PERSONAL DATA PROCESSING AGREEMENT FOR SAP CLOUD SERVICES

1. BACKGROUND

1.1 Purpose.

This document is a data processing agreement ("**DPA**") between SAP and Customer and applies to Personal Data provided by Customer and each Data Controller in connection with their use of the Cloud Service. It states the technical and organizational measures SAP uses to protect Personal Data that is stored in the production system of the Cloud Service.

1.2 Application of the Standard Contractual Clauses Document.

If processing of Personal Data involves an International Transfer, the Standard Contractual Clauses apply as stated in Section 5 and are incorporated by reference.

1.3 Governance.

Except as provided in Section 5.2, Customer is solely responsible for administration of all requests from other Data Controllers. Customer will bind any other Data Controller it permits to use the Cloud Service to the terms of this DPA.

2. APPENDICES

Customer and its Data Controllers determine the purposes of collecting and processing Personal Data in the Cloud Service. Appendix 1 states the details of the processing SAP will provide via the Cloud Service. Appendix 2 states the technical and organizational measures SAP applies to the Cloud Service, unless the Agreement states otherwise.

3. SAP OBLIGATIONS

3.1 Instructions from Customer.

SAP will follow instructions received from Customer (on its own behalf or on behalf of its Data Controllers) with respect to Personal Data, unless they are (i) legally prohibited or (ii) require material changes to the Cloud Service. SAP may correct or remove any Personal Data in accordance with the Customer's instruction. If SAP cannot comply with an instruction, it will promptly notify Customer (email permitted).

3.2 Data Secrecy.

To process Personal Data, SAP and its Subprocessors will only use personnel who are bound to observe data and telecommunications secrecy under the Data Protection Law. SAP and

PERJANJIAN PEMROSESAN DATA PRIBADI UNTUK LAYANAN CLOUD SAP

1. LATAR BELAKANG

1.1 Tujuan.

Dokumen ini merupakan perjanjian pemrosesan data (*data processing agreement* - "**DPA**") antara SAP dan Pelanggan dan berlaku untuk Data Pribadi yang diberikan oleh Pelanggan dan setiap Pengendali Data sehubungan dengan penggunaannya atas Layanan Cloud. Perjanjian ini menyatakan tindakan teknis dan organisasional yang digunakan SAP untuk melindungi Data Pribadi yang disimpan dalam sistem produksi Layanan Cloud.

1.2 Aplikasi Dokumen Klausul Kontraktual Standar.

Jika pemrosesan Data Pribadi mencakup Transfer Internasional, Klausul Kontraktual Standar berlaku sebagaimana yang dinyatakan dalam Pasal 5 dan digabungkan melalui referensi.

1.3 Tata Kelola.

Kecuali sebagaimana yang ditentukan dalam Pasal 5.2, Pelanggan bertanggung jawab penuh atas administrasi semua permintaan dari Pengendali Data lainnya. Pelanggan akan mengikat setiap Pengendali Data lain yang diizinkan oleh Pelanggan untuk menggunakan Layanan Cloud berdasarkan syarat-syarat DPA ini.

2. APENDIKS

Pelanggan dan Pengendali Datanya menentukan tujuan pengumpulan dan pemrosesan Data Pribadi dalam Layanan Cloud. Apendiks 1 menyatakan detail pemrosesan yang akan disediakan oleh SAP melalui Layanan Cloud. Apendiks 2 menyatakan tindakan teknis dan organisasional yang diberlakukan oleh SAP pada Layanan Cloud, kecuali apabila Perjanjian menyatakan lain.

3. KEWAJIBAN SAP

3.1 Instruksi dari Pelanggan.

SAP akan mengikuti instruksi yang diterima dari Pelanggan (atas namanya sendiri atau atas nama Pengendali Datanya) sehubungan dengan Data Pribadi, kecuali apabila instruksi tersebut (i) dilarang oleh hukum atau (ii) mewajibkan perubahan material pada Layanan Cloud. SAP dapat memperbaiki atau menghapus setiap Data Pribadi berdasarkan instruksi Pelanggan. Apabila SAP tidak dapat mematuhi instruksi, SAP akan segera memberi tahu Pelanggan (email diizinkan).

3.2 Kerahasiaan Data.

Untuk memproses Data Pribadi, SAP dan Subprosesornya hanya akan menggunakan personel yang terikat untuk mematuhi kerahasiaan telekomunikasi dan data

its Subprocessors will regularly train individuals having access to Personal Data in data security and data privacy measures.

3.3 Technical and Organizational Measures.

(a) SAP will use the appropriate technical and organizational measures stated in Appendix 2.

(b) Appendix 2 applies to the production system of the Cloud Service. Customer should not store any Personal Data in non-production environments.

(c) SAP provides the Cloud Service to SAP's entire customer base hosted out of the same data center and receiving the same Cloud Service. Customer agrees SAP may improve the measures taken in Appendix 2 in protecting Personal Data so long as it does not diminish the level of data protection.

3.4 Security Breach Notification.

SAP will promptly inform Customer if it becomes aware of any Security Breach.

3.5 Cooperation.

At Customer's request, SAP will reasonably support Customer or any Data Controller in dealing with requests from Data Subjects or regulatory authorities regarding SAP's processing of Personal Data.

4. SUBPROCESSORS

4.1 Permitted Use.

(a) Customer and Data Controllers authorize SAP to subcontract the processing of Personal Data to Subprocessors. SAP is responsible for any breaches of the Agreement caused by its Subprocessors.

(b) Subprocessors will have the same obligations as SAP does as a Data Processor (or Subprocessor) with regard to their processing of Personal Data.

(c) SAP will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection. Subprocessors may have security certifications that evidence their use of appropriate security measures. If not, SAP will regularly evaluate each

berdasarkan Undang-undang Perlindungan Data. SAP dan Subprosesornya akan secara rutin melatih individu yang memiliki akses ke Data Pribadi dalam tindakan kerahasiaan data dan keamanan data.

3.3 Tindakan Teknis dan Organisasional.

(a) SAP akan menggunakan tindakan teknis dan organisasional yang tepat yang dinyatakan dalam Apendiks 2.

(b) Apendiks 2 berlaku pada sistem produksi Layanan Cloud. Pelanggan tidak dapat menyimpan Data Pribadi apa pun dalam lingkungan nonproduksi.

(c) SAP menyediakan Layanan Cloud untuk seluruh pusat pelanggan SAP yang diselenggarakan di luar pusat data yang sama dan menerima Layanan Cloud yang sama. Pelanggan menyetujui bahwa SAP dapat meningkatkan tindakan yang dilakukan dalam Apendiks 2 untuk melindungi Data Pribadi sepanjang hal tersebut tidak mengurangi tingkat perlindungan data.

3.4 Pemberitahuan Mengenai Pelanggaran Keamanan.

SAP akan segera memberi tahu Pelanggan apabila pihaknya menyadari adanya Pelanggaran Keamanan apa pun.

3.5 Kerja Sama.

Atas permintaan Pelanggan, SAP akan mendukung Pelanggan atau Pengendali Data mana pun secara wajar dalam menangani permintaan dari Subjek Data atau badan pengawas mengenai pemrosesan Data Pribadi oleh SAP.

4. SUBPROSESOR

4.1 Penggunaan yang Diizinkan.

(a) Pelanggan dan Pengendali Data memberikan wewenang kepada SAP untuk mensubkontrakkan pemrosesan Data Pribadi kepada Subprosesor. SAP bertanggung jawab atas setiap pelanggaran terhadap Perjanjian yang disebabkan oleh Subprosesornya.

(b) Subprosesor akan memiliki kewajiban yang sama seperti yang dimiliki SAP sebagai Prosesor Data (atau Subprosesor) yang berkaitan dengan pemrosesannya pada Data Pribadi.

(c) SAP akan mengevaluasi praktik keamanan, privasi dan kerahasiaan Subprosesor sebelum pemilihan. Subprosesor dapat memiliki sertifikasi keamanan yang membuktikan penggunaannya atas tindakan keamanan yang tepat. Jika tidak, SAP akan secara

Subprocessor's security practices as they relate to data handling.

(d) If Customer requests, SAP will inform Customer of the name, address and role of each Subprocessor it uses to provide the Cloud Service.

4.2 New Subprocessors.

SAP's use of Subprocessors is at its discretion, provided that:

(a) SAP will notify Customer in advance (by email or by posting on the Support Portal) of any changes to the list of Subprocessors in place on the Effective Date (except for Emergency Replacements or deletions of Subprocessors without replacement).

(b) If Customer has a legitimate reason that relates to the Subprocessors' processing of Personal Data, Customer may object to SAP's use of a Subprocessor, by notifying SAP in writing within thirty days after receipt of SAP's notice. If Customer objects to the use of the Subprocessor, the parties will come together in good faith to discuss a resolution. SAP may choose to: (i) not use the Subprocessor or (ii) take the corrective steps requested by Customer in its objection and use the Subprocessor. If none of these options are reasonably possible and Customer continues to object for a legitimate reason, either party may terminate the Agreement on thirty days' written notice. If Customer does not object within thirty days of receipt of the notice, Customer is deemed to have accepted the new Subprocessor.

(c) If Customer's objection remains unresolved sixty days after it was raised, and SAP has not received any notice of termination, Customer is deemed to accept the Subprocessor.

4.3 Emergency Replacement.

SAP may change a Subprocessor where the reason for the change is outside of SAP's reasonable control. In this case, SAP will inform Customer of the replacement Subprocessor as soon as possible. Customer retains its right to object to a replacement Subprocessor under Section 4.2(b).

rutin mengevaluasi setiap praktik keamanan sepanjang praktik tersebut berhubungan dengan penanganan data.

(d) Jika Pelanggan Meminta, SAP akan memberi tahu Pelanggan mengenai nama, alamat dan peran dari masing-masing Subprosesor yang digunakan untuk menyediakan Layanan Cloud.

4.2 Subprosesor Baru.

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

(a) SAP akan memberi tahu Pelanggan di awal (melalui email atau melalui kiriman pada Portal Dukungan) atas setiap perubahan pada daftar Subprosesor yang tersedia pada Tanggal Mulai Berlaku (kecuali untuk Penggantian Darurat atau penghapusan Subprosesor tanpa penggantian).

(b) Jika Pelanggan memiliki alasan yang sah secara hukum yang berkaitan dengan pemrosesan Subprosesor terhadap Data Pribadi, Pelanggan dapat menolak Penggunaan Subprosesor oleh SAP, dengan memberi tahu SAP secara tertulis dalam tiga puluh hari setelah penerimaan pemberitahuan SAP. Jika Pelanggan menolak penggunaan Subprosesor, para pihak akan bertemu dengan iktikad baik untuk mendiskusikan penyelesaian. SAP dapat memilih untuk: (i) tidak menggunakan Subprosesor atau (ii) melakukan tindakan perbaikan yang diminta oleh Pelanggan dalam penolakannya dan menggunakan Subprosesor. Jika tidak satu pun opsi tersebut memungkinkan secara wajar dan Pelanggan terus menolak karena alasan yang sah secara hukum, pihak mana pun dapat mengakhiri Perjanjian dengan pemberitahuan tertulis tiga puluh hari. Jika Pelanggan tidak menolak dalam tiga puluh hari penerimaan pemberitahuan, Pelanggan dianggap telah menerima Subprosesor yang baru.

(c) Jika penolakan Pelanggan tetap tidak terselesaikan dalam enam puluh hari setelah diajukan, dan SAP belum menerima pemberitahuan pengakhiran apa pun, Pelanggan dianggap menerima Subprosesor.

4.3 Penggantian Darurat.

SAP dapat mengubah Subprosesor, dengan ketentuan bahwa alasan perubahan tersebut di luar kendali wajar SAP. Dalam hal ini, SAP akan memberi tahu Pelanggan mengenai Subprosesor pengganti sesegera mungkin. Pelanggan memiliki haknya untuk menolak Subprosesor pengganti berdasarkan Pasal 4.2(b).

5. INTERNATIONAL TRANSFERS

5.1 Limitations on International Transfer. Personal Data from an EEA or Swiss Data Controller(s) may only be exported or accessed by SAP or its Subprocessors outside the EEA or Switzerland (**"International Transfer"**):

(a) If the recipient, or the country or territory in which it processes or accesses Personal Data, ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data as determined by the European Commission; or

(b) in accordance with Section 5.2.

5.2 Standard Contractual Clauses and Multi-tier Framework.

(a) The Standard Contractual Clauses apply where there is an International Transfer to a country that does not ensure an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data as determined by the European Commission.

(b) For Third Country Subprocessors, SAP has entered into the unchanged version of the Standard Contractual Clauses prior to the Subprocessor's processing of Personal Data. Customer hereby (itself as well as on behalf of each Data Controller) accedes to the Standard Contractual Clauses between SAP and the Third Country Subprocessor. SAP will enforce the Standard Contractual Clauses against the Subprocessor on behalf of the Data Controller if a direct enforcement right is not available under Data Protection Law.

(c) Nothing in this DPA will be construed to prevail over any conflicting clause of the Standard Contractual Clauses.

6. CERTIFICATIONS AND AUDITS

6.1 Customer Audits. Customer or its independent third party auditor may audit SAP's control environment and security practices relevant to Personal Data processed by SAP only if:

(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

5. TRANSFER INTERNASIONAL.

5.1 Batasan pada Transfer Internasional. Data Pribadi dari EEA atau Pengendali(-pengendali) Data Swiss hanya dapat diekspor atau diakses oleh SAP atau Subprosesornya di luar EEA atau Swiss (**"Transfer Internasional"**):

(a) Jika penerima, atau negara atau teritori di mana hal tersebut memproses atau mengakses Data Pribadi, memastikan adanya tingkat perlindungan yang memadai atas hak dan kebebasan Subjek Data sehubungan dengan pemrosesan Data Pribadi sebagaimana yang ditentukan oleh Komisi Eropa; atau

(b) sesuai dengan Pasal 5.2.

5.2 Klausul Kontraktual Standar dan Kerangka kerja Multi-*tier*.

(a) Klausul Kontraktual Standar ini berlaku apabila terdapat Transfer Internasional pada sebuah negara yang tidak memastikan adanya tingkat perlindungan yang memadai atas hak dan kebebasan Subjek Data sehubungan dengan pemrosesan Data Pribadi sebagaimana yang ditentukan oleh Komisi Eropa.

(b) Untuk Subprosesor Negara Ketiga, SAP telah mengadakan versi Klausul Kontraktual Standar yang tidak diubah sebelum pemrosesan Data Pribadi oleh Subprosesor. Pelanggan dengan ini (dirinya sendiri serta atas nama setiap Pengendali Data) menyetujui Klausul Kontraktual Standar antara SAP dan Subprosesor Negara Ketiga. SAP akan memberlakukan Klausul Kontraktual Standar terhadap Subprosesor atas nama Pengendali Data jika hak penegakan langsung tidak tersedia berdasarkan Undang-undang Perlindungan Data.

(c) Tidak ada satu pun dalam DPA ini yang akan ditafsirkan sebagai pengganti setiap klausul yang bertentangan pada Klausul Kontraktual Standar.

6. SERTIFIKASI DAN AUDIT

6.1 Audit Pelanggan. Pelanggan atau auditor pihak ketiganya yang independen dapat mengaudit praktik keamanan dan lingkungan kendali SAP sehubungan dengan Data Pribadi yang diproses oleh SAP hanya jika:

(a) SAP belum memberikan bukti kepatuhannya yang memadai atas tindakan teknis dan organisasional yang melindungi sistem produksi Layanan Cloud dengan menyediakan: (i) sertifikasi untuk kepatuhan dengan ISO 27001 atau

with ISO 27001 or other standards (scope as defined in the certificate); or (ii) a valid ISAE3402 and/or ISAE3000 attestation report. Upon Customer's request -SOC Audit reports or ISO certifications are available through the third party auditor or SAP;

(a) A Security Breach has occurred;

(b) Customer or another Data Controller has reasonable grounds to suspect that SAP is not in compliance with its obligations under this DPA;

(c) An audit is formally requested by Customer's or another Data Controller's data protection authority; or

(d) Mandatory Data Protection Law provides Customer with a direct audit right.

Where Customer audits SAP's environment, SAP will reasonably support Customer in its audit processes.

6.2 Audit Restrictions.

The Customer audit will be limited to once in any twelve month period, and limited in time to a maximum of 3 business days and scope as reasonably agreed in advance between the parties. Reasonable advance notice of at least sixty days is required, unless Data Protection Law requires earlier audit. SAP and Customer will use current certifications or other audit reports to minimize repetitive audits. Customer and SAP will each bear their own expenses of audit, unless the Customer is auditing under Section 6.1 (c) (unless such audit reveals a breach by SAP in which case SAP shall bear its own expenses of audit), 6.1 (d) or 6.1 (e). In those cases, Customer will bear its own expense and the cost of SAP's internal resources required to conduct the audit. If an audit determines that SAP has breached its obligations under the Agreement, SAP will promptly remedy the breach at its own cost.

7. EU ACCESS

7.1 Optional Service.

If included in the Order Form, SAP agrees to provide EU Access for the eligible Cloud Service as stated in this Section 7.

7.2 EU Access.

SAP will use only European Subprocessors to provide support requiring access to Personal Data in the Cloud Service.

standar lainnya (cakupan sebagaimana yang dijelaskan dalam sertifikat); atau (ii) laporan pengesahan ISAE3000 dan/atau ISAE3402 yang sah. Sesuai permintaan Pelanggan -Laporan SOC-Audit atau sertifikasi ISO tersedia melalui auditor pihak ketiga atau SAP;

(a) Telah terjadi Pelanggaran Keamanan;

(b) Pelanggan atau Pengendali Data lain memiliki alasan-alasan yang wajar untuk mencurigai bahwa SAP tidak mematuhi kewajiban-kewajibannya berdasarkan DPA ini;

(c) Audit diminta secara resmi oleh otoritas perlindungan data Pelanggan atau Pengendali Data yang lain.

(d) Undang-undang Perlindungan Data yang diwajibkan memberikan hak audit langsung kepada Pelanggan.

Jika Pelanggan mengaudit lingkungan SAP, SAP akan secara wajar mendukung Pelanggan dalam proses auditnya.

6.2 Pembatasan Audit.

Audit Pelanggan akan dibatasi hingga sekali dalam periode dua belas bulan mana pun, dan terbatas dalam waktu hingga maksimum 3 hari kerja dan cakupan sebagaimana yang disetujui secara wajar sebelumnya antara para pihak. Diperlukan pemberitahuan di muka yang wajar dalam sekurang-kurangnya enam puluh hari, kecuali apabila Undang-undang Perlindungan Data mewajibkan audit lebih awal. SAP dan Pelanggan akan menggunakan sertifikasi terbaru atau laporan audit lain untuk meminimalkan audit berulang. Pelanggan dan SAP masing-masing akan menanggung pengeluaran atas auditnya sendiri, kecuali apabila Pelanggan mengaudit berdasarkan Pasal 6.1 (c) (kecuali apabila audit tersebut mengungkapkan pelanggaran oleh SAP di mana SAP yang akan menanggung pengeluaran atas auditnya sendiri), 6.1 (d) atau 6.1 (e). Dalam hal tersebut, Pelanggan akan menanggung pengeluarannya sendiri dan biaya sumber daya internal SAP yang diperlukan untuk melakukan audit. Jika audit menentukan bahwa SAP telah melanggar kewajibannya berdasarkan Perjanjian, SAP akan segera mengganti rugi pelanggaran tersebut dengan biayanya sendiri.

7. AKSES UE

7.1 Layanan Opsional.

Jika dicakup dalam Formulir Pemesanan, SAP setuju untuk menyediakan Akses UE untuk Layanan Cloud yang memenuhi syarat sebagaimana yang dinyatakan dalam Pasal 7 ini.

7.2 Akses UE.

SAP hanya akan menggunakan Subprosesor Eropa untuk memberikan dukungan yang memerlukan akses ke Data Pribadi dalam

7.3 Data Center Location.
Upon the Order Form Effective Date, 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.

7.4 Exclusions.
The following Personal Data is not subject to the requirements in 7.2-7.3:

(a) Contact details of the sender of a support ticket;

(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;

(c) Personal Data in non-production systems.

8. DEFINITIONS
Capitalized terms not defined herein will have the meanings given to them in the Agreement. **"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.

8.2 "Data 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.

8.3 "Data Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

8.4 "Data Protection Law" means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to

Layanan Cloud.

7.3 Lokasi Pusat Data.
Setelah Tanggal Mulai Berlaku Formulir Pemesanan, Pusat Data yang digunakan untuk menyelenggarakan 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.

7.4 Pengecualian.
Data Pribadi berikut ini tidak tunduk pada persyaratan dalam 7.2-7.3:

(a) Detail narahubung pengirim tiket dukungan;

(b) 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;

(c) Data Pribadi dalam sistem non-produksi.

8. DEFINISI
Istilah-istilah yang ditulis dengan huruf kapital yang tidak didefinisikan di sini akan dijelaskan maknanya dalam Perjanjian.

8.1 "Pusat Data" adalah lokasi di mana *instance* produksi Layanan Cloud diselenggarakan 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 lain dalam Formulir Pemesanan.

8.2 "Pengendali Data" berarti orang perorangan atau orang perorangan sebagai subjek hukum, otoritas publik, lembaga atau badan lain, yang secara sendiri atau bersama-sama dengan yang lainnya, menentukan tujuan dan cara pemrosesan Data Pribadi.

8.3 "Prosesor Data" berarti orang perorangan atau orang perorangan sebagai subjek hukum, otoritas publik, lembaga atau badan lain yang memproses data pribadi atas nama pengendali.

8.4 "Undang-undang Perlindungan Data" berarti legislasi yang berlaku yang melindungi hak mendasar dan kebebasan manusia dan hak

privacy with regard to the processing of Personal Data under the Agreement.

8.5 "Data Subject" means an identified or identifiable natural person.

8.6 "EEA" means the European Economic Area, namely the European Union Member States along with Iceland, Lichtenstein and Norway.

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

8.8 "Personal Data" means any information relating to a Data Subject For the purposes of this DPA, it includes only personal data entered by Customer or its Authorized Users into or derived from their use of the Cloud Service. It also includes personal data 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.

8.9 "Security Breach" means a confirmed (1) accidental or unlawful destruction, loss, alteration, or disclosure of Customer Personal Data or Confidential Data, or (2) similar incident involving Personal Data for which a Data Processor is required under applicable law to provide notice to the Data Controller.

8.10 "Standard Contractual Clauses" or sometimes also referred to the "EU Model Clauses" means the (Standard Contractual Clauses (processors)) or any subsequent version thereof released by the Commission (which will automatically apply). The current Standard Contractual Clauses are located at http://ec.europa.eu/justice/data-protection/international-transfers/files/clauses_for_personal_data_transfer_processors_c2010-593.doc. They include Appendices 1 and 2 attached to this DPA.

8.11 "Subprocessor" means SAP Affiliates and third parties engaged by SAP or SAP's Affiliates to process personal data.

8.12 "Third Country Subprocessor" means any Subprocessor incorporated outside the EEA and outside any country for which the European Commission has published an adequacy decision as published at http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

mereka atas privasi yang berkaitan dengan pemrosesan Data Pribadi berdasarkan Perjanjian.

8.5 "Subjek Data" berarti orang perorangan yang telah diidentifikasi atau dapat diidentifikasi.

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

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

8.8 "Data Pribadi" berarti setiap informasi yang berhubungan dengan Subjek Data Untuk tujuan DPA ini, Data Pribadi ini hanya mencakup data pribadi yang dimasukkan oleh Pelanggan atau Pengguna Resminya ke atau berasal dari penggunaannya atas Layanan Cloud. Data Pribadi ini juga mencakup data pribadi yang dipasok atau diakses oleh SAP atau Subprosesornya untuk memberikan dukungan sesuai dengan Perjanjian. Data Pribadi merupakan suatu subset Data Pelanggan.

8.9 "Pelanggaran Keamanan" berarti kepastian mengenai (1) penghancuran, kehilangan, perubahan, atau pengungkapan Data Rahasia atau Data Pribadi Pelanggan yang tidak disengaja atau yang melanggar hukum, atau (2) insiden serupa yang melibatkan Data Pribadi yang atasnya Prosesor Data diwajibkan berdasarkan hukum yang berlaku untuk memberikan pemberitahuan kepada Pengendali Data.

8.10 "Klausul Kontraktual Standar" atau kadang disebut sebagai "Klausul Model UE" berarti (Klausul Kontraktual Standar (prosesor) atau versi apa pun sesudahnya yang diterbitkan oleh Komisi (yang secara otomatis akan berlaku). Klausul Kontraktual Standar terbaru berada di http://ec.europa.eu/justice/data-protection/international-transfers/files/clauses_for_personal_data_transfer_processors_c2010-593.doc. Klausul tersebut mencakup Apendiks 1 dan 2 yang dilampirkan pada DPA ini.

8.11 "Subprosesor" berarti pihak ketiga dan Afiliasi SAP yang terlibat dengan SAP atau Afiliasi SAP untuk memproses data pribadi.

8.12 "Subprosesor Negara Ketiga" berarti Subprosesor mana pun yang tergabung di luar EEA dan di luar negara mana pun yang untuknya Komisi Eropa telah memublikasikan keputusan kecukupan di http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

Appendix 1 to Data processing agreement and Standard Contractual Clauses

Data Exporter

The Data Exporter subscribed to a Cloud Service that allows Authorized Users to enter, amend, use, delete or otherwise process Personal Data.

Data Importer

SAP and its Subprocessors provide the Cloud Service that includes the following support:

SAP 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:

- Monitoring the Cloud Service
- Backup & restoration of Customer Data stored in the Cloud Service
- Release and development of fixes and upgrades to the Cloud Service
- Monitoring, troubleshooting and administering the underlying Cloud Service infrastructure and database
- Security monitoring, network-based intrusion detection support, penetration testing

SAP 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.

Data Subjects

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.

Data Categories

The transferred Personal Data transferred concerns the following categories of data:

Customer determines the categories of data per Cloud Service subscribed. Customer can configure the data fields during

Apendiks 1 pada Perjanjian pemrosesan data dan Klausul Kontraktual Standar

Pengekspor Data

Pengekspor Data yang berlangganan Layanan Cloud yang memungkinkan Pengguna Resmi untuk memasukkan, mengamendemen, menggunakan, menghapus atau memproses Data Pribadi.

Pengimpor Data

SAP dan Subprosesornya menyediakan Layanan Cloud yang meliputi dukungan berikut:

Afiliasi SAP mendukung pusat data Layanan Cloud jarak jauh dari fasilitas-fasilitas SAP di St. Leon/Rot (Jerman), India, dan lokasi-lokasi lain di mana SAP memperkerjakan personel dalam fungsi Penyampaian Cloud/Operasi. Dukungan mencakup:

- Pemantauan Layanan Cloud
- Pencadangan dan pemulihan Data Pelanggan yang disimpan dalam Layanan Cloud
- Rilis dan pengembangan perbaikan dan peningkatan (*upgrade*) Layanan Cloud
- Pemantauan, penyelesaian masalah dan pengurusan basis data dan infrastruktur Layanan Cloud dasar.
- Pemantauan keamanan, dukungan deteksi intrusi berbasis jaringan, uji penetrasi

Afiliasi SAP 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.

Subjek Data

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.

Kategori Data

Data Pribadi yang ditransfer yang dialihkan berkaitan dengan kategori data berikut:

Pelanggan menentukan kategori data per Layanan Cloud yang dilanggankan. Pelanggan dapat mengonfigurasikan

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.

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)

The transferred Personal Data concerns the following special categories of data: As set out in the Order Form, if any.

Kategori Data Khusus (apabila sesuai)

Data Pribadi yang ditransfer berhubungan dengan kategori khusus untuk data berikut: Sebagaimana yang ditetapkan dalam Formulir Pemesanan, apabila ada.

Processing Operations

The transferred Personal Data is subject to the following basic processing activities:

- use of Personal Data to set up, operate, monitor and provide the Cloud Service (including Operational and Technical Support)
- provision of Consulting Services;
- communication to Authorized Users
- storage of Personal Data in dedicated Data Centers (multi-tenant architecture)
- upload any fixes or upgrades to the Cloud Service
- back up of Personal Data
- computer processing of Personal Data, including data transmission, data retrieval, data access
- network access to allow Personal Data transfer
- execution of instructions of Customer in accordance with this Agreement

Operasi Pemrosesan

Data Pribadi yang ditransfer tunduk pada aktivitas pemrosesan dasar berikut ini:

- Penggunaan Data Pribadi untuk menyiapkan, mengoperasikan, memantau, dan menyediakan Layanan Cloud (termasuk Dukungan Operasional dan Teknis)
- penyediaan Layanan Konsultasi;
- komunikasi dengan Pengguna Resmi
- penyimpanan Data Pribadi di Pusat Data terdedikasi (arsitektur multi-penyewa)
- mengunggah setiap perbaikan atau peningkatan (*upgrade*) ke Layanan Cloud
- pencadangan Data Pribadi
- pemrosesan Data Pribadi pada komputer, termasuk transmisi data, pengambilan data, akses data
- akses jaringan untuk memungkinkan transfer Data Pribadi
- Pelaksanaan instruksi Pelanggan sesuai dengan Perjanjian ini

Appendix 2 – Technical and Organizational Measures

1. TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define the SAP's current security measures. SAP may change these at any time without notice so long as it maintains a comparable or better level of security. This may mean that individual measures are replaced by new measures that serve the same purpose without diminishing the security level.

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.

Measures:

- SAP protects its assets and facilities using the appropriate means based on a security classification conducted by an internal security department.
- In general, buildings are secured through access control systems (e.g., smart card access system).
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- 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.
- 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.
- SAP employees and external personnel must wear their ID cards at all SAP locations.

Additional measures for Data Centers:

- 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.

Apendiks 2 – Tindakan Teknis dan Organisasional

1. TINDAKAN TEKNIS DAN ORGANISASIONAL

Pasal berikut menjelaskan tindakan keamanan saat ini SAP. SAP dapat mengubah hal ini sewaktu-waktu tanpa pemberitahuan sepanjang SAP mempertahankan tingkat keamanan yang setara atau lebih baik. Hal ini dapat berarti bahwa tindakan individu akan digantikan oleh tindakan baru yang bertujuan sama tanpa mengurangi tingkat keamanan.

1.1 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.

Tindakan:

- SAP melindungi aset dan fasilitasnya dengan menggunakan cara yang sesuai berdasarkan klasifikasi keamanan yang dilaksanakan oleh departemen keamanan internal.
- Secara umum, gedung diamankan melalui sistem kendali akses (misalnya, sistem akses kartu pintar).
- Sebagai persyaratan minimum, titik masuk terluar gedung harus dilengkapi dengan sistem kunci tersertifikasi termasuk manajemen kunci aktif dan modern.
- 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 biometrik.
- 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 .
- Karyawan SAP dan personel eksternal harus mengenakan kartu identitas di semua lokasi SAP.

Tindakan tambahan untuk Pusat Data:

- 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

Only authorized representatives have access to systems and infrastructure within the Data Center facilities. To ensure proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.

- SAP and all third party Data Center providers log the names and times of persons entering SAP's private areas within the Data Centers.

1.2 System Access Control.

Data processing systems used to provide the SAP Services must be prevented from being used without authorization.

Measures:

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Processes are in place to ensure that authorized users have the appropriate authorization to add, delete, or modify users.
- All users access SAP's systems with a unique identifier (user ID).
- SAP has procedures in place to ensure that requested authorization changes are implemented only in accordance with the guidelines (for example, no rights are granted without authorization). If a user leaves the company, his or her access rights are revoked.
- 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.
- The company network is protected from the public network by firewalls.
- 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.

pada peralatan dan fasilitas Pusat Data. Hanya perwakilan resmi yang memiliki akses ke sistem dan infrastruktur di dalam fasilitas-fasilitas Pusat Data. Untuk memastikan agar berfungsi dengan tepat, peralatan keamanan fisik (misalnya, sensor gerakan, kamera, dll.) mendapatkan pemeliharaan secara rutin.

- SAP dan semua penyedia Pusat Data pihak ketiga mencatat nama dan waktu saat orang-orang memasuki area khusus SAP di dalam Pusat Data.

1.2 Kendali Akses Sistem.

Sistem pemrosesan data yang digunakan untuk menyediakan Layanan SAP harus dicegah agar tidak digunakan tanpa pengesahan.

Tindakan:

- Sejumlah tingkat otorisasi digunakan ketika memberikan akses ke sistem-sistem yang sensitif, termasuk ke sistem yang menyimpan dan memproses Data Pribadi. Terdapat berbagai proses untuk memastikan bahwa pengguna resmi memiliki pengesahan yang tepat untuk menambahkan, menghapus, atau memodifikasi pengguna.
- Semua pengguna mengakses sistem-sistem SAP dengan kartu identitas unik (ID pengguna).
- SAP memiliki prosedur untuk memastikan bahwa perubahan pengesahan yang diminta telah diimplementasikan hanya sesuai dengan panduan (sebagai contoh, tidak ada hak yang diberikan tanpa pengesahan). Jika pengguna meninggalkan perusahaan, hak aksesnya akan dicabut.
- SAP telah menetapkan kebijakan kata sandi yang melarang pembagian kata sandi, mengatur respons terhadap pengungkapan kata sandi, dan meminta agar kata sandi diubah secara rutin dan kata sandi standar untuk diubah. ID pengguna yang dipersonalisasikan ditentukan untuk otentikasi. Semua kata sandi harus memenuhi persyaratan minimum yang ditetapkan dan disimpan dalam bentuk 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.
- Jaringan perusahaan dilindungi dari jaringan publik dengan *firewall*.
- SAP menggunakan perangkat lunak antivirus terbaru pada titik akses menuju jaringan perusahaan (untuk akun email),

- Security patch management is implemented to ensure regular and periodic deployment of relevant security updates.

- Full remote access to SAP's corporate network and critical infrastructure is protected by strong authentication.

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.

Measures:

- 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.
- Access to personal, confidential or sensitive information is granted on a need-to-know basis. In other words, employees or external third parties have access to the information that they require in order to complete their work. SAP uses authorization concepts that document how authorizations are assigned and which authorizations are assigned to whom. All personal, confidential, or otherwise sensitive data is protected in accordance with the SAP security policies and standards. Confidential information must be processed confidentially.
- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing personal, confidential or other sensitive information are regularly checked. To this end, SAP conducts internal and external security checks and penetration tests on its IT systems.

- SAP does not allow the installation of personal software or other software that has not been approved by SAP.

- An SAP security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

serta pada semua server file dan semua stasiun kerja.

- Manajemen *patch* keamanan diimplementasikan untuk memastikan 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 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.

Tindakan:

- Sebagai bagian dari Kebijakan Keamanan SAP, Data Pribadi mewajibkan setidaknya tingkat perlindungan yang sama dengan informasi "rahasia" sesuai dengan standar Klasifikasi Informasi SAP.
- Akses ke informasi pribadi, rahasia atau sensitif diberikan seperlunya saja (*need-to-know basis*). Dengan kata lain, karyawan atau pihak ketiga eksternal memiliki akses ke informasi yang mereka perlukan untuk menyelesaikan pekerjaan mereka. SAP menggunakan konsep pengesahan yang mencatat bagaimana pengesahan ditetapkan dan pengesahan yang mana yang ditetapkan padanya. Semua data pribadi, rahasia, atau data sensitif lainnya dilindungi sesuai dengan kebijakan dan standar keamanan SAP. Informasi rahasia harus diproses secara rahasia.
- Semua server produksi dioperasikan pada Pusat Data atau dalam ruang server yang aman. Tindakan keamanan yang melindungi aplikasi untuk memproses informasi pribadi, rahasia atau informasi sensitif lainnya diperiksa secara rutin. Untuk mencapai tujuan ini, SAP menjalankan pemeriksaan keamanan internal dan eksternal serta uji penetrasi pada sistem TI-nya.
- SAP tidak mengizinkan instalasi perangkat lunak pribadi atau perangkat lunak lainnya yang belum disetujui oleh SAP.
- 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 Services in accordance with the relevant service 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 ensure the agreed-upon service levels (for example, encryption and lead-lined containers).

- Personal Data transfer over SAP internal networks are protected in the same manner as any other confidential data according to SAP Security Policy.
- 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).

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.

Measures:

- SAP only allows authorized persons to access Personal Data as required in the course of their work.
- SAP has implemented a logging system for input, modification and deletion, or blocking of Personal Data by SAP or its subprocessors within SAP's Products and Services to the fullest extent possible.

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 relevant agreement and related instructions of the customer.

Measures:

- SAP uses controls and processes to ensure compliance with contracts between SAP and its customers, subprocessors or other service providers.
- As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP

1.4 Kendali Transmisi Data.

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

- Transfer Data Pribadi melalui jaringan internal SAP dilindungi dengan cara yang sama seperti data rahasia lainnya sesuai Kebijakan Keamanan SAP.
- Jika data ditransfer antara SAP dan pelanggannya, tindakan-tindakan perlindungan untuk Data Pribadi yang ditransfer disetujui bersama dan menjadi bagian dari 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 Kendali Input Data.

Kendali Input Data akan bertanggung jawab atas pemeriksaan secara retrospektif dan menetapkan apakah dan oleh siapa Data Pribadi telah dimasukkan, dimodifikasi atau dihapus dari sistem pemrosesan data SAP.

Tindakan:

- SAP hanya mengizinkan orang-orang resmi untuk mengakses Data Pribadi sebagaimana yang diperlukan selama pekerjaan mereka.
- SAP telah mengimplementasikan sistem pencatatan untuk input, modifikasi dan penghapusan, atau pemblokiran Data Pribadi oleh SAP atau subprosesornya dalam Produk dan Layanan SAP semaksimal mungkin.

1.6 Kendali Pekerjaan.

Data Pribadi yang diproses pada komisi (yaitu, Data Pribadi yang diproses atas nama pelanggan) diproses sepenuhnya sesuai dengan perjanjian yang relevan dan instruksi terkait dari pelanggan.

Tindakan:

- SAP menggunakan kendali dan proses untuk memastikan kepatuhan dengan kontrak antara SAP dan pelanggan, subprosesor, atau penyedia layanannya yang lain.
- Sebagai bagian dari Kebijakan Keamanan SAP, Data Pribadi mewajibkan setidaknya tingkat perlindungan yang sama dengan

Information Classification standard.

- 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.
- For on premise support services, SAP provides a specially designated, secure support ticket facility in which SAP provides a special access-controlled and monitored security area for transferring access data and passwords. SAP customers have control over their remote support connections at all times. SAP employees cannot access a customer system without the knowledge or full active participation of the customer.

1.7 Availability Control.

Personal Data will be protected against accidental or unauthorized destruction or loss.

Measures:

- SAP employs backup processes and other measures that ensure rapid restoration of business critical systems as and when necessary.
- SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to ensure power availability to the Data Centers.
- SAP has defined contingency plans as well as business and disaster recovery strategies for the provided Services.
- Emergency processes and systems are regularly tested.

1.8 Data Separation Control.

Personal Data collected for different purposes can be processed separately.

Measures:

- 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.
- Customers (including their Affiliates) have access only to their own data.
- If Personal Data is required to handle a support incident from a specific 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.

informasi "rahasia" sesuai dengan standar Klasifikasi Informasi SAP.

- 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.
- Untuk layanan dukungan *on premise*, SAP menyediakan fasilitas tiket dukungan yang aman yang ditujukan secara khusus yang di dalamnya SAP menyediakan area pengamanan termonitor dan terkendali akses khusus untuk mentransfer data dan kata sandi akses. Pelanggan SAP memiliki kendali atas koneksi dukungan jarak jauh mereka setiap saat. Karyawan SAP tidak dapat mengakses sistem pelanggan tanpa sepengetahuan atau partisipasi aktif sepenuhnya dari pelanggan.

1.7 Kendali Ketersediaan.

Data Pribadi akan dilindungi dari kerusakan atau kehilangan yang tidak sah atau tidak disengaja.

Tindakan:

- SAP menjalankan proses pencadangan dan tindakan lain yang memastikan pemulihan sistem penting bisnis dengan cepat dan bila diperlukan.
- SAP menggunakan suplai daya tidak terputus (sebagai contoh: UPS, baterai, generator, dll.) untuk memastikan ketersediaan daya ke Pusat Data.
- SAP telah menetapkan rencana kontingensi serta strategi pemulihan bencana dan bisnis untuk Layanan Cloud yang diberikan.
- Proses dan sistem darurat diuji secara rutin.

1.8 Kendali Pemisahan Data.

Data Pribadi yang dikumpulkan untuk tujuan berbeda dapat diproses secara terpisah.

Tindakan:

- SAP menggunakan kemampuan-kemampuan teknis dari perangkat lunak yang ditempatkan (sebagai contoh: lanskap sistem terpisah, atau kepemilikan majemuk) untuk mencapai pemisahan data antara Data Pribadi yang berasal dari berbagai pelanggan.
- Pelanggan (termasuk Afiliasinya) memiliki akses hanya ke data Pelanggan sendiri.
- Jika Data Pribadi diperlukan untuk menangani insiden dukungan dari pelanggan khusus, 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.

Measures:

SAP has implemented a multi-layered defense strategy as a protection against unauthorized modifications.

In particular, SAP uses the following to implement the control and measure sections described above. In particular:

- Firewalls;
- Security Monitoring Center;
- Antivirus software;
- Backup and recovery;
- External and internal penetration testing;
- Regular external audits to prove security measures.

1.9 Kendali Integritas Data.

Data Pribadi akan tetap terjaga, lengkap dan masih berlaku selama aktivitas pemrosesan.

Tindakan:

SAP telah mengimplementasikan strategi pertahanan multi-lapisan sebagai perlindungan terhadap modifikasi-modifikasi yang tidak sah.

Khususnya, SAP menggunakan hal-hal berikut ini untuk mengimplementasikan pasal-pasal tindakan dan kendali yang diuraikan di atas. Khususnya:

- *Firewall*;
- Pusat Pemantauan Keamanan;
- Perangkat lunak antivirus;
- Pencadangan dan pemulihan;
- Pengujian penetrasi eksternal dan internal;
- Audit eksternal rutin untuk membuktikan tindakan keamanan.