

SYARAT DAN KETENTUAN UMUM PEMROSESAN DATA

Syarat dan Ketentuan Umum Pemrosesan Data (“PPD”) ini merupakan bagian dari Syarat dan Ketentuan Umum Program Ecolab3D (“Syarat dan Ketentuan Umum”) dan dibuat oleh dan antara Ecolab Inc. atau satu atau lebih Afiliasinya dengan Pelanggan (masing-masing disebut sebagai “Pihak” dan secara bersama-sama disebut sebagai “Para Pihak”). Istilah-istilah yang digunakan dalam PPD ini memiliki arti yang ditetapkan di sini. Istilah yang tidak didefinisikan di sini akan memiliki arti sebagaimana dalam Syarat dan Ketentuan Umum, kecuali istilah tersebut memiliki arti khusus di bawah Hukum Perlindungan Data (sebagaimana didefinisikan di bawah), dalam hal ini definisi di bawah Hukum Perlindungan Data yang akan berlaku. Kecuali sebagaimana diubah di sini, ketentuan dalam Syarat dan Ketentuan Umum akan tetap berlaku sepenuhnya.

1. Definisi. Dalam PPD ini, istilah-istilah berikut memiliki arti yang ditetapkan di bawah ini dan istilah-istilah yang serumpun di bawah Hukum Perlindungan Data akan ditafsirkan sebagaimana mestinya:

1.1. "Pengendali" memiliki arti yang diberikan oleh Hukum Perlindungan Data atau, jika tidak ada definisi seperti itu dalam Hukum Perlindungan Data, berarti orang perseorangan atau badan hukum, otoritas publik, agensi, atau badan lain yang, baik secara sendiri maupun bersama-sama dengan orang lain, menentukan tujuan dan cara pemrosesan Informasi Pribadi.

1.2. "Hukum Perlindungan Data" berarti hukum perlindungan data komprehensif negara bagian dan internasional yang berlaku, termasuk, namun tidak terbatas pada (a) Peraturan Perlindungan Data Umum (*General Data Protection Regulation*/"GDPR") Uni Eropa (*European Union*/"UE"), hukum Wilayah Ekonomi Eropa (*European Economic Area*/"EEA"), dan GDPR yang ditransformasikan ke dalam hukum nasional Britania Raya melalui pemberlakuan bagian 3 *European Union (Withdrawal) Act 2018* dan sebagaimana telah diubah dengan *Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019* ("GDPR Britania Raya"), bersama dengan *United Kingdom Data Protection Act 2018* (secara bersama-sama disebut "Undang-Undang Perlindungan Data Britania Raya"); (b) *California Consumer Privacy Act Cal. Civ. Code § 1798.100 et seq.* ("CCPA"), dan undang-undang perlindungan data negara bagian yang serupa atau lainnya; (c) *Brazilian General Law on the Protection of Personal Data* ("LGPD"); dan (d) undang-undang perlindungan data komprehensif lainnya yang berlaku sehubungan dengan Informasi Pribadi apa pun yang diproses berdasarkan Syarat dan Ketentuan Umum.

1.3. "Subjek Data" berarti setiap orang yang teridentifikasi atau dapat diidentifikasi sebagaimana didefinisikan oleh Hukum Perlindungan Data.

DATA PROCESSING GENERAL TERMS AND CONDITIONS

This Data Processing General Terms and Conditions (“DPA”) forms a part of the Ecolab3D Program General Terms and Conditions (“General Terms and Conditions”) and is entered into by and between Ecolab Inc. or one or more of its Affiliates and Customer (each a “Party” and collectively the “Parties”). The terms used in this DPA shall have the meanings set forth herein. Terms not otherwise defined herein shall have the meaning given to them in the General Terms and Conditions, unless such term has a specific meaning under Data Protection Law (as defined below), in which case the definition under Data Protection Law shall control. Except as modified herein, the terms of the General Terms and Conditions shall remain in full force and effect.

1. Definitions. In this DPA, the following terms shall have the meanings set out below and cognate terms under Data Protection Law shall be construed accordingly:

1.1. “Controller” shall have the meaning ascribed to it by Data Protection Law or, if there is no such definition in Data Protection Law, it means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Information.

1.2. "Data Protection Law" means applicable state and international comprehensive data protection laws, including, but not limited to (a) the European Union (“EU”) General Data Protection Regulation (“GDPR”), European Economic Area (“EEA”) laws, and the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019 (“UK GDPR”), together with the United Kingdom Data Protection Act 2018 (collectively “UK Data Protection Law”); (b) the California Consumer Privacy Act Cal. Civ. Code § 1798.100 et seq. (“CCPA”), and similar or other state data protection laws; (c) the Brazilian General Law on the Protection of Personal Data (“LGPD”); and (d) other applicable, comprehensive data protection laws with respect to any Personal Information processed under the General Terms and Conditions.

1.3. “Data Subject” means any identified or identifiable natural person as defined by Data Protection Law.

1.4. "Informasi Pribadi" berarti setiap informasi pribadi, sebagaimana didefinisikan oleh Undang-Undang Perlindungan Data yang berlaku (juga dikenal sebagai Data Pribadi atau Informasi yang Dapat Diidentifikasi Secara Pribadi ("IDDSP")) dan termasuk setiap kategori data yang sensitif atau khusus) yang diproses berdasarkan atau sehubungan dengan Syarat dan Ketentuan Umum.

1.5. "Proses" (termasuk "proses", "pemrosesan", dan istilah-istilah terkait) berarti setiap operasi atau serangkaian operasi yang dilakukan terhadap Informasi Pribadi.

1.6. "Prosesor" memiliki arti yang diberikan kepadanya oleh Hukum Perlindungan Data atau, jika tidak ada definisi seperti itu dalam Hukum Perlindungan Data, berarti orang perseorangan atau badan hukum, otoritas publik, agensi, atau badan lain yang memproses Informasi Pribadi atas nama Pengendali.

1.7. "Insiden Keamanan" berarti pelanggaran keamanan yang mengarah pada penghancuran, kehilangan, perubahan, pengungkapan yang tidak disengaja atau melanggar hukum, pengungkapan yang tidak sah atas, atau akses ke Informasi Pribadi.

1.8. "Subprosesor" berarti siapa pun (termasuk pihak ketiga mana pun, namun tidak termasuk personel Ecolab) yang ditunjuk oleh atau atas nama Ecolab untuk memproses Informasi Pribadi sehubungan dengan Syarat dan Ketentuan Umum.

1.9. Istilah-istilah lain yang menggunakan huruf besar dan huruf kecil yang digunakan dalam PPD memiliki arti yang sama dengan Hukum Perlindungan Data, dan istilah-istilah serumpunnya akan ditafsirkan sesuai dengan itu.

2. Peran Para Pihak

2.1. Para Pihak setuju bahwa, untuk tujuan Hukum Perlindungan Data, Pelanggan adalah Pengendali dan Ecolab adalah Prosesor sehubungan dengan pemrosesan Informasi Pribadi dan bahwa istilah-istilah tersebut akan memiliki arti yang diberikan kepada mereka sesuai dengan Hukum Perlindungan Data.

2.2. Apabila Hukum Perlindungan Data tidak secara khusus menggunakan istilah Pengendali dan Prosesor, Para Pihak akan didefinisikan berdasarkan peran yang sesuai dengan istilah-istilah yang serumpun untuk Pengendali dan Prosesor menurut Hukum Perlindungan Data tertentu yang berlaku.

3. Jaminan Bersama atas Kepatuhan

3.1. Masing-masing Pihak mengakui dan mengonfirmasi bahwa mereka akan mematuhi semua persyaratan yang berlaku dalam Hukum Perlindungan Data dan ketentuan-ketentuan dalam PPD ini sehubungan dengan pemrosesan Informasi Pribadi.

3.2. Pelanggan dan Ecolab bertanggung jawab secara terpisah untuk mematuhi ketentuan-ketentuan perlindungan data menurut hukum yang berlaku untuk masing-masing pihak,

1.4. "Personal Information" means any personal information, as defined by the applicable Data Protection Law (also known as Personal Data or Personally Identifiable Information ("PII")) and including any sensitive or special categories of data) that is processed under or in connection with the General Terms and Conditions.

1.5. "Process" (including "process," "processing," and associated terms) means any operation or set of operations which is performed upon Personal Information.

1.6. "Processor" shall have the meaning ascribed to it by Data Protection Law or, if there is no such definition in Data Protection Law, it means a natural or legal person, public authority, agency or other body which processes Personal Information on behalf of the Controller.

1.7. "Security Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information.

1.8. "Subprocessor" means any person (including any third party but excluding personnel of Ecolab) appointed by or on behalf of Ecolab to process Personal Information in connection with the General Terms and Conditions.

1.9. The other capitalized and non-capitalized terms used in the DPA shall have the same meaning as in Data Protection Law, and their cognate terms shall be construed accordingly.

2. Roles of the Parties

2.1. The Parties agree that, for the purpose of Data Protection Law, Customer is the Controller and Ecolab is the Processor in relation to the processing of Personal Information and that such terms will have the meanings accorded to them pursuant to Data Protection Law.

2.2. Where Data Protection Law does not specifically utilize the terms Controller and Processor, the Parties shall be defined by the roles aligning with the cognate terms for Controller and Processor under the particular, applicable Data Protection Law.

3. Mutual Assurance of Compliance

3.1. Each Party acknowledges and confirms that it will comply with all applicable requirements of Data Protection Law and the terms of this DPA in relation to its processing of Personal Information.

3.2. Customer and Ecolab shall be separately responsible for conforming with such statutory data protection provisions as are applicable to each of them, and nothing in the DPA

dan tidak ada satu pun ketentuan dalam PPD ini yang dapat membebaskan salah satu Pihak dari kewajiban-kewajiban menurut hukumnya sendiri.

4. Kewajiban-Kewajiban Ecolab

4.1. Ecolab harus:

4.1.1 menyimpan, menggunakan, mengungkapkan, memindahkan atau memproses Informasi Pribadi hanya untuk tujuan kinerja yang ditentukan dalam Syarat dan Ketentuan Umum sebagaimana diatur dalam Pasal 8 di bawah ini;

4.1.2. memproses Informasi Pribadi hanya berdasarkan instruksi yang terdokumentasi dari Pelanggan (sebagaimana tercermin dalam Syarat dan Ketentuan Umum atau komunikasi tertulis atau lisan lainnya);

4.1.3. tidak menjual atau "membagikan" Informasi Pribadi, sebagaimana istilah-istilah tersebut didefinisikan oleh Hukum Perlindungan Data tertentu (misalnya CCPA), termasuk untuk konteks silang atau iklan bertarget (batasan apa pun tentang "pembagian" tidak berlaku untuk penggunaan Subprosesor atau pihak ketiga lainnya oleh Ecolab untuk pemrosesan data, apabila diperlukan untuk memenuhi kewajibannya berdasarkan Program dan Ketentuan);

4.1.4. tidak menyimpan, menggunakan, atau mengungkapkan Informasi Pribadi Pelanggan (i) untuk tujuan apa pun selain tujuan bisnis yang disebutkan dalam Syarat dan Ketentuan Umum (termasuk menyimpan, menggunakan, atau mengungkapkan Informasi Pribadi Pelanggan untuk tujuan komersial selain tujuan bisnis yang disebutkan dalam Program) atau sebagaimana yang diizinkan oleh Hukum Perlindungan Data yang berlaku, atau (ii) di luar hubungan bisnis langsung antara Pelanggan dan Ecolab;

4.1.5. tidak menggabungkan Informasi Pribadi Pelanggan seputar seorang individu yang diterima Ecolab dari, atau atas nama, Pelanggan dengan Informasi Pribadi yang diterima Ecolab dari, atau atas nama, orang lain, atau dikumpulkan dari interaksi Ecolab dengan individu tersebut, dengan ketentuan bahwa Ecolab dapat menggabungkan Informasi Pribadi Pelanggan untuk melaksanakan Tujuan Bisnis apa pun sebagaimana yang didefinisikan dan diizinkan berdasarkan Hukum Perlindungan Data yang berlaku;

4.1.6. memastikan bahwa orang yang berwenang untuk memproses Informasi Pribadi telah berkomitmen untuk menjaga kerahasiaan atau berada di bawah kewajiban kerahasiaan yang sesuai menurut hukum;

4.1.7. meninjau dan menerapkan pembaruan atau panduan peraturan yang mengikat sehubungan dengan Hukum Perlindungan Data baru yang berlaku terhadap Syarat dan Ketentuan Umum;

4.1.8. menyediakan kepada Pelanggan seluruh informasi yang diperlukan untuk menunjukkan kepatuhan Ecolab terhadap kewajibannya berdasarkan Syarat dan Ketentuan Umum.

shall relieve a Party of its own statutory obligations.

4. Obligations of Ecolab

4.1. Ecolab shall:

4.1.1 retain, use, disclose, transfer or otherwise process the Personal Information only for the specified purpose of performance under the General Terms and Conditions as set out in Section 8 below;

4.1.2. process Personal Information only on documented instructions from Customer (as reflected in the General Terms and Conditions or other written or verbal communication);

4.1.3. not sell or "share" Personal Information, as those terms are defined by specific Data Protection Law (e.g. CCPA), including for cross context or targeted advertising (any limitation on "sharing" shall not apply to Ecolab's use of Subprocessor or other third parties for data processing where necessary to fulfill its obligations under the Program and Terms);

4.1.4. not retain, use, or disclose Customer's Personal Information (i) for any purpose other than the business purposes specified in the General Terms and Conditions (including retaining, using, or disclosing the Customer Personal Information for a commercial purpose other than the business purpose specified in the Program) or as otherwise permitted by applicable Data Protection Laws, or (ii) outside of the direct business relationship between Customer and Ecolab;

4.1.5 not combine Customer Personal Information regarding an individual that Ecolab receives from, or on behalf of, Customer with Personal Information that it receives from, or on behalf of, another person, or collects from Ecolab's own interaction with the individual, provided that Ecolab may combine Customer's Personal Information to perform any Business Purpose as defined and permitted under applicable Data Protection Law;

4.1.6. ensure that persons authorized to process Personal Information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

4.1.7. review and implement updates or binding regulatory guidance with respect to new Data Protection Law that are applicable to the General Terms and Conditions;

4.1.8. make available to Customer all information necessary to demonstrate Ecolab's compliance with its obligations under the General Terms and Conditions. Customer may,

Pelanggan dapat, dengan pemberitahuan tertulis yang wajar kepada Ecolab, mengambil langkah-langkah yang wajar dan sesuai untuk menghentikan dan memulihkan penggunaan informasi pribadi yang tidak sah oleh Ecolab; dan

4.1.9. dengan segera, dan tanpa penundaan yang tidak semestinya, memberitahukan Pelanggan jika Ecolab memutuskan untuk tidak lagi memenuhi kewajibannya berdasarkan Hukum Perlindungan Data yang berlaku.

4.2. Sejauh mana Ecolab secara langsung menerima permintaan Subjek Data terkait Subjek Data Pelanggan, Ecolab akan memberitahukan Pelanggan tentang permintaan tersebut. Ecolab akan meneruskan permintaan tersebut kepada Pelanggan dan tidak akan memberikan tanggapan kepada Subjek Data kecuali jika diwajibkan oleh hukum. Atas permintaan tertulis yang wajar dari Pelanggan, dan sejauh mana Pelanggan tidak dapat memenuhi permintaan tanpa bantuan dari Ecolab melalui layanan mandiri yang tersedia atau opsi lainnya, Ecolab akan memberikan kerja sama dan bantuan yang wajar kepada Pelanggan untuk memungkinkan tanggapan terhadap permintaan Subjek Data.

4.3. Jika Ecolab menerima permintaan atau pertanyaan yang mengikat secara hukum dari otoritas publik atau regulator untuk pengungkapan Informasi Pribadi, Ecolab akan memberitahukan Pelanggan tentang permintaan tersebut, kecuali jika dilarang oleh hukum. Ecolab setuju untuk memberikan bantuan yang wajar kepada Pelanggan terkait permintaan tersebut, dengan mempertimbangkan sifat dari pemrosesan dan informasi yang tersedia untuk Ecolab, termasuk membantu Pelanggan dalam mengajukan keberatan terhadap permintaan tersebut dan memanfaatkan proses banding yang tersedia.

4.4. Sehubungan dengan pemrosesan Informasi Pribadi, Ecolab akan memberitahukan Pelanggan tentang permintaan atau keluhan lainnya seputar pemrosesan berdasarkan Program atau Ketentuan, termasuk, namun tidak terbatas pada a) permintaan atau keluhan yang diterima dari karyawan atau afiliasi Pelanggan; atau b) permintaan untuk pengungkapan Informasi Pribadi yang belum didefinisikan di sini yang terkait dengan Program.

4.5. Ecolab akan memberikan bantuan yang wajar apabila Pelanggan diwajibkan oleh Hukum Perlindungan Data yang berlaku untuk melakukan penilaian terhadap dampak dari Syarat dan Ketentuan Umum atau Program terhadap perlindungan Informasi Pribadi. Selain itu, Ecolab akan memberikan bantuan yang wajar apabila Pelanggan diwajibkan oleh Hukum Perlindungan Data yang berlaku, untuk berkonsultasi dengan pengatur terkait hal-hal yang berhubungan dengan pemrosesan Informasi Pribadi berdasarkan Syarat dan Ketentuan Umum.

4.6. Pelanggan menyetujui Ecolab untuk melibatkan Subprosesor untuk memproses Informasi Pribadi untuk tujuan kinerja berdasarkan Syarat dan Ketentuan Umum. Ketika Ecolab melibatkan Subprosesor untuk melakukan aktivitas pemrosesan Informasi Pribadi tertentu sebagai bagian dari

upon reasonable written notice to Ecolab, take reasonable and appropriate steps to stop and remediate any unauthorized use of personal information by Ecolab; and

4.1.9. promptly, and without undue delay, notify Customer if Ecolab determines that it can no longer meet its obligations under applicable Data Protection Laws.

4.2. The degree to which Ecolab directly receives a Data Subject request concerning a Customer's Data Subject, Ecolab shall notify Customer of such request. Ecolab shall forward such request to Customer and shall not respond to the Data Subject unless required by law. Upon Customer's reasonable written request, and the degree to which Customer is unable to fulfill a request without the assistance of Ecolab through available self-service or other options, Ecolab shall provide Customer with reasonable cooperation and assistance to enable a response to Data Subject's request.

4.3. If Ecolab receives a legally binding request or inquiry from a public authority or regulator for disclosure of Personal Information, it shall inform Customer of such request, unless prohibited by law. Ecolab agrees to provide Customer with reasonable assistance regarding such request, taking into account the nature of the processing and information available to Ecolab, including assisting Customer in challenging such request and leveraging any available appeals process.

4.4. As related to its processing of Personal Information, Ecolab shall notify Customer of any other requests or complaints regarding processing under the Program or Terms, including, but not limited to a) any requests or complaints received from Customer's employees or affiliates; or b) any request for disclosure of Personal Information not already defined herein that is related to the Program.

4.5. Ecolab shall provide reasonable assistance where Customer is required under applicable Data Protection Law to carry out assessments of the impact of the General Terms and Conditions or Program on the protection of Personal Information. In addition, Ecolab shall provide reasonable assistance where Customer is required under applicable Data Protection Law, to consult with a regulator regarding matters related to the processing of Personal Information under the General Terms and Conditions.

4.6. Customer consents to Ecolab engaging Subprocessors to process Personal Information for the purpose of performance under the General Terms and Conditions. Where Ecolab engages a Subprocessor for carrying out specific Personal Information processing activities as a part of performance

kinerja berdasarkan Syarat dan Ketentuan Umum, Ecolab akan mewajibkan kewajiban perlindungan data yang sesuai dengan hukum dan standar industri berdasarkan layanan yang diberikan dan Informasi Pribadi yang diproses oleh Subprosesor. Daftar Subprosesor Ecolab saat ini yang terlibat dalam pemrosesan Informasi Pribadi atas nama Pelanggan dapat dilihat pada Lampiran II. Ecolab akan memberikan pemberitahuan 30 hari sebelumnya kepada Pelanggan sebelum melibatkan Subprosesor baru. Jika Pelanggan tidak mengajukan keberatan dalam jangka waktu 30 hari terhadap Subprosesor yang baru, Pelanggan dianggap telah menyetujui keterlibatan Ecolab dalam hal tersebut.

5. Kewajiban Pelanggan

5.1. Pelanggan harus memberitahukan Ecolab tanpa penundaan yang tidak semestinya dan secara menyeluruh tentang kesalahan atau ketidakberesan apa pun yang berkaitan dengan ketentuan hukum tentang pemrosesan Informasi Pribadi yang terdeteksi selama pemrosesan tersebut. Pelanggan bertanggung jawab penuh atas keakuratan, kualitas, dan legalitas informasi pribadi yang diproses berdasarkan perjanjian ini, serta cara-cara yang digunakan oleh Pelanggan atau Afiliasi Pelanggan yang terkait untuk mengumpulkan, menyimpan, memproses, dan mengirimkan informasi pribadi tersebut.

5.2. Apabila diwajibkan oleh Hukum Perlindungan Data, Pelanggan bertanggung jawab penuh untuk memenuhi kewajiban pemberituannya sendiri terhadap Subjek Data, pengatur, atau pihak berwenang lainnya.

5.3. Jika Pelanggan menerima keluhan, pemberitahuan, atau komunikasi dari pihak berwenang yang berhubungan dengan: (i) pemrosesan Informasi Pribadi oleh Ecolab; atau (ii) potensi kegagalan untuk mematuhi Hukum Perlindungan Data, Pelanggan harus, sejauh yang diizinkan oleh hukum, segera meneruskan keluhan, pemberitahuan, atau komunikasi tersebut kepada Ecolab dan, jika berhubungan dengan pemrosesan Informasi Pribadi sesuai dengan PPD ini, memberikan Ecolab kerja sama yang wajar dan bantuan untuk merespons keluhan, pemberitahuan, atau komunikasi tersebut.

5.4. Pelanggan menyatakan dan menjamin bahwa Data Pelanggan tidak akan mencakup informasi apa pun yang dianggap sensitif berdasarkan undang-undang atau peraturan apa pun (termasuk Undang-Undang Perlindungan Data), termasuk namun tidak terbatas pada informasi kesehatan, nomor rekening keuangan, informasi apa pun yang jenisnya disebutkan dalam Pasal 9 GDPR, atau Informasi Pribadi sensitif serupa lainnya. Pelanggan menanggung semua risiko yang timbul dari penggunaan informasi sensitif tersebut dengan Program, termasuk risiko pengungkapan yang tidak disengaja atau akses atau penggunaan yang tidak sah.

6. Keamanan

under the General Terms and Conditions, Ecolab shall require legally compliant and industry standard data protection obligations based on the services provided and Personal Information processed by Subprocessor. A current list of Ecolab's Subprocessors engaged in Processing of Personal Information on behalf of Customer are provided in Annex II. Ecolab will provide 30 days' notice to Customer prior to engaging a new Subprocessor. If Customer does not object within 30 days to the new Subprocessor, Customer is deemed to have approved Ecolab's engagement of the same.

5. Obligations of Customer

5.1. Customer shall inform Ecolab without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the processing of Personal Information detected during the course of such processing. Customer shall have sole responsibility for the accuracy, quality, and legality of personal information processed hereunder and the means by which Customer or any relevant Affiliate of Customer collects, stores, processes and transmits such personal information.

5.2. Where required by Data Protection Law, Customer is solely responsible for fulfilling its own notification duties towards Data Subjects, regulators, or other authorities.

5.3. If Customer receives any complaint, notice, or communication from a regulatory authority which relates to Ecolab's: (i) processing of the Personal Information; or (ii) potential failure to comply with Data Protection Law, Customer shall, to the extent permitted by law, promptly forward the complaint, notice, or communication to Ecolab and, where it relates to processing of Personal Information pursuant to this DPA, provide Ecolab with reasonable cooperation and assistance for responding to such complaint, notice, or communication.

5.4 Customer represents and warrants that Customer Data will not include any information deemed to be sensitive under any law or regulation (including any Data Protection Laws), including but not limited to health information, financial account numbers, any information of the type enumerated in Article 9 of the GDPR, or other similarly sensitive Personal Information. Customer assumes all risk arising from use of any such sensitive information with Program, including the risk of inadvertent disclosure or unauthorized access or use thereto.

6. Security

6.1. Dengan mempertimbangkan standar industri, biaya implementasi, dan sifat, cakupan, konteks, dan tujuan dari pemrosesan, serta risiko dari berbagai kemungkinan dan tingkat keparahan terhadap hak-hak dan kebebasan individu, Ecolab dalam kaitannya dengan Informasi Pribadi harus menerapkan langkah-langkah teknis dan organisasi yang wajar secara komersial, seperti yang ditetapkan pada Lampiran I, yang didesain untuk memastikan tingkat keamanan yang sesuai dengan risiko tersebut. Dalam menilai tingkat keamanan yang sesuai, Ecolab harus mempertimbangkan risiko yang ditimbulkan oleh pemrosesan, khususnya dari Insiden Keamanan. Langkah-langkah teknis dan organisasi yang berlaku untuk Program tertentu tersedia berdasarkan permintaan, sesuai dengan langkah-langkah keamanan yang dijelaskan dalam Syarat dan Ketentuan Umum dan/atau Program.

6.2. Jika Ecolab mengetahui adanya Insiden Keamanan terkait Informasi Pribadi yang diproses berdasarkan PPD ini dan/atau Syarat dan Ketentuan Umum, Ecolab akan memberikan pemberitahuan kepada Pelanggan dalam waktu yang wajar. Apabila Insiden Keamanan ditemukan pada sistem yang dikendalikan Ecolab, Ecolab akan (i) menyelidiki Insiden Keamanan tersebut, (ii) memberikan informasi kepada Pelanggan tentang Insiden Keamanan (termasuk, jika memungkinkan, sifat Insiden Keamanan, Informasi Pribadi terkena dampak Insiden Keamanan, dan informasi kontak individu di Ecolab yang dapat diperoleh informasi tambahan), dan (iii) mengambil langkah-langkah yang wajar untuk mengurangi dampak, dan meminimalkan kerusakan apa pun yang diakibatkan oleh Insiden Keamanan.

6.3. Jika salah satu Pihak mengetahui adanya pengungkapan data yang tidak disengaja atau pelanggaran data mengenai data atau sistem Pihak lainnya, Pihak tersebut harus segera memberikan pemberitahuan kepada Pihak lainnya, dan Para Pihak akan secara kooperatif membuat pemberitahuan pelanggaran data dan rencana perbaikan, sesuai dengan Hukum yang Berlaku, dengan tanggung jawab atas pemberitahuan dan rencana perbaikan tersebut ditanggung sesuai dengan tanggung jawab masing-masing Para Pihak, tanggung jawab proporsional atas pengungkapan atau pelanggaran dan kewajiban masing-masing berdasarkan Hukum yang Berlaku.

6.4. Tanggung jawab Ecolab atas Insiden Keamanan atau pengungkapan data yang tidak disengaja atau pelanggaran data harus tunduk pada ketentuan Pasal 4, 12, 13, dan 14 dari Syarat dan Ketentuan Umum.

7. Perpindahan Informasi Pribadi Internasional dan Klausul Standar kontrak

7.1. Jika, sebagai bagian dari Syarat dan Ketentuan Umum, Ecolab atau Subprosesor(-Subprosesor)nya akan memproses Informasi Pribadi yang berasal dari Wilayah Ekonomi Eropa (*European Economic Area*) di negara yang terbukti tidak memberikan tingkat perlindungan yang memadai berdasarkan Hukum Perlindungan Data yang berlaku, Para Pihak setuju

6.1. Taking into account industry standards, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Ecolab shall in relation to the Personal Information implement commercially reasonable technical and organizational measures specified in Annex I designed to ensure a level of security appropriate to that risk. In assessing the appropriate level of security, Ecolab shall take account of the risks that are presented by processing, in particular from a Security Incident. The technical and organizational measure applicable to a particular Program are available upon request, pursuant to the security measures described in the General Terms and Conditions and/or the Program.

6.2. If Ecolab learns of a Security Incident related to Personal Information processed under this DPA and/or the General Terms and Conditions, it shall give notification to Customer within a reasonable time. In the event of a Security Incident discovered on Ecolab-controlled systems, Ecolab will (i) investigate the Security Incident, (ii) provide Customer with information about the Security Incident (including, where possible, the nature of the Security Incident, Personal Information impacted by the Security Incident, and contact information of an individual at Ecolab from whom additional can be obtained), and (iii) take reasonable steps to mitigate the effects of, and to minimize any damage resulting from, the Security Incident.

6.3. If either Party learns of any inadvertent data disclosure or data breach concerning the other Party's data or systems, that Party shall give prompt notification to the other Party, and the Parties shall cooperatively establish a data breach notification and remediation plan, in compliance with Applicable Laws, with the responsibility for such notification and remediation plan being borne according to the Parties' respective, proportionate responsibility for the disclosure or breach and respective obligations under Applicable Laws.

6.4. Ecolab's liability for any Security Incident or any inadvertent data disclosure or data breach shall be subject to the provisions of Sections 4, 12, 13, and 14 of the General Terms and Conditions.

7. International Transfer of Personal Information and the Standard Contractual Clauses

7.1. If, as a part of the General Terms and Conditions, Ecolab or its Subprocessor(s) will process Personal Information originating from the European Economic Area in a country that has not been found to provide an adequate level of protection under applicable Data Protection Law, the Parties agree to enter into the EU Standard Contractual

untuk menandatangani Klausul Kontrak Standar UE (*EU Standard Contractual Clauses*/"KKS UE") dan Klausul Kontrak Standar Britania Raya (*United Kingdom Standard Contractual Clauses*/"KKS Britania Raya") dan secara kolektif dengan KKS UE, "KKS") sebagaimana dijelaskan dalam bagian ini.

7.2. Untuk memfasilitasi pemindahan Informasi Pribadi ke negara ketiga dari UE, Swiss, atau negara EEA lainnya yang mengakui kecukupan KKS UE, Para Pihak setuju untuk masuk ke dalam KKS UE, sebagaimana diterapkan oleh *Commission Implementing Decision (EU) 2021/914* dan oleh karena itu, KKS UE dapat direvisi atau diganti dari waktu ke waktu. Para Pihak akan menggunakan Modul 2 KKS UE untuk transfer Pengendali ke Prosesor. Pelanggan, sebagai Pengekspor Data, dan Ecolab, sebagai Pengimpor Data, dengan ini menyetujui, sejak Tanggal Efektif, Modul 2 KKS UE, yang disertakan dalam referensi ini dan merupakan bagian integral dari PPD ini. Para Pihak dianggap telah menerima dan melaksanakan KKS UE secara keseluruhan, termasuk lampirannya. Sehubungan dengan KKS UE, Para Pihak menyetujui hal-hal berikut:

7.2.1. Pasal 7, "*Docking Clause*" tidak berlaku;

7.2.2. Pasal 9, Opsi 2 harus berlaku dan "jangka waktu" harus tiga puluh (30) hari;

7.2.3. Tidak ada Pihak yang telah melibatkan badan penyelesaian sengketa independen sebagaimana dijelaskan dalam Pasal 11, dan karena itu, ketentuan opsional tersebut tidak akan berlaku;

7.2.4. Negara Anggota UE yang berlaku untuk Opsi 1 dari Pasal 17 akan menjadi (1) Jerman atau (2) Negara Anggota UE dimana sengketa antara Para Pihak timbul, atau Negara Anggota UE di mana seorang Subjek Data mengajukan tindakan tertentu; dan

7.2.5. Negara Anggota UE yang berlaku untuk Pasal 18 akan menjadi (1) Jerman atau (2) Negara Anggota UE di mana sengketa antara Para Pihak timbul, atau Negara Anggota UE di mana seorang Subjek Data mengajukan tindakan tertentu.

7.2.6. *Lampiran I* dari KKS UE dianggap telah dilengkapi dengan bagian-bagian yang relevan dari Pasal 8 PPD ini;

7.2.7. *Lampiran II* dari KKS UE dianggap telah dilengkapi dengan bagian-bagian yang relevan dari Lampiran I dari PPD ini; dan

7.2.8. *Lampiran III* dari KKS UE dianggap telah dilengkapi dengan bagian-bagian yang relevan dari Lampiran II dari PPD ini.

7.3. Untuk memfasilitasi transfer Informasi Pribadi dari Britania Raya ke negara-negara ketiga, Para Pihak setuju untuk menandatangani Addendum Pemindahan Data Internasional ke Klausul Kontrak Standar Komisi UE (*International Data Transfer Addendum to the EU Commission Standard Contractual Clauses*), sebagaimana dikeluarkan oleh Pejabat Komisioner Informasi Britania Raya

Clauses ("EU SCCs") and the United Kingdom Standard Contractual Clauses ("UK SCCs") and collectively with the EU SCCs, the "SCCs") as described in this section.

7.2. To facilitate transfer to third countries of Personal Information from the EU, Switzerland, or other EEA countries recognizing the sufficiency of the EU SCCs, the Parties agree to enter into the EU SCCs, as implemented by Commission Implementing Decision (EU) 2021/914 and as such EU SCCs may be revised or replaced from time to time. The Parties shall utilize Module 2 of the EU SCCs for controller-to-processor transfers. Customer, as Data Exporter, and Ecolab, as Data Importer, hereby enter into, as of the Effective Date, the EU SCCs Module 2, which are incorporated by this reference and constitute an integral part of this DPA. The Parties are deemed to have accepted and executed the EU SCCs in their entirety, including the appendices. With regard to the EU SCCs, the Parties agree as follows:

7.2.1. Clause 7, "Docking Clause," shall not apply;

7.2.2. Clause 9, Option 2 shall apply and the "time period" shall be thirty (30) days;

7.2.3. Neither Party has engaged an independent dispute resolution body as described in Clause 11, and, as such, the optional provision shall not apply;

7.2.4. The EU Member State applicable for Option 1 of Clause 17 shall be (1) Germany or (2) the EU Member State in which a dispute between the Parties arises, or the EU Member State where a Data Subject brings a particular action;

7.2.5. The EU Member State applicable for Clause 18 shall be (1) Germany or (2) the EU Member State in which a dispute between the Parties arises, or the EU Member State where a Data Subject brings a particular action;

7.2.6. *Annex I* of the EU SCCs shall be deemed completed with the relevant sections of Section 8 of this DPA;

7.2.7. *Annex II* of the EU SCCs shall be deemed completed with the relevant sections of Annex I to this DPA; and

7.2.8. *Annex III* of the EU SCCs shall be deemed completed with the relevant sections of Annex II to this DPA.

7.3. To facilitate transfer of Personal Information from the UK to third countries, the Parties agree to enter into the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, as issued by the UK's Information Commissioner's Officer ("ICO") under S119A(1) Data Protection Act 2018 (herein referred to as the "UK SCCs"). Customer, as Data Exporter, and Ecolab,

(UK's Information Commissioner's Officer/"PKI") berdasarkan S119A(1) *Data Protection Act 2018* (selanjutnya disebut sebagai "KKS Britania Raya"). Pelanggan, sebagai Pengekspor Data, dan Ecolab, sebagai Pengimpor Data, dengan ini menyetujui, sejak Tanggal Efektif, KKS Britania Raya, dimasukkan dengan referensi ini dan merupakan bagian yang tidak terpisahkan dari PPD ini. Para Pihak dianggap telah menerima dan menandatangani KKS Britania Raya secara keseluruhan, termasuk lampiran-lampirannya, dengan tabel Klausul Standar UE yang relevan dianggap lengkap dengan informasi yang relevan yang terdapat di Pasal 8 di bawah ini dan Lampiran PPD ini.

7.4. Berkenaan dengan seluruh transfer Informasi Pribadi secara internasional, termasuk, namun tidak terbatas pada KKS yang dirujuk di sini:

7.4.1. Pada saat Komisi UE, PKI, Otoritas Pengawas UE, atau pengatur yang berlaku lainnya memodifikasi salah satu KKS atau menerapkan KKS baru, KKS tersebut akan berlaku sejak tanggal efektifnya. Para Pihak setuju bahwa referensi yang disediakan di sini dapat dimodifikasi untuk menyertakan KKS baru setelah pemberitahuan oleh salah satu Pihak, tanpa perlu PPD berikutnya, kecuali jika diperlukan oleh hukum;

7.4.2. Pada saat sebuah negara dengan Hukum Perlindungan Data yang berlaku menetapkan klausul kontrak standar atau dokumen serupa yang harus ditandatangani antara Para Pihak, klausul tersebut akan berlaku sejak tanggal efektifnya. Para Pihak setuju bahwa PPD ini dapat dimodifikasi untuk menyertakan klausul kontrak standar baru setelah pemberitahuan kepada salah satu Pihak, tanpa perlu Syarat dan Ketentuan Umum berikutnya, kecuali jika diperlukan oleh hukum; dan

7.4.3. Untuk Hukum Perlindungan Data yang mirip dengan GDPR yang membutuhkan syarat dan ketentuan umum untuk transfer internasional, tetapi tanpa klausul kontrak standar yang disyaratkan (misalnya, Brasil, Afrika Selatan), Para Pihak setuju bahwa PPD ini akan memberikan perlindungan yang diperlukan dan syarat dan ketentuan umum sesuai dengan Hukum Perlindungan Data tersebut.

8. Deskripsi Pengolahan

8.1. Kategori Subjek Data yang Informasi Pribadinya diolah akan mencakup yang berikut, kecuali secara khusus ditentukan dalam Program atau Ketentuan: staf (misalnya, karyawan, kontraktor) dari Pelanggan.

8.2. Kategori Informasi Pribadi yang diproses akan mencakup hal-hal sebagai berikut, kecuali secara khusus ditentukan dalam Program atau Ketentuan: informasi kontak dasar (misalnya, email bisnis, telepon, dan alamat).

as Data Importer, hereby enter into, as of the Effective Date, the UK SCCs, which are incorporated by this reference and constitute an integral part of this DPA. The Parties are deemed to have accepted and executed the UK SCCs in their entirety, including the appendices, with the relevant UK SCC tables deemed completed with the relevant information contained in Section 8 below and the Annexes to this DPA.

7.4. With regard to all international transfers of Personal Information, including, but not limited to the herein referenced SCCs:

7.4.1. At such time as the EU Commission, ICO, an EU Supervisory Authority, or other applicable regulator modifies any of the SCCs or implements new SCCs, such SCCs shall apply upon their effective date. The Parties agree that the references provided herein may be modified to include the new SCCs upon notice by either Party, without the need for subsequent DPA, unless otherwise required by law;

7.4.2. At such time as a country with applicable Data Protection Law established standard contractual clauses or similar documents that must be executed between the Parties, such clauses shall apply on their effective date. The Parties agree that this DPA may be modified to include the new standard contractual clauses upon notice to either Party, without the need for subsequent General Terms and Conditions, unless otherwise required by law; and

7.4.3. For Data Protection Law similar to GDPR requiring general terms and conditions for international transfer, but without required standard contractual clauses (e.g. Brazil, South Africa), the Parties agree that this DPA shall provide the required protection and general terms and conditions under said Data Protection Law.

8. Description of Processing

8.1. The categories of Data Subjects whose Personal Information is processed shall include the following, unless specifically defined in the Program or Terms: staff (e.g. employees, contractors) of Customer.

8.2. The categories of Personal Information processed shall include the following, unless specifically defined in the Program or Terms: basic contact information (e.g. business email, phone, and address).

8.3. Tidak ada Informasi Pribadi yang diklasifikasikan sebagai “sensitif” atau “spesial” berdasarkan Hukum Perlindungan Data akan diproses kecuali secara khusus ditentukan dalam Program atau Ketentuan.

8.4. Informasi Pribadi akan diproses dan ditransfer secara terus-menerus selama Jangka Waktu Program dan Ketentuan.

8.5. Sifat pemrosesan Informasi Pribadi akan ditentukan dalam Program dan Ketentuan.

8.6. Tujuan(-tujuan) dari pemrosesan dan transfer Informasi Pribadi adalah untuk menyediakan layanan sebagaimana yang dijabarkan dalam Syarat dan Ketentuan Umum serta Program.

8.7. Periode dimana Informasi Pribadi akan disimpan akan menjadi Jangka Waktu Program atau untuk periode yang lebih pendek, sebagaimana diinstruksikan oleh Pelanggan.

8.8. Untuk transfer ke Subprosesor, pokok bahasan dan durasi dari pemrosesan seperti yang diuraikan di atas dalam Pasal 8 ini. Sifat layanan subpemrosesan yang spesifik dijelaskan lebih lanjut dalam Daftar Subprosesor yang disediakan oleh Ecolab.

9. Jangka Waktu dan Pengakhiran

9.1. PPD ini akan memiliki jangka waktu yang sama dengan Syarat dan Ketentuan Umum.

9.2. Tanpa mengurangi hak pengakhiran lain apapun yang mungkin dimiliki oleh Para Pihak berdasarkan PPD ini dan/atau hukum yang berlaku, setiap Pihak dapat mengakhiri partisipasinya dalam PPD ini jika menemukan bahwa Pihak lain tidak mematuhi ketentuan PPD ini, dengan syarat bahwa Pihak yang ditemukan tidak mematuhi akan diberikan kesempatan untuk menyembuhkan sesuai dengan Syarat dan Ketentuan Umum.

9.3. Setelah pengakhiran, setiap Pihak akan berhak untuk menyimpan Informasi Pribadi hanya sejauh yang diperlukan untuk memenuhi tujuan atau persyaratan berkelanjutan dari Syarat dan Ketentuan Umum. Setiap Informasi Pribadi yang tidak lagi diperlukan untuk memenuhi tujuan atau persyaratan berkelanjutan yang ditentukan dalam Syarat dan Ketentuan Umum dapat dihapus oleh Ecolab dalam waktu 90 hari setelah Pengakhiran, dengan pengecualian yang sesuai untuk penghapusan di mana salinan cadangan dari Informasi Pribadi secara logis dihapus dalam jadwal yang lebih lama, atau jika retensi untuk jadwal yang lebih lama disyaratkan atau diizinkan oleh Hukum yang Berlaku.

10. Lain-Lain

10.1. PPD ini hanya menguntungkan Para Pihak dan pihak ketiga tidak akan memiliki hak di bawah ini, kecuali dinyatakan lain dalam PPD ini.

10.2. Penentuan bahwa ketentuan apa pun dalam PPD ini tidak sah atau tidak dapat dilaksanakan tidak akan mempengaruhi ketentuan lain dalam PPD. Dalam hal tersebut, ketentuan yang

8.3. No Personal Information classified as “sensitive” or “special” under Data Protection Law shall be processed unless specifically defined in a Program or Terms.

8.4. Personal Information shall be processed and transferred on a continuous basis for the Term of the Program and Terms.

8.5. The nature of the Personal Information processing shall be defined in the Program and Terms.

8.6. The purpose(s) of the Personal Information processing and transfer shall be to provide services as described in the General Terms and Conditions and Program.

8.7. The period for which the Personal Information will be retained shall be the Term of the Program or for a shorter period as instructed by Customer.

8.8. For transfers to Subprocessors, the subject matter and duration of the processing is as outlined above within this Section 8. The nature of the specific subprocessing services is as further described in the Subprocessor List provided by Ecolab.

9. Term and termination

9.1. This DPA shall have the same term as the General Terms and Conditions.

9.2. Without prejudice to any other termination rights that a Party may have under this DPA and/or applicable law, each Party may terminate its participation in this DPA if it finds the other Party is not in compliance with the terms of this DPA, provided that the Party found not in compliance shall have opportunity to cure consistent with the General Terms and Conditions.

9.3. Upon termination, each Party shall be entitled to keep Personal Information only as may be necessary to fulfill any ongoing purposes or requirements of the General Terms and Conditions. Any Personal Information no longer needed to fulfill ongoing purposes or requirements defined in the General Terms and Conditions may be deleted by Ecolab within 90 days of Termination, with appropriate exception for deletion where backup copies of Personal Information are logically deleted on a longer schedule, or if retention for a longer schedule is required or permitted by Applicable Laws.

10. Miscellaneous

10.1. This DPA inures to the benefit of the Parties only and no third party shall have any rights hereunder, except as otherwise stated herein.

10.2. A determination that any provision of the DPA is invalid or unenforceable shall not affect the other provisions of the DPA. In such case the invalid or unenforceable

tidak sah atau tidak dapat dilaksanakan akan secara otomatis diganti dengan ketentuan yang sah dan dapat dilaksanakan yang paling mendekati tujuan ketentuan aslinya. Hal yang sama akan berlaku jika PPD mengandung celah yang tidak disengaja.

10.3. Sejauh ada konflik antara Perjanjian, PPD ini, dan/atau KKS, berbagai perjanjian akan berlaku dalam urutan sebagai berikut: (i) KKS, (ii) PPD ini, (iii) Syarat dan Ketentuan Umum.

10.4 PPD ini ditandatangani dalam bahasa Inggris dan bahasa Indonesia. Sejauh yang diizinkan oleh hukum, jika terjadi pertentangan antara ketentuan dalam versi bahasa Inggris dan terjemahan apapun ke dalam bahasa lain apapun, maka ketentuan dalam versi bahasa Inggris akan berlaku. Terjemahan PPD ini ke dalam bahasa lain apapun selain bahasa Inggris hanya untuk tujuan informasi. Para Pihak sepakat bahwa PPD ini dan seluruh dokumen yang berkaitan dengan PPD ini ditulis dalam bahasa Inggris dan tidak ada terjemahan dari dokumen tersebut yang mengikat salah satu Pihak.

provision shall automatically be replaced by a valid and enforceable provision that comes closest to the purpose of the original provision. The same shall apply if the DPA contains an unintended gap.

10.3 To the extent there is any conflict between the Agreement, this DPA, and/or the SCCs, the various agreements will control in the following order of preference: (i) the SCCs, (ii) this DPA, (iii) the General Terms and Conditions.

10.4 This DPA is executed in the English language and the Indonesian language. To the maximum extent permitted by law, in the event a conflict arises between the terms of the English version and any translation into any other language, the terms of the English version shall prevail. Translations of this DPA into any language other than English are for informational purposes only. The Parties agree that this DPA and all documents relating to this DPA are written in the English language and no translation of any such document shall be binding on either Party.

LAMPIRAN 1 – LANGKAH-LANGKAH TEKNIS DAN ORGANISASI /
ANNEX I - TECHNICAL AND ORGANIZATIONAL MEASURES

Penjelasan tentang langkah-langkah teknis dan organisasi yang diterapkan oleh Ecolab untuk memastikan tingkat keamanan yang sesuai, dengan mempertimbangkan sifat, ruang lingkup, konteks, dan tujuan pemrosesan, serta risiko-risiko terhadap hak-hak dan kebebasan individu: /

Description of the technical and organizational measures implemented by Ecolab 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:

**(A) Kontrol akses
fisik ke lokasi /
Control of
physical access
to premises**

Langkah-langkah teknis dan organisasi untuk mengontrol akses fisik ke tempat dan fasilitas, terutama untuk mengidentifikasi personel yang diizinkan masuk: /
Technical and organizational measures to control physical access to premises and facilities, particularly to identify permitted personnel at entry:

- ☒ Pintu terkunci di semua pintu masuk/keluar / *Locked doors on all entrances / exits*
- ☒ Kehadiran petugas keamanan / *Presence of security personnel*
- ☒ Sistem kontrol akses / *Access control systems*
- ☒ Sistem CCTV / *CCTV systems*
- ☒ Sistem alarm pencuri / *Burglar alarm systems*

**(B) Pengendalian akses ke sistem TI /
Control of access to IT systems**

Langkah-langkah teknis dan organisasi keamanan yang dirancang untuk memastikan bahwa pengguna yang memiliki akses ke sistem TI yang relevan diidentifikasi dan diautentikasi: /

Technical and organizational security measures designed to ensure that users with access to the relevant IT systems are identified and authenticated:

- ☒ Sistem keamanan TI yang mengharuskan pengguna individu untuk masuk menggunakan nama pengguna yang unik / *IT security systems requiring individual users to log in using unique user names*
- ☒ Sistem keamanan TI yang membutuhkan penggunaan kata sandi yang kuat/kompleks / *IT security systems requiring the use of strong / complex passwords*
- ☒ Sistem keamanan TI yang mensyaratkan penggunaan autentikasi multi-faktor / *IT security systems requiring the use of multi-factor authentication*
- ☒ Persyaratan masuk sistem tambahan untuk aplikasi tertentu / *Additional system log-in requirements for particular applications*
- ☒ Perubahan kata sandi wajib dengan interval tetap / *Mandatory password changes at fixed intervals*
- ☒ Enkripsi diterapkan pada data pribadi yang 'sedang transit' / *Encryption applied to personal data 'in transit'*
- ☒ Enkripsi diterapkan pada data pribadi 'saat tidak aktif' / *Encryption applied to personal data 'at rest'*
- ☒ Penguncian otomatis terminal dan perangkat TI setelah periode tidak digunakan, dengan kata sandi yang diperlukan untuk 'membangunkan' terminal atau perangkat / *Automatic locking of IT terminals and devices after periods of non-use, with passwords required to 'wake' the terminal or device*
- ☒ Basis data kata sandi tunduk pada enkripsi / hashing yang kuat / *Password databases are subject to strong encryption / hashing*
- ☒ Audit rutin terhadap prosedur keamanan / *Regular audits of security procedures*
- ☒ Pelatihan untuk karyawan mengenai akses ke sistem TI / *Training for employees regarding access to IT systems*

**(C) Kontrol akses ke data pribadi /
Control of access to personal data**

Langkah-langkah teknis dan organisasi keamanan yang dirancang untuk memastikan bahwa pengguna yang memiliki akses ke data pribadi yang relevan diidentifikasi dan diautentikasi: /

Technical and organizational security measures designed to ensure that users with access to the relevant personal data are identified and authenticated:

- ☒ Hak 'Baca' untuk sistem yang berisi data pribadi yang dibatasi untuk peran personel tertentu / *'Read' rights for systems containing personal data restricted to specified personnel roles*
- ☒ Hak 'Edit' untuk sistem yang berisi data pribadi yang dibatasi untuk peran atau profil personel tertentu / *Edit' rights for systems containing personal data restricted to specified personnel roles or profiles*
- ☒ Pencatatan upaya untuk mengakses sistem yang berisi data pribadi / *Logging of attempts to access systems containing personal data*
- ☒ Enkripsi pada drive dan media yang berisi data pribadi / *Encryption on drives and media containing personal data*
- ☒ Pelatihan untuk karyawan mengenai akses ke data pribadi / *Training for employees regarding access to personal data*

**(D) Pengendalian
Pengungkapan
Data Pribadi /
Control of
disclosure of
personal data**

Langkah-langkah teknis dan organisasi untuk mentransfer, mengirim, dan mengomunikasikan atau menyimpan data dengan aman pada media data dan untuk pengecekan selanjutnya: /

Technical and organizational measures to securely transfer, transmit and communicate or store data on data media and for subsequent checking:

- ☒ Pembatasan hak transfer untuk sistem yang berisi data pribadi / *Restrictions on transfer rights for systems containing personal data*
- ☒ Mengamankan jaringan data / *Secure data networks*
- ☒ Enkripsi untuk sistem yang digunakan untuk mengirim data pribadi / *Encryption for systems used to send personal data*
- ☒ Enkripsi SSL untuk semua portal akses internet / *SSL encryption for all internet access portals*
- ☒ Perlindungan media penyimpanan data dan wadah selama pengangkutan fisik / *Protection of data storage media and containers during physical transport*
- ☒ Pelatihan untuk karyawan mengenai transfer data pribadi / *Training for employees regarding transfers of personal data*

**(E) Kontrol
Mekanisme
Masukan /
Control of input
mechanisms**

Langkah-langkah teknis dan organisasi keamanan untuk mengizinkan pencatatan dan analisis informasi di kemudian hari mengenai kapan input ke sistem data (misalnya, pengeditan, penambahan, penghapusan, dll.) terjadi dan siapa yang bertanggung jawab atas input tersebut: /

Technical and organizational security measures to permit the recording and later analysis of information about when input to data systems (e.g., editing, adding, deleting, etc.) occurred and who was responsible for such input:

- ☒ Pencatatan semua tindakan input dalam sistem yang berisi data pribadi / *Logging of all input actions in systems containing personal data*
- ☒ Hak 'Edit' untuk sistem yang berisi data pribadi yang dibatasi untuk peran atau profil personel tertentu / *'Edit' rights for systems containing personal data restricted to specified personnel roles or profiles*
- ☒ Perjanjian yang mengikat secara tertulis atau kewajiban kerahasiaan lainnya dengan karyawan yang memproses data pribadi / *Binding agreements in writing or other obligations of confidentiality with employees who process personal data*
- ☒ Peninjauan rutin atas kepatuhan terhadap perjanjian yang relevan / *Regular reviews of compliance with the relevant agreements*
- ☒ Pelatihan untuk karyawan mengenai pengeditan data pribadi / *Training for employees regarding editing of personal data*

(F) Kontrol Alur Kerja antara pengendali dan prosesor / Control of workflows between controllers and processors

Langkah-langkah teknis dan organisasi untuk memisahkan tanggung jawab antara pengendali dan prosesor yang memproses data pribadi yang relevan: / *Technical and organizational measures to segregate the responsibilities between controllers and processors processing the relevant personal data:*

- ☒ Perjanjian yang mengikat secara tertulis yang mengatur penunjukan dan tanggung jawab prosesor yang memiliki akses ke data pribadi yang relevan / *Binding agreements in writing governing the appointment and responsibilities of processors with access to the relevant personal data*
- ☒ Perjanjian yang mengikat secara tertulis yang mengatur alokasi tanggung jawab kepatuhan perlindungan data antara semua pengendali yang memiliki akses ke data pribadi yang relevan / *Binding agreements in writing governing the allocation of data protection compliance responsibilities between all controllers with access to the relevant personal data*
- ☒ Peninjauan rutin atas kepatuhan terhadap perjanjian yang relevan / *Regular reviews of compliance with the relevant agreements*
- ☒ Pelatihan untuk karyawan mengenai pemrosesan data pribadi / *Training for employees regarding processing of personal data*

(G) Mekanisme kontrol untuk memastikan ketersediaan data pribadi yang relevan / Control mechanisms to ensure availability of the relevant personal data

Langkah-langkah teknis dan organisasi untuk memastikan ketersediaan dan aksesibilitas fisik dan elektronik dari data pribadi yang relevan: / *Technical and organizational measures to ensure the physical and electronic availability and accessibility of the relevant personal data:*

- ☒ Prosedur pemulihan bencana yang terdokumentasi / *Documented disaster recovery procedures*
- ☒ Prosedur pencadangan yang aman, dengan pencadangan penuh yang dijalankan secara teratur / *Secure backup procedures in place, with full backups run regularly*
- ☒ Fasilitas dan lokasi pencadangan / *Backup facilities and locations*
- ☒ Catu daya tak terputus di fasilitas pencadangan / *Uninterruptible power supplies at backup facilities*
- ☒ Keamanan fisik fasilitas pencadangan / *Physical security of backup facilities*
- ☒ Sistem alarm keamanan di fasilitas pencadangan / *Security alarm systems at backup facilities*
- ☒ Keamanan elektronik dari fasilitas pencadangan / *Electronic security of backup facilities*
- ☒ Kontrol lingkungan di fasilitas pencadangan / *Environmental controls at backup facilities*
- ☒ Proteksi kebakaran di fasilitas pencadangan / *Fire protection at backup facilities*
- ☒ Deidentifikasi atau penghapusan data pribadi yang tidak lagi diperlukan untuk tujuan pemrosesan yang sah / *Deidentification or deletion of personal data that are no longer required for lawful processing purposes*
- ☒ Pelatihan untuk karyawan mengenai pencadangan dan pemulihan bencana / *Training for employees regarding backups and disaster recovery*

(H) Mekanisme control untuk memastikan pemisahan data pribadi yang relevan dari data lainnya / Control mechanisms to ensure separation of the relevant personal data from other data

Langkah-langkah teknis dan organisasi untuk memastikan bahwa data pribadi yang relevan disimpan dan diproses secara terpisah dari data lainnya: / *Technical and organizational measures to ensure that the relevant personal data are stored and processed separately from other data:*

- ☒ Pemisahan logis data live atau produksi dari data cadangan dan data pengembangan atau pengujian / *Logical separation of live or production data from backup data and development or test data*
- ☒ Pemisahan personel yang memproses data pribadi yang relevan dari personel lain / *Separation of personnel processing the relevant personal data from other personnel*
- ☒ Pelatihan untuk karyawan mengenai pemisahan data / *Training for employees regarding data separation*

LAMPIRAN II – DAFTAR SUBPROSESOR /
ANNEX II – LIST OF SUBPROCESSORS

Pengendali telah mengotorisasi penggunaan Subprosesor yang terdapat pada Daftar Subprosesor yang tersedia di bawah ini: /
The controller has authorized the use of the Subprocessors found in its Subprocessor List available below:

Subprosesor / Subprocessor	Alamat Subprosesor / Subprocessor Address
Microsoft	1 Microsoft Way, Redmond, WA 98052
Cisco AppDynamics	500 Terry A Francois Blvd, 3 rd fl San Francisco, CA 94158
Sales Force	415 Mission Street, 3 rd Floor, San Francisco, CA
LinkedIn Sales Navigator	1000 W. Maude Ave, Sunnyvale, CA 94085
Microsoft Dynamics CRM	1 Microsoft Way, Redmond, WA 98052
Soprano Design Pty	Level 15, 132 Arthur St North Sydney NSW 2060 Australia
ServiceNow	2225 Lawson Lane, Santa Clara, CA 95054 Hoekenroder 3, Amsterdam Zuidoost, North Holland 1102 BR 80 Robinson Road, #02-00, Singapore 068898
FiveTran	1221 Broadway Street, Floor 20, San Francisco, CA