

Adendum Pemrosesan Data

Adendum Pemrosesan Data ini (“**DPA**”) adalah adendum untuk Perjanjian Lisensi Pengguna Akhir Lincoln Electric Company (“**EULA**”) dan berlaku antara Lincoln Electric Company (“**Pemroses Data**”) dan Pengguna yang Sah sesuai dengan EULA (“**Pengendali Data**”), (masing-masing disebut sebagai “**Pihak**”, dan secara bersama-sama disebut sebagai “**Para Pihak**”).

BAHWA

EULA ini mengatur hak Pengguna yang Sah untuk menggunakan Aplikasi Berlisensi dan, sebagaimana berlaku, layanan online lainnya yang disediakan oleh Lincoln Electric Company. Untuk tujuan memenuhi kewajibannya berdasarkan EULA, Lincoln Electric Company akan bertindak sebagai Pemroses Data atas nama Pengguna yang Sah. Untuk memastikan kepatuhan terhadap regulasi Data Pribadi, Para Pihak telah sepakat untuk melengkapi EULA ini guna menetapkan syarat dan ketentuan yang berlaku untuk Pemrosesan Data Pribadi oleh Pemroses Data atas nama Pengendali Data.

DENGAN INI DISEPAKATI BAHWA

1. DEFINISI

1.1 Dalam DPA ini, istilah dengan huruf kapital memiliki arti sebagai berikut, kecuali jika didefinisikan dalam EULA atau diwajibkan lain berdasarkan konteksnya:

“ Pengendali Data ”	berarti entitas yang menentukan tujuan dan sarana Pemrosesan Data Pribadi;
“ Pemroses Data ”	berarti entitas yang Memproses Data Pribadi atas nama Pengendali Data;
“ Subjek Data ”	berarti individu yang teridentifikasi atau dapat diidentifikasi yang Data Pribadinya sedang diproses;
“ Instruksi ”	berarti instruksi yang diberikan oleh Pengendali Data kepada Pemroses Data guna Memproses Data Pribadi sesuai dengan penyediaan layanan berdasarkan EULA;
“ Data Pribadi ”	berarti setiap informasi yang berkaitan dengan individu yang teridentifikasi atau dapat diidentifikasi; individu yang dapat diidentifikasi adalah orang yang dapat diidentifikasi, baik secara langsung maupun tidak langsung, khususnya dengan mengacu pada pengenalan seperti nama, nomor identifikasi, data lokasi, pengenalan online, atau satu atau lebih faktor khusus dari segi fisik, identitas fisiologis, genetik, mental, ekonomi, budaya atau sosialnya;
“ Pelanggaran Data Pribadi ”	berarti pelanggaran keamanan yang mengarah pada penghancuran yang tidak disengaja atau melanggar hukum, penghilangan, perubahan, pengungkapan yang tidak sah atas, atau akses ke, Data Pribadi yang dikirimkan, disimpan, atau Diproses;
“ Memproses ”/“ Pemrosesan ”/“ Diproses ”	berarti setiap tindakan yang dilakukan pada Data Pribadi seperti pengumpulan, perekaman, pengelolaan, penyimpanan, adaptasi atau perubahan, pengambilan, konsultasi, penggunaan, pengungkapan melalui transmisi, penyebaran, transfer atau penyediaan, penyesuaian atau kombinasi, pembatasan, penghapusan atau penghancuran;
“ Layanan Pemrosesan ”	berarti Pemrosesan Data Pribadi oleh Pemroses Data sehubungan dengan EULA;
“ Kategori Khusus Data Pribadi ”	berarti Data Pribadi apa pun yang mengungkapkan asal ras atau etnis, pendapat politik, keyakinan agama atau filosofis, atau keanggotaan dalam serikat pekerja, asosiasi atau yayasan, penampilan, hukuman pidana dan tindakan keamanan, informasi keuangan dan properti, informasi keberadaan, atau informasi kredit dan Pemrosesan data genetik, data biometrik dengan tujuan untuk secara unik mengidentifikasi seseorang, data mengenai kesehatan atau data mengenai kehidupan seks atau orientasi seksual seseorang atau data tentang anak di bawah umur yang berusia 14 tahun ke bawah;

“Klausul Kontrak Standar”

berarti Klausul Kontrak Standar yang diadopsi oleh Keputusan Komisi UE 2010/87 tanggal 5 Februari 2010 tentang Klausul Kontrak Standar untuk transfer data pribadi ke pemroses yang didirikan di negara ketiga atau setiap set klausul standar pengganti yang disepakati antara Para Pihak. Jika Pengendali Data ditetapkan di yurisdiksi yang berada di luar Uni Eropa, maka rujukan ke Negara Anggota dalam ketentuan substantif Klausul Kontrak Standar akan ditafsirkan sebagai rujukan ke yurisdiksi tempat didirikannya Pengendali Data;

“Sub-pemroses”

berarti setiap pemroses yang dilibatkan oleh Pemroses Data (atau oleh Sub-pemroses lain dari Pemroses Data) untuk Memproses Data Pribadi atas nama Pengendali Data sesuai dengan Instruksinya dan ketentuan sub-kontrak tertulis.

- 1.2 Keterangan dan judul bagian yang digunakan adalah sebagai rujukan dan untuk memudahkan saja, bukan merupakan bagian dari DPA ini, dan tidak boleh digunakan dalam menafsirkan DPA ini.

2. RUANG LINGKUP DAN PENERAPAN DPA INI

- 2.1 DPA ini hanya melengkapi ketentuan EULA sehubungan dengan Layanan Pemrosesan yang disediakan oleh Pemroses Data kepada Pengendali Data sesuai dengan EULA.

3. PEMROSESAN DATA

- 3.1 Pemroses Data sepakat untuk Memproses Data Pribadi sesuai dengan syarat dan ketentuan yang ditetapkan dalam DPA ini, dan khususnya Pemroses Data berjanji:

3.1.1 untuk Memproses Data Pribadi hanya atas nama Pengendali Data dan selalu menyesuaikan dengan Instruksi Pengendali Data sebagaimana didefinisikan dalam DPA ini, dan semua undang-undang perlindungan data yang berlaku;

3.1.2 untuk memastikan bahwa setiap personel yang diberikan kepercayaan atas Layanan Pemrosesan berkomitmen terhadap kerahasiaan atau terikat dengan kewajiban kerahasiaan yang sesuai dengan undang-undang;

3.1.3 untuk mengambil langkah-langkah teknis, fisik, dan organisasi guna memastikan keamanan dan kerahasiaan Data Pribadi dan secara tepat melindungi Data Pribadi yang Diproses atas nama Pengendali Data dari penyalahgunaan dan kehilangan, sebagaimana diatur dalam Lampiran 2 DPA ini;

3.1.4 bahwa Pemroses Data akan segera memberi tahu Pengendali Data tentang: (a) setiap permintaan yang mengikat secara hukum untuk pengungkapan Data Pribadi oleh otoritas pemerintah kecuali jika dilarang, seperti larangan menurut hukum pidana untuk menjaga kerahasiaan penegakan hukum atau penyelidikan intelijen, (b) setiap Pelanggaran Data Pribadi yang memengaruhi Data Pribadi yang diproses atas nama Pengendali Data, (c) setiap permintaan yang diterima langsung dari Subjek Data (termasuk hak atas akses, pembetulan, penghapusan, keberatan, pembatasan, transfer data, dan hak untuk tidak tunduk pada keputusan yang hanya didasarkan pada Pemrosesan otomatis, termasuk pembuatan profil); Pemroses Data (i) tidak akan menanggapi permintaan tersebut secara langsung, kecuali untuk memberi tahu Subjek Data bahwa Pemroses Data bertindak atas nama Pengendali Data dan untuk memberikan informasi kontak Pengontrol Data kepada Subjek Data, dan (ii) mempertimbangkan sifat Pemrosesan, akan membantu Pengendali Data dengan langkah-langkah teknis, fisik, dan organisasi yang sesuai, sejauh hal ini memungkinkan, untuk pemenuhan kewajiban Pengendali Data dalam menanggapi permintaan pelaksanaan hak-hak Subjek Data;

3.1.5 untuk memberikan kerja sama yang wajar secara komersial kepada Pengendali Data guna membantu Pengontrol Data dalam mematuhi kewajiban hukumnya sendiri terkait dengan keamanan Data Pribadi, seperti: pemberitahuan Pelanggaran Data Pribadi kepada otoritas pengawas yang kompeten, mengkomunikasikan Pelanggaran Data Pribadi tersebut kepada Data Subjek yang terpengaruh dan, jika berlaku, menerapkan penilaian dampak perlindungan data dan melakukan konsultasi sebelumnya dengan otoritas pengawas, dengan mempertimbangkan sifat Pemrosesan dan informasi yang tersedia untuk Pemroses Data;

3.1.6 untuk menyediakan kepada Pengendali Data semua informasi yang diperlukan guna membuktikan kepatuhannya terhadap kewajiban yang ditetapkan dalam DPA ini dan memungkinkan serta berkontribusi dalam hal audit, termasuk inspeksi, yang dilakukan oleh Pengendali Data atau auditor lain yang diamanatkan oleh Pengendali Data sebagaimana diatur dalam Bagian 6; dan,

3.1.7 bahwa setiap Layanan Pemrosesan yang dilakukan oleh Sub-pemroses akan dilakukan sesuai dengan ketentuan Bagian 7.

3.2 Sehubungan dengan Layanan Pemrosesan, Pengendali Data akan bertanggung jawab untuk mematuhi semua persyaratan yang diberlakukan padanya berdasarkan undang-undang yang berlaku mengenai Pemrosesan Data Pribadi dan Instruksi yang diberikannya kepada Pemroses Data. Secara khusus tetapi tanpa mengurangi keumuman hal tersebut di atas, Pengendali Data mengakui dan menyepakati bahwa Pengendali Data akan bertanggung jawab penuh atas hal-hal berikut: (i) keakuratan, kualitas, dan legalitas Data Pribadi; (ii) mematuhi semua persyaratan transparansi dan keabsahan yang disyaratkan berdasarkan hukum yang berlaku untuk pengumpulan dan penggunaan Data Pribadi, termasuk memperoleh persetujuan dan otorisasi yang diperlukan dari Subjek Data atau lainnya; (iii) memastikan bahwa Pengendali Data memiliki hak untuk mentransfer, atau memberikan akses atas, Data Pribadi kepada Pemroses Data dan bahwa Pengendali Data telah memberikan pemberitahuan yang diperlukan dan memperoleh persetujuan dan/atau otorisasi yang diperlukan sehubungan dengan transfer atau akses tersebut dan, secara lebih umum, untuk melakukan Pemrosesan sesuai dengan ketentuan EULA (termasuk DPA ini); dan (iv) memastikan bahwa Instruksinya mematuhi hukum yang berlaku. Atas permintaan dari Pemroses Data, Pengendali Data harus memberikan kepada Pemroses Data dalam waktu tiga (3) hari kerja bukti tertulis dari pemberitahuan, persetujuan, dan otorisasi tersebut. Pengendali Data tidak akan memasukkan ke dalam Layanan Pemrosesan, atau memberikan kepada Pemroses Data, Kategori Khusus Data Pribadi apa pun, kecuali jika disetujui secara terpisah dan tertulis oleh Pengendali Data. Pengendali Data akan memberi tahu Pemroses Data, segera dan tanpa penundaan yang tidak semestinya, jika Pengendali Data tidak dapat memenuhi tanggung jawabnya sebagaimana yang ditetapkan dalam DPA ini. Pengguna yang Sah bertanggung jawab sepenuhnya untuk meninjau Layanan Pemrosesan, termasuk semua dokumentasi dan fitur keamanan yang tersedia, guna menentukan apakah layanan tersebut memenuhi persyaratan, kebutuhan bisnis, dan kewajiban hukum Pengguna yang Sah.

3.3 Pengendali Data memberi wewenang kepada Pemroses Data untuk menganonimkan Data Pribadi yang Diproses sesuai dengan EULA guna mendapatkan data analitik yang berkaitan dengan penggunaan Aplikasi Berlisensi serta produk dan peralatan Lincoln. Penggunaan lebih lanjut dari data statistik yang dihasilkan oleh Pemroses Data tidak tunduk pada otorisasi sebelumnya dari Pengendali Data.

4. TRANSFER DATA INTERNASIONAL

4.1 Pengendali Data dengan ini mengakui dan menyetujui bahwa, untuk menyediakan Layanan Pemrosesan berdasarkan EULA, Pemroses Data dapat mentransfer dan menyimpan Data Pribadi di Amerika Serikat, dan negara lain tempat Pemroses Data berada, untuk tujuan menyediakan Layanan Pemrosesan. Oleh karena itu, selama penyediaan Layanan Pemrosesan, mungkin akan diperlukan pentransferan Data Pribadi ke Pemroses Data yang berlokasi di luar negara tempat didirikannya Pengendali Data. Jika Pengendali Data berlokasi di Wilayah Ekonomi Eropa atau di Swiss, Para Pihak berjanji untuk menerapkan ketentuan Klausul Kontrak Standar untuk transfer Data Pribadi oleh Pengendali Data (bertindak sebagai pengekspor data sesuai dengan Klausul Kontrak Standar) untuk Pemroses Data (bertindak sebagai pengimpor data sesuai dengan Klausul Kontrak Standar).

4.2 Jika Pengendali Data berlokasi di luar Wilayah Ekonomi Eropa dan Swiss, Para Pihak juga berjanji untuk menerapkan ketentuan Klausul Kontrak Standar untuk transfer Data Pribadi oleh Pengendali Data (bertindak sebagai pengekspor data sesuai dengan Klausul Kontrak Standar) kepada Pemroses Data (bertindak sebagai pengimpor data sesuai dengan Klausul Kontrak Standar), dengan ketentuan bahwa Klausul Kontrak Standar diwajibkan secara hukum dan cukup untuk memenuhi persyaratan regulasi perlindungan data yang berlaku untuk transfer Data Pribadi oleh Pengendali Data kepada Pemroses Data sesuai dengan EULA.

4.3 Jika Para Pihak menerapkan Klausul Kontrak Standar sesuai dengan Bagian 4.1 atau 4.2 DPA ini:

4.3.1 Apendiks 1 Klausul Kontrak Standar harus diterapkan atas dasar berikut: (a) Pengekspor data: Pengendali Data, (b) Pengimpor data: Pemroses Data, (c) Subjek data: personel Pengendali Data

(Pengguna yang Sah), (d) Kategori data: data yang berkaitan dengan penggunaan produk dan peralatan yang dimiliki, dilisensikan, atau dikelola oleh Pemroses Data, sebagaimana dipantau oleh Aplikasi Berlisensi sesuai dengan EULA, termasuk data pendaftaran (yaitu, nama pengguna dan kata sandi), (e) Kategori Khusus Data Pribadi: N/A, dan (f) Operasi pemrosesan: pengumpulan, penyalinan, transfer, penyimpanan, modifikasi, penghapusan, dan operasi lain yang diperlukan untuk Layanan Pemrosesan sesuai dengan EULA.

4.3.2 Uraian tentang langkah-langkah keamanan teknis, fisik, dan organisasional yang diterapkan oleh Pemroses Data yang bertindak sebagai pengimpor data untuk tujuan Apendiks 2 Klausul Kontrak Standar harus ditetapkan dalam Lampiran 2 DPA ini.

4.4 Jika Klausul Kontrak Standar berlaku antara Para Pihak sesuai dengan Bagian 4.1 atau 4.2, ketentuan klausul tersebut akan dianggap digabungkan sebagai rujukan dalam DPA ini, kecuali Para Pihak menandatangani Klausul Kontrak Standar sebagai dokumen mandiri sesuai dengan Bagian 4.5.

4.5 Sejauh yang disyaratkan oleh regulasi perlindungan data yang berlaku, Para Pihak akan menandatangani dan melaksanakan Klausul Kontrak Standar sebagai dokumen terpisah.

5. PENGAKHIRAN

5.1 DPA ini akan berlaku efektif pada tanggal efektif EULA.

5.2 DPA ini akan berakhir secara otomatis setelah pengakhiran atau berakhirnya (a) EULA atau (b) kewajiban Pemroses Data terkait dengan Layanan Pemrosesan, dan pengakhiran tersebut tidak akan memerlukan penetapan pengadilan atau proses pengadilan atau tindakan lain apa pun dari Pemroses Data, Pengendali Data, atau pihak lain mana pun agar efektif. Jika berlaku, pada saat pengakhiran DPA ini, Pemroses Data akan mengembalikan kepada Pengendali Data atau menghapus, atas permintaan Pengendali Data, semua Data Pribadi Pengendali Data yang dimiliki atau yang berada dalam kendalinya. Atas permintaan Pengendali Data, Pemroses Data harus memastikan kepatuhannya terhadap kewajiban tersebut secara tertulis dan menghapus semua salinan yang ada, kecuali hukum yang berlaku mengharuskan penyimpanan atau mengizinkan penyimpanan Data Pribadi.

5.3 Pengendali Data berhak untuk mengakhiri DPA ini dengan pemberitahuan secara tertulis kepada Pemroses Data jika Pemroses Data melakukan pelanggaran material atau pelanggaran terus-menerus terhadap DPA ini, jika pelanggaran yang dapat diperbaiki, tidak diperbaiki dalam waktu tiga puluh (30) hari kerja sejak tanggal diterimanya oleh Pengendali Data atas pemberitahuan dari Pemroses Data yang mengidentifikasi pelanggaran tersebut dan menghendaki pemulihannya.

5.4 Pemroses Data berhak untuk mengakhiri DPA ini dengan pemberitahuan secara tertulis kepada Pengendali Data jika Pengendali Data melakukan pelanggaran material atau pelanggaran terus-menerus terhadap DPA ini, jika pelanggaran yang dapat diperbaiki, tidak diperbaiki dalam waktu tiga puluh (30) hari kerja sejak tanggal diterimanya oleh Pengendali Data atas pemberitahuan dari Pemroses Data yang mengidentifikasi pelanggaran tersebut dan menghendaki pemulihannya.

6. PERMINTAAN AUDIT DAN INFORMASI

6.1. Dengan batasan satu (1) audit per tahun dan tunduk pada pemberitahuan oleh Pengendali Data dengan pemberitahuan tiga puluh (30) hari sebelumnya, kecuali dalam kasus audit yang diminta oleh otoritas pengawas, Pengendali Data dapat selama jam bisnis biasa, tanpa secara tidak wajar mengganggu operasi bisnis Pemroses Data, mengaudit Pemroses Data secara pribadi, atau menunjuk auditor pihak ketiga yang tunduk pada kewajiban kerahasiaan untuk melaksanakan audit tersebut.

6.2. Pemroses Data harus bekerja sama terkait dengan audit berdasarkan Bagian 6 ini dan memberikan kepada Pengendali Data semua informasi yang diperlukan guna melaksanakan audit tersebut. Pengendali Data akan menanggung biaya dan pengeluaran yang dikeluarkan oleh masing-masing pihak sehubungan dengan audit berdasarkan Bagian 6 ini.

7. PENUNJUKAN SUB-PEMROSES

- 7.1 Pengendali Data memberi wewenang kepada Pemroses Data untuk menggunakan layanan Sub-pemroses yang tercantum di halaman yang dapat diakses di [<https://www.lincolnelectric.com/en/Legal-Information/Subprocessors>], hanya sebagaimana yang disyaratkan untuk pelaksanaan Layanan sehubungan dengan EULA.
- 7.2 Pengendali Data memberi wewenang kepada Pemroses Data untuk menggunakan layanan Sub-pemroses baru, dengan tunduk pada pemberitahuan sebelumnya kepada Pengendali Data oleh Pemroses Data melalui pemberitahuan lima belas (15) hari sebelum penggantian Sub-pemroses. Jika Pengendali Data keberatan dengan penggantian Sub-pemroses yang diberitahukan, Pengendali Data dapat, selama periode pemberitahuan, mengakhiri DPA ini secara tertulis. Jika Pengendali Data tidak mengakhiri dalam periode pemberitahuan, maka tindakan ini mengesahkan persetujuan Pengendali Data atas penggantian Sub-pemroses sebagaimana diberitahukan.
- 7.3 Dalam hal apa pun, ketika Pemroses Data menggunakan layanan dari Sub-pemroses, sebagaimana keadaannya, melalui kontrak, terikat untuk mematuhi kewajiban yang sama seperti yang mengikat Pemroses Data dalam hal Pemrosesan Data Pribadi berdasarkan DPA ini.

8. KETENTUAN LAINNYA

- 8.1 Amendemen atau penambahan DPA ini harus dibuat secara tertulis untuk diberlakukan. Terlepas dari hal tersebut di atas, Pemroses Data dapat, kapan saja dan tanpa pemberitahuan kepada Pengendali Data, melakukan amendemen langkah-langkah teknis, fisik, dan organisasi yang ditetapkan dalam Lampiran 2, dengan ketentuan bahwa amendemen tersebut tidak berdampak material terhadap keamanan, kerahasiaan, atau integritas Data Pribadi .
- 8.2 Rujukan terkait "menulis" atau "tertulis" dalam DPA ini mencakup komunikasi melalui email dan layanan pos bersertifikat.
- 8.3 Jika ada ketentuan dalam DPA ini yang tidak valid atau menjadi tidak valid, hal ini tidak akan memengaruhi keabsahan persyaratan lainnya. Dalam hal terjadi pembatalan ketentuan dalam DPA ini, Para Pihak harus, dalam hal apa pun, berusaha, dengan itikad baik, untuk mengganti ketentuan yang tidak berlaku dengan ketentuan lain, yang dapat diberlakukan, valid dan sah yang mempunyai dampak hukum yang sedapat mungkin sama atau setara dengan salah satu ketentuan awal.
- 8.4 DPA ini diatur oleh hukum yang sama dengan yang mengatur EULA.

LAMPIRAN 1 - PERSYARATAN KHUSUS YURISDIKSI

Jika Pengendali Data didirikan di salah satu yurisdiksi yang tercantum dalam Lampiran 1 ini, persyaratan berikut berlaku untuk DPA, dan persyaratan tersebut akan menggantikan dan mengendalikan jika terdapat perbedaan dengan ketentuan lain dari DPA ini. Semua persyaratan dalam EULA yang tidak secara khusus dimodifikasi oleh persyaratan khusus yurisdiksi yang berlaku dalam Lampiran ini tetap tidak berubah dan berlaku secara penuh.

Brazil:

Para Pihak mengakui dan menyetujui bahwa perubahan DPA berikut akan berlaku:

- a) Semua kemunculan "Data Pribadi Kategori Khusus" di DPA akan diganti dengan "Data Pribadi Sensitif".

Meksiko:

Para Pihak mengakui dan menyetujui bahwa perubahan DPA berikut akan berlaku:

- a) Semua kemunculan "Data Pribadi Kategori Khusus" di DPA akan diganti dengan "Data Pribadi Sensitif";
- b) Untuk penerapan Klausul Kontrak Standar, semua rujukan terhadap "transfer" data pribadi akan ditafsirkan sebagai penghapusan data pribadi sesuai dengan undang-undang Federal Meksiko tentang Perlindungan Data Pribadi yang dipegang oleh Pihak Swasta ("*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*").

Rusia:

Selain ketentuan dalam DPA ini, Para Pihak berjanji sebagai berikut:

- a) Pemroses Data dengan ini menegaskan bahwa Pemroses Data sepenuhnya menyadari bahwa tujuan dari kegiatan Pemrosesan Data Pribadi berdasarkan DPA hanya untuk menyediakan Layanan Pemrosesan dan akan memproses Data Pribadi hanya untuk tujuan yang mana Data Pribadi diungkapkan dan Pengontrol Data memerlukannya dari Pemroses Data. Selain itu, Pemroses Data harus segera mengkonfirmasi secara tertulis bahwa aturan ini dipatuhi atas permintaan dari Pengendali Data.
- b) Sebelum mengungkapkan Data Pribadi yang berasal dari warga negara Rusia ke Pemroses Data, Pengendali Data harus memastikan bahwa semua Data Pribadi tersebut telah dicatat, disistematisasikan, diakumulasikan, disimpan, diklarifikasi (diperbarui, diubah), dan diekstraksi dengan menggunakan database yang berlokasi di wilayah Federasi Rusia ketika Data Pribadi tersebut dikumpulkan dengan cara apa pun, termasuk melalui Internet.
- c) Jika Pengendali Data mendeteksi pemrosesan ilegal atau ketidakakuratan Data Pribadi, Pengendali Data harus segera menginstruksikan kepada Pemroses Data untuk memblokir Data Pribadi ini dan memulai inspeksi. Data Pribadi yang terpengaruh akan diblokir selama seluruh periode inspeksi. Jika inspeksi tersebut memastikan ketidakakuratan Data Pribadi, Pengontrol Data harus meminta Subjek Data yang relevan (perwakilannya) atau otoritas perlindungan data (jika berlaku) untuk melakukan amendemen dan meneruskannya ke Pemroses Data. Data Pribadi yang Tidak Akurat akan segera diamendemen, dan selambat-lambatnya dalam waktu tujuh (7) hari kerja, sejak hari amendemen tersebut dikirimkan ke Pemroses Data. Data Pribadi akan segera dibuka blokirnya setelah amendemen.
- d) Jika terdeteksi bahwa Data Pribadi diproses secara ilegal, Pengendali Data harus menginstruksikan kepada Pemroses Data untuk menghentikan pemrosesan ilegal tersebut dalam waktu tiga (3) hari kerja sejak tanggal deteksi. Jika tampaknya tidak mungkin untuk menghilangkan pelanggaran dan memastikan legalitas pemrosesan Data Pribadi, maka Pengendali Data harus menginstruksikan kepada Pemroses Data untuk memusnahkan Data Pribadi yang diproses secara ilegal dalam waktu sepuluh (10) hari kerja sejak tanggal deteksi. Pengendali Data juga wajib memberi tahu Subjek Data yang relevan (perwakilannya) dan, bila diwajibkan oleh hukum, otoritas perlindungan data tentang penghilangan pelanggaran.
- e) Jika Subjek Data mencabut persetujuannya untuk pemrosesan Data Pribadi, Pengendali Data harus segera memberi tahu Pemroses Data dan Pemroses Data akan menghentikan pemrosesan dan memusnahkan Data Pribadi Subjek Data ini dalam waktu tiga puluh (30) hari sejak tanggal penerimaan pemberitahuan pembatalan oleh Pengendali Data.
- f) Jika tidak mungkin untuk mematuhi periode yang ditetapkan dalam Klausul d) dan e) di atas, Pemroses Data harus memblokir Data Pribadi yang relevan atas permintaan Pengendali Data paling lambat dalam waktu enam (6) bulan dan memusnahkan Data Pribadi ini dalam periode yang sama kecuali undang-undang yang berlaku menentukan lain.

Afrika Selatan:

Para Pihak mengakui dan menyepakati bahwa perubahan DPA berikut akan berlaku sehubungan dengan definisi yang diberikan dalam bagian 1 DPA:

- a) "Subjek Data" berarti orang yang Data Pribadinya sedang diproses.
- b) "Data Pribadi" berarti informasi pribadi sebagaimana didefinisikan dalam POPIA, termasuk setiap informasi yang berkaitan dengan individu yang teridentifikasi atau dapat diidentifikasi.
- c) "POPIA" berarti Undang-Undang Perlindungan Informasi Pribadi Afrika Selatan 4 tahun 2013, dan setiap regulasi, arahan, keputusan, penetapan atau pedoman yang mengikat yang diterbitkan berdasarkan POPIA.

Amerika Serikat:

Selain ketentuan dalam DPA ini, Para Pihak berjanji sebagai berikut:

- a) Masing-masing Pihak mengakui dan menyetujui bahwa pengumpulan dan pengungkapan Data Pribadi yang dikirimkan ke Layanan Pemrosesan (i) bukan merupakan, dan tidak dimaksudkan oleh salah satu pihak untuk melakukan kegiatan yang merupakan, penjualan Data Pribadi, dan (ii) jika imbalan berharga, dalam bentuk uang atau lainnya, diberikan oleh Pengguna yang Sah kepada Pemroses Data, maka imbalan berharga tersebut, dalam bentuk uang atau lainnya, disediakan untuk penggunaan Layanan Pemrosesan dan bukan untuk pengungkapan Data Pribadi. Pemroses Data tidak boleh menyimpan, menggunakan, mengungkapkan, atau menjual Data Pribadi untuk tujuan apa pun selain untuk tujuan khusus dalam melakukan Layanan Pemrosesan, atau sebagaimana diizinkan oleh hukum atau EULA. Untuk menghindari keraguan, Pemroses Data tidak boleh menjual Data Pribadi atau memberi wewenang atau mengizinkan Sub-pemroses mana pun untuk melakukan hal yang sama, kecuali jika diizinkan oleh EULA atau hukum yang berlaku.

Lampiran 2 - Tindakan Keamanan yang diterapkan oleh Pemroses Data

1. Kontrol akses fisik ke tempat dan fasilitas

Pemroses Data akan menerapkan langkah-langkah teknis dan organisasi untuk mengontrol akses ke tempat dan fasilitas, terutama untuk memeriksa otorisasi guna memastikan pencegahan akses yang tidak sah.

Secara khusus:

- Sistem kontrol akses
- Pembaca ID, kartu magnetik, kartu chip
- Masalah kunci
- Penguncian pintu
- Staf keamanan, penjaga
- Fasilitas pengawasan
- Sistem alarm, monitor video/CCTV

2. Kontrol akses ke sistem

Pemroses Data akan menerapkan langkah-langkah teknis (keamanan ID/kata sandi) dan organisasi untuk identifikasi dan autentikasi pengguna untuk mencegah akses tidak sah ke sistem TI.

Secara khusus:

- Prosedur kata sandi (termasuk karakter khusus, panjang minimum, perubahan kata sandi)
- Pemblokiran otomatis (misalnya kata sandi atau batas waktu)
- Enkripsi media data, termasuk yang dapat dihapus dan portabel.

3. Kontroln Akses Logis ke data

Pemroses Data akan memastikan bahwa aktivitas dalam sistem TI yang tidak tercakup oleh hak akses yang dialokasikan akan dicegah dengan memanfaatkan definisi berdasarkan persyaratan skema otorisasi dan hak akses, serta pemantauan dan pencatatan akses.

Secara khusus:

- Hak akses berbasis peran (profil, peran, transaksi, dan objek)
- Penggunaan solusi Manajemen Akun Istimewa komersial guna memfasilitasi autentikasi akun administratif yang aman ke sistem untuk pemeliharaan atau tujuan administratif lainnya
- Laporan otomatis untuk aktivitas yang tidak wajar atau mencurigakan ditinjau dan ditindaklanjuti secara berkala
- Akses, menggunakan model hak istimewa terkecil untuk hanya mengizinkan akses ke sistem dan/atau data berdasarkan kebutuhan untuk mengetahui

4. Pengungkapan dan Kontrol Perlindungan Data

Pemroses Data akan mengontrol pengungkapan Data Pribadi dengan menggabungkan langkah-langkah untuk melakukan transportasi, pengiriman dan komunikasi atau penyimpanan data pada media data (manual atau elektronik) dan untuk pemeriksaan selanjutnya melalui transfer elektronik, transportasi data, dan kontrol transmisi.

Secara khusus:

- Enkripsi/tunneling
- Tanda tangan elektronik
- Pencatatan dan pemantauan berkelanjutan atas peristiwa dan peringatan keamanan
- Keamanan transportasi untuk mengenkripsi data saat transit
- Enkripsi data dalam keadaan mati
- Rotasi berkala pada kunci enkripsi
- Pembatasan akses ke kunci enkripsi untuk orang yang dibatasi
- Kompleksitas kata sandi diaktifkan, dengan autentikasi dua faktor yang diperlukan untuk semua sesi akses jarak jauh

5. Kontrol input

Pemroses Data akan memelihara dokumentasi lengkap pengelolaan dan pemeliharaan data harus dijaga, termasuk langkah-langkah untuk pemeriksaan selanjutnya apakah data telah dimasukkan, diubah atau dibuang (dihapus), dan oleh siapa:

Secara khusus:

- Sistem pencatatan dan pelaporan

6. Kontrol pekerjaan

Pemroses Data akan Memproses Data Pribadi sesuai dengan instruksi Pengendali Data dan menyetujui tindakan (teknis/organisasi) untuk memisahkan tanggung jawab antara Pengendali Data dan Pemroses Data: Secara khusus:

- Susunan kata kontrak yang tidak ambigu
- Komisioning formal (formulir permintaan)
- Kriteria untuk memilih Pemroses Data
- Pemantauan pelaksanaan kontrak

7. Kendali ketersediaan

Pemroses Data akan memastikan bahwa data akan dilindungi dari kerusakan atau kehilangan yang tidak disengaja atau berbahaya dengan mengambil langkah-langkah guna menjamin keamanan fisik dan logis data.

Secara khusus:

- Prosedur pencadangan
- Mirroring hard disk, mis. teknologi RAID
- Suplai daya bebas gangguan (UPS)
- Penyimpanan jarak jauh atau berbasis disk yang direplikasi ke pusat data alternatif
- Perangkat lunak anti-virus dan/atau anti-malware yang diperbarui secara berkala dan sistem application-aware firewall dikonfigurasi dengan pernyataan penolakan default, hanya mengizinkan lalu lintas yang secara eksplisit diizinkan untuk tujuan bisnis
- Rencana Kesenambungan Bisnis dan Pemulihan Bencana

8. Kendali segregasi

Pemroses Data akan berusaha memastikan bahwa data yang dikumpulkan untuk tujuan yang berbeda akan Diproses secara terpisah dan tidak digabungkan dengan data pelanggan lainnya dengan menerapkan langkah-langkah khusus guna menyediakan Pemrosesan terpisah (penyimpanan, amendemen, penghapusan, transmisi) atas data untuk tujuan yang berbeda:

Secara khusus:

- Konsep/batasan penggunaan “klien internal”
- Segregasi fungsi (produksi/pengujian)