Artikel I, Informasi Kontak Bisnis

Artikel ini berlaku jika Pemasok atau Kyndryl Memproses BCI pihak lain.

1.1 Kyndryl dan Pemasok dapat Memproses BCI pihak lain di mana pun mereka menjalankan bisnis berkaitan dengan penyampaian Layanan dan Hasil Kerja oleh Pemasok.

1.2 Suatu pihak:

(a) tidak akan menggunakan atau mengungkapkan BCI pihak lain untuk tujuan lain apa pun (demi kejelasan, tidak satu pun pihak akan Menjual BCI pihak lain atau menggunakan atau mengungkapkan BCI pihak lain untuk tujuan pemasaran apa pun tanpa persetujuan tertulis sebelumnya dari pihak lainnya, dan apabila diperlukan, persetujuan tertulis sebelumnya dari Subjek Data yang terdampak), dan

(b) akan menghapus, memodifikasi, mengoreksi, mengembalikan, memberikan informasi tentang Pemrosesan, membatasi Pemrosesan, atau mengambil tindakan lain yang diminta secara wajar sehubungan dengan BCI pihak lain segera atas permintaan tertulis dari pihak lainnya, kapan pun terjadi penggunaan informasi pribadi yang tidak sah, dan pihak tersebut ingin berhenti memproses dan meremediasi.

1.3 Para pihak tidak mengadakan hubungan Pengontrol bersama terkait BCI satu sama lain dan tidak ada ketentuan Dokumen Transaksi yang akan diinterpretasikan atau ditafsirkan sebagai indikasi maksud apa pun untuk membangun hubungan Pengontrol bersama.

1.4 Pernyataan Privasi Kyndryl di https://www.kyndryl.com/us/en/privacy berisi detail tambahan tentang Pemrosesan BCI oleh Kyndryl.

1.5 Para pihak telah mengimplementasikan dan akan mempertahankan tindakan keamanan teknis dan organisasi untuk melindungi BCI pihak lainnya terhadap kehilangan, kerusakan, perubahan, pengungkapan secara tidak sengaja atau tidak sah, akses secara tidak sengaja atau tidak sah, dan Pemrosesan yang melanggar hukum.

1.6 Pemasok akan segera (dan tidak lebih dari 48 jam) memberi tahu Kyndryl setelah mengetahui adanya Pelanggaran Keamanan yang melibatkan BCI Kyndryl. Pemasok akan memberikan pemberitahuan tersebut ke cyber.incidents@kyndryl.com. Pemasok akan memberikan kepada Kyndryl informasi yang diminta secara wajar terkait pelanggaran tersebut dan status aktivitas remediasi serta restorasi Pemasok apa pun. Sebagai contoh, informasi yang diminta secara wajar dapat mencakup log yang mempertunjukkan akses istimewa, administratif, dan akses lain ke Perangkat, sistem atau aplikasi, gambar forensik Perangkat, sistem atau aplikasi, dan item serupa lainnya, sejauh relevan dengan pelanggaran atau aktivitas remediasi dan restorasi Pemasok.

1.7 Apabila Pemasok hanya Memproses BCI Kyndryl, dan tidak memiliki akses ke data atau materi apa pun lainnya dalam bentuk apa pun atau ke setiap Sistem Korporasi Kyndryl, Artikel ini dan Artikel X (Kerja Sama, Verifikasi, dan Remediasi) adalah satu-satunya Artikel yang berlaku untuk Pemrosesan tersebut.

Artikel II, Tindakan Teknis dan Organisasi, Keamanan Data

Artikel ini berlaku jika Pemasok Memproses Data Kyndryl, selain BCI Kyndryl. Pemasok akan mematuhi persyaratan Artikel ini dalam memberikan semua Layanan dan Hasil Kerja, dan dengan demikian melindungi Data Kyndryl terhadap kehilangan, kerusakan, perubahan, pengungkapan secara tidak sengaja atau tidak sah, akses secara tidak sengaja atau tidak sah, dan bentuk Pemrosesan yang melanggar hukum. Persyaratan Artikel ini menjangkau semua aplikasi, platform, dan infrastruktur TI yang dioperasikan atau dikelola oleh Pemasok dalam memberikan Hasil Kerja dan Layanan, termasuk semua pengembangan, pengujian, hosting, dukungan, operasi, dan lingkungan pusat data.

1. Penggunaan Data

1.1 Pemasok tidak dapat menambahkan ke Data Kyndryl atau menyertakan dengan Data Kyndryl setiap informasi atau data lain, termasuk setiap Data Pribadi, tanpa persetujuan tertulis sebelumnya dari Kyndryl, dan Pemasok tidak dapat menggunakan Data Kyndryl dalam bentuk apa pun, secara agregat atau sebaliknya, untuk tujuan apa pun selain menyediakan Layanan dan Hasil Kerja (sebagai contoh, Pemasok tidak diizinkan untuk menggunakan atau menggunakan kembali Data Kyndryl untuk mengevaluasi efektivitas atau sarana untuk meningkatkan tawaran Pemasok, untuk penelitian dan pengembangan guna membuat tawaran baru, atau untuk menghasilkan laporan terkait tawaran Pemasok). Kecuali jika diizinkan secara tersurat dalam Dokumen Transaksi, Pemasok dilarang Menjual Data Kyndryl.

1.2 Pemasok tidak akan menyematkan teknologi pelacakan web apa pun dalam Hasil Kerja atau sebagai bagian dari Layanan (teknologi tersebut mencakup HTML5, penyimpanan lokal, tag atau token pihak ketiga, dan web beacon) kecuali jika secara tegas diizinkan dalam Dokumen Transaksi.

2. Kerahasiaan dan Permintaan Pihak Ketiga

2.1 Pemasok tidak akan mengungkapkan Data Kyndryl kepada pihak ketiga mana pun, kecuali jika diberi wewenang sebelumnya oleh Kyndryl secara tertulis. Jika pemerintah, termasuk setiap pembuat peraturan, meminta akses ke Data Kyndryl (misalnya, jika pemerintah AS menyerahkan pemberitahuan ketertiban keamanan nasional kepada Pemasok untuk memperoleh Data Kyndryl), atau jika pengungkapan Data Kyndryl diwajibkan oleh hukum, Pemasok akan memberi tahu Kyndryl secara tertulis mengenai permintaan atau persyaratan tersebut dan memberi Kyndryl peluang yang wajar untuk mengajukan keberatan terhadap pengungkapan apa pun (apabila hukum melarang pemberitahuan, Pemasok akan mengambil langkah yang diyakini secara wajar sesuai untuk mengajukan keberatan terhadap pelarangan dan pengungkapan Data Kyndryl melalui tindakan yudisial atau cara lainnya).

2.2 Pemasok memastikan Kyndryl bahwa: (a) hanya karyawannya yang perlu akses ke Data Kyndryl untuk menyediakan Layanan atau Hasil Kerja yang akan memiliki akses tersebut, kemudian hanya sejauh diperlukan untuk menyediakan Layanan dan Hasil Kerja tersebut; dan (b) Pemasok telah mengikat karyawannya pada kewajiban kerahasiaan yang mensyaratkan karyawan tersebut untuk hanya menggunakan dan mengungkapkan Data Kyndryl sebagaimana yang diizinkan dalam Syarat-Syarat ini.

3. **Pengembalian atau Penghapusan Data Kyndryl**

3.1 Pemasok akan, atas pilihan Kyndryl, menghapus atau mengembalikan Data Kyndryl kepada Kyndryl setelah pengakhiran atau habis masa berlaku Dokumen Transaksi, atau lebih awal atas permintaan dari Kyndryl. Jika Kyndryl mensyaratkan penghapusan, maka Pemasok akan, sesuai dengan Praktik Terbaik Industri, menyajikan data yang tidak dapat dibaca dan tidak dapat disusun ulang atau direkonstruksi, dan akan menjamin penghapusan ke Kyndryl. Jika Kyndryl mewajibkan pengembalian Data Kyndryl, maka Pemasok akan melakukannya dengan jadwal Kyndryl yang wajar dan sesuai dengan instruksi tertulis Kyndryl yang wajar.

Artikel III, Privasi

Artikel ini berlaku jika Pemasok Memproses Data Pribadi Kyndryl.

1. Pemrosesan

1.1 Kyndryl menunjuk Pemasok sebagai Prosesor untuk Memproses Data Pribadi Kyndryl semata untuk tujuan memberikan Hasil Kerja dan Layanan sesuai dengan instruksi Kyndryl, termasuk yang termuat dalam Syarat-Syarat ini, Dokumen Transaksi, dan perjanjian dasar terkait di antara para pihak. Jika Pemasok tidak mengakomodasi instruksi, Kyndryl dapat mengakhiri bagian Layanan yang terdampak dengan pemberitahuan tertulis. Jika Pemasok meyakini bahwa suatu instruksi melanggar undang-undang perlindungan data, Pemasok akan segera menginformasikan kepada Kyndryl dan dalam kerangka waktu kapan pun yang diwajibkan oleh hukum. Jika Pemasok gagal memenuhi kewajibannya berdasarkan Syarat-Syarat ini dan kegagalan tersebut menyebabkan penggunaan Informasi Pribadi yang tidak sah, atau, secara umum, dalam hal penggunaan Informasi Pribadi yang tidak sah, Kyndryl berhak menghentikan pemrosesan dan memperbaiki kegagalan dan meremediasi dampak berbahaya dari penggunaan yang tidak sah, dengan kinerja dan remediasi tersebut sesuai arahan dan jadwal yang wajar dari Kyndryl.

1.2 Pemasok akan mematuhi semua undang-undang perlindungan data yang berlaku untuk Layanan dan Hasil Kerja.

1.3 Ekshibit untuk Dokumen Transaksi, atau Dokumen Transaksi itu sendiri, menjabarkan hal-hal berikut berkenaan dengan Data Kyndryl:

(a) kategori Subjek Data;
(b) jenis Data Pribadi Kyndryl;
(c) tindakan data dan aktivitas Pemrosesan;
(d) durasi dan frekuensi Pemrosesan; dan
(e) daftar Subprosesor.

2. Tindakan Teknis dan Organisasi

2.1 Pemasok akan mengimplementasikan dan mempertahankan tindakan teknis dan organisasi yang dijabarkan dalam Artikel II (Tindakan Teknis dan Organisasi, Keamanan Data) dan Artikel VIII (Tindakan Teknis dan Organisasi, Keamanan Umum), dan dengan demikian memastikan tingkat keamanan yang sesuai untuk risiko yang dihadirkan Layanan dan Hasil Kerjanya. Pemasok menyatakan dan memahami bahwa pembatasan dalam Artikel II, Artikel III ini, dan Artikel VIII serta akan mematuhinya.

3. Permintaan dan Hak Subjek Data

3.1 Pemasok akan segera menginformasikan kepada Kyndryl (dengan jadwal yang mengizinkan Kyndryl dan setiap Pengontrol Lainnya untuk memenuhi kewajiban hukum mereka) mengenai setiap permintaan dari Subjek Data untuk melaksanakan setiap hak Subjek Data (misalnya, pembetulan, penghapusan, atau pemblokiran data) terkait Data Pribadi Kyndryl. Pemasok juga dapat segera mengarahkan Subjek Data yang mengajukan permintaan tersebut kepada Kyndryl. Pemasok tidak akan memberikan jawaban atas permintaan apa pun dari Subjek Data kecuali jika diwajibkan secara hukum atau diinstruksikan secara tertulis oleh Kyndryl untuk melakukan hal tersebut.

3.2 Apabila Kyndryl berkewajiban untuk memberikan informasi mengenai Data Pribadi Kyndryl kepada Pengontrol Lain atau pihak ketiga lainnya (misalnya, Subjek Data atau pembuat peraturan), Pemasok akan membantu Kyndryl dengan memberikan informasi dan mengambil tindakan lain yang wajar sebagaimana yang diminta oleh Kyndryl, dengan jadwal yang memungkinkan Kyndryl untuk menanggapi secara tepat waktu terhadap Pengontrol Lain atau pihak ketiga tersebut.

4. Subprosesor

4.1 Pemasok akan memberikan Kyndryl pemberitahuan tertulis sebelumnya sebelum menambahkan Subprosesor baru atau memperluas cakupan Pemrosesan oleh Subprosesor yang sudah ada, dengan pemberitahuan tertulis tersebut yang mengidentifikasi nama Subprosesor dan menguraikan cakupan yang baru atau diperluas dari Pemrosesan. Kyndryl dapat mengajukan keberatan terhadap setiap Subprosesor baru tersebut atau cakupan yang diperluas dengan landasan yang wajar kapan pun, dan jika demikian, para pihak akan bekerja bersama dengan iktikad baik untuk mengatasi keberatan Kyndryl. Dengan tunduk pada hak Kyndryl untuk mengajukan keberatan kapan saja, Pemasok dapat menugaskan Subprosesor baru atau memperluas cakupan Pemrosesan Subprosesor yang sudah ada jika Kyndryl tidak mengajukan keberatan dalam waktu 30 Hari sejak tanggal pemberitahuan tertulis dari Pemasok.

4.2 Pemasok akan mengenakan kewajiban perlindungan data, keamanan, dan sertifikasi yang dijabarkan dalam Syarat-Syarat ini pada masing-masing Subprosesor yang disetujui sebelum Subprosesor Memproses setiap Data Kyndryl. Pemasok sepenuhnya bertanggung jawab kepada Kyndryl atas pelaksanaan kewajiban masing-masing Subprosesor.

5. Pemrosesan Data Lintas Batas

Sebagaimana yang digunakan di bawah:

Negara yang Memadai berarti negara yang memberikan tingkat perlindungan data yang memadai sehubungan dengan transfer yang relevan menurut peraturan perundang-undangan perlindungan data yang berlaku atau keputusan pembuat peraturan.

Pengimpor Data berarti Prosesor atau Subprosesor yang tidak didirikan di Negara yang Memadai.

Klausul Kontrak Standar Uni Eropa ("EU SCC") berarti Klausul Kontrak Standar Uni Eropa (Keputusan Komisi 2021/914) dengan klausul opsional yang diterapkan kecuali untuk opsi 1 Klausul 9(a) dan opsi 2 Klausul 17, sebagaimana yang dipublikasikan secara resmi di https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en

Klausul Kontrak Standar Serbia ("Serbian SCC") berarti Klausul Kontrak Standar Serbia sebagaimana yang diadopsi oleh "Komisioner Serbia untuk Informasi Kepentingan Publik dan Perlindungan Data Pribadi", yang dipublikasikan di https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx.

Klausul Kontrak Standar (Standard Contractual Clause - "**SCC**") berarti klausul kontrak yang diwajibkan oleh peraturan perundang-undangan perlindungan data yang berlaku untuk transfer Data Pribadi ke Prosesor yang tidak didirikan di Negara yang Memadai.

Adendum Transfer Data Internasional Inggris untuk Klausul Kontrak Standar Komisi Uni Eropa ("Adendum Inggris") berarti Adendum Transfer Data Internasional Inggris untuk Klausul Kontrak Standar Komisi Uni Eropa sebagaimana yang dipublikasikan secara resmi di https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.

Adendum Swiss untuk Klausul Kontrak Standar Komisi Uni Eropa ("Adendum Swiss") berarti klausul kontrak untuk Klausul Kontrak Standar Komisi Uni Eropa yang berlaku sesuai dengan keputusan Otoritas Perlindungan Data Swiss (**"FDPIC"**) dan sesuai dengan Undang-Undang Federal Swiss tentang Perlindungan Data (**"FADP"**).

5.1 Pemasok tidak akan mentransfer atau mengungkapkan (termasuk melalui akses jarak jauh) setiap Data Pribadi Kyndryl lintas batas tanpa persetujuan tertulis sebelumnya dari Kyndryl. Jika Kyndryl memberikan persetujuan tersebut, para pihak akan bekerja sama untuk memastikan kepatuhan terhadap peraturan perundang-undangan perlindungan data yang berlaku. Jika SCC diwajibkan oleh peraturan perundang-undangan tersebut, Pemasok akan segera menandatangani SCC atas permintaan Kyndryl.

5.2 Mengenai EU SCC:

(a) Jika Pemasok tidak didirikan di Negara yang Memadai: Pemasok dengan ini menyepakati EU SCC sebagai Pengimpor Data dengan Kyndryl, dan Pemasok akan mengadakan perjanjian tertulis dengan setiap Subprosesor yang disetujui, sesuai dengan Klausul 9 EU SCC, dan akan menyediakan salinan perjanjian tersebut sesuai permintaan Kyndryl.

(i) Modul 1 EU SCC tidak berlaku kecuali jika disepakati lain oleh para pihak secara tertulis.

(ii) Modul 2 EU SCC berlaku apabila Kyndryl adalah Pengontrol dan Modul 3 berlaku apabila Kyndryl adalah Prosesor. Sesuai dengan Klausul 13 EU SCC, bila Modul 2 atau 3 berlaku, para pihak setuju bahwa (1) EU SCC akan diatur oleh hukum dari negara anggota Uni Eropa tempat otoritas pengawas yang kompeten berada dan (2) sengketa apa pun yang timbul dari EU SCC akan diselesaikan di pengadilan negara anggota Uni Eropa tempat otoritas pengawas yang kompeten berada. Jika hukum tersebut dalam (1) tidak mengizinkan hak-hak penerima manfaat pihak ketiga, maka EU SCC akan diatur oleh hukum Belanda dan setiap sengketa yang timbul dari EU SCC berdasarkan (2) akan diselesaikan oleh pengadilan Amsterdam di Belanda.

(b) Jika kedua belah pihak, Pemasok dan Kyndryl, didirikan di Negara yang Memadai, Pemasok akan bertindak sebagai Pengekspor Data dan terikat dalam EU SCC dengan masing-masing Subprosesor yang disetujui di Negara yang Tidak Memadai. Pemasok akan melakukan Penilaian Dampak Transfer (Transfer Impact Assessment - "TIA") yang diperlukan dan memberi tahu Kyndryl tanpa penundaan yang tidak semestinya tentang (1) setiap kebutuhan untuk menerapkan tindakan tambahan dan (2) tindakan yang diterapkan. Atas permintaan, Pemasok akan memberikan hasil TIA dan informasi apa pun yang diperlukan untuk memahami dan mengevaluasi hasilnya kepada Kyndryl. Apabila Kyndryl tidak setuju dengan hasil TIA Pemasok atau tindakan tambahan yang diterapkan, Kyndryl dan Pemasok akan bekerja sama untuk mencari solusi yang memungkinkan. Kyndryl tetap berhak untuk menangguhkan atau mengakhiri layanan Pemasok terkait tanpa kompensasi. Untuk menghindari keraguan, hal ini tidak membebaskan Subprosesor Pemasok dari kewajiban untuk menjadi pihak dalam EU SCC dengan Kyndryl atau Pelanggannya sebagaimana yang diuraikan dalam pasal 5.2 (d) di bawah.

(c) Jika Pemasok didirikan dalam Wilayah Ekonomi Eropa dan Kyndryl adalah Pengontrol yang tidak tunduk pada Peraturan Perlindungan Data Umum 2016/679, maka Modul 4 EU SCC berlaku, dan Pemasok dengan ini menandatangani EU SCC sebagai pengekspor data dengan Kyndryl. Jika Modul 4 EU SCC berlaku, maka para pihak setuju bahwa EU SCC akan diatur oleh hukum Belanda dan setiap sengketa yang timbul dari EU SCC akan diselesaikan oleh pengadilan Amsterdam di Belanda.

(d) Apabila Pengontrol Lain, seperti Pelanggan atau afiliasi, meminta untuk menjadi pihak dalam EU SCC sesuai dengan 'klausul docking' dalam Klausul 7, Pemasok dengan ini menyetujui setiap permintaan tersebut.

(e) Tindakan Teknis dan Organisasi yang diperlukan untuk melengkapi Aneks II EU SCC dapat ditemukan dalam Syarat-Syarat ini, Dokumen Transaksi itu sendiri, dan perjanjian dasar terkait di antara para pihak.

(f) Apabila terdapat ketidaksesuaian apa pun antara EU SCC dan Syarat-Syarat ini, maka EU SCC yang akan berlaku.

5.3 Perihal Adendum Inggris:

(a) Jika Pemasok tidak didirikan di Negara Adekuat: (i) Pemasok dengan ini menandatangani Adendum Inggris dengan Kyndryl sebagai Importir untuk menambahkan EU SCC yang ditetapkan di atas (sebagaimana yang berlaku, tergantung pada keadaan terkait aktivitas pemrosesan); dan (ii) Pemasok akan mengadakan perjanjian tertulis dengan setiap Subprosesor yang disetujui, dan akan memberi Kyndryl salinan perjanjian tersebut jika diminta.

(b) Jika Pemasok didirikan di Negara Adekuat, dan Kyndryl adalah Pengendali yang tidak tunduk pada Peraturan Perlindungan Data Umum Inggris (sebagaimana yang digabungkan ke dalam hukum Inggris berdasarkan Undang-Undang Uni Eropa (Penarikan) 2018), maka Pemasok dengan ini menandatangani Adendum Inggris sebagai Eksportir dengan Kyndryl untuk ditambahkan ke EU SCC yang ditetapkan dalam Pasal 5.2(b) di atas.

(c) Jika Pengendali Lain, seperti Pelanggan atau afiliasi, meminta untuk menjadi pihak dalam Adendum Inggris, Pemasok dengan ini menyetujui permintaan tersebut.

(d) Informasi Apendiks (sebagaimana yang ditetapkan dalam Tabel 3) di Adendum Inggris dapat ditemukan di EU SCC yang berlaku, Syarat-Syarat ini, Dokumen Transaksi itu sendiri, serta perjanjian dasar terkait di antara para pihak. Baik Kyndryl maupun Pemasok tidak dapat mengakhiri Adendum Inggris apabila Adendum Inggris mengalami perubahan.

(e) Apabila terdapat ketidaksesuaian antara Adendum Inggris dan Syarat-Syarat ini, maka Adendum Inggris yang akan berlaku.

5.4 Perihal Serbian SCC:

(a) Jika Pemasok tidak didirikan di Negara yang Memadai: (i) Pemasok dengan ini menandatangani Serbian SCC dengan Kyndryl atas nama Pemasok sendiri sebagai Prosesor; dan (ii) Pemasok akan menandatangani perjanjian tertulis dengan masing-masing Subprosesor yang disetujui, sesuai dengan Artikel 8 Serbian SCC, dan akan memberikan salinan perjanjian tersebut kepada Kyndryl atas permintaan.

(b) Apabila Pemasok didirikan di Negara yang Memadai, maka Pemasok dengan ini menandatangani Serbian SCC dengan Kyndryl atas nama masing-masing Subprosesor yang berada di Negara yang Tidak Memadai. Jika Pemasok tidak dapat melakukannya untuk setiap Subprosesor tersebut, maka Pemasok akan memberikan Serbian SCC yang ditandatangani oleh Subprosesor tersebut kepada Kyndryl agar Kyndryl turut menandatangani sebelum mengizinkan Subprosesor untuk Memproses setiap Data Pribadi Kyndryl.

(c) Serbian SCC antara Kyndryl dan Pemasok akan berfungsi sebagai Serbian SCC antara Pengontrol dan Prosesor atau sebagai perjanjian tertulis konsekutif antara 'prosesor' dan 'subprosesor', sebagaimana yang dibutuhkan oleh fakta. Apabila terdapat ketidaksesuaian antara Serbian SCC dan Syarat-Syarat ini, maka Serbian SCC yang akan berlaku.

(d) Informasi yang diperlukan untuk melengkapi Apendiks 1 hingga 8 dari Serbian SCC untuk tujuan mengatur transfer Data Pribadi ke Negara yang Tidak Memadai dapat ditemukan di Syarat-Syarat ini dan Ekshibit pada Dokumen Transaksi atau Dokumen Transaksi itu sendiri.

5.5. Mengenai Adendum Swiss:

(a) Jika dan sejauh transfer Data Pribadi Kyndryl berdasarkan pasal 5.1. tunduk pada Undang-Undang Federal Swiss tentang Perlindungan Data ("FADP") EU SCC yang disetujui di Bagian 5.2. Syarat-Syarat ini akan mengatur transfer, dengan amendemen berikut untuk mengadopsi standar GDPR tentang Data Pribadi Swiss:

- Referensi Peraturan Perlindungan Data Umum ("GDPR") harus dipahami juga sebagai referensi untuk ketentuan yang setara dari FADP,
- Komisi Informasi Perlindungan Data Federal Swiss adalah otoritas pengawas yang kompeten sesuai Klausul 13 dan Lampiran I.C dari EU SCC
- Hukum Swiss sebagai hukum yang mengatur dalam hal transfer secara eksklusif tunduk pada FADP dan
- Syarat "status anggota" dalam Klausul 18 dari EU SCC harus diperluas untuk menyertakan Swiss dengan tujuan memungkinkan subjek data Swiss untuk mengupayakan hak mereka di tempat tinggal tetap mereka.

(b) Untuk menghindari keraguan, tidak satu pun klausul di atas yang dimaksudkan untuk mengurangi tingkat perlindungan data yang diberikan oleh EU SCC dengan cara apa pun, tetapi hanya untuk memperluas tingkat perlindungan ini ke subjek data Swiss. Jika dan sejauh hal tersebut tidaklah demikian, maka EU SCC yang akan berlaku.

6. Bantuan dan Catatan

6.1 Mempertimbangkan sifat Pemrosesan, Pemasok akan membantu Kyndryl dengan menjalankan tindakan teknis dan organisasi yang sesuai untuk memenuhi kewajiban yang berkaitan dengan permintaan dan hak Subjek Data. Pemasok juga akan membantu Kyndryl dalam memastikan kepatuhan terhadap kewajiban yang berkaitan dengan keamanan Pemrosesan, pemberitahuan dan komunikasi Pelanggaran Keamanan, dan pembuatan penilaian dampak perlindungan data, termasuk konsultasi sebelumnya dengan pembuat peraturan yang bertanggung jawab, apabila diperlukan, dengan mempertimbangkan informasi yang tersedia bagi Pemasok.

6.2 Pemasok akan mengelola catatan nama dan detail kontak terbaru dari masing-masing Subprosesor, termasuk masing-masing perwakilan dan pejabat perlindungan data Subprosesor. Atas permintaan, Pemasok akan memberikan catatan ini kepada Kyndryl dengan jadwal yang memungkinkan Kyndryl untuk menanggapi secara tepat waktu setiap permintaan dari Pelanggan atau pihak ketiga lainnya.

Artikel IV, Tindakan Teknis dan Organisasi, Keamanan Kode

Artikel ini berlaku jika Pemasok memiliki akses ke Kode Sumber Kyndryl. Pemasok akan mematuhi persyaratan Artikel ini dan dengan demikian melindungi Kode Sumber Kyndryl terhadap kehilangan, kerusakan, perubahan, pengungkapan secara tidak sengaja atau tidak sah, akses secara tidak sengaja atau tidak sah, dan bentuk Penanganan yang melanggar hukum. Persyaratan Artikel ini diperluaskan ke semua aplikasi, platform, dan infrastruktur TI yang dioperasikan atau dikelola oleh Pemasok dalam memberikan Hasil Kerja dan Layanan, dan dalam Penanganan Teknologi Kyndryl, termasuk semua pengembangan, pengujian, hosting, dukungan, operasi, dan lingkungan pusat data.

1. Persyaratan Keamanan

Sebagaimana yang digunakan di bawah,

Negara yang Dilarang berarti setiap negara: (a) yang ditetapkan oleh Pemerintah AS sebagai musuh asing berdasarkan Perintah Eksekutif perihal Pengamanan Teknologi Informasi dan Komunikasi dan Rantai Pasokan Layanan (Executive Order on Securing the Information and Communications Technology and Services Supply Chain) tertanggal 15 Mei 2019, (b) yang terdaftar sesuai dengan Pasal 1654 Undang-Undang Otorisasi Pertahanan Nasional A.S. (U.S. National Defense Authorization Act) 2019, atau (c) diidentifikasi sebagai "Negara yang Dilarang" dalam Dokumen Transaksi.

1.1 Pemasok tidak akan mendistribusikan atau menempatkan setiap Kode Sumber Kyndryl dalam penangguhan untuk kepentingan pihak ketiga mana pun.

1.2 Pemasok tidak akan mengizinkan setiap Kode Sumber Kyndryl untuk ditempatkan di server yang berlokasi di Negara yang Dilarang.Pemasok tidak akan mengizinkan siapa pun, termasuk Personelnya, yang berlokasi di Negara yang Dilarang atau mengunjungi Negara yang Dilarang (sejauh untuk kunjungan semacam itu), demi alasan apa pun, unutk mengakses atau menggunakan setiap Kode Sumber Kyndryl, terlepas dari lokasi Kode Sumber Kyndryl secara global, dan Pemasok tidak akan mengizinkan setiap pengembangan, pengujian, atau pekerjaan lain dilakukan di Negara yang Dilarang yang akan memerlukan akses atau penggunaan tersebut.

1.3 Pemasok tidak akan menempatkan atau mendistribusikan Kode Sumber Kyndryl di setiap yurisdiksi di mana hukum atau interpretasi hukum memerlukan pengungkapan Kode Sumber kepada pihak ketiga mana pun. Jika terdapat perubahan hukum atau interpretasi hukum dalam yurisdiksi di mana Kode Sumber Kyndryl berlokasi yang dapat menyebabkan Pemasok diwajibkan mengungkap Kode Sumber tersebut kepada pihak ketiga, Pemasok akan segera memusnahkan atau segera menghapus Kode Sumber Kyndryl tersebut dari yurisdiksi tersebut, dan tidak akan menempatkan setiap Kode Sumber Kyndryl tambahan di yurisdiksi tersebut jika hukum atau interpretasi hukum yang demikian masih berlaku.

1.4 Pemasok tidak akan, secara langsung atau tidak langsung, mengambil tindakan apa pun, termasuk menandatangani perjanjian apa pun, yang dapat menyebabkan Pemasok, Kyndryl, atau pihak ketiga mana pun terkena kewajiban pengungkapan berdasarkan Pasal 1654 atau 1655 Undang-Undang Otorisasi Pertahanan Nasional A.S. (U.S. National Defense Authorization Act) tahun 2019. Demi kejelasan, kecuali sebagaimana yang mungkin diizinkan secara tegas dalam Dokumen Transaksi atau perjanjian dasar terkait di antara para pihak, Pemasok tidak diizinkan untuk mengungkapkan Kode Sumber Kyndryl kepada pihak ketiga mana pun, dalam situasi apa pun, tanpa persetujuan tertulis sebelumnya dari Kyndryl.

1.5 Jika Kyndryl memberi tahu Pemasok, atau pihak ketiga memberi tahu salah satu pihak bahwa: (a) Pemasok telah mengizinkan Kode Sumber Kyndryl untuk dibawa ke Negara yang Dilarang atau yurisdiksi mana pun dengan tunduk pada Pasal 1.3 di atas, (b) Pemasok telah merilis, mengakses, atau menggunakan Kode Sumber Kyndryl dengan cara yang tidak diizinkan dalam Dokumen Transaksi atau perjanjian dasar atau perjanjian terkait lainnya di antara para pihak atau (c) Pemasok telah melanggar Pasal 1.4 di atas, kemudian tanpa membatasi hak Kyndryl untuk menangani ketidakpatuhan tersebut menurut aturan hukum atau asas keadilan atau berdasarkan Dokumen Transaksi atau perjanjian dasar atau perjanjian lain yang terkait di antara para pihak: (i) jika pemberitahuan tersebut ditujukan kepada Pemasok, maka Pemasok akan segera membagikan pemberitahuan tersebut kepada Kyndryl; dan (ii) Pemasok, atas arahan Kyndryl yang wajar, akan

menginvestigasi dan meremediasi permasalahan dengan jadwal yang ditentukan oleh Kyndryl secara wajar (setelah berkonsultasi dengan Pemasok).

1.6 Jika Kyndryl meyakini secara wajar bahwa perubahan dalam kebijakan, prosedur, kontrol, atau praktik Pemasok berkaitan dengan akses Kode Sumber mungkin diperlukan untuk menangani keamanan siber, pencurian kekayaan intelektual atau serupa itu atau risiko terkait (termasuk risiko bahwa tanpa perubahan tersebut Kyndryl mungkin dibatasi untuk menjual ke Pelanggan tertentu atau ke pasar tertentu atau sebaliknya tidak dapat memenuhi persyaratan keamanan atau rantai pasokan Pelanggan), maka Kyndryl dapat menghubungi Pemasok untuk membahas tindakan yang diperlukan untuk menangani risiko tersebut, termasuk perubahan pada kebijakan, prosedur, kontrol, atau praktik tersebut. Atas permintaan Kyndryl, Pemasok akan bekerja sama dengan Kyndryl dalam mengevaluasi apakah perubahan tersebut diperlukan dan dalam mengimplementasikan perubahan yang sesuai dan disetujui bersama.

Artikel V, Pengembangan Aman

Artikel ini berlaku jika Pemasok akan memberikan Kode Sumbernya atau Kode Sumber pihak ketiga atau Perangkat Lunak di Lokasi kepada Kyndryl, atau jika ada Hasil Kerja atau Layanan Pemasok yang akan diberikan kepada Pelanggan Kyndryl sebagai bagian dari produk atau layanan Kyndryl.

1. Kesiapan Keamanan

1.1 Pemasok akan bekerja sama dengan proses internal Kyndryl yang menilai kesiapan keamanan produk dan layanan Kyndryl yang bergantung pada setiap Hasil Kerja Pemasok, termasuk menanggapi sepenuhnya dan tepat waktu atas permintaan informasi, baik melalui dokumen, catatan lain, wawancara Personel Pemasok terkait, atau semacamnya.

2. Pengembangan Aman

2.1 Pasal 2 ini hanya berlaku apabila Pemasok memberikan Perangkat Lunak di Lokasi kepada Kyndryl.

2.2 Pemasok telah mengimplementasikan dan akan memelihara selama jangka waktu Dokumen Transaksi, sesuai dengan Praktik Terbaik Industri, jaringan, platform, sistem, aplikasi, perangkat, infrastruktur fisik, tanggapan insiden, dan kebijakan, prosedur, dan kontrol keamanan yang berfokus pada Personel yang diperlukan untuk melindungi: (a) sistem dan lingkungan pengembangan, pembuatan, pengujian, dan operasi di mana Pemasok atau pihak ketiga mana pun yang dilibatkan oleh Pemasok mengoperasikan, mengelola, menggunakan, atau mengandalkan untuk atau sehubungan dengan Hasil Kerja dan (b) semua kode sumber Hasil Kerja terhadap kehilangan, bentuk penanganan yang melanggar hukum, serta akses, pengungkapan, atau perubahan yang tidak sah.

3. Sertifikasi ISO 20243

3.1 Pasal 3 ini hanya berlaku jika ada Hasil Kerja atau Layanan Pemasok yang akan diberikan kepada Pelanggan Kyndryl sebagai bagian dari produk atau layanan Kyndryl.

3.2 Pemasok akan mendapatkan sertifikasi kepatuhan dengan ISO 20243, Teknologi informasi, Open Trusted Technology Provider, TM Standard (O-TTPS), Mitigasi produk yang tercemar dan palsu (sertifikasi yang dinilai secara mandiri atau yang didasarkan pada penilaian auditor independen yang bereputasi). Alternatifnya, jika Pemasok meminta secara tertulis dan Kyndryl menyetujui secara tertulis, Pemasok akan memperoleh sertifikasi kepatuhan dengan standar industri yang setara secara substansial yang menangani pengembangan aman dan praktik rantai pasokan (baik sertifikasi yang dinilai secara mandiri atau yang didasarkan pada penilaian auditor independen yang bereputasi, jika dan sebagaimana disetujui oleh Kyndryl).

3.3 Pemasok akan memperoleh sertifikasi kepatuhan dengan ISO 20243 atau standar industri yang setara secara substansial (jika Kyndryl menyetujui secara tertulis) paling lambat 180 Hari setelah tanggal mulai berlaku Dokumen Transaksi
kemudian memperpanjang sertifikasi setiap 12 bulan setelahnya (dengan masing-masing pembaruan pada versi terbaru saat itu dari standar yang berlaku, yaitu ISO 20243 atau, apabila Kyndryl telah menyetujui secara tertulis, standar industri yang setara secara substansial yang menangani pengembangan aman dan praktik rantai pasokan).

3.4 Pemasok akan, atas permintaan, segera memberikan salinan sertifikasi yang wajib diperoleh oleh Pemasok kepada Kyndryl, sesuai Pasal 2.1 dan 2.2 di atas.

4. Kerentanan Keamanan

Sebagaimana yang digunakan di bawah,

Koreksi Kesalahan berarti perbaikan bug dan revisi yang mengoreksi kesalahan atau defisiensi, termasuk Kerentanan Keamanan, dalam Hasil Kerja.

Mitigasi berarti setiap cara yang diketahui untuk mengurangi atau menghindari risiko Kerentanan Keamanan.

Kerentanan Keamanan berarti kondisi dalam desain, pengodean, pengembangan, implementasi, pengujian, pengoperasian, dukungan, pemeliharaan, atau manajemen Hasil Kerja yang memungkinkan serangan oleh siapa pun yang dapat berakibat pada akses yang tidak sah atau eksploitasi, termasuk: (a) akses ke, kontrol atau gangguan operasi sistem, (b) akses ke, penghapusan, pengubahan, atau ekstraksi data, atau (c) perubahan identitas, otorisasi, atau izin pengguna atau administrator. Kerentanan Keamanan mungkin ada terlepas dari apakah ID Kerentanan dan Eksposur Umum (Common Vulnerabilities and Exposures - "CVE") atau setiap pemberian skor atau klasifikasi resmi ditetapkan untuknya.

4.1 Pemasok menyatakan dan menjamin bahwa pihaknya akan: (a) menggunakan Praktik Terbaik Industri untuk mengidentifikasi Kerentanan Keamanan, termasuk melalui pemindaian keamanan aplikasi kode sumber statis dan dinamis berkelanjutan, pemindaian keamanan sumber terbuka dan pemindaian kerentanan sistem, dan (b) mematuhi persyaratan dari Syarat-Syarat ini untuk membantu mencegah, mendeteksi, dan mengoreksi Kerentanan Keamanan pada Hasil Kerja dan di semua aplikasi, platform, dan infrastruktur TI di mana dan selama Pemasok membuat dan menyediakan Layanan dan Hasil Kerja.

4.2 Jika Pemasok menyadari adanya Kerentanan Keamanan dalam Hasil Kerja atau setiap aplikasi, platform, atau infrastruktur TI tersebut, Pemasok akan memberikan Koreksi Kesalahan dan Mitigasi kepada Kyndryl untuk semua versi dan rilis Hasil Kerja sesuai dengan Tingkat Keparahan dan kerangka waktu yang ditentukan dalam tabel di bawah:

Tingkat Keparahan*
Kerentanan Keamanan Darurat – adalah Kerentanan Keamanan yang merupakan ancaman berat dan berpotensi global. Kyndryl menetapkan Kerentanan Keamanan Darurat menurut diskresinya semata, terlepas dari Skor Dasar CVSS.
Kritis – yaitu Kerentanan Keamanan yang memiliki Skor Dasar CVSS dari 9 hingga 10,0
Tinggi – yaitu Kerentanan Keamanan yang memiliki Skor Dasar CVSS dari 7,0 hingga 8,9
Sedang – yaitu Kerentanan Keamanan yang memiliki Skor Dasar CVSS dari 4,0 hingga 6,9
Rendah – yaitu Kerentanan Keamanan yang memiliki Skor Dasar CVSS dari 0,0 hingga 3,9

Kerangka Waktu				
Darurat	***Kritis***	***Tinggi***	***Sedang***	***Rendah***
4 Hari atau kurang, sebagaimana yang ditentukan oleh Kantor Kepala Keamanan	30 Hari	30 Hari	90 Hari	Sesuai Praktik Terbaik Industri

Informasi (Chief Information Security Office) Kyndryl				

* Apabila Kerentanan Keamanan tidak memiliki Skor Dasar CVSS yang siap ditetapkan, Pemasok akan menerapkan Tingkat Keparahan yang sesuai dengan sifat dan keadaan kerentanan tersebut.

4.3 Untuk Kerentanan Keamanan yang telah diungkapkan kepada publik dan yang Pemasok belum memberikan Koreksi Kesalahan atau Mitigasi kepada Kyndryl, Pemasok akan mengimplementasikan setiap kontrol keamanan tambahan yang layak secara teknis yang dapat memitigasi risiko kerentanan.

4.4 Apabila Kyndryl tidak puas dengan tanggapan Pemasok atas setiap Kerentanan Keamanan dalam Hasil Kerja atau setiap aplikasi, platform, atau infrastruktur yang dirujuk di atas, maka tanpa prasangka pada setiap hak Kyndryl lainnya, Pemasok akan segera mengatur Kyndryl untuk mendiskusikan persoalannya secara langsung dengan Wakil Direktur Pemasok atau eksekutif setara yang bertanggung jawab atas penyampaian Koreksi Kesalahan.

4.5 Contoh Kerentanan Keamanan termasuk kode pihak ketiga atau kode sumber terbuka end-of-service ("EOS"), di mana tipe kode ini sudah tidak lagi menerima perbaikan keamanan.

Artikel VI, Akses Sistem Korporasi

Artikel ini berlaku jika karyawan Pemasok akan memiliki akses ke setiap Sistem Korporasi.

1. Syarat-Syarat Umum

1.1 Kyndryl akan menentukan apakah akan mengotorisasi karyawan Pemasok untuk mengakses Sistem Korporasi. Jika Kyndryl memberikan otorisasi, maka Pemasok akan mematuhi, dan akan menjadikan karyawannya yang memiliki akses untuk patuh dengan persyaratan Artikel ini.

1.2 Kyndryl akan mengidentifikasi cara yang digunakan karyawan Pemasok untuk dapat mengakses Sistem Korporasi, termasuk apakah karyawan tersebut akan mengakses Sistem Korporasi melalui Perangkat yang disediakan Kyndryl atau Pemasok.

1.3 Karyawan pemasok hanya boleh mengakses Sistem Korporasi, dan hanya boleh menggunakan Perangkat yang diotorisasi Kyndryl untuk akses tersebut, untuk menyediakan Layanan. Karyawan pemasok tidak boleh menggunakan Perangkat yang diotorisasi Kyndryl untuk menyediakan layanan kepada setiap orang atau entitas lain, atau untuk mengakses setiap sistem, jaringan, aplikasi, situs web, alat email, alat kolaborasi TI, atau semacamnya milik Pemasok atau pihak ketiga untuk atau berkaitan dengan Layanan.

1.4 Demi kejelasan, karyawan Pemasok tidak boleh menggunakan Perangkat yang diotorisasi Kyndryl untuk mengakses Sistem Korporasi untuk alasan pribadi apa pun (misalnya, karyawan Pemasok tidak boleh menyimpan file pribadi seperti musik, video, gambar, atau item serupa lainnya pada Perangkat tersebut dan tidak boleh menggunakan Internet dari Perangkat tersebut untuk alasan pribadi).

1.5 Karyawan Pemasok tidak akan menyalin Materi Kyndryl yang dapat diakses melalui Sistem Korporasi tanpa persetujuan tertulis sebelumnya dari Kyndryl (dan tidak akan pernah menyalin setiap Materi Kyndryl ke perangkat penyimpanan portabel, seperti USB, hard drive eksternal, atau item serupa lainnya).

1.6 Atas permintaan, Pemasok akan mengonfirmasi, berdasarkan nama karyawan, Sistem Korporasi spesifik di mana karyawannya diberi otorisasi untuk mengakses, dan telah mengakses, selama periode waktu kapan pun yang diidentifikasi Kyndryl.

1.7 Pemasok akan memberi tahu Kyndryl dalam dua puluh empat (24) jam setelah setiap karyawan Pemasok dengan akses ke setiap Sistem Korporasi tidak lagi: (a) dipekerjakan oleh Pemasok atau (b) mengerjakan aktivitas yang memerlukan akses tersebut. Pemasok akan bekerja dengan Kyndryl untuk memastikan bahwa akses untuk mantan karyawan atau karyawan saat ini segera dicabut.

1.8 Pemasok akan segera melaporkan setiap insiden keamanan aktual atau dugaan (seperti kehilangan Perangkat Kyndryl atau Pemasok atau akses yang tidak sah ke Perangkat atau data, materi atau informasi lain dalam bentuk apa pun) kepada Kyndryl dan bekerja sama dengan Kyndryl dalam investigasi insiden tersebut.

1.9 Pemasok tidak boleh mengizinkan setiap agen, kontraktor independen, atau karyawan subkontraktor untuk mengakses setiap Sistem Korporasi, tanpa izin tertulis sebelumnya dari Kyndryl; jika Kyndryl memberikan persetujuan tersebut, maka Pemasok akan menjamin orang tersebut dan perusahaan mereka secara kontraktual untuk mematuhi persyaratan Artikel ini sebagaimana orang tersebut merupakan karyawan Pemasok, dan akan bertanggung jawab kepada Kyndryl untuk semua tindakan dan kelalaian dalam bertindak oleh orang atau karyawan mana pun tersebut sehubungan dengan akses Sistem Korporasi tersebut.

2. Perangkat Lunak pada Perangkat

2.1 Pemasok akan mengarahkan karyawannya untuk secara tepat waktu memasang semua perangkat lunak pada Perangkat yang disyaratkan oleh Kyndryl untuk memfasilitasi akses ke Sistem Korporasi dengan cara yang

aman. Baik Pemasok maupun karyawannya tidak akan mengganggu operasi perangkat lunak atau fitur keamanan yang diaktifkan perangkat lunak.

2.2 Pemasok dan karyawannya akan mengikuti aturan konfigurasi Perangkat yang ditetapkan Kyndryl dan sebaliknya bekerja dengan Kyndryl untuk membantu memastikan bahwa perangkat lunak berfungsi sebagaimana yang dikehendaki oleh Kyndryl. Misalnya, Pemasok tidak akan menimpa pemblokiran situs web perangkat lunak atau fitur patching otomatis.

2.3 Karyawan pemasok tidak boleh membagikan Perangkat yang mereka gunakan untuk mengakses Sistem Korporasi, atau nama pengguna, kata sandi, atau sejenisnya dari Perangkat mereka, dengan siapa pun.

2.4 Jika Kyndryl memberi wewenang kepada karyawan Pemasok untuk mengakses Sistem Korporasi menggunakan Perangkat Pemasok, maka Pemasok akan memasang dan menjalankan sistem operasi pada Perangkat tersebut yang disetujui oleh Kyndryl dan akan memuktahirkan ke versi terbaru dari sistem operasi tersebut atau sistem operasi baru dalam waktu yang wajar setelah Kyndryl memberikan instruksi.

3. Kekeliruan dan Kerja Sama

3.1 Kyndryl memiliki hak yang tidak memenuhi syarat untuk memantau dan meremediasi potensi intrusi dan ancaman keamanan siber lainnya dengan cara apa pun, dari lokasi mana pun, dan menggunakan sarana apa pun yang diyakini Kyndryl perlu atau sesuai, tanpa pemberitahuan sebelumnya kepada Pemasok atau setiap karyawan Pemasok atau pihak lainnya. Sebagai contoh dari hak tersebut, Kyndryl dapat, kapan pun, (a) menjalankan uji keamanan pada Perangkat apa pun, (b) memantau, memulihkan melalui sarana teknis atau lainnya dan meninjau komunikasi (termasuk email dari setiap akun email), catatan, file, dan item lain yang disimpan di Perangkat apa pun atau ditransmisikan melalui setiap Sistem Korporasi, dan (c) memperoleh gambar forensik penuh dari setiap Perangkat. Jika Kyndryl memerlukan kerja sama Pemasok untuk melaksanakan haknya, Pemasok akan memenuhi permintaan Kyndryl sepenuhnya dan tepat waktu untuk kerja sama tersebut (termasuk, misalnya, permintaan untuk mengonfigurasi Perangkat apa pun dengan aman, memasang perangkat lunak pemantauan atau lainnya pada Perangkat apa pun, membagikan detail koneksi tingkat sistem, terlibat dalam tindakan tanggapan insiden pada Perangkat apa pun, dan memberikan akses fisik ke Perangkat apa pun untuk Kyndryl guna memperoleh gambar forensik penuh atau sebaliknya, serta permintaan terkait dan serupa.

3.2 Kyndryl dapat mencabut akses ke Sistem Korporasi kapan pun, untuk setiap karyawan Pemasok atau semua karyawan Pemasok, tanpa pemberitahuan sebelumnya kepada Pemasok atau setiap karyawan Pemasok atau pihak lainnya, jika Kyndryl meyakini bahwa tindakan tersebut diperlukan untuk melindungi Kyndryl.

3.3 Hak Kyndryl tidak diblokir, dikurangi, atau dibatasi dengan cara apa pun oleh setiap ketentuan dari Dokumen Transaksi, perjanjian dasar terkait di antara para pihak, atau perjanjian apa pun lainnya di antara para pihak, termasuk setiap ketentuan yang mungkin memerlukan data, materi, atau informasi lainnya dalam bentuk apa pun untuk ditempatkan hanya di lokasi terpilih atau yang mungkin mensyaratkan bahwa hanya orang-orang dari lokasi terpilih yang dapat mengakses data, materi, atau informasi lain tersebut.

4. Perangkat Kyndryl

4.1 Kyndryl akan memegang hak milik atas semua Perangkat Kyndryl, sementara Pemasok menanggung risiko kehilangan Perangkat, termasuk akibat pencurian, vandalisme, atau kelalaian. Pemasok tidak akan membuat atau mengizinkan perubahan apa pun terhadap Perangkat Kyndryl tanpa persetujuan tertulis sebelumnya dari Kyndryl, dengan perubahan tersebut adalah perubahan apa pun pada Perangkat, termasuk setiap perubahan pada perangkat lunak, aplikasi, desain keamanan, konfigurasi keamanan, atau desain fisik, mekanis, atau elektrik dari Perangkat.

4.2 Pemasok akan mengembalikan semua Perangkat Kyndryl dalam 5 hari kerja setelah kebutuhan akan Perangkat tersebut untuk menyediakan Layanan berakhir, dan jika Kyndryl meminta, memusnahkan semua data, materi, dan informasi lainnya dalam bentuk apa pun pada Perangkat tersebut pada waktu yang sama, tanpa menyimpan salinan apa pun, dengan mengikuti Praktik Terbaik Industri untuk menghapus secara permanen

semua data, materi, informasi lainnya tersebut. Pemasok akan mengemas dan mengembalikan Perangkat Kyndryl dalam kondisi yang sama sebagaimana ketika dikirimkan kepada Pemasok, selain keausan yang wajar, dengan biaya sendiri ke lokasi yang ditunjuk Kyndryl. Kegagalan Pemasok untuk mematuhi setiap kewajiban dalam Pasal 4.2 ini merupakan pelanggaran material terhadap Dokumen Transaksi dan perjanjian dasar yang terkait dan setiap perjanjian terkait di antara para pihak, dengan pemahaman bahwa suatu perjanjian "terkait" jika akses ke setiap Sistem Korporasi memfasilitasi tugas Pemasok atau aktivitas lainnya berdasarkan perjanjian tersebut.

4.3 Kyndryl akan memberikan dukungan untuk Perangkat Kyndryl (termasuk pemeriksaan serta pemeliharaan preventif dan perbaikan Perangkat). Pemasok akan segera memberi tahu Kyndryl mengenai keperluan untuk layanan perbaikan.

4.4. Untuk program perangkat lunak yang Kyndryl miliki atau memiliki hak untuk melisensikannya, Kyndryl memberikan kepada Pemasok hak sementara untuk menggunakan, menyimpan, dan membuat salinan yang memadai untuk mendukung penggunaannya yang sah atas Perangkat Kyndryl. Pemasok tidak dapat mentransfer program kepada siapa pun, membuat salinan informasi lisensi perangkat lunak, atau membongkar, mendekompilasi, merekayasa balik, atau menerjemahkan setiap program kecuali jika diizinkan secara tegas oleh hukum yang berlaku tanpa kemungkinan pengabaian kontraktual.

5. Pembaruan

5.1 Terlepas dari ketentuan apa pun yang bertentangan dalam Dokumen Transaksi atau perjanjian dasar terkait di antara para pihak, setelah pemberitahuan tertulis kepada Pemasok dan tanpa perlu memperoleh persetujuan Pemasok, Kyndryl dapat memperbarui, menambah, atau mengubah Artikel ini untuk mengurus setiap persyaratan berdasarkan hukum yang berlaku atau kewajiban Pelanggan, untuk merefleksikan setiap pengembangan dalam praktik terbaik keamanan, atau sebagaimana yang Kyndryl yakini perlu untuk melindungi Sistem Korporasi atau Kyndryl.

Artikel VII, Penambahan Staf

Artikel ini berlaku bilamana karyawan Pemasok akan mencurahkan semua waktu kerja mereka untuk menyediakan Layanan bagi Kyndryl, akan menjalankan semua Layanan tersebut di lokasi Kyndryl, lokasi Pelanggan, atau dari rumah mereka, dan hanya akan menyediakan Layanan menggunakan Perangkat Kyndryl untuk mengakses Sistem Korporasi.

1. Akses ke Sistem Korporasi; Lingkungan Kyndryl

1.1 Pemasok hanya boleh menjalankan Layanan dengan mengakses Sistem Korporasi menggunakan Perangkat yang diberikan Kyndryl.

1.2 Pemasok akan mematuhi syarat-syarat yang tercantum dalam Artikel VI (Akses Sistem Korporasi), untuk semua akses ke Sistem Korporasi.

1.3 Perangkat yang diberikan Kyndryl adalah satu-satunya Perangkat yang boleh digunakan oleh Pemasok dan karyawannya untuk menyediakan Layanan dan hanya boleh digunakan oleh Pemasok dan karyawannya untuk menyediakan Layanan. Demi kejelasan, dalam hal apa pun Pemasok atau karyawannya tidak boleh menggunakan setiap perangkat lainnya untuk menyediakan Layanan atau menggunakan Perangkat Kyndryl untuk setiap pelanggan Pemasok lainnya atau untuk setiap tujuan selain menyediakan Layanan kepada Kyndryl.

1.4 Karyawan pemasok yang menggunakan Perangkat Kyndryl dapat membagikan Materi Kyndryl kepada satu sama lain dan menyimpan materi tersebut pada Perangkat Kyndryl, tetapi hanya sebatas aktivitas berbagi dan penyimpanan tersebut diperlukan untuk berhasil menjalankan Layanan.

1.5 Kecuali sehubungan dengan penyimpanan tersebut dalam Perangkat Kyndryl, dalam hal apa pun Pemasok atau karyawannya tidak boleh menghapus setiap Materi Kyndryl dari repositori, lingkungan, alat, atau infrastruktur Kyndryl tempat Materi disimpan oleh Kyndryl.

1.6 Demi kejelasan, Pemasok dan karyawannya tidak diberi wewenang untuk mentransfer setiap Materi Kyndryl ke setiap repositori, lingkungan, alat, atau infrastruktur Pemasok, atau setiap sistem, platform, jaringan, atau sejenisnya yang lain dari Pemasok, tanpa persetujuan tertulis sebelumnya dari Kyndryl.

1.7 Artikel VIII (Tindakan Teknis dan Organisasi, Keamanan Umum) tidak berlaku untuk Layanan Pemasok apabila karyawan Pemasok akan mencurahkan semua waktu kerja mereka untuk menyediakan Layanan bagi Kyndryl, akan menjalankan semua Layanan tersebut di lokasi Kyndryl, lokasi Pelanggan, atau dari rumah mereka, dan hanya akan menyediakan Layanan menggunakan Perangkat Kyndryl untuk mengakses Sistem Korporasi. Atau, Artikel VIII berlaku untuk Layanan Pemasok.

Artikel VIII, Tindakan Teknis dan Organisasi, Keamanan Umum

Artikel ini berlaku jika Pemasok menyediakan setiap Layanan atau Hasil Kerja kepada Kyndryl, kecuali jika Pemasok hanya akan memiliki akses ke BCI Kyndryl dalam menyediakan Layanan dan Hasil Kerja tersebut (yaitu, Pemasok tidak akan Memproses Data Kyndryl apa pun lainnya atau memiliki akses ke Materi Kyndryl apa pun lainnya atau ke Sistem Korporasi mana pun), satu-satunya Layanan dan Hasil Kerja Pemasok adalah untuk menyediakan Perangkat Lunak di Lokasi kepada Kyndryl, atau Pemasok menyediakan semua Layanan dan Hasil Kerjanya dalam model penambahan staf sesuai dengan Artikel VII, termasuk Pasal 1.7 tersebut.

Pemasok akan mematuhi persyaratan Artikel ini dan dengan demikian melindungi: (a) Materi Kyndryl terhadap kehilangan, kerusakan, perubahan, pengungkapan secara tidak sengaja atau tidak sah, dan akses secara tidak sengaja atau tidak sah, (b) Data Kyndryl dari bentuk Pemrosesan yang melanggar hukum, dan (c) Teknologi Kyndryl dari bentuk Penanganan yang melanggar hukum. Persyaratan Artikel ini diperluaskan ke semua aplikasi, platform, dan infrastruktur TI yang dioperasikan atau dikelola oleh Pemasok dalam memberikan Hasil Kerja dan Layanan, dan dalam Penanganan Teknologi Kyndryl, termasuk semua pengembangan, pengujian, hosting, dukungan, operasi, dan lingkungan pusat data.

1. Kebijakan Keamanan

1.1 Pemasok akan mempertahankan dan mengikuti kebijakan dan praktik keamanan TI yang merupakan bagian terpadu dari bisnis Pemasok, wajib bagi semua Personel Pemasok, dan sesuai dengan Praktik Terbaik Industri.

1.2 Pemasok akan meninjau kebijakan dan praktik keamanan TI-nya setidaknya setiap tahun dan mengubahnya jika dianggap perlu oleh Pemasok untuk melindungi Materi Kyndryl.

1.3 Pemasok akan mempertahankan dan mengikuti persyaratan verifikasi hubungan kerja standar dan wajib untuk semua perekrutan karyawan baru, dan memperluas persyaratan tersebut untuk semua Personel dan anak perusahaan Pemasok yang dimiliki seluruhnya. Persyaratan tersebut akan mencakup pemeriksaan latar belakang kriminal sejauh yang diizinkan oleh peraturan perundang-undangan setempat, validasi bukti identitas, dan pemeriksaan tambahan apa pun yang dianggap perlu oleh Pemasok. Pemasok akan secara berkala mengulang dan memvalidasi ulang persyaratan tersebut, sebagaimana dianggap perlu.

1.4 Pemasok akan memberikan pendidikan keamanan dan privasi setiap tahun kepada karyawannya dan mewajibkan semua karyawan tersebut untuk menyertifikasi setiap tahunnya bahwa mereka akan mematuhi kode etik bisnis, kerahasiaan, dan kebijakan keamanan Pemasok, sebagaimana yang diatur dalam kode etik Pemasok atau dokumen serupa. Pemasok akan memberikan pelatihan kebijakan dan proses tambahan kepada orang-orang dengan akses administratif ke setiap komponen Layanan, Hasil Kerja, atau Materi Kyndryl, dengan pelatihan tersebut khusus untuk peran dan dukungan mereka pada Layanan, Hasil Kerja, dan Materi Kyndryl, dan sebagaimana yang diperlukan untuk mempertahankan kepatuhan dan sertifikasi yang diwajibkan.

1.5 Pemasok akan merancang tindakan keamanan dan privasi untuk melindungi dan mengelola ketersediaan Materi Kyndryl, termasuk melalui implementasi, pemeliharaan, dan kepatuhannya terhadap kebijakan dan prosedur yang memerlukan keamanan dan privasi berdasarkan rancangan, rekayasa aman, dan operasi yang aman, untuk semua Layanan dan Hasil Kerja serta untuk semua Penanganan Teknologi Kyndryl.

2. Insiden Keamanan

2.1 Pemasok akan mempertahankan dan mengikuti kebijakan tanggapan insiden yang terdokumentasi sesuai dengan Praktik Terbaik Industri untuk penanganan insiden keamanan komputer.

2.2 Pemasok akan menginvestigasi akses yang tidak sah atau penggunaan yang tidak sah atas Materi Kyndryl dan akan menentukan dan melaksanakan rencana tanggapan yang sesuai.

2.3 Pemasok akan segera (dan tidak lebih dari 48 jam) memberi tahu Kyndryl setelah mengetahui adanya Pelanggaran Keamanan. Pemasok akan memberikan pemberitahuan tersebut ke cyber.incidents@kyndryl.com. Pemasok akan memberikan kepada Kyndryl informasi yang diminta secara wajar terkait pelanggaran tersebut dan status aktivitas remediasi serta restorasi Pemasok apa pun. Sebagai contoh, informasi yang diminta secara wajar dapat mencakup log yang mempertunjukkan akses istimewa, administratif, dan akses lain ke Perangkat, sistem atau aplikasi, gambar forensik Perangkat, sistem atau

aplikasi, dan item serupa lainnya, sejauh relevan dengan pelanggaran atau aktivitas remediasi dan restorasi Pemasok.

2.4 Pemasok akan memberikan bantuan yang wajar kepada Kyndryl untuk memenuhi setiap kewajiban hukum (termasuk kewajiban untuk memberi tahu pembuat peraturan atau Subjek Data) Kyndryl, afiliasi Kyndryl, dan Pelanggan (serta pelanggan dan afiliasinya) berkaitan dengan Pelanggaran Keamanan.

2.5 Pemasok tidak akan menginformasikan atau memberi tahu pihak ketiga mana pun bahwa Pelanggaran Keamanan secara langsung atau tidak langsung berkaitan dengan Kyndryl atau Materi Kyndryl kecuali jika Kyndryl menyetujuinya secara tertulis atau jika diwajibkan oleh hukum. Pemasok akan memberi tahu Kyndryl secara tertulis sebelum mendistribusikan setiap pemberitahuan yang diwajibkan secara hukum kepada pihak ketiga mana pun, jika pemberitahuan akan secara langsung atau tidak langsung mengungkapkan identitas Kyndryl.

2.6 Dalam hal Pelanggaran Keamanan yang timbul dari pelanggaran Pemasok terhadap kewajiban apa pun berdasarkan Syarat-Syarat ini:

(a) Pemasok akan bertanggung jawab atas setiap biaya yang dikeluarkannya, serta biaya aktual yang dikeluarkan oleh Kyndryl, dalam memberikan pemberitahuan Pelanggaran Keamanan kepada pembuat peraturan yang berlaku, pemerintah dan lembaga pengatur mandiri industri terkait lainnya, media (jika diwajibkan oleh hukum yang berlaku), Subjek Data, Pelanggan, dan pihak lainnya,

(b) jika Kyndryl meminta, Pemasok akan membuat dan mengelola pusat panggilan dengan biaya yang ditanggung oleh Pemasok sendiri untuk menanggapi pertanyaan dari Subjek Data tentang Pelanggaran Keamanan dan konsekuensinya, selama 1 tahun setelah tanggal Subjek Data tersebut diberi tahu tentang Pelanggaran Keamanan, atau sebagaimana yang diwajibkan oleh undang-undang perlindungan data yang berlaku, mana pun yang memberikan perlindungan lebih besar. Kyndryl dan Pemasok akan bekerja sama untuk membuat skrip dan materi lain yang digunakan oleh staf pusat panggilan saat menanggapi pertanyaan. Atau, dengan pemberitahuan tertulis kepada Pemasok, Kyndryl dapat membuat dan mengelola pusat panggilannya sendiri, sebagai pengganti meminta Pemasok membuat pusat panggilan, dan Pemasok akan mengganti biaya aktual Kyndryl yang ditanggung oleh Kyndryl dalam membuat dan mengelola pusat panggilan tersebut, dan

(c) Pemasok akan mengganti biaya aktual Kyndryl yang ditanggung oleh Kyndryl dalam menyediakan layanan pemantauan kredit dan restorasi kredit selama 1 tahun setelah tanggal individu yang terdampak oleh pelanggaran yang memilih mendaftar untuk layanan tersebut diberi tahu mengenai Pelanggaran Keamanan, atau sebagaimana yang diwajibkan oleh setiap undang-undang perlindungan data yang berlaku, mana pun yang memberikan perlindungan lebih besar.

3. Kontrol Entri dan Keamanan Fisik (sebagaimana yang digunakan di bawah, "Fasilitas" berarti lokasi fisik tempat Pemasok menyelenggarakan, memproses, atau mengakses Materi Kyndryl).

3.1 Pemasok akan mempertahankan kontrol entri fisik yang sesuai, seperti penghalang, titik entri yang dikendalikan kartu, kamera pengawas, dan orang di bagian penerimaan untuk melindungi dari entri yang tidak sah ke dalam Fasilitas.

3.2 Pemasok akan mensyaratkan persetujuan yang sah untuk akses ke Fasilitas dan area yang dikontrol dalam Fasilitas, termasuk setiap akses sementara, dan akan membatasi akses menurut peran pekerjaan dan keperluan bisnis. Jika Pemasok memberikan akses sementara, karyawannya yang sah akan mengantar setiap pengunjung saat berada di Fasilitas dan setiap area yang dikontrol.

3.3 Pemasok akan mengimplementasikan kontrol akses fisik, termasuk kontrol akses multifaktor yang sesuai dengan Praktik Terbaik Industri, untuk membatasi secara tepat pintu masuk ke area yang dikontrol dalam Fasilitas, akan mencatat semua upaya masuk, dan menyimpan log tersebut selama setidaknya satu tahun.

3.4 Pemasok akan mencabut akses ke Fasilitas dan area yang dikontrol dalam Fasilitas setelah a) pengakhiran hubungan kerja karyawan Pemasok yang sah atau b) karyawan Pemasok yang sah tidak lagi memiliki kebutuhan bisnis yang valid untuk akses. Pemasok akan mengikuti prosedur pengakhiran hubungan

kerja formal yang terdokumentasi yang mencakup penghapusan segera dari daftar kontrol akses dan penyerahan tanda pengenal akses fisik.

3.5 Pemasok akan melakukan tindakan pencegahan untuk melindungi semua infrastruktur fisik yang digunakan untuk mendukung Layanan dan Hasil Kerja dan Penanganan Teknologi Kyndryl terhadap ancaman lingkungan, baik yang ditimbulkan oleh alam atau manusia, seperti temperatur sekitar yang berlebih, kebakaran, banjir, kelembapan, pencurian, dan vandalisme.

4. Akses, Intervensi, Transfer, dan Kontrol Pemisahan

4.1 Pemasok akan memelihara arsitektur keamanan jaringan yang terdokumentasi yang dikelolanya dalam pengoperasiannya atas Layanan, penyediaannya atas Hasil Kerja, dan Penanganannya atas Teknologi Kyndryl. Pemasok akan meninjau arsitektur jaringan tersebut secara terpisah, dan menggunakan tindakan-tindakan untuk mencegah koneksi jaringan yang tidak sah ke sistem, aplikasi, dan perangkat jaringan, demi kepatuhan terhadap segmentasi yang aman, isolasi, dan standar pertahanan yang mendalam. Pemasok tidak boleh menggunakan teknologi nirkabel dalam hosting dan operasinya dari setiap Layanan yang Di-Host; atau, Pemasok dapat menggunakan teknologi jaringan nirkabel dalam penyampaian Layanan dan Hasil Kerja dan Penanganan Teknologi Kyndryl, tetapi Pemasok akan mengenkripsi dan mewajibkan autentikasi aman untuk setiap jaringan nirkabel tersebut.

4.2 Pemasok akan mempertahankan tindakan-tindakan yang dirancang untuk secara logis memisahkan dan mencegah Materi Kyndryl diekspos ke atau diakses oleh orang yang tidak sah. Selanjutnya, Pemasok akan mempertahankan isolasi yang tepat dari produksi, non-produksi, dan lingkungan lain miliknya, dan, jika Materi Kyndryl telah ada dalam atau ditransfer ke lingkungan non-produksi (misalnya, untuk mereproduksi kesalahan), maka Pemasok akan memastikan bahwa perlindungan keamanan dan privasi dalam lingkungan non-produksi setara dengan perlindungan dalam lingkungan produksi.

4.3 Pemasok akan mengenkripsi Materi Kyndryl dalam transit dan saat diam (kecuali jika Pemasok mempertunjukkan sesuai dengan kehendak Kyndryl yang wajar bahwa mengenkripsi Materi Kyndryl saat diam secara teknis tidak memungkinkan). Pemasok juga akan mengenkripsi semua media fisik, jika ada, seperti media yang berisi file cadangan. Pemasok akan mempertahankan prosedur yang terdokumentasi untuk pembuatan, penerbitan, distribusi, penyimpanan, rotasi, pencabutan, pemulihan, pencadangan, pemusnahan, akses, dan penggunaan kunci yang aman terkait dengan enkripsi data. Pemasok akan memastikan bahwa metode kriptografis spesifik yang digunakan untuk enkripsi tersebut diselaraskan dengan Praktik Terbaik Industri (seperti NIST SP 800-131a).

4.4 Jika Pemasok memerlukan akses ke Materi Kyndryl, Pemasok akan memperketat dan membatasi akses tersebut ke tingkat terendah yang diperlukan untuk menyediakan dan mendukung Layanan dan Hasil Kerja. Pemasok akan mewajibkan bahwa akses tersebut, termasuk akses administratif ke setiap komponen dasar (yaitu, akses istimewa), akan bersifat individual, berbasis peran, dan tunduk pada persetujuan dan validasi rutin oleh karyawan Pemasok yang sah mengikuti prinsip pemisahan tugas. Pemasok akan mempertahankan tindakan untuk mengidentifikasi dan menghapus akun redundan dan dorman. Pemasok juga akan mencabut akun dengan akses istimewa dalam dua puluh empat (24) jam setelah pengakhiran hubungan kerja pemilik akun atau permintaan oleh Kyndryl atau setiap karyawan Pemasok yang sah, seperti manajer pemilik akun.

4.5 Sesuai dengan Praktik Terbaik Industri, Pemasok akan mempertahankan tindakan teknis yang menerapkan batas waktu sesi tidak aktif, penguncian akun setelah beberapa upaya login gagal secara berurutan, autentikasi kata sandi atau frasa sandi yang kuat, dan tindakan yang memerlukan transfer dan penyimpanan kata sandi dan frasa sandi tersebut dengan aman. Selain itu, Pemasok akan menggunakan autentikasi multifaktor untuk semua akses istimewa berbasis non-konsol ke Materi Kyndryl apa pun.

4.6 Pemasok akan memantau penggunaan akses istimewa dan mempertahankan tindakan informasi keamanan dan manajemen peristiwa yang dirancang untuk: (a) mengidentifikasi akses dan aktivitas yang tidak sah, (b) memfasilitasi tanggapan yang tepat waktu dan sesuai terhadap akses dan aktivitas tersebut, dan (c) memungkinkan audit oleh Pemasok, Kyndryl (menurut hak verifikasinya dalam Syarat-Syarat ini dan hak audit dalam Dokumen Transaksi atau perjanjian dasar terkait atau perjanjian lainnya yang terkait di antara para pihak) dan kepatuhan lainnya terhadap kebijakan Pemasok yang terdokumentasi.

4.7 Pemasok akan menyimpan log yang mencatat, dengan mematuhi Praktik Terbaik Industri, semua akses atau aktivitas administratif, pengguna, atau lainnya ke atau sehubungan dengan sistem yang digunakan dalam menyediakan Layanan atau Hasil Kerja dan dalam Penanganan Teknologi Kyndryl (dan akan memberikan log tersebut kepada Kyndryl atas permintaan). Pemasok akan mempertahankan tindakan yang dirancang untuk melindungi terhadap akses yang tidak sah, modifikasi, dan pemusnahan atas log tersebut secara sengaja atau tidak disengaja.

4.8 Pemasok akan mempertahankan perlindungan komputasi untuk sistem yang dimiliki atau dikelolanya, termasuk sistem pengguna akhir, dan yang digunakannya dalam menyediakan Layanan atau Hasil Kerja atau dalam Penanganan Teknologi Kyndryl, dengan perlindungan tersebut termasuk: firewall titik akhir, enkripsi disk penuh, teknologi deteksi dan tanggapan titik akhir berbasis tanda tangan dan non-tanda tangan untuk mengatasi ancaman malware dan ancaman persisten tingkat lanjut, kunci layar berbasis waktu, dan solusi manajemen titik akhir yang menerapkan persyaratan konfigurasi dan patching keamanan. Selain itu, Pemasok akan mengimplementasikan kontrol teknis dan operasional yang memastikan hanya sistem pengguna akhir yang diketahui dan tepercaya yang diizinkan untuk menggunakan jaringan Pemasok.

4.9 Sesuai dengan Praktik Terbaik Industri, Pemasok akan mempertahankan perlindungan untuk lingkungan pusat data tempat Materi Kyndryl berada atau diproses, dengan perlindungan tersebut yang mencakup deteksi dan pencegahan intrusi dan penolakan penanggulangan serangan layanan dan mitigasi.

5. Integritas Layanan dan Sistem dan Kontrol Ketersediaan

5.1 Pemasok akan: (a) menjalankan penilaian risiko keamanan dan privasi setidaknya setiap tahun, (b) menjalankan pengujian keamanan dan menilai kerentanan, termasuk pemindaian sistem otomatis dan keamanan aplikasi serta peretasan etis manual, sebelum rilis produksi dan setiap tahun setelahnya sebagaimana menyangkut Layanan dan Hasil Kerja dan setiap tahun sehubungan dengan Penanganan Teknologi Kyndryl, (c) menyertakan pihak ketiga independen yang memenuhi syarat untuk menjalankan pengujian penetrasi sesuai dengan Praktik Terbaik Industri setidaknya setiap tahun, dengan pengujian tersebut meliputi pengujian otomatis dan manual, (d) menjalankan manajemen otomatis dan verifikasi kepatuhan rutin dengan persyaratan konfigurasi keamanan untuk masing-masing komponen Layanan dan Hasil Kerja dan berkenaan dengan Penanganan Teknologi Kyndryl, dan (e) meremediasi kerentanan yang diidentifikasi atau ketidakpatuhan terhadap persyaratan konfigurasi keamanannya berdasarkan risiko, eksploitabilitas, dan dampak yang berkaitan. Pemasok akan mengambil langkah yang wajar guna menghindari gangguan Layanan saat menjalankan pengujian, penilaian, pemindaian, dan pelaksanaannya atas aktivitas remediasi. Atas permintaan Kyndryl, Pemasok akan memberikan kepada Kyndryl ringkasan tertulis dari aktivitas pengujian penetrasi terbaru Pemasok pada saat itu, yang akan menyertakan setidaknya nama tawaran yang dicakup oleh pengujian, jumlah sistem atau aplikasi dalam cakupan untuk pengujian, tanggal pengujian, metodologi yang digunakan dalam pengujian, dan ringkasan temuan tingkat tinggi.

5.2 Pemasok akan mempertahankan kebijakan dan prosedur yang dirancang untuk mengelola risiko yang terkait dengan penerapan perubahan terhadap Layanan atau Hasil Kerja atau Penanganan Teknologi Kyndryl. Sebelum mengimplementasikan perubahan tersebut, termasuk sistem, jaringan, dan komponen dasar yang terdampak, Pemasok akan mendokumentasikan dalam permintaan perubahan terdaftar: (a) deskripsi dan alasan perubahan, (b) detail dan jadwal implementasi, (c) pernyataan risiko mengenai dampak terhadap Layanan dan Hasil Kerja, pelanggan Layanan, atau Materi Kyndryl, (d) hasil yang diharapkan, (e) rencana pembatalan, dan (f) persetujuan oleh karyawan Pemasok yang sah.

5.3 Pemasok akan memelihara inventaris dari semua aset TI yang digunakannya dalam pengoperasian Layanan, yang menyediakan Hasil Kerja dan Penanganan Teknologi Kyndryl. Pemasok akan terus memantau dan mengelola kesehatan (termasuk kapasitas) dan ketersediaan aset IT tersebut, Layanan, Hasil Kerja, dan Teknologi Kyndryl, termasuk komponen dasar dari aset, Layanan, Hasil Kerja, dan Teknologi Kyndryl tersebut.

5.4 Pemasok akan membangun semua sistem yang digunakannya dalam pengembangan atau operasi Layanan dan Hasil Kerja dan Penanganan Teknologi Kyndryl dari gambar keamanan sistem atau garis dasar keamanan yang telah ditentukan sebelumnya, yang memenuhi Praktik Terbaik Industri, seperti tolok ukur Center for Internet Security (CIS).

5.5 Tanpa membatasi kewajiban Pemasok atau hak-hak Kyndryl berdasarkan Dokumen Transaksi atau perjanjian dasar yang terkait di antara para pihak sehubungan dengan kesinambungan bisnis, Pemasok akan menilai secara terpisah setiap Layanan dan Hasil Kerja dan masing-masing sistem TI yang digunakan dalam Penanganan Teknologi Kyndryl untuk bisnis dan kesinambungan TI serta persyaratan pemulihan bencana sesuai dengan pedoman manajemen risiko yang terdokumentasi. Pemasok akan memastikan bahwa setiap Layanan, Hasil Kerja, dan sistem TI telah, sejauh dijamin oleh penilaian risiko tersebut, secara terpisah menentukan, mendokumentasikan, memelihara, dan setiap tahun memvalidasi rencana pemulihan bencana dan kesinambungan TI dan bisnis sesuai dengan Praktik Terbaik Industri. Pemasok akan memastikan bahwa rencana tersebut dirancang untuk menyampaikan waktu pemulihan spesifik yang tercantum dalam Pasal 5.6 di bawah.

5.6 Sasaran titik pemulihan (recovery point objective - "**RPO**") dan sasaran waktu pemulihan (recovery time objective - "**RTO**") spesifik sehubungan dengan setiap Layanan yang Di-Host adalah: 24 jam RPO dan 24 jam RTO; meski demikian, Pemasok akan mematuhi setiap durasi RPO atau RTO yang lebih pendek yang telah menjadi komitmen Kyndryl kepada Pelanggan, segera setelah Kyndryl memberi tahu Pemasok secara tertulis mengenai durasi RPO atau RTO yang lebih pendek (email juga dianggap sebagai pernyataan tertulis). Karena menyangkut semua Layanan lain yang diberikan oleh Pemasok kepada Kyndryl, Pemasok akan memastikan bahwa rencana pemulihan bencana dan kesinambungan bisnisnya dirancang untuk menyampaikan RPO dan RTO yang memungkinkan Pemasok untuk tetap mematuhi semua kewajibannya kepada Kyndryl berdasarkan Dokumen Transaksi dan perjanjian dasar terkait di antara para pihak, dan Syarat-Syarat ini, termasuk kewajibannya untuk memberikan pengujian, dukungan, dan pemeliharaan secara tepat waktu.

5.7 Pemasok akan mempertahankan tindakan yang dirancang untuk menilai, menguji, dan menerapkan patch saran keamanan pada Layanan dan Hasil Kerja serta sistem, jaringan, aplikasi, dan komponen dasar terkait dalam cakupan Layanan dan Hasil Kerja tersebut, serta sistem, jaringan, aplikasi, dan komponen dasar yang digunakan untuk Penanganan Teknologi Kyndryl. Setelah menentukan bahwa patch saran keamanan berlaku dan sesuai, Pemasok akan mengimplementasikan patch sesuai dengan pedoman penilaian risiko dan keparahan yang terdokumentasi. Implementasi patch saran keamanan oleh Pemasok akan tunduk pada kebijakan manajemen perubahannya.

5.8 Jika Kyndryl memiliki landasan yang wajar untuk meyakini bahwa perangkat keras atau perangkat lunak yang disediakan oleh Pemasok kepada Kyndryl mungkin berisi elemen intrusif, seperti spyware, malware, atau kode berbahaya, maka Pemasok akan bekerja sama dengan Kyndryl secara tepat waktu dalam menginvestigasi dan meremediasi persoalan Kyndryl.

6. Penyediaan Layanan

6.1 Pemasok akan mendukung metode autentikasi terfederasi yang umum dalam industri untuk setiap akun Pelanggan atau pengguna Kyndryl, dengan Pemasok yang mengikuti Praktik Terbaik Industri dalam mengautentikasi akun Pelanggan atau pengguna Kyndryl tersebut (seperti Single Sign-On multifaktor yang dikelola Kyndryl secara terpusat, menggunakan OpenID Connect atau Security Assertion Markup Language).

7. Subkontraktor. Tanpa membatasi kewajiban Pemasok atau hak-hak Kyndryl berdasarkan Dokumen Transaksi atau perjanjian dasar yang terkait di antara para pihak sehubungan dengan retensi subkontraktor, Pemasok akan memastikan bahwa setiap subkontraktor yang menjalankan pekerjaan untuk Pemasok telah memulai kontrol tata kelola untuk mematuhi persyaratan dan kewajiban yang dikenakan oleh Syarat-Syarat ini kepada Pemasok.

8. Media Fisik. Pemasok akan membersihkan media fisik yang ditujukan untuk penggunaan ulang dengan aman sebelum penggunaan ulang tersebut dan akan memusnahkan media fisik yang tidak ditujukan untuk penggunaan ulang, sesuai dengan Praktik Terbaik Industri untuk pembersihan media.

Artikel IX, Sertifikasi dan Laporan Layanan yang Di-Host

Artikel ini berlaku jika Pemasok menyediakan Layanan yang Di-Host kepada Kyndryl.

1.1 Pemasok akan mendapatkan sertifikasi atau laporan berikut dalam kerangka waktu yang dicantumkan di bawah:

Sertifikasi / Laporan	**Kerangka Waktu**
Berkenaan dengan Layanan yang Di-Host Pemasok: Sertifikasi kepatuhan terhadap ISO 27001, Teknologi informasi, Teknik keamanan, Sistem manajemen keamanan informasi, dengan sertifikasi tersebut yang didasarkan pada penilaian auditor independen yang bereputasi **Atau** SOC 2 Tipe 2: Laporan oleh auditor independen bereputasi yang mempertunjukkan tinjauannya tentang sistem, kontrol, dan operasi Pemasok sesuai dengan SOC 2 Tipe 2 (termasuk setidaknya keamanan, kerahasiaan, dan ketersediaan)	Pemasok akan memperoleh sertifikasi ISO 27001 paling lambat 120 hari setelah tanggal mulai berlaku Dokumen Transaksi ini* atau Tanggal Asumsi** kemudian memperpanjang sertifikasi berdasarkan penilaian auditor independen yang bereputasi setiap 12 bulan setelahnya (dengan masing-masing pembaruan terhadap versi standar terbaru saat itu) Pemasok akan memperoleh laporan SOC 2 Tipe 2 paling lambat 240 Hari setelah tanggal mulai berlaku Dokumen Transaksi* atau Tanggal Asumsi**, kemudian memperoleh laporan baru oleh auditor independen bereputasi yang mempertunjukkan tinjauannya atas sistem, kontrol, dan operasi Pemasok sesuai dengan SOC 2 Tipe 2 (termasuk setidaknya keamanan, kerahasiaan, dan ketersediaan) setiap 12 bulan setelahnya * Apabila, pada tanggal mulai berlaku, Pemasok menyediakan Layanan yang Di-Host ** Tanggal Pemasok mengemban kewajiban untuk menyediakan Layanan yang Di-Host

1.2 Jika Pemasok meminta secara tertulis, dan Kyndryl menyetujui secara tertulis, Pemasok dapat memperoleh sertifikasi atau laporan yang setara secara substansial dengan yang dirujuk di atas, dengan pemahaman bahwa kerangka waktu yang tercantum dalam tabel di atas akan berlaku tanpa perubahan berkenaan dengan sertifikasi atau laporan yang setara secara substansial.

1.3 Pemasok akan: (a) atas permintaan, segera memberikan kepada Kyndryl salinan masing-masing sertifikasi dan laporan yang wajib didapatkan oleh Pemasok dan (b) segera menyelesaikan setiap kelemahan kontrol internal yang tercatat selama tinjauan SOC 2 atau tinjauan yang setara secara substansial (jika Kyndryl menyetujui).

Artikel X, Kerja Sama, Verifikasi, dan Remediasi

Artikel ini berlaku jika Pemasok menyediakan setiap Layanan atau Hasil Kerja kepada Kyndryl.

1. Kerja Sama Pemasok

1.1 Jika Kyndryl memiliki alasan untuk mempertanyakan apakah setiap Layanan atau Hasil Kerja mungkin telah berkontribusi, sedang berkontribusi, atau akan berkontribusi pada setiap persoalan keamanan siber, maka Pemasok akan bekerja sama secara wajar dengan setiap pertanyaan Kyndryl terkait dengan persoalan tersebut, termasuk dengan menanggapi permintaan akan informasi dengan sepenuhnya dan tepat waktu, baik melalui dokumen, catatan lain, wawancara Personel Pemasok yang relevan, atau sejenisnya.

1.2 Para pihak setuju untuk: (a) menyediakan informasi lebih lanjut kepada satu sama lain atas permintaan, (b) menandatangani dan menyampaikan dokumen lain tersebut kepada satu sama lain, dan (c) melakukan hal dan tindakan lain tersebut, semua sebagaimana pihak lain dapat meminta secara wajar untuk tujuan melaksanakan maksud Syarat-Syarat ini dan dokumen yang dirujuk dalam Syarat-Syarat ini. Misalnya, jika Kyndryl meminta, Pemasok akan memberikan syarat-syarat yang berfokus pada privasi dan keamanan secara tepat waktu dalam kontrak tertulisnya dengan Subprosesor dan subkontraktor, termasuk, jika Pemasok memiliki hak untuk melakukannya, dengan memberikan akses ke kontrak itu sendiri.

1.3 Jika Kyndryl meminta, Pemasok akan memberikan informasi secara tepat waktu mengenai negara-negara tempat Hasil Kerja dan komponen Hasil Kerja tersebut diproduksi, dikembangkan, atau bersumber.

2. Verifikasi (sebagaimana yang digunakan di bawah, "Fasilitas" berarti lokasi fisik tempat Pemasok menyelenggarakan, memproses, atau mengakses Materi Kyndryl)

2.1 Pemasok akan mengelola catatan yang dapat diaudit yang mempertunjukkan kepatuhan terhadap Syarat-Syarat ini.

2.2 Kyndryl, sendiri maupun dengan auditor eksternal, dapat, pada 30 Hari sebelum pemberitahuan tertulis kepada Pemasok, memverifikasi kepatuhan Pemasok terhadap Syarat-Syarat ini, termasuk dengan mengakses setiap Fasilitas untuk tujuan tersebut, meski Kyndryl tidak akan mengakses setiap pusat data tempat Pemasok Memproses Data Kyndryl kecuali jika memiliki alasan iktikad baik untuk meyakini bahwa dengan melakukan hal tersebut akan memberikan informasi yang relevan. Pemasok akan bekerja sama dengan verifikasi Kyndryl, termasuk menanggapi permintaan informasi dengan sepenuhnya dan tepat waktu, baik melalui dokumen, catatan lain, wawancara Personel Pemasok terkait, atau sejenisnya.Pemasok dapat menawarkan bukti kepatuhan terhadap kode etik yang disetujui atau sertifikasi industri atau memberikan informasi untuk mempertunjukkan kepatuhan terhadap Syarat-Syarat ini, untuk pertimbangan Kyndryl.

2.3 Verifikasi tidak akan berjalan lebih dari sekali dalam setiap periode 12 bulan, kecuali jika: (a) Kyndryl memvalidasi remediasi masalah Pemasok sebagai hasil dari verifikasi sebelumnya selama periode 12 bulan atau (b) Pelanggaran Keamanan telah timbul dan Kyndryl ingin memverifikasi kepatuhan terhadap kewajiban yang berkaitan dengan pelanggaran. Dalam kasus-kasus tersebut, Kyndryl akan memberikan pemberitahuan tertulis yang sama 30 Hari sebelumnya sebagaimana yang ditetapkan dalam Pasal 2.2 di atas, tetapi urgensi dalam menangani Pelanggaran Keamanan mungkin mengharuskan Kyndryl untuk melakukan verifikasi dengan pemberitahuan tertulis kurang dari 30 Hari sebelumnya.

2.4. Pembuat peraturan atau Pengontrol lain dapat melaksanakan hak yang sama dengan Kyndryl dalam Pasal 2.2 dan 2.3, dengan pemahaman bahwa pembuat peraturan dapat melaksanakan setiap hak tambahan yang dimilikinya berdasarkan hukum.

2.5 Jika Kyndryl memiliki landasan yang wajar untuk menyimpulkan bahwa Pemasok tidak patuh terhadap setiap Syarat-Syarat ini (baik landasan tersebut timbul dari verifikasi berdasarkan Syarat-Syarat ini atau hal lain), maka Pemasok akan segera meremediasi ketidakpatuhan tersebut.

3. Program Anti-Pemalsuan

3.1 Jika Hasil Kerja Pemasok mencakup komponen elektronik (misalnya, hard disk drive, solid-state drive, memori, unit pemrosesan sentral, perangkat logis, atau kabel), Pemasok akan mempertahankan dan mengikuti program pencegahan pemalsuan yang terdokumentasi untuk, pertama dan terutama, mencegah Pemasok dalam memberikan komponen palsu kepada Kyndryl, kedua, segera mendeteksi dan meremediasi setiap kasus di mana Pemasok salah memberikan komponen palsu kepada Kyndryl. Pemasok akan membebankan kewajiban yang sama ini untuk mempertahankan dan mengikuti program pencegahan pemalsuan yang terdokumentasi pada semua pemasoknya yang menyediakan komponen elektronik yang tercakup dalam Hasil Kerja Pemasok kepada Kyndryl.

4. Remediasi

4.1 Jika Pemasok gagal mematuhi setiap kewajibannya berdasarkan Syarat-Syarat ini, dan kegagalan tersebut menyebabkan Pelanggaran Keamanan, maka Pemasok akan mengoreksi kegagalan dalam kinerjanya dan meremediasi dampak berbahaya dari Pelanggaran Keamanan, dengan kinerja dan remediasi tersebut atas arahan dan jadwal Kyndryl secara wajar. Namun, jika Pelanggaran Keamanan timbul dari pengadaan Layanan yang di-Host multi-penyewa oleh Pemasok, dan akibatnya berdampak pada banyak pelanggan Pemasok, termasuk Kyndryl, maka Pemasok akan, berdasarkan sifat Pelanggaran Keamanan, mengoreksi kegagalan secara tepat waktu dan sesuai dalam kinerjanya dan meremediasi dampak yang berbahaya dari Pelanggaran Keamanan, sembari mengupayakan pertimbangan yang sepatutnya atas masukan Kyndryl mengenai koreksi dan remediasi tersebut. Tanpa mengesampingkan hal di atas, Pemasok harus memberi tahu Kyndryl tanpa penundaan yang tidak semestinya jika Pemasok tidak lagi dapat memenuhi kewajiban yang ditetapkan oleh undang-undang perlindungan data yang berlaku.

4.2 Kyndryl akan memiliki hak untuk berpartisipasi dalam remediasi setiap Pelanggaran Keamanan yang dirujuk dalam Pasal 4.1, sebagaimana diyakini tepat atau perlu, dan Pemasok akan bertanggung jawab atas biaya dan pengeluarannya dalam mengoreksi kinerjanya dan atas biaya dan pengeluaran remediasi yang dikeluarkan oleh para pihak sehubungan dengan Pelanggaran Keamanan tersebut.

4.3 Sebagai contoh, biaya dan pengeluaran remediasi yang terkait dengan Pelanggaran Keamanan dapat mencakup biaya dan pengeluaran untuk mendeteksi dan menginvestigasi Pelanggaran Keamanan, menentukan tanggung jawab berdasarkan peraturan perundang-undangan dan regulasi yang berlaku, memberikan pemberitahuan pelanggaran, membuat dan mengelola pusat panggilan, menyediakan layanan pemantauan kredit dan restorasi kredit, memuat ulang data, mengoreksi kecacatan produk (termasuk melalui Kode Sumber atau pengembangan lain), mempertahankan pihak ketiga untuk membantu aktivitas di atas atau aktivitas relevan lainnya, serta biaya dan pengeluaran lain yang diperlukan untuk meremediasi dampak yang berbahaya dari Pelanggaran Keamanan. Demi kejelasan, biaya dan pengeluaran remediasi tidak akan mencakup kehilangan laba, bisnis, nilai, pendapatan, nama baik, atau penghematan yang diharapkan Kyndryl.