atau kesetaraan yang serupa terkait pengalihan data lintas perbatasan). Lebih lanjut, ini merupakan ketentuan kontrak yang berfungsi sebagai perlindungan bagi transfer data pribadi yang aman sebagaimana diwajibkan oleh hukum perlindungan data yang berlaku.*

Untuk menghindari keraguan, Anda harus menandatangani DPA ini di halaman 5. Jika berlaku, Lampiran D akan berlaku melalui referensi.

Perlindungan Data

Definisi: Dalam Klausul ini, istilah berikut memiliki arti berikut ini:

- a) **"Pengontrol", "Pemroses", "Subpemroses", "Pemrosesan Data", dan "Pemrosesan"** (dan **"Proses"**) memiliki arti yang diberikan di dalam Undang-undang Perlindungan Data UE dan istilah setara di dalam Hukum Perlindungan Data yang Berlaku.
- b) **"Hukum Perlindungan Data yang Berlaku"** berarti semua undang-undang, aturan, peraturan, perintah yang berlaku, serta semua amendemen terkait, di semua yurisdiksi di mana Pemasok memberikan Layanan

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.

NetFilter, termasuk semua hukum yang berkaitan dengan privasi, keamanan data, perlindungan data, pembobolan data, dan kerahasiaan, seperti California Consumer Privacy Act tahun 2018 ("CCPA") dan California Privacy Rights Act ("CPRA"); General Data Protection Regulation 2016/279 Uni Eropa, sebagaimana diamendemen, diganti, atau ditiadakan dari waktu ke waktu ("GDPR"); Data Protection Act 2018 Britania Raya sebagaimana diamendemen; The Brazil Law No. 13.709/18 sebagaimana diamendemen ("LGPD") dan peraturan yang diimplementasikan (atau akan diimplementasikan); dan semua hukum semacam ini yang berlaku, termasuk undang-undang privasi siswa dan pendidikan nasional, negara bagian, dan/atau setempat.

- c) **"Personal Data"** is information that relates to an identified or identifiable individual including, but not limited to, students, parents, and school employees.
- 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 Lenovo, 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.

- c) **"Data Pribadi"** adalah informasi yang berkaitan dengan individu yang diidentifikasi atau dapat diidentifikasi termasuk, namun tidak terbatas pada, siswa, orang tua, dan karyawan sekolah.
- d) **"Subjek Data"** adalah individu yang dapat diidentifikasi secara langsung atau tidak langsung termasuk, namun tidak terbatas pada, siswa, orang tua, dan karyawan sekolah.
- e) **"Pelanggan"** adalah Pengontrol. Khusus untuk tujuan DPA ini, istilah "Pelanggan" mencakup Pelanggan dan Afiliasi Sah.
- f) **"Pemasok"** berarti Lenovo, yang bertindak sebagai Pemroses.
- g) **"Pengekspor Data"** berarti pihak yang mengalihkan Data Pribadi (bertindak sebagai Pengontrol) ke Pihak lain sesuai dengan Perjanjian.

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.

h) **"Pengimpor Data"** berarti pihak yang menerima Data Pribadi Pelanggan (bertindak sebagai Pemroses atau Subpemroses) dari Pihak lain (Pengontrol) 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 Lenovo Sales Agreement, Lenovo NetFilter 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: Pengontrol mengakui Pemasok sebagai Pemroses untuk memproses Data Pribadi yang tunduk pada Perjanjian Penjualan Lenovo, Syarat Layanan Lenovo NetFilter, dan EULA dengan Pemasok. Setiap pihak harus mematuhi kewajiban yang berlaku untuknya menurut Hukum 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 NetFilter users leveraging personal data obtained from the use of Lenovo NetFilter. 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 Pemroses dan mematuhi ketat dokumen instruksi Pengontrol ("Tujuan yang Diperbolehkan") sebagaimana didokumentasi di Lampiran A "Detail pemrosesan", kecuali apabila diwajibkan sebaliknya oleh Hukum Perlindungan Data yang Berlaku. Pemasok harus segera memberi tahu Pengontrol jika Pemasok mengetahui bahwa instruksi Pemrosesan Pengontrol melanggar Hukum Perlindungan Data yang Berlaku. Bagaimana pun juga, Pemasok tidak boleh memproses Data Pribadi untuk tujuannya sendiri atau tujuan pihak ketiga mana pun, termasuk untuk tujuan pemasaran. Untuk menghindari keraguan, Pemasok tidak boleh mengirimkan komunikasi pemasaran atau promosi lainnya ke pengguna Lenovo NetFilter dengan memanfaatkan data pribadi yang diperoleh dari penggunaan Lenovo NetFilter. Hal tersebut tidak akan mencegah individu menerima komunikasi promosi atau pemasaran jika komunikasi tersebut berasal dari konteks saluran standar, seperti situs web Lenovo atau Stoneware, dan saluran lain terkait penjualan.

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 Laws and data localization laws. For the avoidance of doubt:

Transfer internasional: Pemasok dapat mentransfer Data Pribadi ke negara mana pun di luar negara dari mana Data Pribadi dikumpulkan, sesuai dengan Hukum Perlindungan Data dan undang-undang

pelokalan 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 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.

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.

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

- a) *Pengalihan Data Pribadi ke luar Area Ekonomi Eropa ("EEA") dan Britania Raya diperbolehkan: (i) jika Data Pribadi dialihkan ke penerima di negara yang telah diputuskan memberikan perlindungan yang memadai untuk Data Pribadi oleh Komisi Eropa, Secretary of State Britania Raya, dan/atau Information Commissioner's Office Britania Raya; dan (ii) ke penerima yang telah menjalankan klausul kontrak standar yang digunakan atau disetujui oleh Komisi Eropa, Secretary of State Britania Raya, dan/atau Information Commissioner's Office Britania Raya.*

Pemasok dapat mengalihkan Data Pribadi ke luar Brazil jika: (i) Data dialihkan ke penerima di negara yang telah diputuskan memberikan perlindungan yang memadai untuk Data Pribadi oleh Pihak Berwenang Nasional; (ii) ke penerima yang telah menjalankan klausul kontrak standar yang digunakan atau disetujui oleh Pihak Berwenang Nasional; atau (iii) ketika penerima mampu menyediakan dan menunjukkan implementasi perlindungan lain sesuai dengan Hukum Perlindungan Data Brazil dan pengalihan internasional disetujui oleh Pengontrol.

- b) *Umumnya, penerimaan DPA ini berarti Pelanggan setuju bahwa Lenovo, Inc. dapat mengalihkan Data Pribadi melintasi perbatasan sejauh Lenovo mematuhi Hukum Perlindungan Data yang berlaku. Dalam hal ini, Lampiran D "Pengalihan Data Internasional" berlaku antara Pengontrol dan Pemasok apabila 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.

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 Lenovo NetFilter Technical and Organizational Measures (TOMs).

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) 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

Kerahasiaan Pemrosesan: Pemasok harus memastikan bahwa setiap orang yang diberikan wewenang untuk memproses Data Pribadi (termasuk staf, agen, dan subpemroses Pemasok) ("Orang yang Berwenang") harus mematuhi secara ketat terhadap kewajiban untuk merahasiakan (baik kewajiban berdasarkan kontrak atau kewajiban berdasarkan undang-undang) dan tidak akan memperbolehkan siapa pun memproses Data Pribadi jika tidak di bawah kewajiban untuk merahasiakannya. Pemasok harus memastikan semua Orang yang Berwenang hanya memproses Data Pribadi sebagaimana diperlukan untuk Tujuan yang Diperbolehkan. Lebih lanjut, Pemasok tidak akan memanfaatkan Data Pribadi secara komersial.

Keamanan: Pemroses harus mengimplementasikan langkah teknis dan organisasi yang sesuai untuk melindungi Data Pribadi (i) dari pemusnahan yang tidak disengaja atau yang melanggar hukum, dan (ii) dari kehilangan, perubahan, pengungkapan yang tidak berwenang, atau akses ke Data Pribadi ("Insiden Keamanan"). Lampiran C berisi Langkah Teknis dan Organisasi (TOM) Lenovo NetFilter.

Subpemrosesan: Pemasok setuju bahwa setiap subpemroses pihak ketiga yang ditunjuknya akan terikat dengan standar perlindungan data yang sama yang diberikan oleh Perjanjian ini; dan bahwa Pemasok akan mengadakan perjanjian sebagaimana mestinya dengan subpemrosesnya untuk menerapkan dengan tepat persyaratan di dalam DPA ini, Pengontrol setuju bahwa Pemasok dapat menggunakan subpemroses mana pun yang tercantum di Lampiran B. Meskipun demikian, Pengontrol menyetujui Pemasok melibatkan subpemroses baru (termasuk penggantian subpemroses yang sudah ada) untuk memproses Data Pribadi, **asalkan:** (i) Pemasok memberikan pemberitahuan minimal 30 hari kerja sebelum penambahan atau penggantian subpemroses (termasuk detail tentang pemrosesan yang dikerjakannya atau akan dikerjakannya), yang dapat diberikan dengan memberikan informasi

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.

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 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.

mendetail tentang penambahan atau penggantian tersebut kepada Pengontrol; dan (ii) Pemasok memberlakukan syarat perlindungan data terhadap subpemroses mana pun yang ditunjuknya yang melindungi Data Pribadi dengan standar yang sama yang diberikan oleh DPA ini. Jika Pengontrol menolak untuk menyetujui penunjukan subpemroses pihak ketiga baru oleh Pemasok, yang tidak boleh ditahan tanpa alasan yang wajar, maka Pemasok tidak akan menunjuk subpemroses atau Pengontrol dapat memilih untuk mengakhiri Perjanjian, asalkan Pengontrol memiliki alasan yang kuat dan didokumentasi atas penolakan perubahan tersebut.

Kerja Sama dan Hak Subjek Data: Pemasok harus memberikan bantuan yang wajar dan tepat waktu kepada Pengontrol untuk memungkinkan Pengontrol merespons: (i) semua permintaan dari Subjek Data untuk menggunakan salah satu dari haknya di bawah Hukum Perlindungan Data yang Berlaku (termasuk haknya atas akses, koreksi, pernyataan keberatan, penghapusan, dan portabilitas Data Pribadi, sebagaimana berlaku); dan (ii) semua korespondensi lain, pertanyaan, atau keluhan yang diterima dari Subjek Data, pihak pengawas peraturan, atau pihak ketiga lain dalam hubungannya dengan Pemrosesan Data Pribadi. Untuk menghindari keraguan, Permintaan Subjek Data (DSR) harus diminta oleh Pengontrol dengan menyerahkan permintaan formal dalam [Webform Privasi DSR Stoneware](#).

Insiden Keamanan: Saat mengetahui tentang Insiden Keamanan, Pemasok harus memberi tahu Pengontrol tanpa penundaan yang tidak semestinya dan harus memberikan secara tepat waktu semua informasi dan kerja sama yang mungkin diperlukan Pengontrol untuk memenuhi kewajiban pelaporan pelanggaran Data Pribadinya di bawah Hukum Perlindungan Data yang Berlaku (dan sesuai dengan skala waktu yang diwajibkan oleh Hukum Perlindungan Data yang Berlaku). Pemasok harus mengambil langkah dan tindakan lebih lanjut yang diperlukan untuk memperbaiki atau

mengurangi efek Insiden Keamanan dan harus terus memberitahu Pengontrol tentang semua perkembangan sehubungan dengan Insiden Keamanan.

Deletion or return of Data: Upon termination or expiry of the Lenovo 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.

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.

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

Penghapusan atau pengembalian Data: Saat Perjanjian Penjualan Lenovo berakhir atau kedaluwarsa, atas permintaan Pengontrol, Pemasok harus memusnahkan atau mengembalikan kepada Pengontrol semua Data Pribadi (termasuk semua salinan Data Pribadi) yang dimilikinya atau dikontrolnya (termasuk semua Data Pribadi yang disubkontrakkan ke pihak ketiga untuk Pemrosesan). Jika Pengontrol tidak memberikan instruksi lebih lanjut kepada Pemasok, jadwal retensi data Pemasok, seperti yang diterangkan di Lampiran A, akan berlaku. Persyaratan ini tidak akan berlaku sejauh Pemasok diwajibkan oleh Hukum Perlindungan Data yang Berlaku untuk menyimpan beberapa atau semua Data Pribadi, di mana Pemasok akan memisahkan dan melindungi Data Pribadi dari Pemrosesan lebih lanjut kecuali sejauh diwajibkan oleh hukum tersebut.

Audit: Selama masa berlaku Perjanjian ini dan selama tiga tahun setelah berakhirnya atau kedaluwarsanya Perjanjian, Pemasok harus mengizinkan Pengontrol (atau auditor pihak ketiganya) mengaudit kepatuhan Pemasok dengan biayanya sendiri dan harus menyediakan informasi yang diperlukan untuk Pengontrol (atau auditor pihak ketiganya) melakukan audit tersebut, asalkan lingkup permintaan audit tersebut bersifat wajar dan Pengontrol memberinya pemberitahuan sebelumnya tentang niatnya untuk melakukan audit. Pengontrol tidak akan menggunakan hak auditnya lebih dari satu kali dalam periode dua belas (12) bulan kalender, kecuali jika dan ketika diwajibkan oleh instruksi dari pihak berwenang perlindungan data yang kompeten.

DEMIKIANLAH, Lenovo dan Pelanggan telah menjalankan Perjanjian ini per tanggal yang tertulis di atas.

Lenovo/Lenovo

Custome/Pelanggan

Signature/Tanda tangan:

Signature/Tanda tangan:

Print Name/Nama /: Kimberly Page

Print Name/Nama: _____

Title/Jabatan: Strategic Operations Manager

Title/Jabatan: _____

ANNEX A – PROCESSING DETAILS/LAMPIRAN A – DETAIL PEMROSESAN

Type of data & data subjects/ <i>Jenis data & subjek data</i>	Retention Period/ <i>Periode Retensi</i>	Nature, purpose, and subject matter / <i>Sifat, tujuan, dan topik bahasan</i>
Student Interface related data/ Data yang terkait Antarmuka Siswa: - 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 e-mail siswa.</i> - IP Address/ <i>Alamat IP</i> - Browsing history and Key word Search history / <i>Riwayat penelusuran dan Riwayat Pencarian kata kunci</i>	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./ <i>Saat diminta pengguna untuk dihapus atau setelah 1 tahun tidak ada lisensi aktif atau uji coba aktif, data akan diarsipkan. Data yang diarsipkan akan dihapus setelah 90 hari.</i>	<i>Data Access (retrieve, copy, examine, modify, transport, scan, or otherwise access Customer Data)/ Akses Data (mengambil, menyalin, memeriksa, memodifikasi, memindahkan, memindai, atau mengakses Data Pelanggan)</i>
School Employee Interface related data/ Data yang terkait Antarmuka Karyawan Sekolah: - The first name of the employee/ <i>Nama depan karyawan.</i> - The last name of the employee/ <i>Nama belakang karyawan.</i> - The e-mail address of the employee/ <i>Alamat e-mail karyawan.</i> - IP Address/ <i>Alamat IP</i> - Browsing history and Key word Search history/ <i>Riwayat penelusuran dan Riwayat Pencarian kata kunci</i>	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./ <i>Saat diminta pengguna untuk dihapus atau setelah 1 tahun tidak ada lisensi aktif atau uji coba aktif, data akan diarsipkan. Data yang diarsipkan akan dihapus setelah 90 hari.</i>	<i>Data Access (retrieve, copy, examine, modify, transport, scan, or otherwise access Customer Data)/ Akses Data (mengambil, menyalin, memeriksa, memodifikasi, memindahkan, memindai, atau mengakses Data Pelanggan)</i>
Client Interface related data/ Data yang terkait Antarmuka Klien:	Upon user's request for deletion or after 1 year of	<i>Data Access (retrieve, copy, examine, modify,</i>

• Host Name/ <i>Nama Host</i> • Username/ <i>Nama Pengguna</i> • IP Address/ <i>Alamat IP</i> • Web History Searches/ <i>Pencarian Riwayat Web</i> • Key word searches/ <i>Pencarian kata kunci</i> • Web App Usage/ <i>Penggunaan Aplikasi Web</i> • Browser/ <i>Browser</i> • Device Type/ <i>Jenis Perangkat</i> • NetFilter App Usage/ <i>Penggunaan Aplikasi NetFilter</i> • Browser Data/ <i>Data Browser</i>	not having an active license or trial, data will be archived. Archived data is purged after 90 days./ <i>Saat diminta pengguna untuk dihapus atau setelah 1 tahun tidak ada lisensi aktif atau uji coba aktif, data akan diarsipkan. Data yang diarsipkan akan dihapus setelah 90 hari.</i>	transport, scan, or otherwise access Customer Data)/ <i>Akses Data (mengambil, menyalin, memeriksa, memodifikasi, memindahkan, memindai, atau mengakses Data Pelanggan)</i>
Organization related data/ <i>Data yang terkait organisasi</i> • The name of the organization/ <i>Nama organisasi.</i> • Organization Domain/ <i>Domain Organisasi</i>	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./ <i>Saat diminta pengguna untuk dihapus atau setelah 1 tahun tidak ada lisensi aktif atau uji coba aktif, data akan diarsipkan. Data yang diarsipkan akan dihapus setelah 90 hari.</i>	<i>Data Storage</i> (record, host, log, archive or otherwise store Customer Data); <i>Data Access</i> (retrieve, copy, examine, modify, transport, scan, or otherwise access Customer Data); <i>Data Analysis</i> (survey, test, study, interpret, organize, report, or otherwise analyse Customer Data)./ <i>Penyimpanan Data</i> (merekam, menghosting, mencatat, mengarsipkan, atau menyimpan Data Pelanggan); <i>Akses Data</i> (mengambil, menyalin, memeriksa, memodifikasi, memindahkan, memindai, atau mengakses Data Pelanggan); <i>Analisis Data</i> (melakukan survei, menguji, mempelajari, menafsirkan,

		<i>mengorganisasi, melaporkan, atau menganalisis Data Pelanggan).</i>
User data/ Data pengguna • The first name of the user/ <i>Nama depan pengguna.</i> • The last name of the user/ <i>Nama belakang pengguna.</i> • The e-mail address of the user/ <i>Alamat e-mail pengguna.</i> • IP Address/ <i>Alamat IP</i> • System/ <i>Sistem</i> • Access/Usage/Authorization Data Box/ <i>Akses/Penggunaan/Kotak Data Otorisasi</i> • Sensitive/special categories of data: Data logs, web browsing history, machine host name, key word search history/ <i>Kategori data sensitif/spesial: Log data, riwayat penelusuran web, nama host mesin, riwayat pencarian kata kunci.</i>	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./ <i>Saat diminta pengguna untuk dihapus atau setelah 1 tahun tidak ada lisensi aktif atau uji coba aktif, data akan diarsipkan. Data yang diarsipkan akan dihapus setelah 90 hari.</i>	<i>Data Access (retrieve, copy, examine, modify, transport, scan, or otherwise access Customer Data)/</i> <i>Akses Data (mengambil, menyalin, memeriksa, memodifikasi, memindahkan, memindai, atau mengakses Data Pelanggan)</i>
License data (Excludes personal data)/ Data lisensi (Tidak termasuk data pribadi)	This data is kept as long as necessary to comply with legal obligations, to enforce our agreements, etc. This does not include personal data./ <i>Data ini disimpan selama diperlukan untuk mematuhi kewajiban hukum, untuk menegakkan perjanjian kami, dll. Ini tidak termasuk data pribadi.</i>	<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> <i>Penyimpanan Data (merekam, menghosting, mencatat, mengarsipkan, atau menyimpan Data Pelanggan);</i>

		Akses Data (mengambil, menyalin, memeriksa, memodifikasi, memindahkan, memindai, atau mengakses Data Pelanggan); Analisis Data (melakukan survei, menguji, mempelajari, menafsirkan, mengorganisasi, melaporkan, atau menganalisis Data Pelanggan).
--	--	---

Duration of the Processing / Durasi Pemrosesan

The duration of the processing corresponds to the duration of the Agreement. Data retention policies as described above will apply./

Durasi pemrosesan sesuai dengan durasi Perjanjian. Kebijakan retensi data seperti yang dijelaskan di atas akan berlaku.

Categories of Data Subjects/ Kategori Subjek Data

Students, Teachers, Organization contacts and Users in general/

Siswa, Guru, Kontak organisasi, dan Pengguna secara umum

ANNEX B – SUBPROCESSORS/ LAMPIRAN B – SUBPEMROSES

Name/ Nama	Data/ Data	Storage Location/ Lokasi Penyimpanan	Purpose/ Tujuan
Amazon Web Services/ <i>Amazon Web Services</i>	All user data as described in Annex A/ <i>Semua data pengguna sebagaimana dijelaskan di Lampiran A</i>	US, EU/ AS, UE	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>
UDS Web Interface/ <i>UDS Web Interface</i>	Identity management data/ <i>Data manajemen identitas</i>	US, EU/ AS, UE	Identity management and authentication authorization. / <i>Manajemen identitas dan otorisasi autentikasi.</i>

**ANNEX C – TECHNICAL AND ORGANIZATIONAL MEASURES (TOMs)/
LAMPIRAN C – LANGKAH 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 mengimplementasikan program keamanan tertulis yang lengkap dengan kontrol fisik, teknis, prosedural, dan administratif yang mencerminkan standar industri yang berlaku untuk perlindungan dan penggunaan Data Pribadi yang bertanggung jawab, termasuk, namun tidak terbatas pada, kontrol berikut ini:

Technical / Teknis	Scope/ Lingkup	Controls/ Kontrol
Access/Akses	Logins (system & application). / Log in (sistem & aplikasi).	NIST-based password policies (multi-factor authentication for admin-level access and interfaces). / <i>Kebijakan kata sandi berbasis NIST</i> (otentikasi multifaktor untuk antarmuka dan akses level admin).
Encryption/Enkripsi	Data storage at rest & in transit. / <i>Penyimpanan data saat tidak aktif & dalam transit.</i>	AES 256-GCM (at rest), TLS 1.2 (in transit) ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA256 ECDHE-RSA-AES128-SHA256 (server preferred cipher suites). / <i>AES 256-GCM (tidak aktif), TLS 1.2 (dalam transit)</i> ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA256 ECDHE-RSA-AES128-SHA256 (cipher suites pilihan server).
Static application security testing / <i>Pengujian keamanan aplikasi statis</i>	All server and micro-service images, All binary clients and extensions/plugins. / <i>Semua server dan gambar layanan mikro, Semua klien binary dan ekstensi/plugin.</i>	Regular vulnerability scans and monitoring. / <i>Pemindaian kerentanan reguler dan pemantauan.</i>
Dynamic application security testing / <i>Pengujian keamanan aplikasi dinamis</i>	External applications APIs. / <i>API aplikasi eksternal.</i>	Web application scans, Penetration testing (On an AdHoc basis as scheduled by SSRB). / <i>Pemindaian aplikasi web, Pengujian penetrasi</i> (Sementara sesuai yang dijadwalkan oleh SSRB).
CIS benchmark hardening /	Cloud platform provider, Server instances. / <i>Penyedia platform cloud,</i>	Cloud CIS compliance checks, Cloud security monitoring,

Penguatan tolok ukur CIS	Kejadian server.	Regular CIS L2 server benchmark assessments./ Pengecekan kepatuhan CIS cloud, Pemantauan keamanan cloud, Penilaian tolok ukur server L2 CIS regular.
Software compositional analysis/ Analisis komposisi perangkat lunak	3 rd party opensource dependencies./ Ketergantungan sumber terbuka pihak ketiga.	Conduct regular vulnerability audits, repository monitoring./ Melakukan audit kerentanan secara rutin, pemantauan repositori.
Infrastructure assessment/ Penilaian infrastruktur	Cloud platform provider./ Penyedia platform cloud.	Regular reviews of all software-defined networks (SDNs) (identify network segmentation, firewall configuration, and resource access misconfigurations)./ Peninjauan reguler atas semua jaringan yang ditetapkan perangkat lunak (SDN) (identifikasi segmentasi jaringan, konfigurasi firewall, dan kesalahan konfigurasi akses sumber daya).
Web application firewall (WAF)/ Firewall aplikasi web (WAF)	Production web applications./ Aplikasi web produksi.	WAF protection (core rules for common attacks)./ Perlindungan WAF (aturan inti untuk serangan umum).
Static code analysis owned by Netsweeper/ Analisis kode statis yang dimiliki oleh Netsweeper	Proprietary code./ Kode eksklusif.	Regular code analysis is conducted using a commercial tool, will be done with each code release./ Analisis kode secara rutin dilakukan menggunakan peralatan komersial, akan dilakukan dengan setiap rilis kode.
Log collection/ Koleksi log	Cloud platform provider, Application./ Penyedia platform cloud, Aplikasi.	Cloud platform API transactions (logs older than one year are purged, accessible through Datadog and available to internal users with Lenovo Active Directory Integration for SAML 2.0 auth), WAF logging for edge detection (logs reside only within the instance, accessible by engineering), Subprocessors, see Annex B, for application purposes./ Transaksi API platform cloud (log yang lebih lama dari satu tahun akan dihapus, dapat diakses melalui Datadog dan tersedia bagi pengguna internal)

		dengan Lenovo Active Directory Integration untuk otorisasi SAML 2.0), pencatatan WAF untuk deteksi edge (log hanya ada di dalam instans, dapat diakses oleh staf teknis), Subpemroses, lihat Lampiran B, untuk tujuan aplikasi.
Infrastructure as code/ Infrastruktur sebagai kode	Cloud platform provider./ Penyedia platform cloud.	Infrastructure as code is used to automate infrastructure deployments and improve the immutability, misconfiguration of infrastructure./ Infrastruktur sebagai kode digunakan untuk mengotomatiskan penerapan infrastruktur dan meningkatkan kekekalan, kesalahan konfigurasi infrastruktur.

Organizational/ Organisasi	Scope/ Lingkup	Controls/ Kontrol
Incident (including data breach) response/ Respons insiden (termasuk pelanggaran data)	Security events related to products in production./ Peristiwa keamanan yang terkait produk dalam produksi.	Product incident response plan in accordance with NIST 800-61 and Lenovo's internal Product Security Incident Response Team (PSIRT) processes./ Rencana respons insiden produk sesuai dengan NIST 800-61 dan proses Tim Respons Insiden Keamanan Produk (PSIRT) internal Lenovo.
Trusted providers list/ Daftar penyedia tepercaya	All subprocessors that directly integrate with products in production./ Semua subpemroses yang secara langsung diintegrasikan dengan produk dalam produksi.	Standard security assessments of integrated providers, DPAs for Personal Data processing providers./ Penilaian keamanan standar dari penyedia yang terintegrasi, DPA untuk penyedia layanan pemrosesan Data Pribadi.
Vulnerability management/ Manajemen kerentanan	Server OSes, Docker containers, Clients, Products in production./ OS Server, Kontainer docker, Klien, Produk dalam produksi.	A program that employs various tools to aid in identifying vulnerabilities across all compute systems./ Program yang menggunakan berbagai alat untuk membantu mengidentifikasi kerentanan di seluruh sistem komputasi.

Software Security Review Board (SSRB) And Cloud Security Review Board (CSRB)/ <i>Software Security Review Board (SSRB) Dan Cloud Security Review Board (CSRB)</i>	Products in production./ <i>Produk dalam produksi.</i>	SSRB reviews are conducted during every release. CSRB reviews are conducted during every change in architecture. During reviews all technical and organizational measures are assessed for the product in question. / <i>Peninjauan SSRB dilakukan dalam setiap rilis. Peninjauan CSRB dilakukan dalam setiap perubahan dalam arsitektur. Selama peninjauan, semua langkah teknis dan organisasi dievaluasi untuk produk yang terkait.</i>
Data retention policy/ <i>Kebijakan retensi data</i>	Personal identifiable information, Application data, Products in production./ <i>Informasi identitas pribadi, Data aplikasi, Produk dalam produksi.</i>	Upon user's request for deletion, or after one year of not having an active license or trial, or after any arbitrary time should the business no longer require the data and the data is void of security implication. / <i>Saat pengguna meminta penghapusan, atau setelah satu tahun tidak ada lisensi yang aktif atau uji coba aktif, atau setelah waktu tertentu bisnis tidak lagi memerlukan data dan data tidak memiliki implikasi keamanan.</i>
Security and privacy awareness/ <i>Kesadaran akan keamanan dan privasi</i>	All employees (Privacy Basics and Security Essentials courses)/ <i>Semua karyawan (kursus Dasar Privasi dan Esensi Keamanan)</i>	Regular trainings for specialized IT and product teams on advanced security topics, such as OWASP Top 10. / <i>Pelatihan secara rutin untuk tim produk dan TI khusus tentang topik keamanan lanjut, seperti OWASP Top 10.</i>
Continuous security/ <i>Keamanan yang berkelanjutan</i>	Products in production./ <i>Produk dalam produksi.</i>	Regular application of Technical Measures. / <i>Aplikasi rutin Langkah Teknis.</i>
Opensource compliance reviews./ <i>Peninjauan kepatuhan sumber terbuka.</i>	Products in production./ <i>Produk dalam produksi.</i>	Assessments conducted to ensure proper licensing and attributions are provided in distributed software. / <i>Penilaian dilakukan untuk memastikan atribusi dan lisensi yang sesuai diberikan dalam</i>

		<i>perangkat lunak yang didistribusikan.</i>
Disaster Recovery/ <i>Pemulihan Bencana</i>	Products in production/ <i>Produk dalam produksi</i>	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>
Backup policy/ <i>Kebijakan cadangan</i>	Databases, Code, Logs. / <i>Database,</i> <i>Kode,</i> <i>Log.</i>	For Database backup / restore, encrypted backup (encrypted at rest) is used which is also highly available on multiple Availability Zone and can be restored within 30 mins. Previous 7-day backup is retained, and they are rotated. Manual snapshot if taken, can be stored indefinitely (1 year or more). Additionally automated (UDS) solution which runs cron job to encrypt and back up databases which retains it for a period of 7 days on rotation is also available. Application source code which includes 'Infrastructure as Code' (as well as DB creation) is on the UDS enterprise version are backed up indefinitely. Production logs are available on DataDog for 30 days. UDS is still in the process of extending these logs to 12 months on a cold archive./ <i>Untuk cadangan/pemulihan Database, cadangan enkripsi (dienkripsi saat tidak aktif) digunakan yang juga tersedia di beberapa Zona Ketersediaan dan dapat dipulihkan dalam waktu 30 menit. Cadangan 7 hari sebelumnya disimpan dan dirotasi. Cuplikan gambar manual, jika diambil, dapat disimpan tanpa batas waktu (1</i>

		tahun atau lebih). Tersedia juga solusi otomatis tambahan (UDS) yang menjalankan cron job untuk mengenkripsi dan mencadangkan database yang menyimpannya selama periode 7 hari berdasarkan rotasi. Kode sumber aplikasi yang mencakup 'Infrastruktur sebagai Kode' (serta kreasi DB) adalah di versi enterprise UDS yang dicadangkan tanpa batas waktu. Log produksi tersedia di DataDog selama 30 hari. UDS masih dalam proses memperpanjang log ini hingga 12 bulan di arsip dingin.
--	--	---

ANNEX D – INTERNATIONAL DATA TRANSFER AGREEMENT

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 (Lenovo.), 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.

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

- 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

LAMPIRAN D – PERJANJIAN PENGALIHAN DATA INTERNASIONAL

Lampiran ini menetapkan persyaratan perlindungan data (termasuk persyaratan di bawah Hukum Privasi yang Berlaku) yang berlaku: (i) untuk Pengekspor Data (Pengontrol) ketika mengalihkan Data Pribadi ke Pengimpor Data (Lenovo), afiliasinya, dan/atau Subpemrosesnya, untuk Pemrosesan Data; dan (ii) untuk Pengimpor Data ketika menerima Data Pribadi dari Pengekspor Data untuk Pemrosesan Data.

Pengimpor Data menjamin dan berjanji bahwa di setiap waktu Pengimpor Data akan:

- a) Memproses Data yang Dialihkan sesuai dengan Hukum Privasi yang Berlaku dan akan memberikan bantuan yang wajar dan tepat waktu kepada Pengekspor Data sebagaimana diperlukan untuk membantu Pengekspor Data mematuhi*

kewajibannya di bawah Hukum Privasi yang Berlaku; dan

- 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.

- b) akan secara sengaja melakukan kewajibannya di bawah Perjanjian ini sedemikian cara sehingga menyebabkan Pengekspor Data melanggar salah satu kewajibannya di bawah Hukum Privasi yang 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.

(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](#)

1. Area Ekonomi Eropa (EEA)

Jika layanan Pemasok diberikan kepada Pengontrol dalam lingkup Area Ekonomi Eropa ("EEA") atau yurisdiksi lain yang tunduk pada Hukum Perlindungan Data UE, ketentuan berikut berlaku:

(A) "Hukum Perlindungan Data UE" berarti (a) Peraturan 2016/679 Parlemen Eropa dan Majelis tentang perlindungan individu terkait Pemrosesan Data Pribadi dan tentang pergerakan bebas data tersebut (General Data Protection Regulation) ("GDPR"); (b) e-Privacy Directive (Directive 2002/58/EC) UE; dan (c) setiap dan semua hukum perlindungan data nasional yang berlaku.

(B) Pemasok harus segera memberitahu Pengontrol (a) tentang semua persyaratan di bawah Hukum Perlindungan Data UE yang mewajibkan Pemrosesan Data Pribadi dengan cara yang lain dari cara pemrosesan menurut instruksi Pengontrol, atau (b) jika, menurut pendapat Pemasok, instruksi Pengontrol dapat melanggar atau tidak mematuhi Hukum Perlindungan Data UE yang berlaku.

(C) **Pengalihan Data:** Jika Pemasok atau Subkontraktornya berada di luar EEA, dengan ini Pemasok dan Pengontrol menjalankan klausul kontrak standar pengontrol ke pemroses sebagaimana ditetapkan di MODUL DUA di [Commission Implementing Decision \(EU\) 2021/914 tertanggal 4 Juni 2021 tentang klausul kontrak standar untuk pengalihan data pribadi ke negara ketiga menurut Peraturan](#)

[\(EU\) 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:

[\(EU\) 2016/679 dari Parlemen Eropa dan Majelis](#) sebagaimana diamendemen atau ditiadakan dari waktu ke waktu ("Klausul Kontrak Standar C2P") dan dengan ini menyertakannya ke dalam Adendum ini melalui referensi. Para pihak mengakui dan setuju bahwa:

a. Pemasok dan Pengontrol masing-masing harus mematuhi kewajiban mereka masing-masing yang ada di dalam Klausul Kontrak Standar C2P;

b. Jika ada pertentangan atau ketidaksesuaian antara Klausul Kontrak Standar C2P dan Adendum ini atau perjanjian dasar, maka Klausul Kontrak Standar C2P yang akan mengontrol pertentangan tersebut; dan

c. Dengan ini informasi di dalam tabel berikut disertakan di dalam Klausul Kontrak Standar C2P antara Para Pihak:

**Information to be incorporated into the
C2P Standard Contractual Clauses between Controller and Supplier:/
Informasi yang harus disertakan di dalam Klausul Kontrak Standar C2P antara Pengontrol
dan Pemasok:**

Clause 9. Use of sub-processors/ <i>Klausul 9. Penggunaan subpemroses</i>	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. Pengimpor data harus memberikan informasi minimal 30 hari di depan sesuai Klausul "Subpemrosesan"</i>
Clause 17. Governing law/ <i>Klausul 17. Hukum yang mengatur</i>	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-klausul ini harus ditafsirkan menurut hukum yang mengaturnya yang ditetapkan di</i>

	<i>dalam perjanjian dasar Para Pihak kecuali hukum yang mengaturnya bukan hukum Negara Anggota UE yang mengizinkan hak penerima manfaat pihak ketiga. Jika demikian, Para Pihak setuju bahwa Klausul-klausul ini akan diatur oleh hukum IRLANDIA.</i>
Clause 18 (b). Choice of forum and jurisdiction/ <i>Klausul 18 (b). Pilihan forum dan yurisdiksi</i>	The Parties agree that any dispute arising from these Clauses shall be resolved by the courts of IRELAND./ <i>Para Pihak setuju bahwa semua perselisihan yang timbul akibat Klausul-klausul ini akan diselesaikan oleh pengadilan IRLANDIA.</i>

***Information to be incorporated into Annex 1, Part A of the C2P Standard Contractual Clauses:/
Informasi yang harus disertakan di dalam Lampiran 1, Bagian A dari Klausul Kontrak Standar C2P:***

<i>Data Exporter's Name/ Nama Pengekspor Data</i>	Controller, and any of its commonly owned or controlled affiliates/ <i>Pengontrol, dan semua afiliasi yang umumnya dimilikinya atau dikontrolnya</i>
<i>Data Exporter's Address/ Alamat Pengekspor Data</i>	To be completed by data exporter/ <i>Untuk diisi oleh pengekspor data</i>
<i>Data Exporter's contact person's name, position and contact details/ Nama, jabatan, dan detail kontak narahubung Pengekspor Data</i>	To be completed by data exporter/ <i>Untuk diisi oleh pengekspor data</i>
<i>Data Exporter's activities relevant to the data transferred under these Clauses/ Aktivitas Pengekspor Data yang relevan dengan data yang dialihkan menurut Klausul-klausul ini</i>	To be completed by data exporter/ <i>Untuk diisi oleh pengekspor data</i>
<i>Data Exporter's signature and date/ Tanda tangan dan tanggal Pengekspor Data</i>	To be completed by data exporter/ <i>Untuk diisi oleh pengekspor data</i>
<i>Data Exporter's role/ Peran Pengekspor Data</i>	Controller/ <i>Pengontrol</i>
<i>Data Importer's name/ Nama Pengimpor Data</i>	Supplier (Lenovo) and its Subcontractors/ <i>Pemasok (Lenovo) dan Subkontraktornya</i>
<i>Data Importer's address/ Alamat Pengimpor Data</i>	3400 E Coliseum Blvd, #310, Fort Wayne, IN 46805 United States of America/
<i>Data Importer's contact person's name, position and contact details/ Nama, jabatan, dan detail kontak narahubung Pengimpor Data</i>	Kimberly Page, Strategic Operations Manager privacy@lanschool.com/ 3400 E Coliseum Blvd, #310, Fort Wayne, IN 46805 United States of America

<i>Data Importer's activities relevant to the data transferred under these Clauses/ Aktivitas Pengimpor Data yang relevan dengan data yang dialihkan menurut Klausul-klausul ini</i>	As set out in Part B of Annex 1/ <i>Sebagaimana ditetapkan di Bagian B Lampiran 1</i>
<i>Data Importer's signature and date/ Tanda tangan dan tanggal Pengimpor Data</i>	To be completed by data importer/ <i>Untuk diisi oleh pengimpor data</i>
<i>Data Importer's Role/ Peran Pengimpor 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 harus disertakan di dalam Lampiran 1, Bagian B dan C dari Klausul Kontrak Standar C2P:

<i>Categories of data subjects/ Kategori subjek data</i>	As set out in Annex A above/ <i>Sebagaimana ditetapkan di Lampiran A di atas</i>
<i>Categories of personal data/ Kategori data pribadi</i>	As set out in Annex A above/ <i>Sebagaimana ditetapkan di Lampiran A di atas</i>
<i>Sensitive data/ Data sensitif</i>	As set out in Annex A above/ <i>Sebagaimana ditetapkan di Lampiran A di atas</i>
<i>Frequency of the Transfer/ Frekuensi Pengalihan</i>	Ongoing frequency, as long as LSA license is active/ <i>Frekuensi terus-menerus, selama lisensi LSA aktif</i>
<i>Nature of the processing/ Sifat pemrosesan</i>	As set out in Annex A above/ <i>Sebagaimana ditetapkan di Lampiran A di atas</i>
<i>Purpose of the processing/ Tujuan pemrosesan</i>	As set out in Annex A above/ <i>Sebagaimana ditetapkan di Lampiran A di atas</i>
<i>Period for which personal data will be retained Periode penyimpanan data pribadi</i>	As set out in Annex A above/ <i>Sebagaimana ditetapkan di Lampiran A di atas</i>
<i>Subject matter, nature and duration of the processing carried out by subprocessors/ Topik bahasan, sifat, dan durasi pemrosesan yang dikerjakan oleh subpemroses</i>	As set out in Annex B above/ <i>Sebagaimana ditetapkan di Lampiran B di atas</i>
<i>Competent Supervisory Authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 ty / Pihak Pengawas Berwenang yang Kompeten dengan tanggung jawab untuk</i>	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

<i>memastikan kepatuhan pengekspor data terhadap Peraturan (EU) 2016/679 ty</i>	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./ <i>Pihak pengawas yang berwenang yang akan bertindak sebagai pihak pengawas berwenang yang kompeten adalah pihak pengawas berwenang dari Negara Anggota EU di mana Pengekspor Data berada di UE. Jika Pengekspor Data (yakni entitas hukum yang dikontrak) tidak berada di UE, maka Pihak Pengawas Berwenang yang Kompeten adalah yang di Negara Anggota UE di mana perwakilan UE Pengekspor Data, dalam arti yang diberikan di Pasal 27(1) Peraturan (UE) 2016/679, berada. Jika Pengekspor Data tidak berada di UE tetapi tidak perlu menunjuk perwakilan UE, maka Pihak Pengawas Berwenang yang Kompeten adalah yang di Negara Anggota UE tempat beradanya subjek data yang data pribadinya dialihkan menurut Klausul-klausul ini dalam kaitannya dengan penawaran barang atau layanan kepada mereka, atau yang perilakunya dipantau.</i>
--	---

Information to be incorporated into Annex 2 of the C2P Standard Contractual Clauses:/
Informasi yang harus disertakan di dalam Lampiran 2 dari Klausul Kontrak Standar C2P:

<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> <i>Deskripsi langkah teknis dan organisasi yang diimplementasikan oleh pengimpor data (termasuk semua sertifikasi yang relevan) untuk memastikan level keamanan yang sesuai, dengan memperhitungkan sifat, lingkup, konteks, dan tujuan pemrosesan, dan risiko terkait hak dan kebebasan individu.</i>	As set out in Annex C above/ <i>Sebagaimana ditetapkan di Lampiran C di atas</i>
---	--

Information to be incorporated into Annex 3 of the C2P Standard Contract Clauses:/
Informasi yang harus disertakan di dalam Lampiran 3 dari Klausul Kontrak Standar C2P:

List of authorized sub-processors/ <i>Daftar subpemroses sah</i>	As set out in Annex B above/ <i>Sebagaimana ditetapkan di Lampiran B di atas</i>
---	---

2. United Kingdom (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:

(A) 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) 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.

(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>).

2. Britania Raya (UK)

Jika layanan Pemasok diberikan kepada Pengontrol di dalam lingkup Britania Raya, atau sifat Data Pribadi memicu penerapan European Union (Withdrawal) Act 2018 ("UK GDPR") dan Data Protection Act 2018 ("DPA 2018"), maka ketentuan tambahan berikut berlaku:

(A) Pengalihan Data Pribadi ke penerima di negara yang oleh Secretary of State UK dianggap menyediakan perlindungan yang memadai untuk Data Pribadi ("Keputusan Kecukupan") akan diperbolehkan di bawah Perjanjian tanpa memerlukan persetujuan Klausul Kontrak Standar UK.

(B) Negara-negara EEA akan dianggap tunduk pada Keputusan Kecukupan untuk tujuan pengalihan Data Pribadi dari UK ke EEA.

(C) Jika tidak ada Keputusan Kecukupan, Pengontrol dan Pemasok akan setuju untuk menjalankan addendum transfer data Internasional UK terhadap klausul kontrak standar Komisi Eropa untuk pengalihan 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: Para Pihak

Information to be incorporated into “Part 1: Tables” of the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses:/ Informasi yang harus disertakan di dalam “Bagian 1: Tabel” dari Adendum Pengalihan Data Internasional terhadap Klausul Kontrak Standar Komisi UE:		
Start date/ Tanggal mulai	As per the above/ Sesuai di atas	
The Parties/ Para Pihak	Exporter (who sends the Restricted Transfer)/ Pengekspor (yang mengirimkan Transfer Terbatas)	Importer (who receives the Restricted Transfer)/ Pengimpor (yang menerima Transfer Terbatas)
Parties’ details/ Detail para pihak	Full legal name, main address (if a company registered address): As per the information in the 2nd table of the Art. 1. European Economic Area (EEA) in the Annex D Official registration number (if any) (company number or similar identifier): As per customer identified under the Sales Agreement / <i>Nama legal lengkap, alamat utama (jika alamat terdaftar untuk perusahaan): Sesuai informasi di tabel ke-2 dari Pasal. 1. Area Ekonomi Eropa (EEA) di Lampiran D</i> <i>Nomor registrasi resmi (jika ada) (nomor perusahaan atau pengidentifikasi serupa): Sesuai pelanggan yang diidentifikasi dalam Perjanjian Penjualan</i>	Full legal name, main address (if a company registered address): As per the information in the 2nd table of the Art. 1. European Economic Area (EEA) in the Annex D Official registration number (if any) (company number or similar identifier): 35-2097171 registered in State of Indiana/ <i>Nama legal lengkap, alamat utama (jika alamat terdaftar untuk perusahaan): Sesuai informasi di tabel ke-2 dari Pasal. 1. Area Ekonomi Eropa (EEA) di Lampiran D</i> <i>Nomor registrasi resmi (jika ada) (nomor perusahaan atau pengidentifikasi serupa): 35-2097171 terdaftar di Negara Bagian Indiana</i>

Key Contact/ Kontak Utama	Full Name (optional), job title, contact details including email: As per the information in the 2 nd table of the Art. 1. European Economic Area (EEA) in the Annex D/ <i>Nama Lengkap (opsional), jabatan, detail kontak termasuk e-mail: Sesuai informasi di tabel ke-2 dari Pasal. 1. Area Ekonomi Eropa (EEA) di Lampiran D</i>	Full Name (optional), job title, contact details including email: As per the information in the 2 nd table of the Art. 1. European Economic Area (EEA) in the Annex D/ <i>Nama Lengkap (opsional), jabatan, detail kontak termasuk e-mail: Sesuai informasi di tabel ke-2 dari Pasal. 1. Area Ekonomi Eropa (EEA) di Lampiran D</i>
--------------------------------------	---	---

Table 2: Selected SCCs, Modules and Selected Clauses/

Tabel 2: SCC Terpilih, Modul, dan Klausul Terpilih

Addendum EU SCCs/ SCC Adendum UE	See Annex D, Art. 1 above/ <i>Lihat Lampiran D, Pasal 1 di atas</i>
---	--

Table 3: Appendix Information/

Tabel 3: Informasi Apendiks

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 Para Pihak Sebagaimana diuraikan dalam Pasal 1. Area Ekonomi Eropa (EEA) di Lampiran D</i>
Annex 1B: Description of Transfer: As set out in Annex A above/ <i>Lampiran 1B: Deskripsi Transfer: Sebagaimana diuraikan di 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: Langkah teknis dan organisasi termasuk langkah teknis dan organisasi untuk memastikan keamanan data: Deskripsi Transfer: Sebagaimana diuraikan di 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 Subpemroses (Modul 2 dan 3 saja): Deskripsi Transfer: Sebagaimana diuraikan di Lampiran B di atas</i>

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

Tabel 4: Mengakhiri Adendum ini ketika Adendum yang Disetujui Diubah

Ending this Addendum when the Approved Addendum changes/ Mengakhiri Adendum ini ketika Adendum yang Disetujui diubah	Which Parties may end this Addendum as set out in Section 19: x Importer ☐ Exporter ☐ neither Party / <i>Pihak mana yang dapat mengakhiri Adendum ini sebagaimana diuraikan di Bagian 19:</i> x Pengimpor ☐ Pengekspor ☐ tidak satu Pihak pun
--	--

Information to be incorporated into “Part 2: Mandatory Clauses” of the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses: /
Informasi yang harus disertakan di dalam “Bagian 2: Klausul Wajib” dari Adendum Pengalihan Data Internasional terhadap Klausul Kontrak 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, yakni template Adendum B.1.0 yang dikeluarkan oleh ICO dan dipresentasikan di hadapan Parlemen sesuai s119A Data Protection Act 2018 tertanggal 2 Februari 2022, sebagaimana direvisi di bawah Bagian 18 dari Klausul Wajib tersebut.

3. Switzerland

Until Swiss relevant authorities release Swiss Model Clauses, C2P Model Clauses as executed under section 1 “European Economic Area (EEA)” above apply by reference. In the event that the European Commission or the Swiss government agrees a successor solution to the Swiss-US Privacy Shield, then provisions under section 2 “United Kingdom (UK)” above apply by reference.

3. Swiss

Sampai pihak berwenang yang relevan di Swiss merilis Klausul Model Swiss, Klausul Model C2P, sebagaimana dijalankan di bawah bagian 1 “Area Ekonomi Eropa (EEA)” di atas berlaku berdasarkan referensi. Apabila Komisi Eropa atau pemerintah Swiss menyepakati solusi penerus untuk Perlindungan Privasi Swiss-US, maka ketentuan di bawah bagian 2 “Britania Raya (UK)” di atas berlaku berdasarkan referensi.

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

5. South Africa

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:

(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,

4. Brasil

Jika ada transfer Data Pribadi yang tunduk pada Undang-Undang Perlindungan Data Pribadi Umum Brasil (sebagaimana diamendemen oleh 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 yang disebutkan di sini akan berlaku dengan amendemen sebagai berikut:

(i) pihak pengawas yang berwenang dari Klausul Kontrak Standar C2P adalah Pihak Berwenang Perlindungan Data Nasional Brasil (ANPD);

(ii) hukum yang mengatur sesuai dengan Klausul 17 dari Klausul Kontrak Standar C2P adalah LGPD;

(iii) pilihan forum dan yurisdiksi sesuai dengan Klausul 18 dari Klausul Kontrak Standar C2P adalah hukum Brasil jika pengalihan data secara eksklusif tunduk pada LGPD; dan

(iv) setiap referensi ke GDPR dalam Klausul Kontrak Standar C2P juga harus menyertakan referensi untuk ketentuan yang setara dengan LGPD (sebagaimana diamendemen atau diganti).

5. Afrika Selatan

Jika layanan Pemasok diberikan kepada Pengontrol dalam lingkup Afrika Selatan atau yurisdiksi lain yang tunduk pada Protection of Personal Information Act (POPIA), ketentuan tambahan berikut berlaku:

(A) Subjek Data berarti individu yang dapat diidentifikasi melalui referensi ke nama, nomor unik, data lokasi, pengidentifikasi online, atau satu faktor atau lebih yang spesifik untuk identitas fisik, fisiologis, genetik, mental,

economic, cultural, or social identity of that natural person as well as an identifiable juristic person or legal entity.

ekonomi, budaya, atau sosial individu tersebut serta entitas hukum atau pribadi hukum yang dapat diidentifikasi.

6. Australia

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

6. Australia

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

ANNEX E – ADDITIONAL PROVISIONS

LAMPIRAN E – KETENTUAN TAMBAHAN

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

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

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

Lenovo adalah sebuah Bisnis. Selain itu, Pemasok adalah Penyedia Layanan Pelanggan yang 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.
- 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 Lenovo 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 Lenovo
- c. This DPA shall serve as Supplier’s certification that Supplier understands

- a. *Pemasok tidak akan menjual Data Pribadi atau Informasi Eksklusif. "Menjual" berarti menjual, menyewakan, merilis, mengungkapkan, menyebarkan, membuat tersedia, mengalihkan, atau mengomunikasikan informasi untuk mendapatkan uang atau pertimbangan lain yang memiliki nilai.*
- b. *Pemasok tidak akan menyimpan, menggunakan, atau mengungkapkan Data Pribadi: (a) untuk tujuan apapun selain tujuan spesifik dari pelaksanaan layanan yang ditetapkan di dalam Perjanjian untuk Lenovo atau sebagaimana diperbolehkan dalam CCPA dan peraturan penerapannya, (b) untuk tujuan komersial selain dari memberikan layanan yang disebutkan di dalam kontrak dengan bisnis tersebut, atau (c) di luar hubungan bisnis langsung antara orang tersebut dan Lenovo*
- c. *DPA ini akan berfungsi sebagai sertifikasi Pemasok yang menyatakan*

the CCPA requirements applicable to businesses and service providers, including the restrictions in Cal. Civ. Code § 1798.140(w)(2)(A), and will comply with them.

bahwa Pemasok memahami persyaratan CCPA yang berlaku pada bisnis dan penyedia layanan, termasuk batasan dalam Cal. Civ. Code § 1798.140(w)(2)(A), dan akan mematuhi.