PERSONAL DATA PROCESSING AGREEMENT FOR SAP CLOUD SERVICES/
PERJANJIAN PEMROSESAN DATA PRIBADI UNTUK LAYANAN CLOUD SAP

1. BACKGROUND/ LATAR BELAKANG

1.1 Purpose and Application. This document ("**DPA**") is incorporated into the Agreement and forms part of a written (including in electronic form) contract between SAP and Customer. This DPA applies to Personal Data processed by SAP and its Subprocessors in connection with its provision of the Cloud Service. This DPA does not apply to non-production environments of the Cloud Service if such environments are made available by SAP, and Customer shall not store Personal Data in such environments./

Tujuan dan Aplikasi. Dokumen ini ("**DPA**") digabungkan ke dalam Perjanjian dan merupakan bagian dari kontrak tertulis (termasuk dalam bentuk elektronik) antara SAP dan Pelanggan. DPA ini berlaku untuk Data Pribadi yang diproses oleh SAP dan Subprosesornya dalam kaitannya dengan ketentuan Layanan Cloud-nya. DPA ini tidak berlaku untuk lingkungan non-produksi dari Layanan Cloud jika lingkungan tersebut disediakan oleh SAP, dan Pelanggan tidak boleh menyimpan Data Pribadi dalam lingkungan tersebut.

1.2 Structure. Appendices 1 and 2 are incorporated into and form part of this DPA. They set out the agreed subject-matter, the nature and purpose of the processing, the type of Personal Data, categories of data subjects and the applicable technical and organizational measures./

Struktur. Lampiran 1 dan 2 digabungkan ke dalam dan merupakan bagian dari DPA ini. Keduanya menetapkan pokok masalah yang disepakati, sifat dan tujuan pemrosesan, jenis Data Pribadi, kategori subjek data dan tindakan teknis dan organisasional yang berlaku.

1.3 GDPR. SAP and Customer agree that it is each party's responsibility to review and adopt requirements imposed on Controllers and Processors by the General Data Protection Regulation 2016/679 ("**GDPR**"), in particular with regards to Articles 28 and 32 to 36 of the GDPR, if and to the extent applicable to Personal Data of Customer/Controllers that is processed under the DPA. For illustration purposes, Appendix 3 lists the relevant GDPR requirements and the corresponding sections in this DPA./

GDPR. SAP dan Pelanggan setuju bahwa masing-masing pihak bertanggung jawab untuk meninjau dan mengadopsi persyaratan yang diberlakukan pada Pengendali dan Prosesor oleh Peraturan Perlindungan Data Umum 2016/679 ("**GDPR**"), khususnya dalam kaitannya dengan Pasal 28 dan 32 hingga 36 GDPR, jika berlaku dan untuk lingkup yang berlaku pada Data Pribadi Pelanggan/Pengendali yang diproses berdasarkan DPA. Sebagai ilustrasi, Lampiran 3 mencantumkan persyaratan GDPR yang relevan dan bagian yang terkait dalam DPA ini.

1.4 Governance. SAP acts as a Processor and Customer and those entities that it permits to use the Cloud Service act as Controllers under the DPA. Customer acts as a single point of contact and is solely responsible for obtaining any relevant authorizations, consents and permissions for the processing of Personal Data in accordance with this DPA, including, where applicable approval by Controllers to use SAP as a Processor. Where authorizations, consent, instructions or permissions are provided by Customer these are provided not only on behalf of the Customer but also on behalf of any other Controller using the Cloud Service. Where SAP informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to use the Cloud Service and it is Customer's responsibility to forward such information and notices to the relevant Controllers./

Tata Kelola. SAP bertindak sebagai Prosesor dan Pelanggan dan entitas-entitas yang diizinkan untuk menggunakan Layanan Cloud bertindak sebagai Pengendali berdasarkan DPA. Pelanggan bertindak sebagai satu titik kontak dan sepenuhnya bertanggung jawab untuk memeroleh otorisasi, persetujuan, dan izin yang relevan untuk pemrosesan Data Pribadi menurut DPA ini, termasuk, jika berlaku, persetujuan dari Pengendali untuk menggunakan SAP sebagai Prosesor. Jika otorisasi, persetujuan, instruksi atau izin diberikan oleh Pelanggan, semua ini disediakan

tidak hanya atas nama Pelanggan tetapi juga atas nama Pengendali lain yang menggunakan Layanan Cloud. Jika SAP memberikan informasi atau menyampaikan pemberitahuan kepada Pelanggan, informasi atau pemberitahuan tersebut dianggap diterima oleh Pengendali yang memperoleh izin dari Pelanggan untuk menggunakan Layanan Cloud dan merupakan tanggung jawab Pelanggan untuk meneruskan informasi dan pemberitahuan tersebut kepada Pengendali yang relevan.

2. SECURITY OF PROCESSING/ KEAMANAN PEMROSESAN

2.1 Appropriate Technical and Organizational Measures. SAP has implemented and will apply the technical and organizational measures set forth in Appendix 2. Customer has reviewed such measures and agrees that as to the Cloud Service selected by Customer in the Order Form the measures are appropriate taking into account the state of the art, the costs of implementation, nature, scope, context and purposes of the processing of Personal Data./

Tindakan Teknis dan Organisasional yang Sesuai. SAP telah melaksanakan dan akan menerapkan tindakan teknis dan organisasional yang ditetapkan dalam Lampiran 2. Pelanggan telah meninjau tindakan tersebut dan setuju bahwa untuk Layanan Cloud yang dipilih oleh Pelanggan dalam Formulir Pesanan, tindakan tersebut sesuai dengan perkembangan terbaru, biaya pelaksanaan, sifat, ruang lingkup, konteks, dan tujuan pemrosesan Data Pribadi.

2.2 Changes. SAP applies the technical and organizational measures set forth in Appendix 2 to SAP's entire customer base hosted out of the same Data Center and receiving the same Cloud Service. SAP may change the measures set out in Appendix 2 at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data./

Perubahan. SAP menerapkan tindakan teknis dan organisasional yang ditetapkan dalam Lampiran 2 untuk seluruh basis pelanggan SAP yang di-hosting dari Pusat Data yang sama dan menerima Layanan Cloud yang sama. SAP dapat mengubah tindakan yang ditetapkan dalam Lampiran 2 setiap saat tanpa pemberitahuan asalkan SAP mempertahankan tingkat keamanan yang sebanding atau lebih baik. Tindakan individu dapat diganti dengan tindakan baru yang berfungsi untuk tujuan yang sama tanpa mengurangi tingkat keamanan yang melindungi Data Pribadi.

3. SAP OBLIGATIONS/ KEWAJIBAN SAP

3.1 Instructions from Customer. SAP will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes such documented initial instructions and each use of the Cloud Service then constitutes further instructions. SAP will use reasonable efforts to follow any other Customer instructions, as long as they are required by Data Protection Law, technically feasible and do not require changes to the Cloud Service. If any of the before-mentioned exceptions apply, or SAP otherwise cannot comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, SAP will immediately notify Customer (email permitted)./

Instruksi untuk Pelanggan. SAP akan memproses Data Pribadi sesuai dengan instruksi yang didokumentasikan dari Pelanggan saja. Perjanjian (termasuk DPA ini) merupakan instruksi awal terdokumentasi tersebut dan setiap penggunaan Layanan Cloud nantinya merupakan bagian dari instruksi lebih lanjut. SAP akan melakukan upaya yang wajar untuk mengikuti setiap instruksi Pelanggan lainnya, jika semua itu diwajibkan oleh Undang-undang Perlindungan Data, yang secara teknis layak dan tidak memerlukan perubahan pada Layanan Cloud. Jika ada pengecualian yang disebutkan sebelumnya dan telah berlaku, atau SAP tidak dapat mematuhi instruksi atau

berpendapat bahwa instruksi melanggar Undang-undang Perlindungan Data, SAP akan segera memberi tahu Pelanggan (email diizinkan).

3.2 **Processing on Legal Requirement.** SAP may also process Personal Data where required to do so by applicable law. In such a case, SAP shall inform Customer of that legal requirement before processing unless that law prohibits such information on important grounds of public interest./
Menjalankan proses berdasarkan Persyaratan Hukum. SAP juga dapat memproses Data Pribadi jika diharuskan untuk melakukannya oleh hukum yang berlaku. Jika demikian, SAP harus menginformasikan persyaratan hukum tersebut kepada Pelanggan sebelum memproses data kecuali jika undang-undang tersebut melarang informasi semacam itu karena alasan penting yang berkaitan dengan kepentingan publik.

3.3 **Personnel.** To process Personal Data, SAP and its Subprocessors shall only grant access to authorized personnel who have committed themselves to confidentiality. SAP and its Subprocessors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures./
Personel. Untuk memproses Data Pribadi, SAP dan Subprosesornya hanya akan memberikan akses ke personel resmi yang telah berkomitmen untuk menjaga kerahasiaan. SAP dan Subprosesornya secara teratur akan melatih personel yang memiliki akses ke Data Pribadi dalam keamanan data yang berlaku dan tindakan privasi data.

3.4 **Cooperation.** At Customer's request, SAP will reasonably cooperate with Customer and Controllers in dealing with requests from Data Subjects or regulatory authorities regarding SAP's processing of Personal Data or any Personal Data Breach. SAP shall notify the Customer as soon as reasonably practical about any request it has received from a Data Subject in relation to the Personal Data processing, without itself responding to such request without Customer's further instructions, if applicable. SAP shall provide functionality that supports Customer's ability to correct or remove Personal Data from the Cloud Service, or restrict its processing in line with Data Protection Law. Where such functionality is not provided, SAP will correct or remove any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Data Protection Law./
Kerja Sama. Atas permintaan Pelanggan, SAP akan bekerja sama dengan cara yang dinilai baik dengan Pelanggan dan Pengendali untuk menangani permintaan dari Subjek Data atau otoritas hukum terkait pemrosesan Data Pribadi milik SAP atau setiap Pelanggaran Data Pribadi. SAP akan memberi tahu Pelanggan sesegera mungkin tentang permintaan apa pun yang diterimanya dari Subjek Data sehubungan dengan pemrosesan Data Pribadi, tanpa menanggapi permintaan tersebut di luar instruksi lebih lanjut dari Pelanggan, jika berlaku. SAP harus menyediakan fungsionalitas yang mendukung kemampuan Pelanggan untuk memperbaiki atau menghapus Data Pribadi dari Layanan Cloud, atau membatasi pemrosesannya sesuai dengan Undang-undang Perlindungan Data. Jika fungsionalitas tersebut tidak tersedia, SAP akan mengoreksi atau menghapus Data Pribadi apa pun, atau membatasi pemrosesan, sesuai dengan instruksi Pelanggan dan Undang-undang Perlindungan Data.

3.5 **Personal Data Breach Notification.** SAP will notify Customer without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Data Protection Law. SAP may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by SAP./
Pemberitahuan Pelanggaran Data Pribadi. SAP akan memberi tahu Pelanggan tanpa penundaan yang tidak semestinya setelah mengetahui adanya Pelanggaran Data Pribadi dan memberikan informasi yang dinilai baik untuk membantu Pelanggan memenuhi kewajiban Pelanggan untuk melaporkan Pelanggaran Data Pribadi sebagaimana disyaratkan menurut Undang-undang Perlindungan Data. SAP dapat memberikan informasi tersebut secara bertahap saat tersedia. Pemberitahuan tersebut tidak boleh ditafsirkan atau dipahami sebagai pengakuan kesalahan atau pertanggungjawaban oleh SAP.

3.6 **Data Protection Impact Assessment.** If, pursuant to Data Protection Law, Customer (or its Controllers) are required to perform a data protection impact assessment or prior consultation with a regulator, at Customer's request, SAP will provide such documents as are generally available for the Cloud Service (for example, this DPA, the Agreement, audit reports or certifications). Any additional assistance shall be mutually agreed between the Parties./

Penilaian Dampak Perlindungan Data. Jika, sesuai dengan Undang-undang Perlindungan Data, Pelanggan (atau Pengendalinya) diharuskan untuk melakukan penilaian dampak perlindungan data atau konsultasi sebelumnya dengan regulator, atas permintaan Pelanggan, SAP akan memberikan dokumen seperti yang umumnya tersedia untuk Layanan Cloud (misalnya, DPA ini, Perjanjian, laporan audit atau sertifikasi). Setiap bantuan tambahan harus disepakati bersama oleh Para Pihak.

4. DATA EXPORT AND DELETION/ EKSPOR DAN PENGHAPUSAN DATA

4.1 **Export and Retrieval by Customer.** During the Subscription Term and subject to the Agreement, Customer can access its Personal Data at any time. Customer may export and retrieve its Personal Data in a standard format. Export and retrieval may be subject to technical limitations, in which case SAP and Customer will find a reasonable method to allow Customer access to Personal Data./

Ekspor dan Pengambilan oleh Pelanggan. Selama Jangka Waktu Langganan dan sesuai dengan Perjanjian, Pelanggan dapat mengakses Data Pribadinya kapan saja. Pelanggan dapat mengekspor dan mengambil Data Pribadinya dalam format standar. Ekspor dan pengambilan dapat diatur menurut batasan teknis, dalam hal ini SAP dan Pelanggan harus menemukan metode yang dianggap baik untuk mengizinkan Pelanggan mengakses Data Pribadi.

4.2 **Deletion.** Before the Subscription Term expires, Customer may use SAP's self-service export tools (as available) to perform a final export of Personal Data from the Cloud Service (which shall constitute a "return" of Personal Data). At the end of the Subscription Term, Customer hereby instructs SAP to delete the Personal Data remaining on servers hosting the Cloud Service within a reasonable time period in line with Data Protection Law (not to exceed six months) unless applicable law requires retention./

Penghapusan. Sebelum Jangka Waktu Langganan berakhir, Pelanggan dapat menggunakan *tool* ekspor mandiri milik SAP (jika tersedia) untuk melakukan ekspor akhir Data Pribadi dari Layanan Cloud (yang merupakan bagian dari "pengembalian" Data Pribadi). Di akhir Jangka Waktu Langganan, Pelanggan dengan ini memerintahkan SAP untuk menghapus Data Pribadi yang tersisa pada server yang meng-hosting Layanan Cloud dalam jangka waktu yang wajar sesuai dengan Undang-undang Perlindungan Data (tidak lebih dari enam bulan) kecuali jika hukum yang berlaku mengharuskan penyimpanan.

5. CERTIFICATIONS AND AUDITS/ SERTIFIKASI DAN AUDIT

5.1 **Customer Audit.** Customer or its independent third party auditor reasonably acceptable to SAP (which shall not include any third party auditors who are either a competitor of SAP or not suitably qualified or independent) may audit SAP's control environment and security practices relevant to Personal Data processed by SAP only if:/

Audit Pelanggan. Pelanggan atau auditor pihak ketiga independennya yang secara wajar dapat diterima oleh SAP (yang tidak mencakup auditor pihak ketiga mana pun yang merupakan pesaing SAP atau yang tidak memenuhi kualifikasi atau tidak independen) dapat mengaudit praktik lingkungan dan keamanan pengendalian SAP yang relevan dengan Data Pribadi yang diproses oleh SAP hanya jika:

(a) SAP has not provided sufficient evidence of its compliance with the technical and organizational measures that protect the production systems of the Cloud Service through providing either: (i) a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or (ii) a valid ISAE3402 and/or ISAE3000 or other SOC1-3 attestation report. Upon Customer's request audit reports or ISO certifications are available through the third party auditor or SAP;/
SAP belum memberikan cukup bukti kepatuhan sehubungan dengan tindakan teknis dan organisasional yang melindungi sistem produksi Layanan Cloud dengan menyediakan: (i) sertifikasi terkait kepatuhan terhadap ISO 27001 atau standar lainnya (cakupan sebagaimana yang dijelaskan dalam sertifikat); atau (ii) laporan pengesahan ISAE3000 dan/atau ISAE3402 atau laporan pengesahan SOC1-3 lainnya yang sah. Sesuai permintaan Pelanggan, laporan audit atau sertifikasi ISO tersedia melalui auditor pihak ketiga atau SAP;

(b) A Personal Data Breach has occurred;/
Pelanggaran Data Pribadi telah terjadi;

(c) An audit is formally requested by Customer's data protection authority; or/
Audit diminta secara resmi oleh otoritas perlindungan data Pelanggan; atau

(d) Mandatory Data Protection Law provides Customer with a direct audit right and provided that Customer shall only audit once in any twelve month period unless mandatory Data Protection Law requires more frequent audits./
Undang-undang Perlindungan Data Wajib menyediakan hak audit langsung kepada Pelanggan dan jika Pelanggan hanya akan mengaudit sekali dalam jangka waktu dua belas bulan kecuali Undang-Undang Perlindungan Data wajib memerlukan audit yang lebih sering.

5.2 Other Controller Audit. Any other Controller may audit SAP's control environment and security practices relevant to Personal Data processed by SAP in line with Section 5.1 only if any of the cases set out in Section 5.1 applies to such other Controller. Such audit must be undertaken through and by Customer as set out in Section 5.1 unless the audit must be undertaken by the other Controller itself under Data Protection Law. If several Controllers whose Personal Data is processed by SAP on the basis of the Agreement require an audit, Customer shall use all reasonable means to combine the audits and to avoid multiple audits./

Audit Pengendali Lainnya. Pengendali lainnya dapat mengaudit praktik lingkungan dan keamanan pengendalian SAP yang relevan dengan Data Pribadi yang diproses oleh SAP sesuai dengan Bagian 5.1 hanya jika ada kasus yang ditetapkan dalam Bagian 5.1 berlaku untuk Pengendali lainnya. Audit tersebut harus dilakukan melalui dan oleh Pelanggan sebagaimana diatur dalam Bagian 5.1 kecuali jika audit harus dilakukan oleh Pengendali lain itu sendiri di bawah Undang-undang Perlindungan Data. Jika beberapa Pengendali yang Data Pribadinya diproses oleh SAP berdasarkan Perjanjian ini memerlukan audit, Pelanggan akan menggunakan semua sarana yang dinilai baik untuk menggabungkan audit dan untuk menghindari audit ganda.

5.3 Scope of Audit. Customer shall provide at least sixty days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited in time to a maximum of three business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Customer shall provide the results of any audit to SAP./

Ruang Lingkup Audit. Pelanggan harus menyampaikan pemberitahuan sekurang-kurangnya enam puluh hari di muka tentang audit apa pun kecuali jika Undang-undang Perlindungan Data wajib atau otoritas perlindungan data yang kompeten memerlukan pemberitahuan yang lebih singkat. Frekuensi dan ruang lingkup dari setiap audit harus disepakati bersama antara pihak-pihak yang bertindak secara wajar dan dengan iktikad baik. Waktu audit pelanggan harus dibatasi hingga maksimal tiga hari kerja. Di luar pembatasan tersebut, para pihak akan menggunakan

sertifikasi saat ini atau laporan audit lainnya untuk menghindari atau meminimalkan audit berulang. Pelanggan harus menyampaikan hasil audit kepada SAP.

5.4 **Cost of Audits.** Customer shall bear the costs of any audit unless such audit reveals a material breach by SAP of this DPA, then SAP shall bear its own expenses of an audit. If an audit determines that SAP has breached its obligations under the DPA, SAP will promptly remedy the breach at its own cost./

Biaya Audit. Pelanggan akan menanggung biaya audit apa pun, kecuali jika audit tersebut mengungkapkan pelanggaran material oleh SAP sehubungan dengan DPA ini, maka SAP akan menanggung biaya auditnya sendiri. Jika audit menentukan bahwa SAP telah melanggar kewajibannya berdasarkan DPA, SAP akan segera mengganti rugi pelanggaran tersebut atas biayanya sendiri.

6. SUBPROCESSORS/ SUBPROSESOR

6.1 **Permitted Use.** SAP is granted a general authorization to subcontract the processing of Personal Data to Subprocessors, provided that:/

Penggunaan yang Diizinkan. SAP diberikan otorisasi umum untuk mensubkontrakkan pemrosesan Data Pribadi ke Subprosesor, dengan ketentuan bahwa:

(a) SAP or SAP SE on its behalf shall engage Subprocessors under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. SAP shall be liable for any breaches by the Subprocessor in accordance with the terms of this Agreement;/

SAP atau SAP SE atas namanya akan melibatkan Subprosesor berdasarkan kontrak tertulis (termasuk dalam bentuk elektronik) yang konsisten dengan syarat-syarat DPA ini sehubungan dengan pemrosesan Data Pribadi oleh Subprosesor. SAP akan bertanggung jawab atas setiap pelanggaran yang dilakukan oleh Subprosesor sesuai dengan syarat-syarat Perjanjian ini;

(b) SAP will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA; and/

SAP akan mengevaluasi praktik keamanan, privasi, dan kerahasiaan dari Subprosesor sebelum pemilihan untuk menilai bahwa ia mampu memberikan tingkat perlindungan Data Pribadi yang diperlukan oleh DPA ini; dan

(c) SAP's list of Subprocessors in place on the effective date of the Agreement is published by SAP or SAP will make it available to Customer upon request, including the name, address and role of each Subprocessor SAP uses to provide the Cloud Service./

Daftar Subprosesor SAP yang ada pada tanggal berlakunya Perjanjian ini diterbitkan oleh SAP atau SAP akan menyediakannya bagi Pelanggan berdasarkan permintaan, termasuk nama, alamat, dan peran dari setiap Subprosesor yang digunakan SAP untuk menyediakan Layanan Cloud.

6.2 **New Subprocessors.** SAP's use of Subprocessors is at its discretion, provided that:/

Subprosesor Baru. Penggunaan SAP atas Subprosesor adalah atas kebijakannya, dengan ketentuan bahwa:

(a) SAP will inform Customer in advance (by email or by posting on the support portal available through SAP Support) of any intended additions or replacements to the list of Subprocessors including name, address and role of the new Subprocessor; and/

SAP sebelumnya akan menginformasikan kepada Pelanggan (melalui email atau dengan memposting pada portal dukungan yang tersedia melalui Dukungan SAP) sehubungan dengan setiap penambahan atau penggantian yang diinginkan ke daftar Subprosesor termasuk nama, alamat dan peran dari Subprosesor baru; dan

(b) Customer may object to such changes as set out in Section 6.3/
Pelanggan dapat berkeberatan atas perubahan tersebut sebagaimana diatur dalam Bagian 6.3.

6.3 Objections to New Subprocessors./
Keberatan terhadap Subprosesor Baru.

(a) If Customer has a legitimate reason under Data Protection Law to object to the new Subprocessors' processing of Personal Data, Customer may terminate the Agreement (limited to the Cloud Service for which the new Subprocessor is intended to be used) on written notice to SAP. Such termination shall take effect at the time determined by the Customer which shall be no later than thirty days from the date of SAP's notice to Customer informing Customer of the new Subprocessor. If Customer does not terminate within this thirty day period, Customer is deemed to have accepted the new Subprocessor./
Jika Pelanggan memiliki alasan yang sah menurut Undang-undang Perlindungan Data untuk menolak pemrosesan Data Pribadi yang dilakukan oleh Subprosesor baru, Pelanggan dapat mengakhiri Perjanjian (terbatas pada Layanan Cloud yang menjadi alasan penggunaan Subprosesor baru) melalui pemberitahuan tertulis kepada SAP. Pengakhiran tersebut akan berlaku pada waktu yang ditentukan oleh Pelanggan yaitu selambat-lambatnya tiga puluh hari sejak tanggal pemberitahuan SAP kepada Pelanggan mengenai Subprosesor baru. Jika Pelanggan tidak melakukan pengakhiran dalam periode tiga puluh hari, Pelanggan dianggap telah menerima Subprosesor baru.

(b) Within the thirty day period from the date of SAP's notice to Customer informing Customer of the new Subprocessor, Customer may request that the parties come together in good faith to discuss a resolution to the objection. Such discussions shall not extend the period for termination and do not affect SAP's right to use the new Subprocessor(s) after the thirty day period./
Dalam jangka waktu tiga puluh hari sejak tanggal pemberitahuan SAP kepada Pelanggan tentang Subprosesor baru, Pelanggan dapat meminta agar para pihak bertemu dengan iktikad baik untuk membahas penyelesaian atas keberatan tersebut. Pembahasan tersebut tidak akan memperpanjang periode pengakhiran dan tidak memengaruhi hak SAP untuk menggunakan Subprosesor baru setelah periode tiga puluh hari.

(c) Any termination under this Section 6.3 shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement./
Setiap pengakhiran dalam Bagian ini 6.3 akan dianggap sebagai iktikad baik oleh para pihak dan harus sesuai dengan syarat-syarat Perjanjian tersebut.

6.4 Emergency Replacement. SAP may replace a Subprocessor without advance notice where the reason for the change is outside of SAP's reasonable control and prompt replacement is required for security or other urgent reasons. In this case, SAP will inform Customer of the replacement Subprocessor as soon as possible following its appointment. Section 6.3 applies accordingly./
Penggantian Darurat. SAP dapat menggantikan Subprosesor tanpa pemberitahuan terlebih dahulu jika alasan perubahan berada di luar kendali wajar SAP dan penggantian segera diperlukan untuk keamanan atau alasan mendesak lainnya. Dalam hal ini, SAP akan memberi tahu Pelanggan mengenai Subprosesor pengganti sesegera mungkin setelah penunjukannya. Bagian 6.3 berlaku sesuai hal tersebut.

7. INTERNATIONAL PROCESSING/ PEMROSESAN INTERNASIONAL

7.1 Conditions for International Processing. SAP shall be entitled to process Personal Data, including by using Subprocessors, in accordance with this DPA outside the country in which the Customer is located as permitted under Data Protection Law./

Ketentuan untuk Pemrosesan Internasional. SAP berhak untuk memproses Data Pribadi, termasuk dengan menggunakan Subprosesor, sesuai dengan DPA ini di luar negara tempat Pelanggan berada sebagaimana diizinkan berdasarkan Undang-undang Perlindungan Data.

7.2 Standard Contractual Clauses. Where (i) Personal Data of an EEA or Swiss based Controller is processed in a country outside the EEA, Switzerland and any country, organization or territory acknowledged by the European Union as safe country with an adequate level of data protection under Art. 45 GDPR, or where (ii) Personal Data of another Controller is processed internationally and such international processing requires an adequacy means under the laws of the country of the Controller and the required adequacy means can be met by entering into Standard Contractual Clauses, then:/

Klausul Kontraktual Standar. Apabila (i) Data Pribadi dari Pengendali berbasis EEA atau Swiss diproses di negara di luar EEA, Swiss dan negara, organisasi atau wilayah mana pun yang diakui oleh Uni Eropa sebagai negara yang aman dengan tingkat perlindungan data yang memadai di bawah Psl. 45 GDPR, atau apabila (ii) Data Pribadi Pengendali lain diproses secara internasional dan pemrosesan internasional tersebut memerlukan sarana yang memadai berdasarkan undang-undang negara Pengendali dan sarana memadai yang disyaratkan dapat dipenuhi dengan menyepakati Klausul Kontrak Standar, maka:

(a) SAP and Customer enter into the Standard Contractual Clauses;/
SAP dan Pelanggan menyepakati Klausul Kontrak Standar;

(b) Customer enters into the Standard Contractual Clauses with each relevant Subprocessor as follows, either (i) Customer joins the Standard Contractual Clauses entered into by SAP or SAP SE and the Subprocessor as an independent owner of rights and obligations ("Accession Model") or, (ii) the Subprocessor (represented by SAP) enters into the Standard Contractual Clauses with Customer ("Power of Attorney Model"). The Power of Attorney Model shall apply if and when SAP has expressly confirmed that a Subprocessor is eligible for it through the Subprocessor list provided under Section 6.1(c), or a notice to Customer; and/or/
Pelanggan menyepakati Klausul Kontrak Standar dengan masing-masing Subprosesor terkait sebagai berikut, (i) Pelanggan bergabung dengan Klausul Kontrak Standar yang disepakati oleh SAP atau SAP SE dan Subprosesor sebagai pemilik independen atas hak dan kewajiban ("Model Aksesi") atau, (ii) Subprosesor (diwakili oleh SAP) menyepakati Klausul Kontrak Standar dengan Pelanggan ("Model Surat Kuasa"). Model Surat Kuasa akan berlaku jika dan ketika SAP telah secara tegas mengonfirmasi bahwa Subprosesor memenuhi syarat untuk itu melalui daftar Subprosesor yang disediakan di bawah Bagian 6.1(c), atau pemberitahuan kepada Pelanggan; dan/atau

(c) Other Controllers whose use of the Cloud Services has been authorized by Customer under the Agreement may also enter into Standard Contractual Clauses with SAP and/or the relevant Subprocessors in the same manner as Customer in accordance with Sections 0 (a) and (b) above. In such case, Customer will enter into the Standard Contractual Clauses on behalf of the other Controllers./
Pengendali lainnya yang penggunaan Layanan Cloud-nya telah diotorisasi oleh Pelanggan berdasarkan Perjanjian ini juga dapat menyepakati Klausul Kontrak Standar dengan SAP dan/atau Subprosesor yang relevan dengan cara yang sama seperti Pelanggan sesuai dengan Bagian 0 (a) dan (b) di atas. Jika demikian halnya, Pelanggan akan menyepakati Klausul Kontrak Standar atas nama Pengendali lainnya.

7.3 **Relation of the Standard Contractual Clauses to the Agreement.** Nothing in the Agreement shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and subprocessor rules in sections 5 and 6, such specifications also apply in relation to the Standard Contractual Clauses./
Hubungan Klausul Kontrak Standar dengan Perjanjian. Tidak ada satu pun dalam Perjanjian ini yang dapat ditafsirkan sebagai pengganti setiap klausul yang bertentangan pada Klausul Kontraktual Standar. Untuk menghindari keraguan, jika DPA ini lebih lanjut menetapkan aturan audit dan subprosesor dalam beberapa bagian 5 dan 6, penetapan tersebut juga berlaku dalam kaitannya dengan Klausul Kontrak Standar.

7.4 **Governing Law of the Standard Contractual Clauses.** The Standard Contractual Clauses shall be governed by the law of the country in which the relevant Controller is incorporated./
Hukum yang Mengatur Klausul Kontrak Standar. Klausul Kontrak Standar tersebut akan diatur oleh hukum negara tempat Pengendali terkait digabungkan.

8. DOCUMENTATION; RECORDS OF PROCESSING/ DOKUMENTASI; CATATAN PEMROSESAN

Each party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under Data Protection Law. Each party shall reasonably assist the other party in its documentation requirements, including providing the information the other party needs from it in a manner reasonably requested by the other party (such as using an electronic system), in order to enable the other party to comply with any obligations relating to maintaining records of processing./
Masing-masing pihak bertanggung jawab atas kepatuhannya terhadap persyaratan dokumentasi, khususnya pemeliharaan catatan pemrosesan bila diperlukan berdasarkan Undang-undang Perlindungan Data. Masing-masing pihak harus secara wajar membantu pihak lain dalam persyaratan dokumentasi, termasuk memberikan informasi darinya yang dibutuhkan pihak lain melalui sarana masuk akal yang diminta oleh pihak lain (seperti penggunaan sistem elektronik), untuk membantu pihak lain mematuhi kewajiban yang berkaitan dengan pemeliharaan catatan pemrosesan.

9. EU ACCESS/ AKSES UE

9.1 **Optional Service.** EU Access is an optional service that may be offered by SAP. SAP shall provide the Cloud Service eligible for EU Access solely for production instances in accordance with this Section 9. Where EU Access is not expressly specified and agreed in the Order Form, this Section 9 shall not apply./
Layanan Opsional. Akses UE adalah layanan opsional yang mungkin ditawarkan oleh SAP. SAP akan menyediakan Layanan Cloud untuk Akses UE hanya untuk instance produksi sesuai dengan Bagian ini 9. Apabila Akses UE tidak secara tegas dirinci dan disetujui dalam Formulir Pesanan, Bagian ini 9 tidak berlaku.

9.2 **EU Access.** SAP will use only European Subprocessors to provide support requiring access to Personal Data in the Cloud Service and SAP shall not export Personal Data outside of the EEA or Switzerland unless expressly authorized by Customer in writing (e-mail permitted) on a case by case basis; or as excluded under Section 9.4./
Akses UE. SAP akan menggunakan Subprosesor Eropa saja dalam memberikan dukungan yang memerlukan akses ke Data Pribadi dalam Layanan Cloud dan SAP tidak akan mengekspor Data Pribadi di luar EEA atau Swiss kecuali secara tegas diizinkan oleh Pelanggan secara tertulis (email diizinkan) sesuai kondisi; atau seperti yang dikecualikan berdasarkan Bagian 9.4.

9.3 **Data Center Location.** Upon the effective date of the Agreement, the Data Centers used to host Personal Data in the Cloud Service are located in the EEA or Switzerland. SAP will not migrate the Customer instance to a Data Center outside the EEA or Switzerland without Customer's prior written consent (email permitted). If SAP plans to migrate the Customer instance to a Data Center

within the EEA or to Switzerland, SAP will notify Customer in writing (email permitted) no later than thirty days before the planned migration./

Lokasi Pusat Data. Setelah tanggal mulai berlaku Perjanjian, Pusat Data yang digunakan untuk menyelenggarakan (host) Data Pribadi dalam Layanan Cloud berada di EEA atau Swiss. SAP tidak akan memigrasikan *instance* Pelanggan ke Pusat Data di luar EEA atau Swiss tanpa persetujuan tertulis sebelumnya dari Pelanggan (email diizinkan). Jika SAP berencana untuk memigrasikan *instance* Pelanggan ke Pusat Data dalam EEA atau ke Swiss, SAP akan memberi tahu Pelanggan secara tertulis (email diizinkan) tidak lebih dari tiga puluh hari sebelum migrasi yang direncanakan.

9.4 **Exclusions.** The following Personal Data is not subject to 9.2 and 9.3:/

Pengecualian. Data Pribadi berikut tidak diatur oleh 9.2 dan 9.3:

(a) Contact details of the sender of a support ticket; and/
Perincian narahubung pengirim tiket dukungan; dan

(b) Any other Personal Data submitted by Customer when filing a support ticket. Customer may choose not to transmit Personal Data when filing a support ticket. If this data is necessary for the incident management process, Customer may choose to anonymize that Personal Data before any transmission of the incident message to SAP./
Setiap Data Pribadi lain yang dikirimkan oleh Pelanggan saat mengajukan tiket dukungan. Pelanggan dapat memilih untuk tidak mengirimkan Data Pribadi saat mengajukan tiket dukungan. Jika data ini diperlukan untuk proses manajemen insiden, Pelanggan dapat memilih untuk menjadikan Data Pribadi tersebut tidak bernama sebelum setiap pengiriman pesan insiden kepada SAP;

10. DEFINITIONS/ DEFINISI

Capitalized terms not defined herein will have the meanings given to them in the Agreement./
Istilah-istilah yang ditulis dengan huruf kapital yang tidak didefinisikan di sini akan dijelaskan maknanya dalam Perjanjian.

10.1 **"Controller"** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; for the purposes of this DPA, where Customer acts as processor for another controller, it shall in relation to SAP be deemed as additional and independent Controller with the respective controller rights and obligations under this DPA./

"Pengendali" adalah orang-perseorangan atau badan hukum, otoritas publik, agen atau badan lain yang, secara mandiri atau bersama dengan pihak lain, menentukan tujuan dan sarana pemrosesan Data Pribadi; untuk keperluan DPA ini, apabila Pelanggan bertindak sebagai prosesor untuk pengendali lain, maka dalam kaitannya dengan SAP hal ini dianggap sebagai Pengendali tambahan dan independen dengan hak dan kewajiban pengendali yang terkait berdasarkan DPA ini.

10.2 **"Data Center"** means the location where the production instance of the Cloud Service is hosted for the Customer in its region, as published at: http://www.sap.com/corporate-en/about/our-company/policies/data-privacy-and-security/location-of-data-center.html or notified to Customer or otherwise agreed in an Order Form./

"Pusat Data" adalah lokasi di mana *instance* produksi Layanan Cloud diselenggarakan (hosted) untuk Pelanggan dalam wilayahnya, sebagaimana yang dipublikasikan di: http://www.sap.com/corporate-en/about/our-company/policies/data-privacy-and-security/location-of-data-center.html atau diberitahukan kepada Pelanggan atau disetujui dalam Formulir Pemesanan.

10.3 **"Data Protection Law"** means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement (and includes, as far as it concerns the relationship between the parties

regarding the processing of Personal Data by SAP on behalf of Customer, the GDPR as a minimum standard, irrespective of whether the Personal Data is subject to GDPR or not)./

"Undang-Undang Perlindungan Data" adalah undang-undang yang berlaku dan melindungi hak-hak dasar dan kebebasan orang dan hak mereka atas privasi terkait dengan pemrosesan Data Pribadi berdasarkan Perjanjian (dan mencakup, dalam hal ini, hubungan antara pihak-pihak yang terkait dengan pemrosesan Data Pribadi oleh SAP atas nama Pelanggan, GDPR sebagai standar minimum, terlepas dari apakah Data Pribadi diatur oleh GDPR atau tidak).

10.4 **"Data Subject"** means an identified or identifiable natural person as defined by Data Protection Law./

"Subjek Data" adalah orang-perseorangan yang teridentifikasi atau dapat diidentifikasi sebagaimana ditentukan oleh Undang-undang Perlindungan Data.

10.5 **"EEA"** means the European Economic Area, namely the European Union Member States along with Iceland, Liechtenstein and Norway./

"EEA" berarti Wilayah Ekonomi Eropa (*European Economic Area*), yaitu Negara Anggota Uni Eropa bersama dengan Islandia, Liechtenstein, dan Norwegia.

10.6 **"European Subprocessor"** means a Subprocessor that is physically processing Personal Data in the EEA or Switzerland./

"Subprosesor Eropa" berarti Subprosesor yang memproses Data Pribadi secara fisik di EEA atau Swiss.

10.7 **"Personal Data"** means any information relating to a Data Subject which is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data which is (i) entered by Customer or its Authorized Users into or derived from their use of the Cloud Service, or (ii) supplied to or accessed by SAP or its Subprocessors in order to provide support under the Agreement. Personal Data is a sub-set of Customer Data (as defined under the Agreement)./

"Data Pribadi" berarti setiap informasi yang berkaitan dengan Subjek Data yang dilindungi oleh Undang-undang Perlindungan Data. Untuk tujuan DPA, hal ini hanya mencakup data pribadi yang (i) dimasukkan oleh Pelanggan atau Pengguna Resminya ke atau yang berasal dari penggunaan Layanan Cloud mereka, atau (ii) dipasok ke atau diakses oleh SAP atau Subprosesornya dalam rangka memberikan dukungan berdasarkan Perjanjian tersebut. Data Pribadi adalah sub-set Data Pelanggan (sebagaimana didefinisikan dalam Perjanjian).

10.8 **"Personal Data Breach"** means a confirmed (1) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data or (2) similar incident involving Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects./

"Pelanggaran Data Pribadi" adalah konfirmasi tentang (1) penghancuran, kehilangan, pengubahan yang tidak disengaja atau melanggar hukum, pengungkapan yang tidak sah atau akses pihak ketiga yang tidak sah ke Data Pribadi atau (2) insiden serupa yang melibatkan Data Pribadi, dalam setiap kasus apabila Pengendali menurut Undang-undang Perlindungan Data diwajibkan untuk menyampaikan pemberitahuan kepada otoritas perlindungan data yang kompeten atau Subjek Data.

10.9 **"Processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, be it directly as processor of a controller or indirectly as subprocessor of a processor which processes personal data on behalf of the controller./

"Prosesor" adalah orang-perseorangan atau badan hukum, otoritas publik, agensi atau badan lain yang memproses data pribadi atas nama pengendali, baik secara langsung sebagai prosesor dari suatu pengendali atau secara tidak langsung sebagai subprosesor dari suatu prosesor yang memproses data pribadi atas nama pengendali.

10.10 **"Standard Contractual Clauses"** or sometimes also referred to the "EU Model Clauses" means the (Standard Contractual Clauses (processors)) or any subsequent version thereof published by

the European Commission (which will automatically apply). The Standard Contractual Clauses *current as of the effective date of the Agreement* are attached hereto as **Appendix 4**./

"Klausul Kontraktual Standar" atau terkadang disebut sebagai "Klausul Model UE" berarti (Klausul KontraktualStandar (prosesor) atau versi apa pun sesudahnya yang dipublikasikan oleh Komisi Eropa (yang secara otomatis akan berlaku). Pasal-pasal Kontraktual Standar terkini pada saat tanggal berlaku dari Perjanjian adalah sebagaimana terlampir disini sebagai **Ketentuan Tambahan 4**.

10.11 **"Subprocessor"** means SAP Affiliates, SAP SE, SAP SE Affiliates and third parties engaged by SAP , SAP SE or SAP SE's Affiliates in connection with the Cloud Service and which process Personal Data in accordance with this DPA./

"Subprosesor" adalah Afiliasi SAP, SAP SE, Afiliasi SAP SE dan pihak ketiga yang terlibat dengan SAP, SAP SE atau Afiliasi SAP SE dalam hubungannya dengan Layanan Cloud dan yang memproses Data Pribadi sesuai dengan DPA ini.

11. GOVERNING LANGUAGE/ BAHASA YANG BERLAKU

This DPA along with its respective appendix is executed in both English language and Bahasa Indonesia. In the event of any inconsistency or contradiction in the meaning, interpretation or dispute between the English language and Bahasa Indonesia herein, the English version of the DPA and its respective appendix shall prevail.

DPA ini Bersama-sama dengan ketentuan tambahan terkait ditandatangani dalam Bahasa Inggris dan Bahasa Indonesia. Dalam hal terjadi setiap ketidakkonsistensian atau pertentangan pada arti, pengertian atau sengketa antara Bahasa Inggris dan Bahasa Indonesia disini, maka versi Bahasa Inggris dari DPA dan ketentuan tambahan terkaitnya yang akan berlaku.

Appendix 1 to the DPA and, if applicable, the Standard Contractual Clauses/
Lampiran 1 terhadap DPA dan, jika berlaku, Klausul Kontrak Standar

Data Exporter/
Pengekspor Data

The Data Exporter is the Customer who subscribed to a Cloud Service that allows Authorized Users to enter, amend, use, delete or otherwise process Personal Data. Where the Customer allows other Controllers to also use the Cloud Service, these other Controllers are also Data Exporters./
Pengekspor Data adalah Pelanggan yang berlangganan Layanan Cloud yang memungkinkan Pengguna Resmi dapat memasukkan, mengubah, menggunakan, menghapus atau memproses Data Pribadi. Jika Pelanggan mengizinkan Pengendali lain untuk ikut menggunakan Layanan Cloud, Pengendali lainnya ini juga merupakan Pengekspor Data.

Data Importer/
Pengimpor Data

SAP and its Subprocessors provide the Cloud Service that includes the following support:/
SAP dan Subprosesornya menyediakan Layanan Cloud yang meliputi dukungan berikut:

SAP SE Affiliates support the Cloud Service data centers remotely from SAP facilities in St. Leon/Rot (Germany), India and other locations where SAP employs personnel in the Operations/Cloud Delivery function. Support includes:/
Afiliasi SAP SE mendukung pusat data Layanan Cloud jarak jauh dari fasilitas-fasilitas SAP di St. Leon/Rot (Jerman), India, dan lokasi-lokasi lain di mana SAP mempekerjakan personel dalam fungsi Penyampaian Cloud/Operasi. Dukungan mencakup:

- Monitoring the Cloud Service/
  Pemantauan Layanan Cloud
- Backup & restoration of Customer Data stored in the Cloud Service/
  Cadangan dan pemulihan Data Pelanggan yang disimpan dalam Layanan Cloud
- Release and development of fixes and upgrades to the Cloud Service/
  Rilis dan pengembangan perbaikan dan peningkatan (*upgrade*) Layanan Cloud
- Monitoring, troubleshooting and administering the underlying Cloud Service infrastructure and database/
  Pemantauan, penyelesaian masalah dan pengurusan basis data dan infrastruktur Layanan Cloud dasar.
- Security monitoring, network-based intrusion detection support, penetration testing/
  Pemantauan keamanan, dukungan deteksi intrusi berbasis jaringan, uji penetrasi

SAP SE Affiliates provide support when a Customer submits a support ticket because the Cloud Service is not available or not working as expected for some or all Authorized Users. SAP answers phones and performs basic troubleshooting, and handles support tickets in a tracking system that is separate from the production instance of the Cloud Service./
Afiliasi SAP SE memberikan dukungan ketika Pelanggan menyerahkan tiket dukungan karena Layanan Cloud tidak tersedia atau tidak berfungsi sebagaimana yang diharapkan untuk beberapa atau semua Pengguna Resmi. SAP menjawab telepon dan melakukan penyelesaian masalah dasar, dan menangani tiket dukungan dalam suatu sistem pelacakan yang terpisah dari *instance* produksi Layanan Cloud.

Data Subjects/
Subjek Data
Unless provided otherwise by the Data Exporter, transferred Personal Data relates to the following categories of Data Subjects: employees, contractors, business partners or other individuals having Personal Data stored in the Cloud Service./
Kecuali apabila ditentukan lain oleh Pengekspor Data, Data Pribadi yang ditransfer berhubungan dengan kategori Subjek Data berikut: pegawai, kontraktor, mitra bisnis atau individu lainnya yang memiliki Data Pribadi yang disimpan dalam Layanan Cloud.

Data Categories/
Kategori Data
The transferred Personal Data concerns the following categories of data:/
Data Pribadi yang dialihkan berkaitan dengan kategori data berikut:

Customer determines the categories of data per Cloud Service subscribed. Customer can configure the data fields during implementation of the Cloud Service or as otherwise provided by the Cloud Service. The transferred Personal Data typically relates to the following categories of data: name, phone numbers, e-mail address, time zone, address data, system access / usage / authorization data, company name, contract data, invoice data, plus any application-specific data that Authorized Users enter into the Cloud Service and may include bank account data, credit or debit card data./
Pelanggan menentukan kategori data per Layanan Cloud yang dilanggankan. Pelanggan dapat mengonfigurasikan bidang data selama implementasi Layanan Cloud atau sebagaimana yang ditentukan lain oleh Layanan Cloud. Data Pribadi yang ditransfer biasanya berhubungan dengan kategori data berikut: nama, nomor telepon, alamat email, zona waktu, data alamat, akses sistem / penggunaan / data otorisasi nama perusahaan, data kontrak, data tagihan, yang ditambah dengan data spesifik aplikasi yang dimasukkan oleh Pengguna Resmi ke dalam Layanan Cloud, dan dapat termasuk data rekening bank, data kartu kredit atau debit.

Special Data Categories (if appropriate)/
Kategori Data Khusus (apabila sesuai)
The transferred Personal Data concerns the following special categories of data: As set out in the Agreement (including the Order Form) if any./
Data Pribadi yang ditransfer berhubungan dengan kategori khusus untuk data berikut: Sebagaimana yang ditetapkan dalam Perjanjian (termasuk Formulir Pemesanan) apabila ada.

Processing Operations / Purposes/
Operasi / Tujuan Pemrosesan
The transferred Personal Data is subject to the following basic processing activities:/
Data Pribadi yang ditransfer tunduk pada aktivitas pemrosesan dasar berikut ini:

- use of Personal Data to set up, operate, monitor and provide the Cloud Service (including Operational and Technical Support)/
  penggunaan Data Pribadi untuk menyiapkan, mengoperasikan, memantau, dan menyediakan Layanan Cloud (termasuk Dukungan Operasional dan Teknis)
- provision of Consulting Services;/
  penyediaan Layanan Konsultasi;
- communication to Authorized Users/
  komunikasi dengan Pengguna Resmi
- storage of Personal Data in dedicated Data Centers (multi-tenant architecture)/
  penyimpanan Data Pribadi di Pusat Data terdedikasi (arsitektur multi-penyewa)
- upload any fixes or upgrades to the Cloud Service/
  mengunggah setiap perbaikan atau peningkatan (*upgrade*) ke Layanan Cloud

- back up of Personal Data/
  pencadangan Data Pribadi
- computer processing of Personal Data, including data transmission, data retrieval, data access/
  pemrosesan Data Pribadi pada komputer, termasuk transmisi data, pengambilan data, akses data
- network access to allow Personal Data transfer/
  akses jaringan untuk memungkinkan transfer Data Pribadi
- execution of instructions of Customer in accordance with the Agreement./
  pelaksanaan instruksi Pelanggan sesuai dengan Perjanjian tersebut.

Appendix 2 to the DPA and, if applicable, the Standard Contractual Clauses – Technical and Organizational Measures/
Lampiran 2 terhadap DPA dan, jika berlaku, Klausul Kontrak Standar – Tindakan Teknis dan Organisasional

This Appendix 2 comprises two sets of technical and organizational measures ("**TOMs**"):/
Lampiran 2 ini terdiri dari dua set Tindakan Teknis dan Organisasional ("**TTO**"):

- **TOMs Set 1 (last updated April 2018, without change):** applies to all Cloud Services, except for the TOMs Set 2 Services defined below./
  TTO Set 1 (terakhir diperbaharui pada April 2018, tanpa perubahan): berlaku untuk semua Layanan Cloud, kecuali Layanan TTO Set 2 yang didefinisikan di bawah ini.

- **TOMs Set 2**: applies to the TOMs Set 2 Services only. As of May 4, 2020, "**TOMs Set 2 Services**" means the following Cloud Services: SAP Analytics Cloud, SAP SuccessFactors and SAP Cloud Platform. SAP may remove a Cloud Service from the list of TOMs Set 2 Services from time to time, in which case such Cloud Service will be subject to TOMs Set 1./
  TTO Set 2: hanya berlaku untuk Layanan TTO Set 2. Per 4 Mei 2020, "**Layanan TTO Set 2**" berarti Layanan-layanan Cloud berikut: SAP Analytics Cloud, SAP SuccessFactors, dan SAP Cloud Platform. SAP dapat menghapus Layanan Cloud dari daftar Layanan TTO Set 2 dari waktu ke waktu, dalam hal ini Layanan Cloud tersebut akan tunduk kepada TTO Set 1.

TOMs SET 1/
TTO SET 1

Last Updated: April 2018/
Terakhir Diperbaharui: April 2018

1. TECHNICAL AND ORGANIZATIONAL MEASURES/ TINDAKAN TEKNIS DAN ORGANISASIONAL

The following sections define SAP's current technical and organizational measures. SAP may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data./
Bagian berikut menjelaskan tindakan teknis dan organisasional SAP saat ini. SAP dapat mengubah hal ini sewaktu-waktu tanpa pemberitahuan sepanjang SAP mempertahankan tingkat keamanan yang setara atau lebih baik. Tindakan individu dapat diganti dengan tindakan baru yang berfungsi untuk tujuan yang sama tanpa mengurangi tingkat keamanan yang melindungi Data Pribadi.

1.1 Physical Access Control. Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/or use Personal Data are located./
Kendali Akses Fisik. Orang yang tidak berwenang dicegah dari mendapatkan akses fisik ke lokasi, gedung, atau ruangan di mana terdapat sistem pemrosesan data yang memproses dan/atau menggunakan Data Pribadi.

Measures:/
Tindakan:

- SAP protects its assets and facilities using the appropriate means based on the SAP Security Policy/ SAP melindungi aset dan fasilitasnya dengan menggunakan sarana yang sesuai berdasarkan Kebijakan Keamanan SAP
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management./

In general, buildings are secured through access control systems (e.g., smart card access system)./
Secara umum, gedung diamankan melalui sistem pengendalian akses (misalnya, sistem akses kartu pintar).

- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management./
  Sebagai persyaratan minimum, titik masuk terluar gedung harus dilengkapi dengan sistem kunci master tersertifikasi termasuk manajemen kunci aktif dan modern.
- Depending on the security classification, buildings, individual areas and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems./
  Bergantung pada klasifikasi keamanan, gedung, area individu, dan lokasi di sekitar dapat selanjutnya dilindungi dengan tindakan-tindakan tambahan. Tindakan-tindakan ini termasuk profil akses spesifik, CCTV, sistem alarm penyusup, dan sistem kendali akses biometri.
- Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 1.2 and 1.3 below). This also applies to visitor access. Guests and visitors to SAP buildings must register their names at reception and must be accompanied by authorized SAP personnel./
  Hak akses diberikan kepada orang-orang resmi secara individual sesuai dengan tindakan Sistem dan Kendali Akses Data (lihat Pasal 1.2 dan 1.3 di bawah). Hal ini juga berlaku untuk akses pengunjung. Tamu dan pengunjung ke gedung SAP harus mendaftarkan nama mereka di bagian penerimaan dan harus didampingi oleh personel resmi SAP .

- SAP employees and external personnel must wear their ID cards at all SAP locations./
  Karyawan SAP dan personel eksternal harus mengenakan kartu identitas di semua lokasi SAP.

Additional measures for Data Centers:/
Tindakan tambahan untuk Pusat Data:

- All Data Centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the Data Center facilities. To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis./
  Semua Pusat Data yang mematuhi prosedur-prosedur keamanan yang ketat yang dilaksanakan oleh penjaga, kamera pengawas, detektor gerakan, mekanisme kendali akses, dan tindakan lain untuk mencegah adanya penyusupan pada peralatan dan fasilitas Pusat Data. Hanya perwakilan resmi yang memiliki akses ke sistem dan infrastruktur di dalam fasilitas-fasilitas Pusat Data. Untuk melindungi agar berfungsi dengan tepat, tindakan keamanan fisik (misalnya, sensor gerakan, kamera, dll.) mendapatkan pemeliharaan secara rutin.
- SAP and all third-party Data Center providers log the names and times of authorized personnel entering SAP's private areas within the Data Centers./
  SAP dan semua penyedia Pusat Data pihak ketiga mencatat nama dan waktu saat personel resmi memasuki area khusus SAP di dalam Pusat Data.

1.2 System Access Control. Data processing systems used to provide the Cloud Service must be prevented from being used without authorization./
Kendali Akses Sistem. Sistem pemrosesan data yang digunakan untuk menyediakan Layanan Cloud harus dicegah agar tidak digunakan tanpa pengesahan.

Measures:/
Tindakan:

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes according to the SAP Security Policy/

Sejumlah tingkat otorisasi digunakan ketika memberikan akses ke sistem-sistem yang sensitif, termasuk ke sistem yang menyimpan dan memproses Data Pribadi. Otorisasi dikelola melalui proses yang ditentukan sesuai dengan Kebijakan Keamanan SAP

- All personnel access SAP's systems with a unique identifier (user ID)./
  Semua personel mengakses sistem-sistem SAP dengan identitas unik (ID pengguna).
- SAP has procedures in place to so that requested authorization changes are implemented only in accordance with the SAP Security Policy (for example, no rights are granted without authorization). In case personnel leaves the company, their access rights are revoked./
  SAP memiliki prosedur untuk memastikan bahwa perubahan pengesahan yang diminta telah diimplementasikan hanya sesuai dengan Kebijakan Keamanan SAP (misalnya, tidak ada hak yang diberikan tanpa pengesahan). Apabila personel berhenti bekerja pada perusahaan, hak mereka untuk mengakses akan dicabut.
- SAP has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver./
  SAP telah menetapkan kebijakan kata sandi yang melarang pembagian kata sandi, mengatur respons terhadap pengungkapan kata sandi, dan meminta agar kata sandi diubah secara berkala dan kata sandi standar untuk diubah. ID pengguna yang dipersonalisasikan ditetapkan untuk otentikasi. Semua kata sandi harus memenuhi persyaratan minimum yang ditetapkan dan disimpan dalam formulir terenkripsi. Dalam kasus kata sandi domain, sistem meminta kata sandi untuk diubah setiap enam bulan sekali sesuai dengan persyaratan kata sandi yang rumit. Setiap komputer memiliki *screensaver* yang dilindungi dengan kata sandi.
- The company network is protected from the public network by firewalls./
  Jaringan perusahaan dilindungi dari jaringan publik dengan *firewall*.
- SAP uses up–to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations./
  SAP menggunakan perangkat lunak antivirus terbaru pada titik akses menuju jaringan perusahaan (untuk akun email), serta pada semua server file dan semua stasiun kerja.
- Security patch management is implemented to provide regular and periodic deployment of relevant security updates. Full remote access to SAP's corporate network and critical infrastructure is protected by strong authentication./
  Manajemen *patch* keamanan diimplementasikan untuk menyediakan penempatan rutin dan berkala untuk pembaruan-pembaruan keamanan yang relevan. Akses penuh jarak jauh ke jaringan perusahaan dan infrastruktur penting SAP dilindungi dengan otentikasi yang kuat.

1.3 Data Access Control. Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage./

Kendali Akses Data. Orang-orang yang berhak untuk menggunakan sistem pemrosesan data memperoleh akses hanya ke Data Pribadi yang berhak mereka akses, dan Data Pribadi tidak dapat dibaca, disalin, dimodifikasi, atau dihapus tanpa pengesahan selama pemrosesan, penggunaan, dan penyimpanan.

Measures:/
Tindakan:

- As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard./

Sebagai bagian dari Kebijakan Keamanan SAP, Data Pribadi mensyaratkan setidaknya tingkat perlindungan yang sama sebagaimana informasi "rahasia" sesuai dengan standar Klasifikasi Informasi SAP.

- Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfill their duty. SAP uses authorization concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the SAP Security Policy./
  Akses ke Data Pribadi diberikan seperlunya saja (*need-to-know basis*). Personel memiliki akses ke informasi yang mereka butuhkan untuk memenuhi tugas mereka. SAP menggunakan konsep pengesahan yang mendokumentasikan proses pemberian dan peran yang ditetapkan per akun (ID pengguna). Seluruh Data Pelanggan dilindungi sesuai dengan Kebijakan Keamanan SAP.
- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. To this end, SAP conducts internal and external security checks and penetration tests on its IT systems./
  Semua server produksi dioperasikan pada Pusat Data atau dalam ruang server yang aman. Tindakan keamanan yang melindungi aplikasi yang memproses Data Pribadi diperiksa secara berkala. Untuk mencapai tujuan ini, SAP menjalankan pemeriksaan keamanan internal dan eksternal serta uji penetrasi pada sistem TI-nya.
- SAP does not allow the installation of software that has not been approved by SAP./
  SAP tidak mengizinkan instalasi perangkat lunak yang belum disetujui oleh SAP.
- An SAP security standard governs how data and data carriers are deleted or destroyed once they are no longer required./
  Standar keamanan SAP mengatur cara data dan pembawa data dihapus atau dimusnahkan setelah hal tersebut tidak lagi diperlukan.

1.4 Data Transmission Control. Except as necessary for the provision of the Cloud Services in accordance with the Agreement, Personal Data must not be read, copied, modified or removed without authorization during transfer. Where data carriers are physically transported, adequate measures are implemented at SAP to provide the agreed-upon service levels (for example, encryption and lead-lined containers)./

Kendali Transmisi Data. Kecuali sebagaimana yang diperlukan untuk penyediaan Layanan Cloud sesuai dengan Perjanjian, Data Pribadi tidak boleh dibaca, disalin, dimodifikasi, atau dihapus tanpa pengesahan selama transfer. Jika pembawa data dipindahkan secara fisik, tindakan yang memadai diimplementasikan di SAP untuk menyediakan tingkat layanan yang telah disetujui (sebagai contoh, enkripsi dan kontainer bersegel timah).

Measures:/
Tindakan:

- Personal Data in transfer over SAP internal networks is protected according to SAP Security Policy./
  Transfer Data Pribadi melalui jaringan internal SAP dilindungi sesuai dengan Kebijakan Keamanan SAP.
- When data is transferred between SAP and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant agreement. This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of SAP-controlled systems (e.g. data being transmitted outside the firewall of the SAP Data Center)./
  Jika data ditransfer antara SAP dan pelanggannya, tindakan-tindakan perlindungan untuk Data Pribadi yang ditransfer disetujui bersama dan menjadi bagian dalam perjanjian yang relevan. Hal ini berlaku untuk transfer data berbasis jaringan dan fisik. Dalam kasus apa pun, Pelanggan menerima tanggung jawab untuk setiap transfer data setelah berada di luar sistem yang dikendalikan oleh SAP (misalnya data yang dikirim di luar *firewall* Pusat Data SAP).

1.5 Data Input Control. It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from SAP data processing systems./
Kendali Input Data. Kendali Input Data bertanggung jawab tas pemeriksaan secara retroaktif dan menetapkan apakah dan oleh siapa Data Pribadi telah dimasukkan, dimodifikasi atau dihapus dari sistem pemrosesan data SAP.

Measures:/
Tindakan:

- SAP only allows authorized personnel to access Personal Data as required in the course of their duty./
  SAP hanya mengizinkan personel resmi untuk mengakses Data Pribadi sebagaimana yang diperlukan selama penugasan mereka.
- SAP has implemented a logging system for input, modification and deletion, or blocking of Personal Data by SAP or its subprocessors within the Cloud Service to the extent technically possible./
  SAP sedapat mungkin telah mengimplementasikan sistem pencatatan untuk input, modifikasi, dan penghapusan, atau pemblokiran Data Pribadi oleh SAP atau subprosesornya dalam Layanan SAP secara teknis.

1.6 Job Control. Personal Data being processed on commission (i.e., Personal Data processed on a customer's behalf) is processed solely in accordance with the Agreement and related instructions of the customer./
Kendali Pekerjaan. Data Pribadi yang diproses pada komisi (yaitu, Data Pribadi yang diproses atas nama pelanggan) diproses sepenuhnya berdasarkan Perjanjian dan instruksi terkait dari pelanggan.

Measures:/
Tindakan:

- SAP uses controls and processes to monitor compliance with contracts between SAP and its customers, subprocessors or other service providers./
  SAP menggunakan kendali dan proses untuk memantau kepatuhan dengan kontrak antara SAP dan pelanggan, subprosesor, atau penyedia layanan lainnya.
- As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard./
  Sebagai bagian dari Kebijakan Keamanan SAP, Data Pribadi mensyaratkan setidaknya tingkat perlindungan yang sama sebagaimana informasi "rahasia" sesuai dengan standar Klasifikasi Informasi SAP.
- All SAP employees and contractual subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of SAP customers and partners./
  Semua karyawan dan subprosesor kontrak atau penyedia layanan lainnya dari SAP terikat berdasarkan kontrak untuk menghargai kerahasiaan semua informasi yang sensitif, termasuk rahasia dagang para pelanggan dan mitra SAP.

1.7 Availability Control. Personal Data will be protected against accidental or unauthorized destruction or loss./
Kendali Ketersediaan. Data Pribadi akan dilindungi dari kerusakan atau kehilangan yang tidak sah atau tidak disengaja.

Measures:/
Tindakan:

- SAP employs regular backup processes to provide restoration of business-critical systems as and when necessary./
  SAP menggunakan proses pencadangan reguler untuk menyediakan pemulihan sistem bisnis penting jika dan bila diperlukan.
- SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centers./

SAP menggunakan suplai daya tidak terputus (sebagai contoh: UPS, baterai, generator, dll.) untuk melindungi ketersediaan daya ke Pusat Data.

- SAP has defined business contingency plans for business-critical processes and may offer disaster recovery strategies for business critical Services as further set out in the Documentation or incorporated into the Order Form for the relevant Cloud Service./
  SAP telah menetapkan rencana cadangan bisnis untuk proses bisnis penting dan dapat menawarkan strategi pemulihan bencana untuk Layanan penting bisnis sebagaimana ditetapkan lebih lanjut dalam Dokumentasi atau digabungkan ke dalam Formulir Pemesanan untuk Layanan Cloud terkait.
- Emergency processes and systems are regularly tested./
  Proses dan sistem darurat diuji secara berkala.

1.8 Data Separation Control. Personal Data collected for different purposes can be processed separately./
Kendali Pemisahan Data. Data Pribadi yang dikumpulkan untuk tujuan berbeda dapat diproses secara terpisah.

Measures:/
Tindakan:

- SAP uses the technical capabilities of the deployed software (for example: multi- tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers./
  SAP menggunakan kemampuan-kemampuan teknis dari perangkat lunak yang ditempatkan (misalnya, lanskap sistem terpisah atau kepemilikan majemuk) untuk mencapai pemisahan data antara Data Pribadi yang berasal dari berbagai pelanggan.
- Customer (including its Controllers) has access only to its own data./
  Pelanggan (termasuk Pengendalinya) memiliki akses hanya ke datanya sendiri.
- If Personal Data is required to handle a support incident from Customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems./
  Jika Data Pribadi diperlukan untuk menangani insiden dukungan dari Pelanggan, data ditetapkan untuk pesan tertentu tersebut dan digunakan hanya untuk memproses pesan tersebut, Data Pribadi tidak diakses untuk memproses pesan lain mana pun. Data ini disimpan dalam sistem dukungan khusus.

1.9 Data Integrity Control. Personal Data will remain intact, complete and current during processing activities./
Kendali Integritas Data. Data Pribadi akan tetap terjaga, lengkap, dan masih berlaku selama kegiatan pemrosesan.

Measures:/
Tindakan:

SAP has implemented a multi-layered defense strategy as a protection against unauthorized modifications./
SAP telah mengimplementasikan strategi pertahanan multi-lapisan sebagai perlindungan terhadap modifikasi-modifikasi yang tidak resmi.
In particular, SAP uses the following to implement the control and measure sections described above.
Khususnya, SAP menggunakan hal-hal berikut ini untuk mengimplementasikan pasal tindakan dan kendali yang dideskripsikan di atas.

- *Firewall*;
- Security Monitoring Center;/
  Pusat Pemantauan Keamanan;
- Antivirus software;/
  Perangkat lunak antivirus;

- Backup and recovery;/
  Pencadangan dan pemulihan;
- External and internal penetration testing;/
  Pengujian penetrasi eksternal dan internal;
- Regular external audits to prove security measures./
  Audit eksternal berkala untuk membuktikan tindakan keamanan.

TOMs SET 2/
TTO SET 2

(*applies to TOMs Set 2 Services defined above*)/
(berlaku untuk Layanan TTO Set 2 sebagaimana didefinisikan di atas)

Last Updated: May 4, 2020/
Terakhir Diperbaharui: 4 Mei 2020

1. TECHNICAL AND ORGANIZATIONAL MEASURES/ TINDAKAN TEKNIS DAN ORGANISASIONAL

The following sections define SAP's current technical and organizational measures. SAP may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data./
Bagian berikut menjelaskan tindakan teknis dan organisasional SAP saat ini. SAP dapat mengubah hal ini sewaktu-waktu tanpa pemberitahuan sepanjang SAP mempertahankan tingkat keamanan yang setara atau lebih baik. Tindakan individu dapat diganti dengan tindakan baru yang berfungsi untuk tujuan yang sama tanpa mengurangi tingkat keamanan yang melindungi Data Pribadi.

1.1 Physical Access Control./ Kendali Akses Fisik.

- SAP protects its assets and facilities using the appropriate means based on the SAP Security Policy/ SAP melindungi aset dan fasilitasnya dengan menggunakan sarana yang sesuai berdasarkan Kebijakan Keamanan SAP
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management./
  In general, buildings are secured through access control systems (e.g., smart card access system)./
  Secara umum, gedung diamankan melalui sistem pengendalian akses (misalnya, sistem akses kartu pintar).
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management./
  Sebagai persyaratan minimum, titik masuk terluar gedung harus dilengkapi dengan sistem kunci master tersertifikasi termasuk manajemen kunci aktif dan modern.
- Depending on the security classification, buildings, individual areas and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems./
  Bergantung pada klasifikasi keamanan, gedung, area individu, dan lokasi di sekitar dapat selanjutnya dilindungi dengan tindakan-tindakan tambahan. Tindakan-tindakan ini termasuk profil akses spesifik, CCTV, sistem alarm penyusup, dan sistem kendali akses biometri.
- Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 1.2 and 1.3 below). This also applies to visitor access. Guests and visitors to SAP buildings must register their names at reception and must be accompanied by authorized SAP personnel./
  Hak akses diberikan kepada orang-orang resmi secara individual sesuai dengan tindakan Sistem dan Kendali Akses Data (lihat Pasal 1.2 dan 1.3 di bawah). Hal ini juga berlaku untuk akses pengunjung. Tamu dan pengunjung ke gedung SAP harus mendaftarkan nama mereka di bagian penerimaan dan harus didampingi oleh personel resmi SAP .

- SAP employees and external personnel must wear their ID cards at all SAP locations./
  Karyawan SAP dan personel eksternal harus mengenakan kartu identitas di semua lokasi SAP.

Additional measures for Data Centers:/
Tindakan tambahan untuk Pusat Data:

- All Data Centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the Data Center facilities. To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis./
  Semua Pusat Data yang mematuhi prosedur-prosedur keamanan yang ketat yang dilaksanakan oleh penjaga, kamera pengawas, detektor gerakan, mekanisme kendali akses, dan tindakan lain untuk mencegah adanya penyusupan pada peralatan dan fasilitas Pusat Data. Hanya perwakilan resmi yang memiliki akses ke sistem dan infrastruktur di dalam fasilitas-fasilitas Pusat Data. Untuk melindungi agar berfungsi dengan tepat, tindakan keamanan fisik (misalnya, sensor gerakan, kamera, dll.) mendapatkan pemeliharaan secara rutin.
- SAP and all third-party Data Center providers log the names and times of authorized personnel entering SAP's private areas within the Data Centers./
  SAP dan semua penyedia Pusat Data pihak ketiga mencatat nama dan waktu saat personel resmi memasuki area khusus SAP di dalam Pusat Data.

1.2 System Access Control./
Kendali Akses Sistem.

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes according to the SAP Security Policy/
  Sejumlah tingkat otorisasi digunakan ketika memberikan akses ke sistem-sistem yang sensitif, termasuk ke sistem yang menyimpan dan memproses Data Pribadi. Otorisasi dikelola melalui proses yang ditentukan sesuai dengan Kebijakan Keamanan SAP
- All personnel access SAP's systems with a unique identifier (user ID)./
  Semua personel mengakses sistem-sistem SAP dengan identitas unik (ID pengguna).
- SAP has policies designed to provide that no rights are granted without authorization and in case personnel leaves the company their access rights are revoked./
  SAP memiliki kebijakan yang didesain untuk menyediakan bahwa tidak ada hak-hak yang diberikan tanpa otorisasi dan jika personel berhenti bekerja dari perusahaan, hak-hak akses mereka akan dicabut.
- SAP has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver./
  SAP telah menetapkan kebijakan kata sandi yang melarang pembagian kata sandi, mengatur respons terhadap pengungkapan kata sandi, dan meminta agar kata sandi diubah secara berkala dan kata sandi standar untuk diubah. ID pengguna yang dipersonalisasikan ditetapkan untuk otentikasi. Semua kata sandi harus memenuhi persyaratan minimum yang ditetapkan dan disimpan dalam formulir terenkripsi. Dalam kasus kata sandi domain, sistem meminta kata sandi untuk diubah setiap enam bulan sekali sesuai dengan persyaratan kata sandi yang rumit. Setiap komputer memiliki *screensaver* yang dilindungi dengan kata sandi.
- The company network is protected from the public network by firewalls./
  Jaringan perusahaan dilindungi dari jaringan publik dengan *firewall*.

- SAP uses up–to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations./
  SAP menggunakan perangkat lunak antivirus terbaru pada titik akses menuju jaringan perusahaan (untuk akun email), serta pada semua server file dan semua stasiun kerja.
- Security patch management processes to deploy relevant security updates on a regular and periodic basis.
  Manajemen *patch* keamanan melakukan proses untuk memasang pembaruan-pembaruan keamanan yang relevan secara teratur dan berkala.
- Full remote access to SAP's corporate network and critical infrastructure is protected by authentication./
  Akses penuh jarak jauh ke jaringan perusahaan dan infrastruktur penting SAP dilindungi oleh otentikasi.

1.3 Data Access Control. /
Kendali Akses Data.

- As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard./
  Sebagai bagian dari Kebijakan Keamanan SAP, Data Pribadi mensyaratkan setidaknya tingkat perlindungan yang sama sebagaimana informasi "rahasia" sesuai dengan standar Klasifikasi Informasi SAP.
- Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfil their duty. SAP uses authorization concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the SAP Security Policy./
  Akses ke Data Pribadi diberikan seperlunya saja (*need-to-know basis*). Personel memiliki akses ke informasi yang mereka butuhkan untuk memenuhi tugas mereka. SAP menggunakan konsep pengesahan yang mendokumentasikan proses pemberian dan peran yang ditetapkan per akun (ID pengguna). Seluruh Data Pelanggan dilindungi sesuai dengan Kebijakan Keamanan SAP.
- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. To this end, SAP conducts internal and external security checks and/or penetration tests on its IT systems./
  Semua server produksi dioperasikan pada Pusat Data atau dalam ruang server yang aman. Tindakan keamanan yang melindungi aplikasi yang memproses Data Pribadi diperiksa secara berkala. Untuk mencapai tujuan ini, SAP menjalankan pemeriksaan keamanan internal dan eksternal dan/atau uji penetrasi pada sistem TI-nya.
- Processes and policies to detect the installation of unapproved software on production systems ./
  Proses-proses dan kebijakan-kebijakan untuk mendeteksi instalasi perangkat lunak yang tidak disetujui pada sistem-sistem produksi.
- An SAP security standard governs how data and data carriers are deleted or destroyed once they are no longer required./
  Standar keamanan SAP mengatur cara data dan pembawa data dihapus atau dimusnahkan setelah hal tersebut tidak lagi diperlukan.

1.4 Data Transmission Control. /
Kendali Transmisi Data.

- Personal Data in transfer over SAP internal networks is protected according to SAP Security Policy./
  Transfer Data Pribadi melalui jaringan internal SAP dilindungi sesuai dengan Kebijakan Keamanan SAP.
- When data is transferred between SAP and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant agreement.

This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of SAP-controlled systems (e.g. data being transmitted outside the firewall of the SAP Data Center)./
Jika data ditransfer antara SAP dan pelanggannya, tindakan-tindakan perlindungan untuk Data Pribadi yang ditransfer disetujui bersama dan menjadi bagian dalam perjanjian yang relevan. Hal ini berlaku untuk transfer data berbasis jaringan dan fisik. Dalam kasus apa pun, Pelanggan menerima tanggung jawab untuk setiap transfer data setelah berada di luar sistem yang dikendalikan oleh SAP (misalnya data yang dikirim di luar *firewall* Pusat Data SAP).

1.5 Data Input Control. /
Kendali Input Data.

- SAP only allows authorized personnel to access Personal Data as required in the course of their duty./
  SAP hanya mengizinkan personel resmi untuk mengakses Data Pribadi sebagaimana yang diperlukan selama penugasan mereka.
- SAP has in most cases implemented a logging system for input, modification and deletion, or blocking of Personal Data by SAP or its subprocessors within the Cloud Service to the extent technically possible./
  SAP telah pada umumnya mengimplementasikan sistem pencatatan untuk input, modifikasi, dan penghapusan, atau pemblokiran Data Pribadi oleh SAP atau subprosesornya dalam Layanan Cloud sejauh mungkin secara teknis.

1.6 Job Control./
Kendali Pekerjaan.

- SAP uses controls and processes to monitor compliance with contracts between SAP and its customers, subprocessors or other service providers./
  SAP menggunakan kendali dan proses untuk memantau kepatuhan dengan kontrak antara SAP dan pelanggan, subprosesor, atau penyedia layanan lainnya.
- As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard./
  Sebagai bagian dari Kebijakan Keamanan SAP, Data Pribadi mensyaratkan setidaknya tingkat perlindungan yang sama sebagaimana informasi "rahasia" sesuai dengan standar Klasifikasi Informasi SAP.
- All SAP employees and contractual subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of SAP customers and partners./
  Semua karyawan dan subprosesor kontrak atau penyedia layanan lainnya dari SAP terikat berdasarkan kontrak untuk menghargai kerahasiaan semua informasi yang sensitif, termasuk rahasia dagang para pelanggan dan mitra SAP.

1.7 Availability Control./
Kendali Ketersediaan.

- SAP employs regular backup processes to provide restoration of business-critical systems as and when necessary./
  SAP menggunakan proses pencadangan reguler untuk menyediakan pemulihan sistem bisnis penting jika dan bila diperlukan.
- SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centers./
  SAP menggunakan suplai daya tidak terputus (sebagai contoh: UPS, baterai, generator, dll.) untuk melindungi ketersediaan daya ke Pusat Data.

- SAP has defined business contingency plans for business-critical processes and may offer disaster recovery strategies for business critical Services as further set out in the Documentation or incorporated into the Order Form for the relevant Cloud Service./
  SAP telah menetapkan rencana cadangan bisnis untuk proses bisnis penting dan dapat menawarkan strategi pemulihan bencana untuk Layanan penting bisnis sebagaimana ditetapkan lebih lanjut dalam Dokumentasi atau digabungkan ke dalam Formulir Pemesanan untuk Layanan Cloud terkait.
- Emergency processes and systems are regularly tested./
  Proses dan sistem darurat diuji secara berkala.

1.8 Data Separation Control./
Kendali Pemisahan Data.

- SAP uses the technical capabilities of the deployed software (for example: multi- tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers./
  SAP menggunakan kemampuan-kemampuan teknis dari perangkat lunak yang ditempatkan (misalnya, lanskap sistem terpisah atau kepemilikan majemuk) untuk mencapai pemisahan data antara Data Pribadi yang berasal dari berbagai pelanggan.
- Customer (including its Controllers) has access only to its own data./
  Pelanggan (termasuk Pengendalinya) memiliki akses hanya ke datanya sendiri.
- If Personal Data is required to handle a support incident from Customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems./
  Jika Data Pribadi diperlukan untuk menangani insiden dukungan dari Pelanggan, data ditetapkan untuk pesan tertentu tersebut dan digunakan hanya untuk memproses pesan tersebut, Data Pribadi tidak diakses untuk memproses pesan lain mana pun. Data ini disimpan dalam sistem dukungan khusus.

1.9 Data Integrity Control./
Kendali Integritas Data.

- SAP has implemented a multi-layered defense strategy as a protection against unauthorized modifications./
  SAP telah mengimplementasikan strategi pertahanan multi-lapisan sebagai perlindungan terhadap modifikasi-modifikasi yang tidak resmi.
- In particular, SAP uses the following to implement the control and measure sections described above.
  Khususnya, SAP menggunakan hal-hal berikut ini untuk mengimplementasikan pasal tindakan dan kendali yang dideskripsikan di atas.
- *Firewall*;
- Security Monitoring Center;/
  Pusat Pemantauan Keamanan;
- Antivirus software;/
  Perangkat lunak antivirus;
- Backup and recovery;/
  Pencadangan dan pemulihan;
- External and internal penetration testing and/or regular external audits to prove security measures./
  Pengujian penetrasi eksternal dan internal dan/atau audit eksternal berkala untuk membuktikan tindakan keamanan.

Appendix 3 to the DPA and, if applicable, the Standard Contractual Clauses/
Lampiran 3 terhadap DPA dan, jika berlaku, Klausul Kontrak Standar

The following table sets out the relevant Articles of GDPR and corresponding terms of the DPA for illustration purposes only./
Tabel berikut menjelaskan Pasal yang relevan dari GDPR dan ketentuan terkait DPA untuk tujuan ilustrasi saja.

Article of GDPR/ Pasal GDPR	**Section of DPA/ Bagian DPA**	**Click on link to see Sectin/ Klik pada tautan untuk melihat Bagian**
28(1)	2 and Appendix 2/ 2 dan Lampiran 2	Security of Processing and Appendix 2, Technical and Organizational Measures./ Security of Processing/Keamanan Pemrosesan dan Lampiran 2, Tindakan Teknis dan Organisasional.
28(2), 28(3) (d) and 28 (4)/ 28(2), 28(3) (d) dan 28 (4)	6	Subprocessors Subprosesor
28 (3) sentence 1/ 28 (3) kalimat 1	1.1 and Appendix 1, 1.2/ 1.1 dan Lampiran 1, 1.2	Purpose and Application Structure/ Tujuan dan Aplikasi./ Struktur.
28(3) (a) and 29/ 28(3) (a) dan 29	3.1 and 3.2 3.1 dan 3.2	Instructions from Customer. Processing on Legal Requirement. Instruksi untuk Pelanggan. Memproses Persyaratan Hukum
28(3) (b)	3.3	Personnel./ Personel.
28(3) (c) and 32/ 28(3) (c) dan 32	2 and Appendix 2/ 2 dan Lampiran 2	Security of Processing and Appendix 2, Technical and Organizational Measures Security of Processing/ Keamanan Pemrosesan dan Lampiran 2, Tindakan Teknis dan Organisasional.
28(3) (e)	3.4	Cooperation Kerja Sama
28(3) (f) and 32-36/ 28(3) (f) dan 32-36	2 and Appendix 2, 3.5, 3.6/ 2 dan Lampiran 2, 3.5, 3.6	Security of Processing and Appendix 2, Technical and Organizational Measures. Personal Data Breach Notification. Data Protection Impact Assessment./ Keamanan Pemrosesan dan Lampiran 2, Tindakan Teknis dan Organisasional. Pemberitahuan Pelanggaran Data Pribadi./ Penilaian Dampak Perlindungan Data.
28(3) (g)	4	Data export and Deletion. Ekspor dan Penghapusan Data.
28(3) (h)	5	Certifications and Audits Sertifikasi dan Audit
28 (4)	6	Subprocessor Subprosesor
30	8	Documentation; Records of processing. Dokumentasi; Catatan Pemrosesan
46(2) (c)	7.2	Standard Contractual Clauses. Klausul Kontraktual Standar.

Appendix 4
Lampiran 4

[*The Standard Contractual Clauses set out in this Appendix 4 are current as at 31 March 2018, and the Indonesia translation is provided as a matter of convenience only. These Standard Contractual Clauses are automatically subject to all updates by the European Commission and as subsequently published by the European Commission. Customer should always access the URL https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010D0087 for the current versions of the Standard Contractual Clauses. Customer's local language may not be supported at the European Commission, or at its URL. It will be Customer's responsibility to ensure that it is aware of the current version/s of the Standard Contractual Clauses and to manage for itself and its Controllers all required translations of the updated Standard Contractual Clauses]* // [*Pasal Kontraktual Standar yang diatur pada Ketentuan Tambahan 4 ini adalah yang terkini pada tanggal 31 Maret 2018, dan terjemahan dalam Bahasa Indonesia disediakan hanya untuk kenyamanan saja. Pasal-pasal Kontraktual Standar ini secara otomatis tergantung pada seluruh update yang dilakukan Komisi Eropa dan yang selanjutnya dipublikasikan oleh Komisi Eropa. Pelanggan selalu dapat mengakses URL https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010D0087 untuk mendapat versi terkini dari Pasal-Pasal Kontraktual Standar. Adalah tanggung jawab Pelanggan untuk memastikan bahwa pihaknya mengetahui versi(-versi) terkini dari Pasal-Pasal Kontraktual Standard an mengatur seluruh terjemahan yang diperlukan atas Pasal-Pasal Kontraktual Standar untuk pihaknya dan Kontrolernya*]

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)[1]/ KLAUSUL KONTRAKTUAL STANDAR (PROSESOR)[1]

For the purposes of Article 26(2) of Directive 95/46/EC (or, after 25 May 2018, Article 44 et seq. of Regulation 2016/79) for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection/
Untuk tujuan Pasal 26(2) dalam Directive 95/46/EC (atau, setelah 25 Mei 2018, Pasal 44 et seq. dari Undang-undang 2016/79) untuk pengalihan data pribadi kepada prosesornya yang diadakan di negara-negara ketiga yang tidak menjamin tingkat perlindungan data yang memadai

Customer also on behalf of the other Controllers/
Pelanggan juga atas nama Pengendali lainnya
(in the Clauses hereinafter referred to as the '**data exporter'**)/
(Dalam Klausul ini disebut sebagai**'pengekspor data'**)

and/
dan

SAP
(in the Clauses hereinafter referred to as the **'data importer'**)/
(dalam Klausul ini disebut sebagai **'pengimpor data'**)

each a 'party'; together 'the parties',/
masing-masing sebagai 'pihak'; bersama-sama sebagai 'para pihak',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1./

[1] Sesuai dengan Commission Decision tertanggal 5 Februari 2010 (2010/87/EU)

TELAH MENYEPAKATI mengenai Klausul-klausul Kontraktual berikut ini (Klausul-klausul) untuk mengemukakan pelindung yang memadai terkait dengan perlindungan privasi dan hak-hak dasar dan kebebasan individu untuk pengalihan dengan pengekspor data ke pengimpor data dari data pribadi yang disebutkan dalam Apendiks 1.

Clause 1/
Klausul 1

Definitions/
Definisi

For the purposes of the Clauses:/
Untuk tujuan Klausul-klausul:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;/
'data pribadi', 'kategori data khusus', 'proses/pemrosesan', 'pengendali', 'prosesor', 'subjek data' dan 'otoritas pengawas', akan memiliki arti yang sama seperti yang di Undang-Undang 95/46/EC Parlemen Eropa dan dari Dewan tanggal 24 Oktober 1995 mengenai perlindungan individu terkait pemrosesan data pribadi dan pergerakan bebas data tersebut;

(b) 'the data exporter' means the controller who transfers the personal data;/
'pengekspor data' berarti pengendali yang mengalihkan data pribadi;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;/
'pengimpor data' berarti prosesor yang sepakat untuk menerima dari data pribadi dari pengekspor data yang dimaksudkan untuk pemrosesan atas namanya setelah pengalihan sesuai dengan instruksinya dan syarat Klausul-klausul dan yang tidak tunduk pada sistem negara ketiga yang memastikan perlindungan yang memadai dalam makna dari Pasal 25(1) Undang-Undang 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;/
'sub-prosesor' berarti setiap prosesor yang dilibatkan oleh pengimpor data atau oleh setiap sub-prosesor lain dari pengimpor data yang sepakat untuk menerima dari pengimpor data atau dari sub-prosesor lain data pribadi pengimpor data yang secara ekslusif dimaksudkan untuk kegiatan pemrosesan yang akan dilaksanakan atas nama pengekspor data setelah pengalihan sesuai dengan instruksinya, syarat-syarat dari Klausul-klausul dan syarat-syarat subkontrak tertulis;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the

processing of personal data applicable to a data controller in the Member State in which the data exporter is established;/

'undang-undang perlindungan data yang berlaku' berarti perundang-undangan yang melindungi hak-hak dasar dan kebebasan individu, khususnya, hak mereka atas privasi terkait dengan pemrosesan data pribadi yang berlaku bagi pengendali data di Negara Anggota di mana pengekspor data berada;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing./

'tindakan keamanan organisasi dan teknis' berarti tindakan-tindakan yang ditujukan pada perlindungan data pribadi terhadap kerusakan yang tidak sengaja atau melanggar hukum atau kerugian yang tidak disengaja, perubahan, akses atau pengungkapan yang tidak sah, khususnya jika pemrosesan melibatkan transmisi data pada jaringan, dan terhadap semua bentuk pemrosesan yang melanggar hukum.

Clause 2/
Klausul 2

Details of the transfer/
Detail pengalihan

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses./
Detail pengalihan tersebut dan terutama kategori khusus data pribadi jika ada disebutkan dalam Apendiks 1 yang membentuk bagian tak terpisahkan dari Klausul-klausul.

Clause 3/
Klausul 3

Details of the transfer/
Klausul Penerima Pihak Ketiga

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary./

Subjek data dapat memberlakukan Klausul ini pada pengekspor data, Klausul 4(b) hingga (i), Klausul 5(a) hingga (e), dan (g) hingga (j), Klausul 6(1) dan (2), Klausul 7, Klausul 8(2), dan Klausul 9 hingga 12, sebagai penerima pihak ketiga.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7,Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity./

Subjek data dapat memberlakukan Klausul ini pada pengimpor data, Klausul 5(a) hingga (e) dan (g), Klausul 6, Klausul 7, Klausul 8(2), Klausul 9 hingga 12, jika pengekspor data secara faktanya telah menghilang atau telah berhenti dari keberadaan secara hukum kecuali setiap badan penerus telah mengasumsikan keseluruhan kewajiban hukum dari pengekspor data

dengan kontrak atau dengan tindakan hukum, sebagai akibatnya hal ini mengambil hak dan kewajiban pengekspor data, jika subjek data dapat memberlakukan hal tersebut kepada badan tersebut.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses./

Subjek data dapat memberlakukan Klausul ini pada subprosesor, Klausul 5(a) hingga (e) dan (g), Klausul 6, Klausul 7, Klausul 8(2), Klausul 9 hingga 12, jika pengekspor data dan pengimpor data secara faktanya telah menghilang atau telah berhenti dari keberadaan secara hukum atau telah menjadi bangkrut, kecuali setiap badan penerus telah mengasumsikan keseluruhan kewajiban hukum dari pengekspor data dengan kontrak atau dengan tindakan hukum, sebagai akibatnya hal ini mengambil hak dan kewajiban pengekspor data, jika subjek data dapat memberlakukan hal tersebut kepada badan tersebut. Kewajiban pihak ketiga tersebut dari subprosesornya akan dibatasi untuk operasi pemrosesannya sendiri sesuai Klausul tersebut.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law./

Para pihak tidak keberatan subjek data diwakili oleh asosiasi atau badan lain jika subjek data secara tegas menginginkannya dan jika diizinkan oleh hukum nasional.

Clause 4/
Klausul 4

Obligations of the data exporter/
Kewajiban pengekspor data

The data exporter agrees and warrants:/
Pengekspor data setuju dan menjamin:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;/

bahwa pemrosesan tersebut, termasuk pengalihan itu sendiri, dari data pribadi telah dan akan tetap dilaksanakan sesuai dengan ketentuan terkait undang-undang perlindungan data yang berlaku (dan, jika ada, telah diberitahukan kepada otoritas terkait dari Negara Anggota di mana pengekspor data berada) dan tidak melanggar ketentuan terkait dari Negara tersebut;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;/

bahwa telah diinstruksikan dan selama durasi layanan pemrosesan data pribadi akan menginstruksikan pengimpor data untuk memroses data pribadi tersebut yang dialihkan hanya atas nama pengekspor data dan sesuai dengan undang-undang perlindungan data yang berlaku dan Klausul tersebut;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;/

bahwa pengimpor data akan memberikan jaminan yang mencukupi terkait dengan tindakan keamanan organisasi dan teknis yang dinyatakan dalam Apendiks 2 kontrak ini;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;/

bahwa setelah penilaian persyaratan undang-undang perlindungan data yang berlaku, tindakan keamanan sesuai untuk melindungi data pribadi terhadap kerusakan yang melanggar hukum atau tidak sengaja atau kerugian yang tidak sengaja, perubahan, akses atau pengungkapan tidak sah, khususnya jika pemrosesan melibatkan transmisi data pada jaringan, dan terhadap semua bentuk pemrosesan yang melanggar hukum, dan bahwa tindakan-tindakan ini memastikan tingkat keamanan yang sesuai dengan risiko yang ada pada pemrosesan dan sifat data yang akan dilindungi tersebut dengan memerhatikan keadaan seni dan biaya pelaksanaannya;

(e) that it will ensure compliance with the security measures;/

bahwa pengimpor data akan memastikan kepatuhan dengan tindakan keamanan;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;/

bahwa, jika pengalihan melibatkan kategori data, subjek data telah diinformasikan atau akan diinformasikan sebelumnya, atau sesegera mungkin setelahnya, pengalihan di mana data tersebut akan ditransmisikan kepada negara ketiga yang tidak memberikan perlindungan yang memadai dalam makna Undang-Undang 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;/

akan meneruskan pemberitahuan yang diperoleh dari pengimpor data atau sub-prosesor sesuai Klausul 5(b) dan Klausul 8(3) kepada otoritas pengawas perlindungan data jika pengekspor data memutuskan untuk tetap mengalihkan atau untuk mengangkat penangguhan;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;/

akan menyediakan bagi subjek data sesuai permintaan salinan Klausul-klausul, dengan pengecualian Apendiks 2, dan uraian ringkasan tindakan keamanan, serta salinan kontrak untuk layanan pemrosesan yang telah dibuat sesuai dengan Klausul-klausul, kecuali Klausul-kausul atau kontrak tersebut mencakup informasi komersil, di mana importir dapat menghilangkan informasi komersil tersebut;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and/
bahwa, dalam hal subpemrosesan, kegiatan pemrosesan dilaksanakan sesuai dengan Klausul 11 oleh sub prosesor yang memberikan setidaknya tingkat perlindungan yang sama untuk data pribadi dan hak-hak subjek data sebagai pengimpor data sesuai dengan Klausul-klausul tersebut; dan

(j) that it will ensure compliance with Clause 4(a) to (i)./
bahwa pengimpor data akan memastikan kepatuhan terhadap Klausul 4(a) hingga (i).

Clause 5/
Klausul 5

Obligations of the data importer/
Kewajiban pengimpor data

The data importer agrees and warrants:/
Pengimpor data setuju dan menjamin:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;/
akan memroses data pribadi hanya atas nama pengekspor data dan sesuai dengan instruksinya dan Klausul-klausul; jika importir tidak dapat memberikan kepatuhan tersebut karena alasan apapun, importir sepakat untuk segera memberitahuan pengekspor data atas ketidakmampuannya untuk mematuhi, dalam hal ini pengekspor data tersebut berhak menangguhkan pengalihan data dan/atau mengakhiri kontrak;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;/
bahwa tidak ada alasan untuk menyakini bahwa perundang-undangan yang berlaku padanya mencegah importir dari mematuhi instruksi yang diterima dari pengekspor data dan kewajibannya sesuai dengan kontrak dan jika ada perubahan pada perundang-undangan ini yang mungkin memiliki pengaruh bertentangan penting pada jaminan dan kewajiban yang diberikan oleh Klausul-klausul, importir akan segera memberitahu perubahan tersebut kepada pengekspor data sesegera mungkin setelah diketahui, dalam hal ini pengekspor data berhak untuk menangguhkan pengalihan data dan/atau mengakhiri kontrak tersebut;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;/

bahwa importir telah melaksanakan tindakan keamanan organisasi dan teknis yang disebutkan dalam Apendiks 2 sebelum pemrosesan data pribadi dialihkan;

(d) that it will promptly notify the data exporter about:/

bahwa importir akan segera memberitahu pengekspor data tentang:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;/

setiap permintaan yang mengikat secara hukum untuk pengungkapan data pribadi oleh otoritas penegak hukum kecuali dilarang, misalnya larangan sesuai undang-undang kriminal untuk menjaga kerahasiaan penyelidikan penegakkan hukum;

(ii) any accidental or unauthorised access; and/

setiap akses yang tidak sah atau tidak sengaja; dan

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;/

setiap permintaan yang diterima langsung dari subjek data tanpa menanggapi permintaan tersebut, kecuali telah diberi wewenang untuk melakukannya;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;/

untuk menangani dengan segera dan benar semua pertanyaan dari pengekspor data kepada pemrosesan data pribadinya sesuai dengan pengalihan dan untuk mematuhi saran otoritas pengawas terkait dengan pemrosesan data yang dialihkan;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;/

atas permintaan pengekspor data untuk menyerahkan fasilitas pemrosesan data untuk mengaudit kegiatan pemrosesan yang tercakup dalam Klausul-klausul yang harus dilaksanakan oleh pengekspor data atau badan penyelidik yang tergabung dari para anggota independen dan memiliki kualifikasi profesional yang diperlukan terikat oleh tugas kerahasiaan, yang dipilih oleh pengekspor data, jika ada, dalam perjanjian dengan otoritas pengawas;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;/

akan memberikan kepada subjek data atas permintaan salinan Klausul-klausul, atau setiap kontrak yang ada untuk sub pemrosesan kecuali Klausul-klausul atau kontrak tersebut mencakup informasi komersil, dalam hal ini importir dapat menghilangkan informasi komersil tersebut, dengan pengecualian Apendiks 2 yang akan diganti dengan uraian ringkasan tindakan

keamanan dalam kasus-kasus tersebut di mana subjek data tidak dapat memeroleh salinan dari pengekspor data tersebut;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;/
bahwa, dalam hal sub pemrosesan, importer telah sebelumnya memberitahukan pengekspor data dan memeroleh persetujuan tertulis;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;/
bahwa layanan pemrosesan oleh subprosesor akan dilaksanakan sesuai dengan Klausul 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter./
akan segera mengirimkan salinan perjanjian subprosesor yang ada yang terdapat dalam Klausul kepada pengekspor data.

Clause 6/
Klausul 6

Liability/
Kewajiban

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered./
Para pihak sepakat bahwa setiap subjek data, yang menderita kerugian sebagai akibat pelanggaran kewajiban yang tercantum dalam Klausul 3 atau dalam Klausul 11 oleh pihak mana pun atau subprosesor berhak mendapatkan ganti rugi dari pengekspor data untuk kerugian yang dialami.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity./
Jika subjek data tidak dapat mengajukan klaim atas ganti rugi tersebut sesuai dengan ayat 1 kepada pengekspor data, yang timbul dari pelanggaran pengimpor data atau subprosesornya atas kewajiban mereka yang tercantum dalam Klausul 3 atau Klausul 11, karena pengekspor data secara faktanya telah menghilang atau menyudahi keberadaannya secara hukum atau bangkrut, pengimpor data sepakat bahwa subjek data dapat mengeluarkan klaim terhadap pengimpor data seolah-olah ia adalah pengekspor data, kecuali badan penggantinya telah mengasumsikan seluruh kewajiban hukum pengekspor data dengan kontrak pelaksanaan hukum, di mana dalam hal ini subjek data dapat menegakkan haknya terhadap badan tersebut.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities./

Pengimpor data tidak dapat mengandalkan pelanggaran oleh subprosesor terhadap kewajibannya guna menghindari kewajibannya sendiri.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses./

Jika subjek data tidak dapat mengajukan klaim kepada pengekspor data atau pengimpor data yang dinyatakan dalam ayat 1 dan 2, yang timbul dari pelanggaran subprosesor atas kewajiban mereka yang dinyatakan dalam Klausul 3 atau Klausul 11 karena pengekspor data maupun pengimpor data secara faktanya telah menghilang atau menyudahi keberadaannya secara hukum atau bangkrut, subprosesor sepakat bahwa subjek data dapat mengeluarkan klaim terhadap subprosesor terkait dengan operasi pemrosesannya sendiri sesuai dengan Klausul tersebut seolah-olah ia adalah pengekspor data ataupun pengimpor data, kecuali badan penggantinya telah mengasumsikan seluruh kewajiban hukum pengekspor data dengan kontrak pelaksanaan hukum, di mana dalam hal ini subjek data dapat menegakkan haknya terhadap badan tersebut. Kewajiban subprosesor akan terbatas pada operasi pemrosesannya sendiri sesuai Klausul ini.

Clause 7/
Klausul 7

Mediation and jurisdiction/
Mediasi dan Yurisdiksi

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:/

Pengimpor data sepakat bahwa jika subjek data memohon kepada penerima pihak ketiga hak dan/atau mengklaim ganti rugi untuk kerugian sesuai dengan Klausul ini, pengimpor data akan menerima keputusan subjek data tersebut:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;/

untuk menyerahkan perselisihan tersebut pada proses mediasi, oleh personel independen atau, jika berlaku, oleh otoritas pengawas;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established./

akan menyerahkan perselisihan tersebut pada pengadilan di Negara Anggota di mana pengekspor data berada.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law./

Para pihak menyetujui bahwa pilihan yang diambil oleh subjek data tidak akan mengabaikan hak substantif atau prosedural untuk mengupayakan ganti rugi sesuai dengan ketentuan hukum nasional atau internasional lainnya.

Clause 8/
Klausul 8

Cooperation with supervisory authorities/
Kerja sama dengan otoritas pengawas

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law./
Pengekspor data sepakat akan mendepositokan salinan kontrak ini dengan otoritas pengawas jika permintaan atau deposito tersebut diperlukan sesuai undang-undang perlindungan data yang berlaku.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law./
Para pihak sepakat bahwa otoritas pengawas berhak melaksanakan audit atas pengimpor data, dan atas sub prosesor yang memiliki cakupan yang sama dan tunduk pada ketentuan yang sama yang akan berlaku pada audit atas pengekspor data sesuai dengan undang-undang perlindungan data yang berlaku.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b)./
Pengimpor data akan segera memberitahukan pengekspor data tentang adanya perundang-undangan yang berlaku padanya atau kepada sub prosesor yang mencegah pelaksanaan audit pengimpor data, atau subprosesor, sesuai dengan ayat 2. Dalam hal ini pengekspor data akan berhak untuk melakukan tindakan yang disebutkan dalam Klausul 5(b).

Clause 9/
Klausul 9

Governing law/
Undang-undang yang mengatur

The Clauses shall be governed by the law of the Member State in which the data exporter is established./
Klausul-klausul tersebut akan diatur oleh undang-undang Negara Anggota di mana pengekspor data berada.

Clause 10/
Klausul 10

Variation of the contract/
Variasi Kontrak

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause./
Para pihak berusaha tidak mengubah atau memodifikasi Klausul-klausul. Ini tidak menghalangi para pihak dari menambahkan klausul tentang masalah terkait bisnis jika diperlukan selama hal tersebut tidak bertentangan dengan Klausul ini.

Clause 11/
Klausul 11

Sub-processing/
Subpemrosesan

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement./

Pengimpor data tidak akan mensubkontrakkan operasi pemrosesan yang dilakukan atas nama pengekspor data sesuai dengan Klausul ini tanpa persetujuan tertulis sebelumnya dari pengekspor data. Jika pengimpor data mensubkontrakkan kewajibannya sesuai dengan Klausul ini, dengan persetujuan pengekspor data, importir hanya akan melakukannya dengan cara perjanjian tertulis sesuai dengan Klausul ini. Jika subprosesor tidak dapat memenuhi kewajiban perlindungan datanya sesuai dengan perjanjian tertulis tersebut pengimpor data akan tetap berkewajiban kepada pengekspor data untuk kinerja kewajiban subprosesor sesuai dengan perjanjian tersebut.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses./

Kontrak tertulis sebelumnya antara pengimpor data dan subprosesor juga akan menyediakan untuk klausul penerima pihak ketiga seperti yang tercantum dalam Klausul 3 untuk kasus-kasus di mana subjek data tidak dapat mengajukan klaim untuk ganti rugi yang dinyatakan dalam ayat 1 dari Klausul 6 kepada pengekspor data atau pengimpor data karena mereka secara faktanya telah menghilang atau menyudahi keberadaannya secara hukum atau bangkrut dan tidak ada badan pengganti telah mengasumsikan seluruh kewajiban hukum dari

pengekspor data atau pengimpor data dengan kontrak atau operasi hukum. Kewajiban pihak ketiga tersebut dari subprosesornya akan dibatasi pada operasi pemrosesannya sendiri sesuai Klausul tersebut.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established./

Ketentuan terkait aspek perlindungan data untuk subpemrosesan kontrak yang terdapat dalam ayat 1 akan diatur oleh undang-undang Negara Anggota di mana pengekspor data berada.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority./

Pengekspor data akan menyimpan daftar perjanjian subpemrosesan yang termasuk dalam Klausul dan diberitahukan oleh pengimpor data sesuai dengan Klausul 5(j), yang akan diperbarui setidaknya setahun sekali. Daftar tersebut harus tersedia bagi otoritas pengawas perlindungan data pengekspor data.

Clause 12/
Klausul 12

Obligation after the termination of personal data-processing services/
Kewajiban setelah pengakhiran layanan pemrosesan data pribadi

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore./

Para pihak sepakat bahwa pada saat pengakhiran ketentuan layanan pemrosesan data, pengimpor data dan subprosesor akan, atas pilihan pengekspor data, mengembalikan semua data pribadi yang dialihkan dan salinannya kepada pengekspor data atau akan menghancurkan semua data pribadi tersebut dan menyatakan kepada pengekspor data bahwa ia telah melakukannya, kecuali perundang-undangan yang dikenakan pada pengimpor data mencegahnya dari mengembalikan atau menghancurkan semua atau sebagian data pribadi yang dialihkan tersebut. Jika seperti itu, pengimpor data menjamin bahwa ia akan menjaga kerahasiaan dari data pribadi yang dialihkan dan tidak akan secara aktif memroses lagi data pribadi yang dialihkan tersebut.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1./

Pengimpor data dan sub prosesor menjamin bahwa sesuai permintaan pengekspor data dan/atau otoritas pengawas, ia akan menyerahkan fasilitas pemrosesan datanya untuk audit atas tindakan yang dinyatakan dalam ayat 1.