DATA PROCESSING AGREEMENT / PERJANJIAN PEMROSESAN DATA

This Data Processing Agreement ("DPA") reflects the parties' agreement with respect to the terms governing the Processing of Personal Data on behalf of the Customer under any applicable written agreement between Customer and Dynatrace governing the use of the Dynatrace Offerings (paid or otherwise), and any related order forms, attachments, and statements of work (collectively, the "Agreement"). To the extent the parties have not executed a separate Data Processing Agreement, this DPA will become effective as of the date the Dynatrace Offerings start as listed in the applicable Order Form.

Perjanjian Pemrosesan Data ("PPD") ini mencerminkan persetujuan para pihak sehubungan dengan ketentuan yang mengatur Pemrosesan Data Pribadi atas nama Pelanggan berdasarkan perjanjian tertulis ~~apa pun~~ yang berlaku antara Pelanggan dan Dynatrace yang mengatur penggunaan Penawaran Dynatrace (berbayar atau tidak), dan formulir pesanan, lampiran, dan deskripsi pekerjaan terkait (secara bersama disebut sebagai "Perjanjian"). Sejauh para pihak belum menandatangani Perjanjian Pemrosesan Data terpisah, PPD ini akan berlaku sejak tanggal Penawaran Dynatrace dimulai sebagaimana tercantum dalam Formulir Pesanan yang berlaku.PPD ini berlaku pada tanggal ditandatangani oleh kedua pihak.

This DPA is subject to the terms of, and fully incorporated and made part of, the Agreement. This DPA shall replace any existing data processing agreement unless otherwise explicitly stated herein. In the event of any conflict between this DPA and any other provision of the Agreement with respect to personal data, this DPA shall govern and apply. Capitalized terms used but not defined in this DPA have the same meanings as set out in the Subscription Agreement available at https://assets.dynatrace.com/global/legal/Online-SA-April-2024-Indonesian.pdf.

PPD ini diatur oleh ketentuan dan sepenuhnya dimasukkan serta menjadi bagian dari Perjanjian. PPD ini akan menggantikan perjanjian pemrosesan data yang sudah ada kecuali dinyatakan secara jelas di sini. Jika terjadi pertentangan antara PPD ini dan ketentuan lain dalam Perjanjian sehubungan dengan data pribadi, PPD ini yang akan mengatur dan berlaku. Istilah dalam huruf besar yang digunakan tetapi tidak didefinisikan dalam PPD ini memiliki arti yang sama seperti yang dijelaskan dalam Perjanjian Berlangganan yang tersedia di https://assets.dynatrace.com/global/legal/Online-SA-April-2024-Indonesian.pdf.

1. Definitions. / Definisi.

(a) "APPI" means the Japanese Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in 2016).

"APPI" berarti Undang-Undang Jepang tentang Perlindungan Informasi Pribadi (Undang-Undang No. 57 tahun 2003 sebagaimana yang diubah pada tahun 2016).

(b) "Data Protection Law" means all data protection and data privacy laws and regulations applicable to Dynatrace's Processing of Customer Personal Data under the Agreement.

"Undang-Undang Perlindungan Data" berarti semua undang-undang dan peraturan perlindungan data dan privasi data yang berlaku untuk Pemrosesan Data Pribadi Pelanggan oleh Dynatrace berdasarkan Perjanjian.

(c) "Controller" has the same meaning given under the applicable Data Protection Law and includes "Database Owner" under the Protection of Privacy Law of Israel and "Business" under the applicable US State Privacy Law.

"Pengendali" memiliki arti yang sama dengan yang diberikan berdasarkan Undang-Undang Perlindungan Data yang berlaku dan mencakup "Pemilik Basis Data" menurut Undang-Undang Perlindungan Privasi Israel dan "Bisnis" menurut Undang-Undang Privasi Negara Bagian AS yang berlaku.

(d) "Customer Personal Data" means any Personal Data submitted, stored, posted, displayed, or otherwise transmitted by or on behalf of Customer in the course of using the Dynatrace Offerings; and excludes Personal Data (such as Restricted Information) submitted, stored, posted, displayed, or otherwise transmitted by or on behalf of Customer in violation of any provision of the Agreement and/or this DPA.

"Data Pribadi Pelanggan" berarti setiap Data Pribadi yang dikirimkan, disimpan, diposting, ditampilkan, atau ditransmisikan oleh atau atas nama Pelanggan dalam proses penggunaan Penawaran Dynatrace; dan tidak termasuk

Data Pribadi (seperti Informasi Terbatas) yang dikirimkan, disimpan, diposting, ditampilkan, atau ditransmisikan oleh atau atas nama Pelanggan yang melanggar ketentuan apa pun dalam Perjanjian dan/atau PPD ini.

(e) "Dynatrace Group" means one or more of Dynatrace LLC, a Delaware limited liability company, and its Affiliates that may assist Dynatrace to provide the Dynatrace Offerings, and/or related support or services, under the Agreement and this DPA.

"Grup Dynatrace" berarti satu atau lebih dari Dynatrace LLC, perseroan terbatas di Delaware, dan Afiliasinya yang dapat membantu Dynatrace untuk menyediakan Penawaran Dynatrace, dan/atau dukungan atau layanan terkait, berdasarkan Perjanjian dan PPD ini.

(f) "Europe" means the European Union, European Economic Area ("EEA"), and/or their member states, Switzerland, and the United Kingdom.

"Eropa" berarti Uni Eropa, Wilayah Ekonomi Eropa ("EEA"), dan/atau negara anggotanya, Swiss, dan Inggris.

(g) "GDPR" means the 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).

"GDPR" berarti Peraturan 2016/679 Parlemen Eropa dan Dewan Eropa tentang perlindungan orang perorangan terkait pemrosesan data pribadi dan pergerakan bebas data tersebut (Peraturan Perlindungan Data Umum).

(h) "LGPD" means the Lei Geral de Proteção de Dados Pessoais (General Personal Data Protection Act in Brazil).

"LGPD" berarti Lei Geral de Proteção de Dados Pessoais (Undang-Undang Perlindungan Data Pribadi Umum di Brasil).

(i) "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, Customer Personal Data while being transmitted, stored, or otherwise Processed by Dynatrace.

"Pelanggaran Data Pribadi" berarti pelanggaran keamanan yang menyebabkan pemusnahan, kehilangan, perubahan, atau pengungkapan yang tidak disengaja atau melanggar hukum, atau pengungkapan tanpa izin atas, atau akses ke, Data Pribadi Pelanggan ketika sedang dikirim, disimpan, atau diproses oleh Dynatrace.

(j) "PIPL" means the China Personal Information Protection Law.

"PIPL" berarti Undang-Undang Perlindungan Informasi Pribadi Tiongkok.

(k) "Personal Data" means "Personal Data," or "Personal Information" as defined under applicable Data Protection Laws that Dynatrace collects or receives on behalf of Customer. Personal Data does not include information that Dynatrace obtains or Processes independent of the performance of its respective obligations under the Agreement with Customer.

"Data Pribadi" berarti "Data Pribadi," atau "Informasi Pribadi" sebagaimana yang didefinisikan dalam Undang-Undang Perlindungan Data yang berlaku yang dikumpulkan atau diterima oleh Dynatrace atas nama Pelanggan. Data Pribadi tidak termasuk informasi yang diperoleh atau diproses Dynatrace secara independen dari pelaksanaan kewajibannya berdasarkan Perjanjian dengan Pelanggan.

(l) "Processor" has the same meaning given under the applicable Data Protection Law and includes "Holder" as defined under the Protection of Privacy Law of Israel, and "Service Provider" under the applicable US State Privacy Law.

“Pemroses” memiliki arti yang sama dengan yang diberikan dalam Hukum Perlindungan Data yang berlaku dan mencakup "Pemegang" sebagaimana yang didefinisikan dalam Hukum Perlindungan Privasi Israel, dan "Penyedia Layanan" berdasarkan Hukum Privasi Negara Bagian AS yang berlaku.

(m) “Standard Contractual Clauses” means the Standard Contractual Clauses promulgated by the EU Commission Decision 2021/914/EU incorporated herein by reference as updated amended or replaced from time to time.

“Klausul Kontrak Standar” berarti Klausul Kontrak Standar yang diberlakukan dengan Keputusan Komisi Uni Eropa 2021/914/EU yang dimasukkan dalam Perjanjian ini dengan penyebutan sebagaimana yang diperbarui, diubah, atau diganti sewaktu-waktu.

(n) “Sub-processor” means Processors engaged by Dynatrace or members of the Dynatrace Group to enable Dynatrace to deliver/provide the Dynatrace Offerings under the terms of the Agreement or this DPA.

“Sub-pemroses” berarti Pemroses yang dilibatkan oleh Dynatrace atau anggota Grup Dynatrace untuk memungkinkan Dynatrace mengirimkan/menyediakan Penawaran Dynatrace berdasarkan ketentuan dalam Perjanjian atau PPD ini.

(o) “Supervisory Authority” means the government agency, department, or other competent organization with authority over the processing of Personal Data relevant to this DPA.

“Lembaga Pengawas” berarti lembaga pemerintah, departemen, atau organisasi berwenang lainnya yang memiliki wewenang atas pemrosesan Data Pribadi yang relevan dengan PPD ini.

(p) “UK Addendum” means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner’s office under S119A (1) Data Protection Act 2018, as updated, amended or replaced from time to time.

“Adendum Inggris” berarti Adendum Pemindahan Data Internasional pada Klausul Kontrak Standar Komisi Uni Eropa yang dikeluarkan oleh kantor Komisioner Informasi Inggris berdasarkan S119A (1) Undang-Undang Perlindungan Data 2018, sebagaimana yang diperbarui, diubah, atau diganti sewaktu-waktu.

(q) “Business”, "Controller", “Consumer,” "Processor," “Service Provider,” "Data Subject", “Sell,” “Supervisory Authority”, and "Processing" (and "process") shall have the meanings given under under applicable Data Protection Law.

“Bisnis”, "Pengendali", “Konsumen,” "Pemroses," “Penyedia Jasa,” "Subjek Data", “Menjual,” “Lembaga Pengawas”, dan "Pemrosesan" (dan "memproses") memiliki arti yang diberikan dalam Undang-Undang Perlindungan Data yang berlaku.

2. Applicability of DPA and Parties’ Roles / Penerapan PPD dan Peran Para Pihak

(a) This DPA applies to Processing of Customer Personal Data by Dynatrace on behalf of the Customer to perform its obligations and exercise its rights under the Agreement and this DPA. For the avoidance of doubt this DPA does not apply to Processing of Customer Personal Data by Dynatrace as a Controller.

PPD ini berlaku untuk Pemrosesan Data Pribadi Pelanggan oleh Dynatrace atas nama Pelanggan untuk melaksanakan kewajibannya dan menggunakan hak-haknya berdasarkan Perjanjian dan PPD ini. Untuk menghindari keraguan, PPD ini tidak berlaku untuk Pemrosesan Data Pribadi Pelanggan oleh Dynatrace sebagai Pengendali.

(b) Customer is a Controller or a Processor and Dynatrace is a Processor. To the extent applicable under Data Protection Law, Customer appoints Dynatrace as a Processor to process the Customer Personal Data on Customer's behalf.

Pelanggan adalah Pengendali atau Pemroses dan Dynatrace adalah Pemroses. Sejauh yang berlaku berdasarkan Undang-Undang Perlindungan Data, Pelanggan menunjuk Dynatrace sebagai Pemroses untuk memproses Data Pribadi Pelanggan atas nama Pelanggan.

3. Processing of Customer Personal Data / Pemrosesan Data Pribadi Pelanggan

(a) The nature and extent of Processing Customer Personal Data by Dynatrace to deliver the Dynatrace Offerings is determined and controlled by Customer and is supplemented by Schedule A. The nature, purpose and duration of the Processing, as well as the types of Personal Data collected and categories of Data Subjects whose Personal Data may be Processed by Dynatrace, are described in Schedule A to this DPA. Customer acknowledges that Dynatrace does not have any knowledge of the actual data or types of Personal Data contained in the Customer Data. The parties agree that the Customer's complete and final instructions about the nature and purposes of the Processing in connection with the Dynatrace Offerings are set out in the Agreement and this DPA.

Sifat dan tingkat Pemrosesan Data Pribadi Pelanggan oleh Dynatrace untuk memberikan Penawaran Dynatrace ditentukan dan dikendalikan oleh Pelanggan serta dilengkapi dengan Lampiran A. Sifat, tujuan, dan lama Pemrosesan, serta jenis Data Pribadi yang dikumpulkan dan kategori Subjek Data yang Data Pribadinya dapat Diproses oleh Dynatrace, dijelaskan pada Lampiran A dalam PPD ini. Pelanggan mengakui bahwa Dynatrace tidak memiliki pengetahuan tentang data aktual atau jenis Data Pribadi yang terdapat dalam Data Pelanggan. Para pihak setuju bahwa petunjuk lengkap dan final Pelanggan tentang sifat dan tujuan Pemrosesan sehubungan dengan Penawaran Dynatrace diatur dalam Perjanjian dan PPD ini.

(b) Any changes or modifications to the instructions shall be communicated in writing and acknowledged by both parties. Dynatrace shall inform Customer if, in its reasonable opinion, Customer's processing instructions are likely to infringe any applicable Data Protection Law; in such event, Dynatrace is entitled to refuse Processing of Customer Personal Data that it believes to be in violation of any applicable Data Protection Law until Customer amends its instruction so as not to be infringing.

Setiap perubahan atau modifikasi pada petunjuk tersebut harus disampaikan secara tertulis dan diketahui oleh kedua belah pihak. Dynatrace akan memberi tahu Pelanggan jika, menurut pendapatnya yang wajar, petunjuk pemrosesan Pelanggan mungkin akan melanggar Undang-Undang Perlindungan Data yang berlaku; dalam hal ini, Dynatrace berhak untuk menolak Pemrosesan Data Pribadi Pelanggan yang diyakini melanggar Undang-Undang Perlindungan Data yang berlaku sampai Pelanggan mengubah petunjuknya sehingga tidak melanggar.

(c) To the extent Customer's configuration of Dynatrace Offerings results in Dynatrace capturing Customer Personal Data, Customer represents and warrants that, it will, at all times, comply with all applicable Data Protection Law. As between Customer and Dynatrace, Customer is responsible for: (i) protecting Customer Personal Data while using Dynatrace by configuring Dynatrace Data Privacy Settings as described at ttps://docs.dynatrace.com/docs/manage/data-privacy-and-security (Dynatrace instructions on how to configure data privacy settings) to granularly control the scope of Customer Personal Data to be captured by the Dynatrace Offerings; (ii) the accuracy, quality and legality of Customer Personal Data,

and the means by which Customer or any relevant third-party acquired Personal Data.

Sejauh konfigurasi Pelanggan atas Penawaran Dynatrace mengakibatkan Dynatrace mengambil Data Pribadi Pelanggan, Pelanggan menyatakan dan menjamin bahwa, Pelanggan akan selalu mematuhi semua Undang-Undang Perlindungan Data yang berlaku. Sebagaimana antara Pelanggan dan Dynatrace, Pelanggan bertanggung jawab untuk: (i) melindungi Data Pribadi Pelanggan saat menggunakan Dynatrace dengan mengkonfigurasi Pengaturan Privasi Data Dynatrace seperti yang dijelaskan di https://docs.dynatrace.com/docs/manage/data-privacy-and-security (petunjuk Dynatrace tentang cara mengkonfigurasi pengaturan privasi data) untuk mengendalikan secara terperinci cakupan Data Pribadi Pelanggan yang akan diambil oleh Penawaran Dynatrace; (ii) keakuratan, kualitas, dan keabsahan Data Pribadi Pelanggan, dan cara Pelanggan atau pihak ketiga memperoleh Data Pribadi yang relevan.

(d) If Customer is a processor acting on behalf of a third-party Controller, Customer warrants to Dynatrace that Customer's instructions and actions with respect to that Customer Personal Data, including its appointment of Dynatrace as another Processor, have been authorized by the relevant Controller.

Jika Pelanggan menjadi pemroses yang bertindak atas nama Pengendali pihak ketiga, Pelanggan menjamin kepada Dynatrace bahwa petunjuk dan tindakan Pelanggan sehubungan dengan Data Pribadi Pelanggan tersebut, termasuk penunjukan Dynatrace sebagai Pemroses lain, telah diberi izin oleh Pengendali yang relevan.

(e) Customer represents and warrants that: (i) it will inform its Data Subjects as legally required about its use of Processors to Process their Customer Personal Data, including Dynatrace, including where required providing notice to Data Subjects about the use of the Dynatrace Offerings; (ii) it has obtained, and continues to have, during the term, all necessary rights, lawful basis, authorizations, and/or valid consents, including from Data Subjects, for the Processing of Customer Personal Data by Dynatrace as contemplated by the Agreement; (iii) Customer's use of the Dynatrace Offerings will not, and will not cause Dynatrace to, violate any Data Protection Laws or other applicable laws or regulations, or any agreement or obligation between Customer and any third party.

Pelanggan menyatakan dan menjamin: (i) akan memberi tahu Subjek Data sebagaimana diwajibkan secara hukum tentang penggunaan Pemroses untuk Memproses Data Pribadi Pelanggan mereka, termasuk Dynatrace, termasuk jika diperlukan, memberikan pemberitahuan kepada Subjek Data tentang penggunaan Penawaran Dynatrace; (ii) telah memperoleh, dan terus memiliki, selama masa berlaku, semua hak yang diperlukan, dasar hukum, otorisasi, dan/atau persetujuan yang sah dari Subjek Data termasuk dari Subjek Data, untuk Pemrosesan Data Pribadi Pelanggan oleh Dynatrace sebagaimana dimaksud dalam Perjanjian; (iii) Penggunaan Penawaran Dynatrace yang dilakakan oleh Plenggan tidak akan, dan tidak bisa membuat Dynatrace melanggar Undang-Undang Perlindungan Data atau peraturan dan hukum hukam lain yang berlaku, atau persetujuan dan kewajiban antara Pelanggan dengan pihak ketiga.

(f) Customer will provide Dynatrace only with the Customer Personal Data necessary for Dynatrace to perform its obligations under the Agreement with respect to the Dynatrace Offerings and any related services. Customer acknowledges that the use of the Dynatrace Offerings does not require and is not suitable for the Processing of any Restricted Information and will not, through its use of the Dynatrace Offerings, provide any Restricted Information to be Processed by Dynatrace.

Pelanggan hanya akan memberikan Data Pribadi Pelanggan kepada Dynatrace yang diperlukan Dynatrace untuk melaksanakan kewajibannya berdasarkan Perjanjian sehubungan dengan Penawaran Dynatrace dan jasa terkait lainnya. Pelanggan mengakui bahwa penggunaan Penawaran Dynatrace tidak memerlukan dan tidak sesuai untuk Pemrosesan Informasi Terbatas apa pun dan melalui penggunaan Penawaran Dynatrace tidak akan memberikan Informasi Terbatas apa pun untuk Diproses oleh Dynatrace.

4. Requests from Third Parties. / Permintaan dari Pihak Ketiga.

(a) Dynatrace Offerings provide Customer with functionality to access Customer Personal Data in order to assist Customers with requests from Data Subjects exercising their rights granted to them under Data Protection Law ("Data Subject Requests") or requests from regulatory or judicial bodies relating to the
Processing of Customer Personal Data. To the extent that Customer is unable to access the relevant Customer Personal Data within Dynatrace Offerings or the access to Customer Personal Data does not provide sufficient assistance to answer such requests in accordance with Data Protection Law, and where required by applicable Data Protection Law, Dynatrace agrees, at the Customer's request, to provide reasonable assistance to Customer, to enable Customer to respond to Data Subject Requests or requests from regulatory or judicial bodies relating to the Processing of Customer Personal Data under the Agreement. If a request is made directly to Dynatrace relating to Customer Personal Data for which Dynatrace can identify Customer as the Controller, Dynatrace shall without undue delay refer such communication to Customer and shall not respond to such request without Customer' express authorization. The foregoing shall not prohibit Dynatrace from communicating with a Data Subject or regulatory or judicial body if it is not reasonably apparent on the face of the communication that the request relates to the Customer or if Dynatrace has a legal obligation to respond itself.

Penawaran Dynatrace menyediakan fungsi kepada Pelanggan untuk mengakses Data Pribadi Pelanggan guna membantu Pelanggan terkait permintaan dari Subjek Data yang menggunakan hak-hak mereka yang diberikan kepada mereka berdasarkan Undang-Undang Perlindungan Data ("Permintaan Subjek Data") atau permintaan dari badan pengawas atau badan peradilan yang berkaitan dengan Pemrosesan Data Pribadi Pelanggan. Sejauh Pelanggan tidak

dapat mengakses Data Pribadi Pelanggan yang relevan dalam Penawaran Dynatrace atau akses ke Data Pribadi Pelanggan tidak cukup membantu dalam menjawab permintaan tersebut sesuai dengan Undang-Undang Perlindungan Data, dan jika diwajibkan oleh UndangUndang Perlindungan Data yang berlaku, atas permintaan Pelanggan, Dynatrace setuju untuk memberikan bantuan yang wajar kepada Pelanggan, agar Pelanggan dapat menanggapi Permintaan Subjek Data atau permintaan dari badan pengawas atau badan peradilan yang berkaitan dengan Pemrosesan Data Pribadi Pelanggan berdasarkan Perjanjian. Jika permintaan ditujukan secara langsung kepada Dynatrace terkait dengan Data Pribadi Pelanggan yang membuat Dynatrace dapat mengidentifikasi Pelanggan sebagai Pengendali, tanpa penundaan yang tidak semestinya, Dynatrace akan merujuk komunikasi tersebut kepada Pelanggan dan tidak akan menanggapi permintaan tersebut tanpa izin yang jelas dari Pelanggan. Hal-hal di atas tidak akan melarang Dynatrace untuk berkomunikasi dengan Subjek Data atau badan pengawas atau badan peradilan jika tidak terlihat jelas dari komunikasi tersebut bahwa permintaan tersebut terkait dengan Pelanggan atau jika Dynatrace memiliki kewajiban hukum untuk menanggapinya sendiri.

(b) If Dynatrace is compelled to disclose Personal Data for which Customer is the Controller due to a request by a law enforcement agency or other third-party, Dynatrace will give Customer notice of such request before granting access and/or providing Personal Data, to allow Customer to seek a protective order or other appropriate remedy. If Dynatrace is legally prohibited from providing Customer notice, Dynatrace will take measures to protect Personal Data from undue disclosure, as if it were Dynatrace's own Confidential Information being requested.

Jika Dynatrace terpaksa mengungkapkan Data Pribadi Pelanggan yang merupakan Pengendali karena permintaan dari lembaga penegak hukum atau pihak ketiga lainnya, Dynatrace akan memberi tahu Pelanggan tentang permintaan tersebut sebelum memberikan akses dan/atau menyediakan Data Pribadi, untuk memungkinkan Pelanggan memohon perintah perlindungan atau pemulihan hak lainnya yang sesuai. Jika Dynatrace dilarang secara hukum untuk memberikan pemberitahuan kepada Pelanggan, Dynatrace akan melakukan tindakan untuk melindungi Data Pribadi dari pengungkapan yang tidak semestinya, seolah-olah yang diminta itu adalah Informasi Rahasia Dynatrace sendiri.

5. Assistance and Cooperation. Subject to the nature of the processing and the Personal Data available to Dynatrace and where required by applicable Data Protection Law, Dynatrace will, upon Customer's written request, provide reasonable assistance and information to Customer, where, in Customer's judgement, the type of Processing performed by Dynatrace requires a data protection impact assessment, and/or prior consultation with the relevant data protection authorities and provide reasonable assistance to Customer in complying with its other obligations under applicable Data Protection Law relating to data security and Personal Data Breach notifications, to the extent applicable to the Processing of Customer Personal Data. Customer shall reimburse Dynatrace for all non-negligible costs Dynatrace incurs in performing its obligations under this section.

Bantuan dan Kerja Sama. Sesuai dengan sifat pemrosesan dan Data Pribadi yang tersedia bagi Dynatrace dan jika diwajibkan oleh Undang-Undang Perlindungan Data yang berlaku, atas permintaan tertulis dari Pelanggan, Dynatrace akan memberikan bantuan dan informasi yang wajar kepada Pelanggan, jika menurut penilaian Pelanggan, jenis Pemrosesan yang dilakukan oleh Dynatrace memerlukan penilaian dampak perlindungan data, dan/atau konsultasi terlebih dahulu dengan lembaga perlindungan data yang relevan dan memberikan bantuan yang wajar kepada Pelanggan dalam mematuhi kewajibannya yang lain berdasarkan Undang-Undang Perlindungan Data yang berlaku yang berkaitan dengan keamanan data dan pemberitahuan Pelanggaran Data Pribadi, sejauh yang berlaku pada Pemrosesan Data Pribadi Pelanggan. Pelanggan harus mengganti semua biaya yang tidak dapat diabaikan yang dikeluarkan Dynatrace dalam melaksanakan kewajibannya berdasarkan bagian ini.

6. Demonstrable Compliance. Dynatrace agrees to provide information necessary to demonstrate compliance with this DPA upon Customer's reasonable request.

Kepatuhan yang Dapat Dibuktikan. Dynatrace setuju untuk memberikan informasi yang diperlukan untuk menunjukkan kepatuhan terhadap PPD ini atas permintaan yang wajar dari Pelanggan.

7. Audits and Assessments. / Audit dan Penilaian.

(a) Where applicable Data Protection Laws afford Customer an audit or assessment right and subject to the scope of such right, Customer may carry out, upon Customer's written request and up to once per year, an audit or assessment of

Dynatrace's policies, procedures, and records relevant to the Processing of Customer Personal Data, in accordance with applicable Data Protection Laws.

Apabila Undang-Undang Perlindungan Data yang berlaku memberikan hak audit atau penilaian kepada Pelanggan dan sesuai dengan ruang lingkup hak tersebut, atas permintaan tertulis Pelanggan dan hingga satu kali per tahun, Pelanggan dapat melakukan audit atau penilaian terhadap kebijakan, prosedur, dan catatan Dynatrace yang relevan dengan Pemrosesan Data Pribadi Pelanggan, sesuai dengan UndangUndang Perlindungan Data yang berlaku.

(b) To request an audit, Customer must submit a detailed audit plan at least four (4) weeks in advance of the proposed audit date to Dynatrace, which plan describes the proposed scope, duration, and start date of the audit. Dynatrace will review the audit plan and provide Customer with any concerns or questions. Before the commencement of any audit, the parties shall agree on a detailed audit plan, including fees, timing, scope of controls, evidence to be produced, and duration. If the requested audit scope is addressed in a similar audit report within the prior twelve months and Dynatrace confirm there are no material changes in the controls audited, Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.

Untuk meminta audit, Pelanggan harus menyerahkan rencana audit terperinci setidaknya empat (4) minggu sebelum tanggal audit yang diusulkan kepada Dynatrace, dan rencana tersebut menjelaskan ruang lingkup, durasi, dan tanggal mulai audit yang diusulkan. Dynatrace akan meninjau rencana audit tersebut dan memberikan informasi kepada Pelanggan jika ada masalah atau pertanyaan. Sebelum dimulainya audit, para pihak harus menyepakati rencana audit yang terperinci, termasuk biaya, waktu, ruang lingkup pengendalian, bukti yang akan dihasilkan, dan durasi. Jika ruang lingkup audit yang diminta telah dibahas dalam laporan audit serupa dalam dua belas bulan sebelumnya dan Dynatrace mengonfirmasi bahwa tidak ada perubahan mendasar dalam pengendalian yang diaudit, Pelanggan setuju untuk menerima temuan-temuan tersebut sebagai pengganti permintaan audit atas pengendalian yang tercakup dalam laporan tersebut.

(c) Any audit or assessment must be: (i) conducted during Dynatrace's normal business hours; (ii) subject to the parties' confidentiality obligations. If a third-party is to conduct the audit, the third-party must not be a competitor to Dynatrace, and such third-party is subject to Dynatrace's prior consent, and must execute a written confidentiality agreement with the parties before conducting the audit.

Setiap audit atau penilaian harus: (i) dilakukan selama jam kerja normal Dynatrace; (ii) sesuai dengan kewajiban kerahasiaan para pihak. Jika pihak ketiga akan melakukan audit, pihak ketiga tersebut tidak boleh menjadi pesaing Dynatrace, dan pihak ketiga tersebut harus mendapatkan persetujuan Dynatrace terlebih dahulu, dan harus menandatangani perjanjian kerahasiaan tertulis dengan para pihak sebelum melakukan audit.

(d) Any audits are at Customer's expense. Any request for Dynatrace to provide assistance with an audit is considered a separate service if such audit assistance requires the use of resources different from, or in addition to, those required for the provision of the Dynatrace Offerings. Dynatrace will seek Customer's written confirmation that it will pay any applicable fees before performing such audit assistance.

Setiap audit dilakukan dengan biaya yang ditanggung oleh Pelanggan. Setiap permintaan kepada Dynatrace untuk memberikan bantuan audit dianggap sebagai jasa terpisah jika bantuan audit tersebut memerlukan penggunaan sumber daya yang berbeda dengan, atau sebagai tambahan bagi, sumber daya yang diperlukan untuk penyediaan Penawaran Dynatrace. Dynatrace akan meminta konfirmasi tertulis dari Pelanggan bahwa Pelanggan akan membayar biaya yang berlaku sebelum melakukan bantuan audit tersebut.

8. Confidentiality. Dynatrace shall ensure that any person that it authorizes to process the Customer Personal Data (including its staff, agents, and subcontractors) shall be subject to a contractual, statutory duty, or other binding obligations of confidentiality.

Kerahasiaan. Dynatrace harus memastikan bahwa setiap orang yang diberi wewenang untuk memproses Data Pribadi Pelanggan (termasuk staf, agen, dan subkontraktornya) harus mematuhi kontrak, kewajiban hukum, atau kewajiban kerahasiaan yang mengikat lainnya.

9. Security / Keamanan

(a) Security Measures. Taking into account the state of the art, 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, Dynatrace has implemented and shall maintain appropriate technical and organizational measures designed to provide a level of security appropriate to the risk of Processing Customer Personal Data ("Security Measures"). Customer confirms that Dynatrace's implementation of the Security Measures identified at Schedule B is sufficient for the purposes of complying with its obligations under this DPA. Notwithstanding the above, Customer acknowledges and agrees it is responsible for its own secure use of the Dynatrace Offerings.

Tindakan Keamanan. Dengan mempertimbangkan keadaan terkini, biaya pelaksanaan dan sifat, ruang lingkup, konteks, serta tujuan Pemrosesan serta risiko berbagai kemungkinan dan tingkat keparahan terhadap hak-hak dan kebebasan orang perorangan, Dynatrace telah menerapkan dan akan mempertahankan tindakan teknis dan organisasi yang sesuai yang dirancang untuk memberikan tingkat keamanan yang sesuai dengan risiko Pemrosesan Data Pribadi Pelanggan ("Tindakan Keamanan"). Pelanggan mengonfirmasi bahwa penerapan Tindakan Keamanan yang disebutkan pada Lampiran B oleh Dynatrace sudah cukup untuk memenuhi kewajibannya berdasarkan PPD ini. Terlepas dari hal di atas, Pelanggan mengakui dan menyetujui bahwa Pelanggan sendiri bertanggung jawab atas penggunaan Penawaran Dynatrace secara aman.

(b) Personal Data Breach. Dynatrace will notify Customer without undue delay and no later than required of Dynatrace by applicable Data Protection Law, after it becomes aware of a Personal Data Breach. Dynatrace will promptly initiate an investigation into the circumstances surrounding the Personal Data Breach and make its findings available to Customer. Dynatrace will endeavour to take all steps required by applicable Data Protection Law to mitigate the effects of such Personal Data Breach. At Customer's request and taking into account the nature of the Processing and information available to Dynatrace, Dynatrace will take commercially reasonable steps to assist Customer in complying with its obligations necessary to enable Customer to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if Customer is required to do so under applicable Data Protection Law. Notification of a Personal Data Breach

will be delivered to one or more of Customer's administrators by any means Dynatrace selects including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on the online portal or as otherwise required by Dynatrace in a written notice to Customer's administrator(s). Dynatrace's obligation to report or respond to a Personal Data Breach under this Section is not an acknowledgement by Dynatrace of any fault or liability with respect to the Personal Data Breach.

Pelanggaran Data Pribadi. Dynatrace akan memberi tahu Pelanggan tanpa penundaan yang tidak semestinya dan tidak lebih lambat daripada yang diwajibkan oleh Undang-Undang Perlindungan Data yang berlaku, setelah Dynatrace mengetahui adanya Pelanggaran Data Pribadi. Dynatrace akan segera memulai penyelidikan terhadap keadaan seputar Pelanggaran Data Pribadi dan menyediakan temuannya kepada Pelanggan. Dynatrace akan berusaha untuk melakukan semua langkah yang diwajibkan oleh UndangUndang Perlindungan Data yang berlaku untuk mengurangi dampak dari Pelanggaran Data Pribadi tersebut. Atas permintaan Pelanggan dan dengan mempertimbangkan sifat Pemrosesan serta informasi yang tersedia bagi Dynatrace, Dynatrace akan melakukan langkah-langkah yang wajar secara komersial untuk membantu Pelanggan mematuhi kewajibannya yang diperlukan agar Pelanggan dapat memberitahukan Pelanggaran Data Pribadi yang relevan kepada instansi yang berwenang dan/atau Subjek Data yang terdampak, jika Pelanggan diharuskan untuk melakukannya berdasarkan Undang-Undang Perlindungan Data yang berlaku. Pemberitahuan tentang Pelanggaran Data Pribadi akan disampaikan kepada satu atau lebih administrator Pelanggan dengan cara apa pun yang dipilih Dynatrace termasuk melalui email. Pelanggan bertanggung jawab penuh untuk memastikan agar administrator Pelanggan memelihara informasi kontak yang akurat di portal daring atau sebagaimana diwajibkan oleh Dynatrace dalam pemberitahuan tertulis kepada administrator Pelanggan. Kewajiban Dynatrace untuk melaporkan atau menanggapi Pelanggaran Data Pribadi berdasarkan Bagian ini bukan merupakan pengakuan Dynatrace atas kesalahan atau tanggung jawab apa pun sehubungan dengan Pelanggaran Data Pribadi.

10. Sub-processing Sub-pemrosesan

(a) Customer gives its general authorization to appoint members of the Dynatrace Group as sub-processors under this DPA and authorizes Dynatrace and members of the Dynatrace Group to engage further Subprocessors. A current list of

current Sub-processors for the Dynatrace Offerings is available at https://www.dynatrace.com/company/trust-center/customers/subprocessors-dynatrace-services/. To be notified of new Sub-processors or changes in Sub-processors, Customer must register for notifications available at https://www.dynatrace.com/company/trust-center/customers/subprocessors-dynatraceservices/ ("Data Protection Notices"). Dynatrace shall update the Sub-processor List to reflect any addition or change in third-party Sub-processors not less than thirty (30) days prior to the effective date of the change. Customers that have subscribed to get updates to the Sub-processor List will be notified of the change.

Pelanggan memberi izin umum untuk menunjuk anggota Grup Dynatrace sebagai sub-pemroses berdasarkan PPD ini dan memberikan izin kepada Dynatrace dan anggota Grup Dynatrace untuk melibatkan Sub-pemroses lebih lanjut. Daftar Sub-pemroses Penawaran Dynatrace saat ini tersedia di https://www.dynatrace.com/company/trust-center/customers/subprocessors-dynatrace-services/. Untuk mendapatkan pemberitahuan tentang Sub-pemroses baru atau perubahan Sub-pemroses, Pelanggan harus mendaftar untuk mendapatkan pemberitahuan yang tersedia di https://www.dynatrace.com/company/trust-center/customers/subprocessors-dynatrace-services/ ("Pemberitahuan Perlindungan Data"). Dynatrace akan memperbarui Daftar Sub-pemroses untuk memberi tahu penambahan atau perubahan Sub-pemroses pihak ketiga tidak kurang dari tiga puluh (30) hari sebelum tanggal berlakunya perubahan. Pelanggan yang telah berlangganan untuk mendapatkan pembaruan pada Daftar Sub-pemroses akan diberi tahu tentang perubahan tersebut.

(b) To the extent required by applicable Data Protection Law, Customer may object to the processing of Customer Personal Data by any newly appointed Sub-processor on reasonable grounds relating to the protection of Customer Personal Data and shall inform Dynatrace in writing within fifteen (15) days after notice of the changes are posted on the Sub-processor List, setting out the specific reasons for its objection.

Customer's objection must be in writing and provide commercially reasonably justification for the objection, based on reasonable concerns concerning the proposed Sub-processor's practices relating to data protection. Following an objection, the parties will then work together in good faith to address Customer's reasonable objections and proceed with the change in Sub-processor. If an agreement cannot be reached within fifteen (15) days of the objection, at Dynatrace's option: (a) Dynatrace will instruct the Sub-processor not to process Customer Personal Data, which may result in a Dynatrace Offerings feature being suspended and unavailable to Customer, or (b) Customer may immediately terminate this DPA and the Agreement and Dynatrace will promptly refund a prorated portion of any prepaid fees for the period after such suspension or termination date. If no objection is received by Dynatrace within the time period specified above, Customer shall be deemed to have approved the use of the new sub-processor.

Sejauh yang diwajibkan oleh Undang-Undang Perlindungan Data yang berlaku, Pelanggan dapat mengajukan keberatan atas pemrosesan Data Pribadi Pelanggan oleh Sub-pemroses yang baru ditunjuk dengan alasan yang masuk akal terkait dengan perlindungan Data Pribadi Pelanggan dan harus memberi tahu Dynatrace secara tertulis dalam waktu lima belas (15) hari setelah pemberitahuan perubahan diposting di Daftar Sub-pemroses, dengan menjelaskan alasan spesifik atas keberatannya. Keberatan Pelanggan harus diajukan secara tertulis dan memberikan alasan yang wajar secara komersial atas keberatan tersebut, berdasarkan kekhawatiran yang wajar mengenai praktik Sub-pemroses yang diusulkan terkait dengan perlindungan data. Setelah pengajuan keberatan, para pihak akan bekerja sama dengan iktikad baik untuk menangani keberatan yang wajar dari Pelanggan dan melanjutkan perubahan Sub-pemroses. Jika kesepakatan tidak dapat dicapai dalam waktu lima belas (15) hari setelah pengajuan keberatan, atas pilihan Dynatrace: (a) Dynatrace akan memerintahkan Sub-pemroses untuk tidak memproses Data Pribadi Pelanggan, yang dapat mengakibatkan fitur Penawaran Dynatrace ditangguhkan dan tidak tersedia bagi Pelanggan, atau (b) Pelanggan dapat segera mengakhiri PPD dan Perjanjian ini dan Dynatrace akan segera mengembalikan bagian prorata dari setiap biaya prabayar selama periode setelah tanggal penangguhan atau pengakhiran tersebut. Jika tidak ada keberatan yang diterima oleh Dynatrace dalam jangka waktu yang disebutkan di atas, Pelanggan akan dianggap telah menyetujui penggunaan sub-pemroses baru.

(c) Dynatrace shall: (i) enter into a written agreement with each Sub-processor containing data protection obligations that provide substantially similar appropriate contractual obligations but not less restrictive than those set forth in this DPA, to the extent appropriate to the nature of the service provided by such Subprocessor; and (ii) remain responsible for such Sub-processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-processor that cause Dynatrace to breach any of its obligations under this DPA.

Dynatrace akan: (i) mengadakan perjanjian tertulis dengan setiap Sub-pemroses yang memuat kewajiban perlindungan data yang memberikan kewajiban kontrak yang sesuai dan serupa secara substansial, tetapi tidak kurang ketat daripada yang tercantum dalam PPD ini, sejauh sesuai dengan sifat jasa yang disediakan oleh Sub-pemroses tersebut; dan (ii) tetap bertanggung jawab atas kepatuhan Sub-pemroses tersebut terhadap kewajiban dalam PPD ini serta atas tindakan atau kelalaian Sub-pemroses tersebut yang menyebabkan Dynatrace melanggar salah satu kewajibannya berdasarkan PPD ini.

11. Deletion of Customer Data on Termination. Following termination or expiry of the Agreement Customer Personal Data will be deleted within thirty (30) days, or, at the choice of customer, returned, except as required to be retained by applicable law or to the extent archived on back-up systems, in which case the terms of this DPA shall survive.

Penghapusan Data Pelanggan saat Pengakhiran. Setelah pengakhiran atau berakhirnya Perjanjian, Data Pribadi Pelanggan akan dihapus dalam waktu tiga puluh (30) hari, atau dikembalikan sesuai pilihan pelanggan, kecuali jika diwajibkan untuk disimpan oleh hukum yang berlaku atau sejauh yang diarsipkan pada sistem cadangan, dalam hal ini ketentuan dalam PPD ini tetap berlaku.

12. International Data Transfers / Pemindahan Data Internasional

(a) Customer authorizes Dynatrace and its Sub-processors to transfer Customer Personal Data across international borders, including without limitation from the EEA, UK, and/or Switzerland, Israel, and China to the United States. If Customer Personal Data originating from the EEA or Switzerland is transferred to a country that has not been found to provide an adequate level of protection under applicable Data Protection Law ("Restricted Transfer"), the parties agree that the transfer shall be governed by the Standard Contractual Clauses that are hereby incorporated by reference into this DPA as follows. The signatures on this DPA or the Agreement constitute signing the Standard Contractual Clauses and any annexes attached thereto. When the transfer of Customer Personal Data from Customer ("Data Exporter") to Dynatrace ("Data Importer") is a Restricted Transfer and Data Protection Laws require that a valid transfer mechanism be put in place, the transfers shall be subject to the Standard Contractual Clauses.

Pelanggan memberikan izin kepada Dynatrace dan Sub-pemrosesnya untuk mentransfer Data Pribadi Pelanggan melintasi batas internasional, termasuk, tanpa batasan, dari Kawasan Ekonomi Eropa (KEE), Inggris, dan/atau Swiss, Israel, dan Tiongkok ke Amerika Serikat. Jika Data Pribadi Pelanggan yang berasal dari KEE atau Swiss dipindahkan ke negara yang belum dinyatakan memberikan tingkat perlindungan yang memadai berdasarkan Undang-Undang Perlindungan Data yang berlaku ("Pemindahan Terbatas"), para pihak setuju bahwa Pemindahan tersebut akan diatur oleh Klausul Kontrak Standar yang dengan ini dimasukkan dengan penyebutan ke dalam PPD ini sebagai berikut. Tanda tangan pada PPD atau Perjanjian ini merupakan penandatanganan Klausul Kontrak Standar dan setiap lampiran yang dilampirkan pada Perjanjian ini. Jika pemindahan Data Pribadi Pelanggan dari Pelanggan ("Pengekspor Data") ke Dynatrace ("Pengimpor Data") merupakan Pemindahan Terbatas dan Undang-Undang Perlindungan Data mewajibkan adanya mekanisme pemindahan yang sah, pemindahan tersebut harus sesuai dengan Klausul Kontrak Standar.

(b) The Standard Contractual Clauses shall be completed as follows:

Klausul Kontrak Standar harus dilengkapi sebagai berikut:

i. Module Two will apply (as applicable);

Modul Dua akan berlaku (jika sesuai); ii. In Clause 7

(Docking), the optional docking clause will apply;

Pada Klausul 7 (Penambahan), klausul penambahan opsional akan berlaku; iii. In Clause 8.5 and Clause 16 (d), the certification of deletion will be provided upon data exporter's written request;

Pada Klausul 8.5 dan Klausul 16(d), sertifikasi penghapusan akan diberikan atas permintaan tertulis dari pengekspor data;

iv. In Clause 8.9, the audit right shall be carried out in accordance with Section 7 of the DPA;

Pada Klausul 8.9, hak audit harus dilakukan sesuai dengan Bagian 7 dalam PPD;

v. In Clause 9 (Use of Sub-processors), option 2 “General Written Authorization” for subprocessors shall apply and the time period for prior notice shall be as set out in section 11 of this DPA;

Pada Klausul 9 (Penggunaan Sub-pemroses), opsi 2 "Izin Tertulis Umum" untuk sub-pemroses akan berlaku dan jangka waktu untuk pemberitahuan sebelumnya adalah seperti yang dijelaskan pada bagian 11 PPD ini;

vi. In Clause 11 (Redress), the optional language shall not apply;

Pada Klausul 11 (Ganti Rugi), bahasa opsional tidak berlaku; vii. In Clause 13 (Supervision), the competent supervisory authority shall be the Commission nationale de l’informatique et des libertes (CNIL).

Pada Klausul 13 (Pengawasan), lembaga pengawas yang berwenang adalah Commission nationale de l'informatique et des libertes (CNIL).

viii. In Clause 14 (f) and Clause 16 (c), the termination right will be limited to the termination of the Clauses; Pada Klausul 14 (f) dan Klausul 16 (c), hak pengakhiran akan terbatas pada pengakhiran Klausul; ix. In Clause 17 (Governing Law), the Standard Contractual Clauses shall be governed by French law;

Pada Klausul 17 (Hukum yang Mengatur), Klausul Kontrak Standar akan diatur oleh hukum Prancis;

x. In Clause 18(b) (Choice of Forum and Jurisdiction), the parties agree that disputes shall be resolved before the courts of France;

Pada Klausul 18(b) (Pilihan Pengadilan dan Yurisdiksi), para pihak setuju bahwa perselisihan akan diselesaikan di pengadilan Prancis;

xi. Annex 1 of the Standard Contractual Clauses shall be completed with the information set out in Schedule A of this DPA;

Lampiran 1 Klausul Kontrak Standar harus dilengkapi dengan informasi yang dijelaskan pada Lampiran A PPD ini; xii. Annex 2 of the Standard Contractual Clauses shall be completed with the information set out in Schedule B of this DPA; and

Lampiran 2 Klausul Kontrak Standar harus dilengkapi dengan informasi yang dijelaskan pada Lampiran B PPD ini; dan xiii. A new Clause 1 (e) is added to the Standard Contractual Clauses which shall read: “To the extent applicable hereunder, these Clauses also apply mutatis mutandis to the parties’ Processing of Customer Personal Data that is subject to the Swiss Federal Act on Data Protection. Where applicable, reference to EU Member State law or EU supervisory authorities shall be modified to include the appropriate reference under Swiss law as it relates to the transfer of Customer Personal Data that are subject to the Swiss Federal Act on Data Protection and the Swiss Federal Data Protection and Information Commissioner as the supervisory authority under these Clauses.”.

Klausul 1 (e) baru ditambahkan pada Klausul Kontrak Standar yang berbunyi: "Sejauh yang berlaku berdasarkan Perjanjian ini, Klausul-klausul ini juga berlaku mutatis mutandis pada Pemrosesan Data Pribadi Pelanggan oleh para pihak yang sesuai dengan Undang-Undang Federal Swiss tentang Perlindungan Data. Jika berlaku, penyebutan hukum Negara Anggota UE atau lembaga pengawas UE akan diubah sehingga mencakup penyebutan yang sesuai berdasarkan hukum Swiss terkait dengan pemindahan Data Pribadi Pelanggan yang sesuai dengan Undang-Undang Federal Swiss tentang Perlindungan Data dan Komisioner Perlindungan Data serta Informasi Federal Swiss sebagai lembaga pengawas berdasarkan Klausul ini."

(c) To the extent Dynatrace’s provision of the Dynatrace Offerings involves the transfer of Customer Personal Data originated from the UK to a third country that has not been designated as providing an adequate level of protection for Customer Personal Data under the Applicable Laws in the UK, the Standard Contractual Clauses shall: (i) be used and completed as set forth in section 13; (ii) a new Clause 1(f) is added to the Standard Contractual Clauses which shall read: “To the extent applicable hereunder, these Clauses, as supplemented by Section 13, also apply mutatis mutandis to the parties’ Processing of Customer Personal Data that is subject to the UK Data Protection Laws; and (iii) the UK Addendum shall be completed as follows:

Sejauh ketentuan Penawaran Dynatrace melibatkan pemindahan Data Pribadi Pelanggan yang berasal dari Inggris ke negara ketiga yang belum ditetapkan sebagai negara yang memberikan tingkat perlindungan yang memadai untuk Data Pribadi Pelanggan berdasarkan Hukum yang Berlaku di Inggris, maka Klausul Kontrak Standar harus: (i) digunakan

dan dilengkapi sebagaimana dijelaskan pada bagian 13; (ii) Klausul 1(f) baru ditambahkan pada Klausul Kontrak Standar yang akan berbunyi: “Sejauh yang berlaku berdasarkan Perjanjian ini, sebagaimana dilengkapi dengan Bagian 13, Klausul-klausul ini juga berlaku mutatis mutandis pada Pemrosesan Data Pribadi Pelanggan para pihak yang sesuai dengan UndangUndang Perlindungan Data Inggris; dan (iii) Adendum Inggris harus dilengkapi sebagai berikut:

i. Table 1 of the UK Addendum shall be completed with the information in Schedule A.

Tabel 1 pada Adendum Inggris harus dilengkapi dengan informasi pada Lampiran A.

ii. Table 2 of the UK Addendum shall be completed with the information located in Section 13 (c) of this DPA.

Tabel 2 pada Adendum Inggris harus dilengkapi dengan informasi yang terdapat pada Bagian 13 (c) PPD ini.

iii. Table 3 of the UK Addendum shall be completed as follows:

Tabel 3 pada Adendum Inggris harus dilengkapi sebagai berikut:

1) The list of parties is set forth in Schedule A;

Daftar para pihak tercantum pada Lampiran A;

2) A description of the transfer is set forth in Schedule A;

Penjelasan mengenai pemindahan tersebut tercantum pada Lampiran A;

3) A description of the technical and organizational measures is set forth in Schedule B;

Penjelasan mengenai tindakan teknis dan organisasi diuraikan pada Lampiran B;

4) The list of sub-processors is in section 11 of this DPA;

Daftar sub-pemroses terdapat pada bagian 11 PPD ini;

5) For purposes of completing Table 4 of the UK Addendum, both the importer and the exporter may end the UK Addendum as set out in Section 19 of the UK Addendum.

Untuk keperluan melengkapi Tabel 4 Adendum Inggris, baik pengimpor maupun pengekspor dapat mengakhiri Adendum Inggris sebagaimana dijelaskan pada Bagian 19 Adendum Inggris.

(d) To the extent Dynatrace’s provision of the Dynatrace Offerings involves the transfer of Customer Personal Data originated from China to a third country that has not been designated as providing an adequate level of protection for Customer Personal Data under the Applicable Laws in China), Customer shall be responsible for fulfilling all the following obligations for exporting Customer Personal Data (where Customer is the Controller) or ensuring that all the following obligations have been fulfilled by the relevant third-party controller (where Customer is the Processor):

Sejauh ketentuan Penawaran Dynatrace melibatkan pemindahan Data Pribadi Pelanggan yang berasal dari Tiongkok ke negara ketiga yang belum ditetapkan sebagai negara yang memberikan tingkat perlindungan yang memadai untuk Data Pribadi Pelanggan berdasarkan Hukum yang Berlaku di Tiongkok), Pelanggan bertanggung jawab untuk memenuhi semua kewajiban berikut untuk mengekspor Data Pribadi Pelanggan (jika Pelanggan adalah Pengendali) atau memastikan bahwa semua kewajiban berikut telah dipenuhi oleh pengendali pihak ketiga yang relevan (jika Pelanggan adalah Pemroses):

i. informing the individuals of the name and contact information of the overseas receiving party of Customer Personal Data, the purpose and means of the Processing, the categories of Customer Personal Data, and the methods and procedures via which the individuals may raise requests to exercise the rights to Customer Personal Data with the overseas receiving party of Customer Personal Data;

memberitahukan kepada individu tentang nama dan informasi kontak pihak penerima Data Pribadi Pelanggan di luar negeri, tujuan dan cara Pemrosesan, kategori Data Pribadi Pelanggan, serta metode dan prosedur yang dapat digunakan pengguna untuk mengajukan permintaan guna menjalankan haknya atas Data Pribadi Pelanggan kepada pihak penerima Data Pribadi Pelanggan di luar negeri;

ii. securing a lawful basis for the export of Customer Personal Data, and where consent of the individuals is the lawful basis, obtaining separate consent of the individuals;

mengamankan dasar hukum untuk ekspor Data Pribadi Pelanggan, dan apabila persetujuan individu merupakan dasar hukum tersebut, memperoleh persetujuan terpisah dari individu;

iii. conducting a personal information protection impact assessment on the exporting of Customer Personal Data; and

melakukan penilaian dampak perlindungan informasi pribadi pada ekspor Data Pribadi Pelanggan; dan iv. adopting the appropriate safeguard measure required by the PIPL and accompanying administrative regulations (i.e., passing the government security assessment, filing the executed standard contractual clauses or obtaining the certification) unless exemption applies.

melakukan tindakan perlindungan yang sesuai yang diwajibkan oleh PIPL dan peraturan administratif yang menyertainya (yaitu, lulus penilaian keamanan pemerintah, mengajukan klausul kontrak standar yang telah ditandatangani, atau mendapatkan sertifikasi) kecuali jika ada pengecualian.

(e) In addition to the foregoing, if a Supervisory Authority adopts, updates or replaces any standard contractual clauses or similar data transfer mechanisms, Dynatrace reserves the right to adopt an alternative compliance standard to replace or supplement the Standard Contractual Clauses or the UK Addendum for the lawful transfer of Personal Data, or add new data transfer mechanisms for other countries, provided these are recognized under Data Protection Law. Dynatrace will provide thirty (30) days advance notice of the adoption of the alternative compliance standard to customers who subscribe to Data Protection Notices. The variation will automatically apply as set out in Dynatrace's notification at the end of the notice period.

Selain hal-hal yang disebutkan di atas, jika Lembaga Pengawas menerapkan, memperbarui, atau mengganti klausul kontrak standar atau mekanisme pemindahan data serupa, Dynatrace berhak menerapkan standar kepatuhan alternatif untuk menggantikan atau menambahkan Klausul Kontrak Standar atau Adendum Inggris untuk pemindahan Data Pribadi yang sah, atau menambahkan mekanisme pemindahan data baru untuk negara lain, asalkan mekanisme tersebut diakui berdasarkan Undang-Undang Perlindungan Data. Dynatrace akan memberikan pemberitahuan tiga puluh (30) hari sebelumnya mengenai penerapan standar kepatuhan alternatif kepada pelanggan yang berlangganan Pemberitahuan Perlindungan Data. Perubahan tersebut akan otomatis berlaku seperti yang dijelaskan dalam pemberitahuan Dynatrace pada akhir periode pemberitahuan.

(f) In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the Standard Contractual Clauses (provided however, Processor may appoint Sub-processors as set out, and subject to the requirements of, Section 11 of this DPA) or a similar mechanism required by applicable Data Protection Laws specifically for international data transfers; (2) this DPA; and (3) the Agreement.

Jika terjadi konflik atau ketidaksesuaian di antara dokumen-dokumen berikut, urutan prioritasnya adalah: (1) Klausul Kontrak Standar (dengan ketentuan bahwa Pemroses dapat menunjuk Sub-pemroses seperti yang dijelaskan dan sesuai dengan persyaratan pada Bagian 11 PPD ini) atau mekanisme serupa yang diwajibkan oleh Undang-Undang Perlindungan Data yang berlaku khusus untuk pemindahan data internasional; (2) PPD ini; dan (3) Perjanjian.

(g) To the extent Dynatrace transfers Customer Data originating from and protected by applicable Data Protection Law in Brazil, Dynatrace shall comply with the principles and rights of Data Subjects and the data protection obligations provided in the LGPD.

Sejauh Dynatrace memindahkan Data Pelanggan yang berasal dari dan dilindungi oleh Undang-Undang Perlindungan Data yang berlaku di Brasil, Dynatrace harus mematuhi prinsip dan hak Subjek Data serta kewajiban perlindungan data yang diatur dalam LGPD.

(h) To the extent Dynatrace transfers Customer Data originating from and protected by applicable Data Protection Law in Japan, Dynatrace shall comply with the principles and rights of Data Subjects and the data protection obligations provided in the APPI.

Sejauh Dynatrace memindahkan Data Pelanggan yang berasal dari dan dilindungi oleh Undang-Undang Perlindungan Data yang berlaku di Jepang, Dynatrace harus mematuhi prinsip dan hak Subjek Data serta kewajiban perlindungan data yang diatur dalam APPI.

(i) To the extent Dynatrace's provision of the Dynatrace Offerings involves the transfer of Customer Personal Data originated from Israel to a third country that has not been designated as providing an adequate level of protection for Customer Personal Data under the Applicable Laws in Israel), Customer shall be responsible for securing a lawful basis for the export of Customer Personal Data. For clarity, this DPA constitute as Dynatrace's written obligation for adopting the appropriate safeguard measures required by the Protection of Privacy Regulations (International Data Transfer), 2001. For the sake of clarity, the obligations in this DPA are deemed sufficient by the Customer to facilitate the transfer of information outside the Israel in accordance with Regulation 3 of the Privacy Protection Regulations (Transfer of Data to Databases Outside the Borders of the Country), 2001.

Sejauh ketentuan Dynatrace atas Penawaran Dynatrace melibatkan pemindahan Data Pribadi Pelanggan yang berasal dari Israel ke negara ketiga yang belum ditetapkan memberikan tingkat perlindungan yang memadai untuk Data Pribadi Pelanggan berdasarkan Hukum yang Berlaku di Israel), Pelanggan bertanggung jawab untuk mendapatkan dasar yang sah untuk ekspor Data Pribadi Pelanggan. Demi kejelasan, PPD ini merupakan kewajiban tertulis Dynatrace untuk melakukan tindakan perlindungan yang sesuai yang diwajibkan oleh Peraturan Perlindungan Privasi (Pemindahan Data Internasional), 2001. Demi kejelasan, kewajiban dalam PPD ini dianggap cukup oleh Pelanggan untuk memfasilitasi pemindahan informasi di luar Israel sesuai dengan Peraturan 3 dalam Peraturan Perlindungan Privasi (pemindahan Data ke Basis Data di Luar Perbatasan Negara), 2001.

13. Supplemental US State Privacy Laws Specific Terms. / Ketentuan Khusus Tambahan Hukum Privasi Negara Bagian AS.

(a) The definition of "Applicable Data Protection Law" includes US State Privacy Laws. "US State Privacy Laws" means all state laws relating to the protection and processing of personal data in effect in the United States of America, which may include, without limitation, the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA"), and similar consumer privacy laws in other states, in each case, as amended, supplemented or replaced from time to time.

Definisi "Hukum Perlindungan Data yang Berlaku" mencakup Hukum Privasi Negara Bagian AS. "Hukum Privasi Negara Bagian AS" berarti semua hukum negara bagian yang berkaitan dengan perlindungan dan pemrosesan data pribadi yang berlaku di Amerika Serikat, yang dapat mencakup, tetapi tidak terbatas pada, Undang-Undang Privasi Konsumen California, sebagaimana telah diubah oleh Undang-Undang Hak Privasi California ("CCPA"),dan hukum hukum privasi yang serupa di negara bagian lainnya, dalam setiap kasus, sebagaimana telah diubah, dikengkapi atau diubah dari waktu ke waktu.

(a) Where Dynatrace processes Customer Personal Data subject to US State Privacy Laws, Dynatrace is a 'service provider' or "processor" (as applicable) when processing Customer Personal data. Customer discloses, or otherwise makes available, Customer Personal Data to Dynatrace for a limited and specified purpose of providing Dynatrace Offerings in accordance with the Agreement (the "Purpose"). Dynatrace shall (and will require that its Sub-processors):

Ketika Dynatrace memproses Data Pribadi Pelanggan sesuai dengan Hukum Privasi Negara Bagian AS, Dynatrace adalah penyedia jasa, atau pemroses (sebagaimana berlaku) saat memproses data Pribadi Pelanggan. Pelanggan mengungkapkan, atau menyediakan, Data Pribadi Pelanggan kepada Dynatrace dengan tujuan terbatas dan tertentu dalam menyediakan Penawaran Dynatrace sebagaimana dijelaskan menurut Perjanjian ("Tujuan"). Dynatrace harus (dan akan mewajibkan Sub-pemrosesnya):

i. comply with obligations applicable to it as a service provider or processor under US State Privacy Laws;
mematuhi kewajiban yang berlaku untuknya sebagai penyedia jasa atua pemroses berdasarkan Hukum Privasi Negara Bagian AS;

ii. notify if it can no longer meet its obligations under US State Privacy Laws;
memberi tahu jika tidak dapat lagi memenuhi kewajibannya berdasarkan Hukum Privasi Negara Bagian AS;

iii. not 'sell' or 'share' (as such terms are defined by the CCPA) Customer Content or retain, use, or disclose Customer Personal Data: (1) for any purpose other than the Purpose, including retaining, using, or disclosing Customer Personal Data for a commercial purpose other than the Purpose, or as otherwise permitted by US State Privacy Laws; or (2) outside of the direct business relationship between Customer

and Dynatrace; or, unless otherwise permitted by US State Privacy Laws, not combine Customer Personal Data with Personal Data that Dynatrace receives from or on behalf of another business or person, or that it collects from its own interactions with individuals, unless such combination is required to perform any business purpose as permitted by US State Privacy Laws. tidak menjual atau membagikan (sebagasi istillah yang didefinishikan oleh CPPA) Konten Pelanggan atau menyimpan, menggunakan, atau mengungkapkan Data Pribadi Pelanggan: (1) untuk keperluan apa pun selain Tujuan, termasuk menyimpan, menggunakan, atau mengungkapkan Data Pribadi Pelanggan untuk keperluan komersial selain Tujuan, atau sebagaimana diizinkan oleh Hukum Privasi Negara Bagian AS; atau (2) di luar hubungan bisnis langsung antara Pelanggan dan Dynatrace; atau, kecuali jika diizinkan oleh Hukum Privasi Negara Bagian AS, tidak menggabungkan Data Pribadi Pelanggan dengan Data Pribadi yang diterima Dynatrace dari atau atas nama bisnis atau orang lain, atau yang dikumpulkannya dari interaksinya sendiri dengan individu, kecuali jika penggabungan tersebut diperlukan untuk melaksanakan tujuan bisnis apa pun sebagaimana diizinkan oleh Hukum Privasi Negara Bagian AS.

iv. Customer will: (1) upon notice, have the right to take reasonable and appropriate steps agreed upon by the parties to help ensure that Dynatrace Processes Customer Personal Data in a manner consistent with Customer's obligations under US State Privacy Laws and to stop and remediate unauthorized Processing of Customer Personal Data by Dynatrace Processing of Customer Personal Data by Dynatrace; (2) notify Customer if it makes a determination that it can no longer meet its obligations under US State Privacy Laws in relation to Customer Personal Data.

Pelanggan akan: (1) setelah pemberitahuan, memiliki hak untuk melakukan langkah-langkah yang wajar dan sesuai yang disepakati oleh para pihak untuk membantu memastikan bahwa Dynatrace Memproses Data Pribadi Pelanggan dengan cara yang sesuai dengan kewajiban Pelanggan berdasarkan Hukum Privasi Negara Bagian AS dan untuk menghentikan serta memperbaiki Pemrosesan Data Pribadi Pelanggan oleh Dynatrace yang tidak sah; (2) memberi tahu Pelanggan jika Dynatrace memutuskan bahwa mereka tidak lagi dapat memenuhi kewajibannya sebagai berdasarkan Hukum Privasi Negara Bagian AS terkait dengan Data Pribadi Pelanggan

v. Dynatrace acknowledges and confirms that it does not receive Customer Personal Data as consideration for any Offerings provided to Customer. Dynatrace certifies that it understands and will comply with its obligations under US State Privacy Laws.

Dynatrace mengakui dan menegaskan bahwa Dynatrace tidak menerima Data Pribadi Pelanggan sebagai pertimbangan untuk setiap Penawaran yang diberikan kepada Pelanggan. Dynatrace menyatakan bahwa mereka memahami dan akan mematuhi kewajibannya berdasarkan Hukum Privasi Negara Bagian AS.

5 Miscellaneous / Lain-lain

(a) Except as amended by this DPA, the Agreement will remain in full force and effect. Any amendments to this DPA shall be in writing duly signed by authorized representatives of the parties.

Kecuali sebagaimana diubah oleh PPD ini, Perjanjian akan tetap berlaku sepenuhnya. Setiap perubahan pada PPD ini harus dilakukan secara tertulis dan ditandatangani oleh perwakilan yang berwenang dari para pihak.

(b) Notwithstanding anything to the contrary in the Agreement or this DPA, each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, any order or the Agreement, whether in contract, tort or under any other theory of liability, shall remain subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and this DPA, including all Schedules hereto. Dynatrace shall not be liable to Customer for indirect or consequential loss or damage,

loss of profit, loss of sales, loss of business, loss of anticipated savings, loss of or damage to goodwill, or otherwise in each case whether direct or indirect which arise out of or in connection with this DPA. Without limiting either of the parties' obligations under the Agreement or this DPA, Customer agrees that any liability incurred by Dynatrace in relation to the Customer Personal Data that arises as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or applicable Data Protection Law shall count toward and reduce Dynatrace's liability limit under the Agreement (or if applicable, under this DPA) as if it were liability to the Customer. Notwithstanding anything to the contrary in this DPA (including, without limitation, either party's indemnification obligations), neither party will be responsible for any GDPR fines issued or levied under Article 83

of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the GDPR.

Terlepas dari ketentuan apa pun yang bertentangan dalam Perjanjian atau PPD ini, tanggung jawab masing-masing pihak dan semua Afiliasinya, secara keseluruhan, yang timbul dari atau terkait dengan PPD ini, setiap pesanan, atau Perjanjian, baik dalam kontrak, ~~tort~~ perbuatan melawan hukum, atau berdasarkan teori tanggung jawab lainnya, akan tetap mematuhi bagian 'Batasan Tanggung Jawab' dalam Perjanjian, dan setiap penyebutan tanggung jawab suatu pihak pada bagian tersebut berarti tanggung jawab keseluruhan pihak tersebut dan semua Afiliasinya berdasarkan Perjanjian dan PPD ini, termasuk semua Lampirannya. Dynatrace tidak bertanggung jawab kepada Pelanggan atas kerugian atau kerusakan tidak langsung atau konsekuensial, hilangnya keuntungan, kerugian penjualan, kerugian bisnis, hilangnya penghematan yang diharapkan, hilangnya atau rusaknya reputasi, atau hal lainnya, dalam setiap kasus baik secara langsung maupun tidak langsung, yang timbul dari atau sehubungan dengan PPD ini. Tanpa membatasi kewajiban kedua pihak berdasarkan Perjanjian atau PPD ini, Pelanggan setuju bahwa setiap tanggung jawab yang ditanggung oleh Dynatrace terkait dengan Data Pribadi Pelanggan yang timbul akibat atau sehubungan dengan kegagalan Pelanggan untuk mematuhi kewajibannya berdasarkan PPD ini atau Undang-Undang Perlindungan Data yang berlaku akan diperhitungkan dan mengurangi batas tanggung jawab Dynatrace berdasarkan Perjanjian (atau jika berlaku, berdasarkan PPD ini) seolah-olah itu adalah tanggung jawab kepada Pelanggan. Terlepas dari ketentuan apa pun yang bertentangan dalam PPD ini (termasuk, tanpa batasan, kewajiban ganti rugi kedua pihak), tidak ada pihak yang akan bertanggung jawab atas denda GDPR yang diterbitkan atau dikenakan berdasarkan Pasal 83 GDPR terhadap pihak lain oleh lembaga pengawas atau badan pemerintah sehubungan dengan pelanggaran GDPR oleh pihak tersebut.

(c) This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement provided that the Standard Contractual Clauses will be governed as set out in section 13 of this DPA.

PPD ini akan diatur dan ditafsirkan sesuai dengan ketentuan hukum dan yurisdiksi yang diatur dalam Perjanjian, dengan ketentuan bahwa Klausul Kontrak Standar akan diatur sebagaimana dijelaskan pada bagian 13 dalam PPD ini.

SCHEDULE A / LAMPIRAN A

DETAILS OF THE PROCESSING / PERINCIAN PEMROSESAN

Description of Data Exporter / Deskripsi Pengekspor Data

The data exporter is the entity identified as the “Customer” or “Dynatrace”, as the case may be in case of any Sub-processing, in the Data Processing Agreement in place between data exporter and data importer and to which this Schedule is appended.

Pengekspor data adalah badan hukum yang diidentifikasi sebagai "Pelanggan" atau "Dynatrace", sebagaimana berlaku dalam hal Sub-pemrosesan, dalam Perjanjian Pemrosesan Data yang berlaku antara pengekspor data dan pengimpor data serta tempat Lampiran ini disematkan.

Description of Data Importer / Deskripsi Pengimpor Data

The data importer is the entity identified as “Dynatrace” or a duly authorized Sub-processor in the Data Processing Agreement in place between data exporter and data importer and to which this schedule is appended.

Pengimpor data adalah badan hukum yang diidentifikasi sebagai 'Dynatrace' atau Sub-pemroses yang berwenang dalam Perjanjian Pemrosesan Data yang berlaku antara pengekspor data dan pengimpor data serta tempat Lampiran ini disematkan.

Subject Matter and Duration of the Processing / Pokok Bahasan dan Durasi Pemrosesan

The subject-matter and duration of the processing is as follows:

Pokok bahasan dan durasi pemrosesan adalah sebagai berikut:

As between the parties, Customer shall be the Controller of certain Customer Personal Data provided to Dynatrace by Customer in connection to its use of Dynatrace Offerings. The duration of the processing shall be the term of the Agreement.
Di antara para pihak, Pelanggan akan menjadi Pengendali Data Pribadi Pelanggan tertentu yang diberikan kepada Dynatrace oleh Pelanggan sehubungan dengan penggunaan Penawaran Dynatrace. Durasi pemrosesan adalah masa berlaku Perjanjian.

Purposes of the Processing / Tujuan Pemrosesan The processing

is necessary for the following purposes:

Pemrosesan diperlukan dengan tujuan berikut:

To enable Dynatrace to provide the Dynatrace Offerings to Customer and exercise its rights and obligations under the Agreement.

Untuk memungkinkan Dynatrace memberikan Penawaran Dynatrace kepada Pelanggan dan melaksanakan hak dan kewajibannya berdasarkan Perjanjian.

Data Subjects / Subjek Data

The data subjects may include: (i) users authorized by the Customer to use the Dynatrace Offerings and (ii) users of or visitors to Customer’s monitored applications and/or websites (including but not limited to the Customer’s employees, customers or clients, agents, contractors, and advisors) as determined in the Customer’s sole discretion.

Subjek data dapat mencakup: (i) pengguna yang diberi izin oleh Pelanggan untuk menggunakan Penawaran Dynatrace dan (ii) pengguna atau pengunjung aplikasi dan/atau situs web yang dipantau oleh Pelanggan (termasuk tetapi tidak terbatas pada karyawan, pelanggan atau klien, agen, kontraktor, dan penasihat Pelanggan) sebagaimana ditentukan atas kebijaksanaan Pelanggan.

Type of Personal Data / Jenis Data Pribadi

Customer is required to provide certain Personal Data in order to use the Dynatrace Offerings, including IP address and first and last name if included in a user's e-mail address and user credentials. Customer may submit additional Personal Data to the Dynatrace Offerings, the extent of which is determined and controlled by Customer in its sole discretion.

Pelanggan wajib memberikan Data Pribadi tertentu untuk menggunakan Penawaran Dynatrace, termasuk alamat IP dan nama depan dan belakang jika disertakan dalam alamat email pengguna dan kredensial pengguna. Pelanggan dapat mengirimkan Data Pribadi tambahan ke Penawaran Dynatrace, yang detailnya ditentukan dan dikendalikan oleh Pelanggan atas kebijakannya sendiri.

Special categories of data or sensitive personal data (if appropriate) / Kategori data khusus atau data pribadi yang sensitif (jika ada)

The Personal Data transferred concern the following special categories of data or sensitive personal data:

Data Pribadi yang dipindahkan mencakupkategori data khusus atau data pribadi yang sensitif berikut ini:

Not applicable. Customer may not use the Dynatrace Offerings to process any data classified as "special category data" or "sensitive personal data" unless explicitly agreed in writing.

Tidak berlaku. Pelanggan tidak boleh menggunakan Penawaran Dynatrace untuk memproses data apa pun yang diklasifikasikan sebagai "data kategori khusus" atau "data pribadi sensitif" kecuali jika secara eksplisit disetujui secara tertulis.

Processing Operations / Operasi Pemrosesan

The personal data transferred will be subject to the following basic processing activities:

Data pribadi yang dipindahkan akan mengikuti kegiatan pemrosesan dasar berikut ini:

Dynatrace shall process the Customer Personal Data only as necessary to provide the Dynatrace Offerings and exercise its rights and obligations as contained in the terms of the Agreement and this Data Processing Agreement, including but not limited to customer enablement, technical support, professional services, improving Dynatrace Offerings performance and functions, user authentication and communications and account administration.

Dynatrace akan memproses Data Pribadi Pelanggan hanya jika diperlukan untuk menyediakan Penawaran Dynatrace dan melaksanakan hak dan kewajibannya sebagaimana tercantum dalam ketentuan Perjanjian dan Perjanjian Pemrosesan Data ini, termasuk tetapi tidak terbatas pada pemberdayaan pelanggan, dukungan teknis, jasa profesional, meningkatkan kinerja dan fungsi Penawaran Dynatrace, autentikasi pengguna serta komunikasi dan administrasi akun.

SCHEDULE B / LAMPIRAN B

SECURITY MEASURES / TINDAKAN KEAMANAN

Dynatrace (also referred to herein as the "Processor"), will implement, at least, the technical and organizational security measures described below in respect of the Customer Personal Data it Processes on behalf of the Customer (also referred to herein as the "Controller"). These security measures shall be applied to all Customer
Personal Data that is subject to the underlying agreement between the Processor and the Controller (the "Agreement"). In relation to third party sub-processors that may process Personal Data on Dynatrace's behalf, such third party will have its own security requirements to protect the Personal Data.

Dynatrace (yang dalam Perjanjian ini disebut juga sebagai "Pemroses"), akan menerapkan, setidaknya, tindakan keamanan teknis dan organisasi yang dijelaskan di bawah ini sehubungan dengan Data Pribadi Pelanggan yang diprosesnya atas nama Pelanggan (yang dalam Perjanjian ini disebut juga sebagai "Pengendali"). Tindakan keamanan ini akan diterapkan pada semua Data Pribadi Pelanggan yang sesuai dengan perjanjian yang mendasari antara Pemroses dan Pengendali ("Perjanjian"). Sehubungan dengan sub-pemroses pihak ketiga yang mungkin memproses Data Pribadi atas nama Dynatrace, pihak ketiga tersebut akan menerapkan persyaratan keamanannya sendiri untuk melindungi Data Pribadi.

Technical measures / Tindakan teknis

1.1 Authorization / Otorisasi

(a) An authorization system shall be used where different authorization profiles are used for different purposes.

Sistem otorisasi harus digunakan jika profil otorisasi yang berbeda digunakan untuk keperluan yang berbeda.

1.2 Identification / Identifikasi

(a) Every Authorized User must be issued with a personal and unique identification code for that purpose ("User ID"). A User ID may not be assigned to another person, even at a subsequent time.

Setiap Pengguna yang Sah harus diberi kode identifikasi pribadi dan unik untuk tujuan tersebut ("ID Pengguna"). ID Pengguna tidak dapat diberikan kepada orang lain, bahkan pada waktu berikutnya.

(b) An up-to-date record shall be kept of Authorized Users, and the authorized access available to each, and identification and authentication procedures shall be established for all access to information systems or for carrying out any Processing of Data. As used herein, "Processing" refers to any operation or set of operations which is performed on Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Catatan terbaru mengenai Pengguna yang Sah harus disimpan, serta akses yang sah bagi masing-masing pengguna, dan prosedur identifikasi serta autentikasi harus ditetapkan untuk semua akses ke sistem informasi atau untuk melakukan Pemrosesan Data apa pun.
Sebagaimana digunakan dalam Perjanjian ini, "Pemrosesan" mengacu pada setiap operasi atau serangkaian operasi yang dilakukan pada Data, baik dengan cara otomatis maupun tidak, seperti pengumpulan, pencatatan, penyusunan, penataan, penyimpanan, penyesuaian atau perubahan, pencarian, konsultasi, penggunaan, pengungkapan melalui transmisi, penyebarluasan, atau penyediaan, penyelarasan atau penggabungan, pembatasan, penghapusan, atau pemusnahan.

(c) Passwords shall be modified periodically as set forth in the Information Security Policies.

Kata sandi harus diubah secara berkala sebagaimana dijelaskan dalam Kebijakan Keamanan Informasi.

1.3 Authentication / Autentikasi

(a) Authorized Users shall be allowed to Process Data if they are provided with authentication credentials such as to successfully complete an authentication procedure relating either to a specific Processing operation or to a set of Processing operations.

Pengguna yang Sah dapat diizinkan untuk Memproses Data jika mereka diberi kredensial autentikasi yang memungkinkan mereka berhasil menyelesaikan prosedur autentikasi yang terkait dengan operasi Pemrosesan tertentu atau serangkaian operasi Pemrosesan.

(b) Authentication must be based on a secret password associated with User ID, and which password shall only be known to the Authorized User.

Autentikasi harus didasarkan pada kata sandi rahasia yang terkait dengan ID Pengguna, dan kata sandi tersebut hanya boleh diketahui oleh Pengguna yang Sah.

(c) One or more authentication credentials shall be assigned to, or associated with, an Authorized User.

Satu atau lebih kredensial autentikasi akan diberikan kepada, atau terkait dengan, Pengguna yang Sah.

(d) There must be a procedure for password confidentiality and integrity. Passwords must be stored in a way that makes them unintelligible while they remain valid. There must be a procedure for assigning, distributing and storing passwords.

Harus ada prosedur untuk kerahasiaan dan integritas kata sandi. Kata sandi harus disimpan dengan cara yang membuatnya tidak dapat dibaca selama masih berlaku. Harus ada prosedur untuk menetapkan, mendistribusikan, dan menyimpan kata sandi.

(e) Passwords shall consist of at least twelve characters, or, if this is not technically permitted by the relevant information systems, a password shall consist of the maximum permitted number of characters. Passwords shall not contain any item that can be easily related to the Authorized User in charge of the Processing and must be changed at regular intervals, which intervals must be set out in the security document. Passwords shall be modified by the Authorized User to a secret value known only to the Authorized User when it is first used and periodically thereafter.

Kata sandi harus terdiri dari setidaknya dua belas karakter, atau, jika hal ini tidak diizinkan secara teknis oleh sistem informasi terkait, kata sandi harus terdiri dari jumlah maksimum karakter yang diizinkan. Kata sandi tidak boleh mengandung item apa pun yang mudah dikaitkan dengan Pengguna yang Sah yang bertanggung jawab atas Pemrosesan dan harus diubah secara berkala, yang intervalnya harus dijelaskan dalam dokumen keamanan. Kata sandi harus diubah oleh Pengguna yang Sah menjadi nilai rahasia yang hanya diketahui oleh Pengguna yang Sah saat pertama kali digunakan dan secara berkala setelahnya.

(f) In addition to a valid user ID and password combination, all access to Dynatrace data or systems must be secured by a Multi-Factor Authentication (“MFA”) solution. The MFA solution can be either software or hardware in nature.

Selain ID pengguna dan kombinasi kata sandi yang benar, semua akses ke data atau sistem Dynatrace harus diamankan dengan solusi Autentikasi Multi-Faktor ("AMF"). Solusi AMF dapat berupa perangkat lunak atau perangkat keras.

(g) Authentication credentials shall be also de-activated if the Authorized User is terminated or transferred or de- authorized from accessing the information systems or Processing Data.

Kredensial autentikasi juga akan dinonaktifkan jika Pengguna yang Sah diberhentikan atau dipindahkan atau dibatalkan izinnya untuk mengakses sistem informasi atau Data Pemrosesan.

1.4 Access controls / Kendali akses

(a) Only Authorized Users shall have access to Data, including when stored on any electronic or portable media or when transmitted. Authorized Users shall have authorized access only to those data and resources necessary for them to perform their duties.

Hanya Pengguna yang Sah yang dapat mengakses Data, termasuk saat disimpan di media elektronik atau media portabel apa pun atau saat dikirimkan. Pengguna yang Sah hanya memiliki akses yang sah ke data dan sumber daya yang diperlukan untuk melaksanakan tugas mereka.

(b) A system for granting Authorized Users access to designated data and resources shall be used.

Sistem untuk memberikan akses kepada Pengguna yang Sah ke data dan sumber daya yang ditentukan harus digunakan.

(c) It shall be verified semi-annually, that the prerequisites for retaining the relevant authorization profiles still apply. This may also include the list of Authorized Users drawn up by homogeneous categories of task and corresponding authorization profile.

Sistem ini harus diverifikasi setiap setengah tahun, sehingga prasyarat untuk mempertahankan profil autorisasi yang relevan tetap berlaku. Sistem ini juga dapat mencakup daftar Pengguna yang Sah yang dibuat berdasarkan kategori tugas yang homogen dan profil autorisasi yang sesuai.

(d) Measures shall be put in place to prevent a user gaining unauthorized access to, or use of, the information systems. In particular, intrusion detection systems reflecting industry best practice should be installed to protect the information systems from unauthorized access.

Beberapa tindakan harus dilakukan untuk mencegah pengguna mendapatkan akses yang tidak sah ke, atau menggunakan, sistem informasi. Lebih jelasnya, sistem deteksi penyusupan yang mencerminkan praktik terbaik industri harus dipasang untuk melindungi sistem informasi dari akses yang tidak sah.

(e) Operating system or database access controls must be correctly configured to ensure authorized access only.

Sistem operasi atau kendali akses basis data harus dikonfigurasi dengan benar untuk memastikan akses yang sah saja.

(f) Only those staff authorized shall be able to grant, alter or cancel access by users to the information systems.

Hanya staf yang sah yang dapat memberikan, mengubah, atau membatalkan akses pengguna ke sistem informasi.

1.5 Management of computer systems and removable media / Manajemen sistem komputer dan media yang dapat dipindahkan

(a) Network information systems and physical media storing Data must be housed in a secure environment with physical access restricted to staff that are authorized to have such access. Strong authorization and access controls must be maintained.

Sistem informasi jaringan dan media fisik yang menyimpan Data harus ditempatkan di lingkungan yang aman dengan akses fisik yang dibatasi hanya untuk staf yang berwenang untuk memiliki akses tersebut. Autorisasi dan kendali akses yang kuat harus dipertahankan.

(b) The software, firmware and hardware used in the information systems shall be reviewed annually in order to detect vulnerabilities and flaws in the information systems and resolve such vulnerabilities and flaws.

Perangkat lunak, firmware, dan perangkat keras yang digunakan dalam sistem informasi harus ditinjau setiap tahun untuk mendeteksi kerentanan dan kelemahan dalam sistem informasi serta mengatasi kerentanan dan kelemahan tersebut.

(c) Policies and training shall be issued with regard to keeping and using media on which Data are stored in order to prevent unauthorized access and Processing.

Kebijakan dan pelatihan harus disediakan terkait penyimpanan dan penggunaan media tempat menyimpan Data untuk mencegah akses dan Pemrosesan yang tidak sah.

(d) When media are to be disposed of or reused, necessary measures shall be taken to prevent any subsequent retrieval of the Data and other information previously stored on them, or to otherwise make the information intelligible or be re-constructed by any technical means before they are withdrawn from the inventory. All reusable media used for the storage of Data will be

overwritten a minimum of three times with randomized data prior to disposal or re-use.

Ketika media akan dibuang atau digunakan kembali, tindakan yang diperlukan harus dilakukan untuk mencegah pengambilan Data dan informasi lain yang sebelumnya tersimpan di dalamnya, atau untuk membuat informasi tersebut dapat dibaca atau direkonstruksi dengan cara teknis apa pun sebelum media tersebut dikeluarkan dari inventaris. Semua media yang dapat digunakan kembali yang digunakan untuk penyimpanan Data akan ditimpa minimal tiga kali dengan data acak sebelum dibuang atau digunakan kembali.

(e) The removal of media containing Data from the designated premises must be specifically authorized by the Controller and in compliance with Dynatrace policies.

Pembuangan media yang berisi Data dari tempat yang ditentukan harus diberi izin secara khusus oleh Pengendali dan sesuai dengan kebijakan Dynatrace.

(f) Media containing Data must be erased or rendered unreadable if it is no longer used and prior to proper disposal.

Media yang berisi Data harus dihapus atau dibuat tidak dapat dibaca jika sudah tidak digunakan lagi dan sebelum dibuang dengan benar.

1.6 Distribution or transmission / Distribusi atau pengiriman

(a) Data must only be available to Authorized Users.

Data hanya boleh tersedia bagi Pengguna yang Sah.

(b) Encryption (128-bit or stronger) or another equivalent form of protection must be used to protect Data that is electronically transmitted over a public network or stored on a portable device, or where there is a requirement to store or Process Data in a physically insecure environment.

Enkripsi (128-bit atau lebih kuat) atau bentuk perlindungan lain yang setara harus digunakan untuk melindungi Data yang dikirimkan secara elektronik melalui jaringan publik atau disimpan di perangkat portabel, atau jika ada persyaratan untuk menyimpan atau Memproses Data di lingkungan yang tidak aman secara fisik.

(c) When Data are to leave the designated premises as a result of maintenance operations, the necessary measures shall be taken to prevent any unauthorized retrieval of the Data and other information stored therein.

Jika Data harus keluar dari lokasi yang ditentukan karena operasi pemeliharaan, tindakan yang diperlukan harus dilakukan untuk mencegah pengambilan Data dan informasi lain yang tersimpan di dalamnya secara tidak sah.

(d) Where Data is transmitted or transferred over an electronic communications network, measures shall be put in place to control the flow of data and record the timing of the transmission or transfer, the Data transmitted or transferred, the destination of any Data transmitted or transferred, and details of the Authorized User conducting the transmission or transfer.

Jika Data dikirimkan atau dipindahkan melalui jaringan komunikasi elektronik, tindakan harus dilakukan untuk mengendalikan aliran data dan mencatat waktu pengiriman atau pemindahan, Data yang dikirimkan atau dipindahkan, tujuan Data yang dikirimkan atau dipindahkan, dan detail Pengguna yang Sah yang melakukan pengiriman atau pemindahan.

1.7 Preservation, back-up copies and recovery / Pelestarian, salinan cadangan, dan pemulihan

(a) Procedures must be defined and laid down for making back-up copies and for recovering Data. These procedures must provide for Data to be reconstructed in the state they were in at the time they were lost or destroyed.

Prosedur harus ditetapkan dan ditentukan untuk membuat salinan cadangan dan untuk pemulihan Data. Prosedur ini harus memungkinkan Data direkonstruksi ke kondisi semula pada saat Data tersebut hilang atau musnah.

(b) Back-up copies must be made at least once a week, unless no Data have been updated during that period.

Salinan cadangan harus dibuat setidaknya sekali seminggu, kecuali jika tidak ada Data yang telah diperbarui selama periode tersebut.

(c) A back-up copy and data recovery procedures must be kept at a different location from the site of the information systems Processing the Data and these minimum security requirements shall apply to such back- up copies.

Salinan cadangan dan prosedur pemulihan data harus disimpan di lokasi yang berbeda dengan lokasi sistem informasi yang Memproses Data dan persyaratan keamanan minimum ini akan berlaku untuk salinan cadangan tersebut.

1.8 Anti-virus and intrusion detection / Deteksi anti-virus dan penyusupan

(a) Anti-virus software and intrusion detection systems should be installed on the information systems to protect against attacks or other unauthorized acts in respect of information systems. Antivirus software and intrusion detection systems should be updated regularly in accordance with the industry best practice for the information systems concerned (and at least annually).

Perangkat lunak anti-virus dan sistem deteksi penyusupan harus dipasang pada sistem informasi untuk melindunginya dari serangan atau tindakan tidak sah lainnya sehubungan dengan sistem informasi. Perangkat lunak antivirus dan sistem deteksi penyusupan harus diperbarui secara berkala sesuai dengan praktik terbaik industri untuk sistem informasi yang bersangkutan (dan setidaknya setiap tahun).

1.9 Testing / Pengujian

(a) Testing prior to the implementation or modification of the information systems Processing Data shall not use real or ‘live’ data unless such use is necessary and there is no reasonable alternative. Where real or ‘live’ data is used, it shall be limited to the extent necessary for the purposes of testing and the level of security corresponding to the type of Data Processed must be guaranteed.

Pengujian sebelum penerapan atau perubahan sistem informasi Pemrosesan Data tidak boleh menggunakan data nyata atau data 'langsung' kecuali jika penggunaan tersebut diperlukan dan tidak ada alternatif yang wajar. Jika menggunakan data nyata atau 'langsung', data tersebut harus dibatasi sejauh yang diperlukan untuk keperluan pengujian dan harus dijamin tingkat keamanannya sesuai dengan jenis Data yang Diproses.

1.10 Audit

(a) Regular audits of compliance with these security requirements, at least annually, should be performed.

Audit rutin atas kepatuhan terhadap persyaratan keamanan ini harus dilakukan setidaknya setiap tahun.

(b) The results must provide an opinion on the extent to which the security measures and controls adopted comply with these security requirements, identify any shortcomings and (if any) propose corrective or supplementary measures as necessary. It should also include the data, facts and observations on which the opinions reached, and the recommendations proposed.

Hasilnya harus memberikan pendapat tentang sejauh mana tindakan keamanan dan pengendalian yang diterapkan sesuai dengan persyaratan keamanan ini, mengidentifikasi setiap kekurangan dan (jika ada) mengusulkan tindakan perbaikan atau tambahan yang diperlukan. Audit ini juga harus mencakup data, fakta, dan pengamatan yang mendasari opini yang disimpulkan, serta rekomendasi yang diajukan.

2. Organizational measures / Tindakan organisasi

2.1 Security plan and document / Rencana dan dokumen keamanan

- The measures adopted to comply with these security requirements shall be the subject of the Company’s Information Security Policies and set out in a security portal, which shall be kept up to date, and revised whenever relevant changes are made to the information system(s) or to technical or organizational measures.

  Tindakan yang dilakukan untuk memenuhi persyaratan keamanan ini harus sesuai dengan Kebijakan Keamanan Informasi Perusahaan dan dijelaskan di portal keamanan, yang harus selalu diperbarui, dan direvisi setiap kali ada perubahan yang relevan pada sistem informasi atau tindakan teknis atau organisasi.

- The Information Security Policies shall address:

  Kebijakan Keamanan Informasi harus membahas:

  (i) Security measures relating to the modification and maintenance of the system(s) used to Process Data, including development and maintenance of applications, appropriate vendor support and an inventory of hardware and software;

Tindakan keamanan yang berkaitan dengan perubahan dan pemeliharaan sistem yang digunakan untuk Memproses Data, termasuk pengembangan dan pemeliharaan aplikasi, dukungan vendor yang sesuai, dan inventaris perangkat keras serta perangkat lunak;

(ii) Physical security, including security of the buildings or premises where Data Processing occurs, security of data equipment and telecommunication infrastructure and environmental controls; and

Keamanan fisik, termasuk keamanan gedung atau tempat Pemrosesan Data dilakukan, keamanan peralatan data dan infrastruktur telekomunikasi serta pengendalian lingkungan; dan

(iii) Security of computers and telecommunication systems including procedures for managing back-up copies, procedures dealing with computer viruses, procedures for managing signal/codes, security for software implementation, security related to databases, security for connecting systems to the Internet, inspection of circumvention of data system(s), mechanisms for keeping account of attempts to break system security or gain unauthorized access.

Keamanan komputer dan sistem telekomunikasi termasuk prosedur untuk mengelola salinan cadangan, prosedur untuk menangani virus komputer, prosedur untuk mengelola sinyal/kode, keamanan untuk penerapan perangkat lunak, keamanan yang terkait dengan basis data, keamanan untuk menghubungkan sistem ke Internet, pemeriksaan terhadap usaha mengelabui sistem data, mekanisme untuk mencatat usaha untuk membobol keamanan sistem atau mendapatkan akses yang tidak sah.

- The security plan shall include all Dynatrace policies, as updated from time to time, including but not limited to:

Rencana keamanan harus mencakup semua kebijakan Dynatrace, yang sewaktu-waktu diperbarui, termasuk tetapi tidak terbatas pada:

(i) Code of Business Conduct and Ethics Pedoman Perilaku dan Etika Bisnis

(ii) Global Data Protection Policy
Kebijakan Perlindungan Data Global

(iii) Dynatrace IT Acceptable Use Policy
Kebijakan Penggunaan TI yang Dapat Diterima Dynatrace

(iv) System Security Policies: Dynatrace Access Control Management Policy; Backup Retention Standard; Change Management Policy; Change Management Policy - Business Systems; Compliance Policy ; Cyber and Data Security Incident Response Plan; Data Classification Policy; Data Loss Prevention Policy; Electronic Monitoring Policy; Encryption Policy; Human Resources Security Policy; Information Resource Management Policy; Information Risk Management Policy; IT Operations Policy; Mobile Device Policy; Network Access Policy; Network Account Password Policy; Network Firewall Policy; Physical Security & Environmental Policy; Returning of Assets for Terminated Employees Policy; Secure; Security Phishing Policy; Service Account Lifecycle Policy; Vendor Management Policy; Vulnerability Management Policy; Workstation Security Policy.

Kebijakan Keamanan Sistem: Kebijakan Manajemen Kendali Akses Dynatrace; Standar Penyimpanan Cadangan; Kebijakan Manajemen Perubahan; Kebijakan Manajemen Perubahan - Sistem Bisnis; Kebijakan Kepatuhan; Rencana Tanggap Insiden Keamanan Siber dan Data; Kebijakan Klasifikasi Data; Kebijakan Pencegahan Kehilangan Data; Kebijakan Pemantauan Elektronik; Kebijakan Enkripsi; Kebijakan Keamanan Sumber Daya Manusia; Kebijakan Manajemen Sumber Daya Informasi; Kebijakan Manajemen Risiko Informasi; Kebijakan Operasi TI; Kebijakan Perangkat Seluler; Kebijakan Akses Jaringan; Kebijakan Kata Sandi Akun Jaringan; Kebijakan Firewall Jaringan; Kebijakan Keamanan Fisik & Lingkungan; Kebijakan Pengembalian Aset bagi Karyawan yang di-PHK;

Pengamanan; Kebijakan Phishing Keamanan; Kebijakan Masa Pakai Akun Jasa; Kebijakan Manajemen Vendor; Kebijakan Manajemen Kerentanan; Kebijakan Keamanan Tempat Kerja.

(v) The security plan shall be available to staff who have access to Data and the information systems, and must cover the following aspects at a minimum:
Rencana keamanan harus tersedia bagi staf yang memiliki akses ke Data dan sistem informasi, dan minimal harus mencakup aspek-aspek berikut:

(vi) The scope, with a detailed specification of protected resources;
Ruang lingkup, dengan spesifikasi terperinci sumber daya yang dilindungi;

(vii) The measures, standards, procedures, code of conduct rules and norms to guarantee security, including the control, inspection and supervision of the information systems; Tindakan, standar, prosedur, aturan pedoman perilaku dan norma untuk menjamin keamanan, termasuk pengendalian, pemeriksaan, dan pengawasan sistem informasi;

(viii)The procedures for reporting, managing and responding to incidents; and Prosedur untuk melaporkan, mengelola, dan menanggapi insiden; dan

(ix) The procedures for making back-up copies and recovering Data including the member of staff who undertook the Processing activity, the Data restored and, as appropriate, which data had to be input manually in the recovery process.
Prosedur untuk membuat salinan cadangan dan memulihkan Data termasuk anggota staf yang melakukan kegiatan Pemrosesan, pemulihan Data dan, jika perlu, penentuan data yang harus dimasukkan secara manual dalam proses pemulihan.

2.2 Functions and obligations of staff / Fungsi dan kewajiban staf

- Only members of staff that have a legitimate operational need to access the information systems or carry out any Processing of Data shall be authorized to do so (“Authorized Users”).

  Hanya anggota staf yang memiliki kebutuhan operasional yang sah untuk mengakses sistem

  informasi atau melakukan Pemrosesan Data yang diizinkan untuk melakukannya ("Pengguna yang Sah").

- The necessary measures shall be adopted to train and make staff familiar with these minimumsecurity requirements, any relevant policies and applicable laws concerning the performance of their functions and duties in respect of the Processing of Data and the consequences of any breach of these requirements.

  Tindakan yang diperlukan harus dilakukan untuk melatih dan membiasakan staf dengan persyaratan keamanan minimum ini, kebijakan yang relevan, dan hukum yang berlaku terkait pelaksanaan fungsi dan tugas mereka sehubungan dengan Pemrosesan Data dan konsekuensi dari setiap pelanggaran persyaratan ini.

- The functions and obligations of staff having access to Data and the information systems shall be clearly defined through application security roles.

  Fungsi dan kewajiban staf yang memiliki akses ke Data dan sistem informasi harus didefinisikan dengan jelas melalui peran keamanan aplikasi.

- Authorized Users shall be instructed to the effect that electronic equipment should not be left unattended or made accessible during Processing sessions. Physical access to areas where any Data is stored shall be restricted to Authorized Users. The disciplinary measures for a breach of the security plan shall be clearly defined and documented and communicated to staff.

  Pengguna yang Sah harus diberi tahu bahwa peralatan elektronik tidak boleh ditinggalkan tanpa pengawasan atau dapat diakses selama sesi Pemrosesan. Akses fisik ke tempat penyimpanan Data harus dibatasi hanya untuk Pengguna yang Sah. Tindakan hukuman atas pelanggaran rencana keamanan harus didefinisikan dengan jelas dan didokumentasikan serta disampaikan kepada staf.

2.3 Chief Security Officer / Direktur Keamanan

- A person or persons responsible for the overall compliance with these minimum-security requirements shall be designated as the Chief Information Security Officer (“CISO”). The CISO shall be suitably trained and experienced in managing information security and provided with appropriate resources to effectively ensure compliance.

  Seseorang atau beberapa orang yang bertanggung jawab atas seluruh kepatuhan terhadap persyaratan keamanan minimum ini akan ditunjuk sebagai Direktur Keamanan Informasi ("CISO"). CISO harus terlatih dan berpengalaman dalam mengelola keamanan informasi dan dilengkapi dengan sumber daya yang sesuai untuk memastikan kepatuhan secara efektif.

- The contact details of the CISO shall be provided to the Controller upon request.

  Detail kontak CISO harus diberikan kepada Pengendali jika diminta.

2.4 Record keeping / Penyimpanan catatan

- A history of Authorized User access to, or disclosure of, Data shall be recorded with a secure audit trail.

  Riwayat akses Pengguna yang Sah ke, atau pengungkapan, Data harus dicatat dengan jejak audit yang aman.

- Only those staff duly authorized may have physical access to the premises where information systems and media storing Data are stored.

  Hanya staf yang sah yang dapat memiliki akses fisik ke lokasi tempat sistem informasi dan media penyimpanan Data disimpan.

- There shall be a procedure for reporting, responding to and managing security incidents such as data security breaches. This shall include at a minimum:

  Harus ada prosedur untuk melaporkan, menanggapi, dan mengelola insiden keamanan seperti pelanggaran keamanan data. Hal ini minimal harus mencakup:

  (i) A procedure for reporting such incidents/breaches to appropriate management;

  Prosedur untuk melaporkan insiden/pelanggaran tersebut kepada manajemen yang tepat;

  (ii) A clearly designated team for managing and coordinating the response to an incident led by the CISO;

  Tim yang ditunjuk dengan jelas untuk mengelola dan mengoordinasikan respons terhadap insiden yang dipimpin oleh CISO;

  (iii) A documented process for managing the response to an incident including the requirement to keep appropriate issues and action logs to include the time at which the incident occurred, the person reporting the incident, to whom it was reported and the effects thereof;

  Proses yang terdokumentasi untuk mengelola respons terhadap suatu insiden termasuk persyaratan untuk menyimpan catatan masalah dan tindakan yang sesuai untuk memasukkan waktu terjadinya insiden, orang yang melaporkan insiden, kepada siapa insiden tersebut dilaporkan, dan dampaknya;

  (iv) The requirement on the Processor to notify the Controller without undue delay if there is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Data transmitted, stored or otherwise processed by Processor; and

  Persyaratan bagi Pemroses untuk memberi tahu Pengendali tanpa penundaan yang tidak semestinya jika terjadi pelanggaran keamanan yang menyebabkan pemusnahan, kehilangan, perubahan yang tidak sengaja atau melanggar hukum, pengungkapan, atau akses yang tidak sah ke, Data yang dikirim, disimpan, atau diproses oleh Pemroses; dan

(v) The Processor security/incident management team should where appropriate work together with the Controller security representatives until the incident or breach has been satisfactorily resolved.

Tim manajemen keamanan/insiden Pemroses harus bekerja sama dengan perwakilan keamanan Pengendali jika diperlukan hingga insiden atau pelanggaran diselesaikan dengan memuaskan.

(vi) The procedure for reporting, managing and responding to incidents shall be tested at least once a year.

Prosedur untuk melaporkan, mengelola, dan menanggapi insiden harus diuji setidaknya satu tahun sekali.