

Adendum Pemrosesan Data Cloud (Pelanggan)

Adendum Pemrosesan Data Cloud ini (termasuk lampirannya, "Adendum") dimasukkan ke dalam Perjanjian(-Perjanjian) (sebagaimana didefinisikan di bawah) antara Google dan Pelanggan. Adendum ini sebelumnya dikenal sebagai "Ketentuan Pemrosesan dan Keamanan Data" berdasarkan Perjanjian untuk Google Cloud Platform, Looker (original), Layanan Google SecOps, atau Google Cloud Skills Boost for Organizations; "Amendemen Pemrosesan Data" berdasarkan Perjanjian untuk Google Workspace atau Cloud Identity; dan "Adendum Pemrosesan Data" berdasarkan Perjanjian untuk Mandiant Consulting Services dan Mandiant Managed Services.

Ketentuan Umum

1. Gambaran Umum

Adendum ini menjelaskan kewajiban para pihak, termasuk berdasarkan undang-undang privasi, keamanan data, dan perlindungan data yang berlaku, sehubungan dengan pemrosesan dan keamanan Data Pelanggan (sebagaimana didefinisikan di bawah). Adendum ini akan berlaku efektif pada Tanggal Efektif Adendum (sebagaimana didefinisikan di bawah ini), dan akan menggantikan setiap ketentuan yang sebelumnya berlaku untuk pemrosesan dan keamanan Data Pelanggan. Istilah-istilah dalam huruf besar yang digunakan tetapi tidak didefinisikan dalam Adendum ini memiliki arti sebagaimana yang ditentukan dalam Perjanjian.

2. Definisi

2.1 Dalam Adendum ini:

- "*Tanggal Efektif Adendum*" berarti tanggal di mana Pelanggan menerima, atau para pihak menyetujui Adendum ini.
- "*Pengendalian Keamanan Tambahan*" berarti sumber daya, fitur, fungsionalitas, dan pengendalian keamanan yang dapat digunakan oleh Pelanggan sesuai pilihannya dan sebagaimana ditentukannya, termasuk Konsol Admin, enkripsi, *logging* dan pemantauan, manajemen identitas dan akses, pemindaian keamanan, dan *firewall*.
- "*Perjanjian*" berarti kontrak yang telah disetujui oleh Google dalam rangka menyediakan Layanan yang berlaku kepada Pelanggan.
- "*Hukum Privasi Yang Berlaku*" berarti sebagaimana berlaku pada pemrosesan Data Pribadi Pelanggan, setiap undang-undang atau peraturan nasional, federal, Uni Eropa, negara bagian, provinsi, atau undang-undang atau peraturan privasi atau keamanan data, atau perlindungan data.

- “*Layanan Yang Diaudit*” berarti Layanan yang berlaku pada saat itu yang diindikasikan masuk dalam ruang lingkup sertifikasi atau laporan yang relevan dalam <https://cloud.google.com/security/compliance/services-in-scope>. Google tidak boleh menghapus Layanan apa pun dari LSS ini kecuali Layanan tersebut telah dihentikan sesuai dengan Perjanjian.
- “*Sertifikasi Kepatuhan*” memiliki arti yang didefinisikan dalam Bagian 7.4 (Sertifikasi Kepatuhan dan Laporan SOC).
- “*Data Pelanggan*”, jika tidak didefinisikan dalam Perjanjian, memiliki arti yang diberikan dalam Lampiran 4 (Produk Khusus).
- “*Data Pribadi Pelanggan*” berarti data pribadi yang terdapat dalam Data Pelanggan, termasuk kategori khusus data pribadi atau data sensitif yang didefinisikan dalam Hukum Privasi Yang Berlaku.
- “*Insiden Data*” berarti pelanggaran keamanan Google yang mengakibatkan pemusnahan, kehilangan, perubahan, pengungkapan tidak sah dari, atau akses ke Data Pelanggan secara tidak disengaja atau melanggar hukum, pada sistem yang dikelola atau dikendalikan oleh Google.
- “*EMEA*” berarti Eropa, Timur Tengah, dan Afrika.
- “*GDPR UE*” berarti Peraturan (UE) 2016/679 Parlemen dan Dewan Eropa (*European Parliament and of the Council*) tanggal 27 April 2016 tentang perlindungan individu sehubungan dengan pemrosesan data pribadi dan pergerakan bebas data tersebut, dan mencabut Petunjuk (*Directive*) 95/46/EC.
- “*Hukum Perlindungan Data Eropa*” berarti, sebagaimana berlaku: (a) GDPR; atau (b) FADP Swiss.
- “*Hukum Eropa*” berarti, sebagaimana berlaku: (a) undang-undang UE atau Negara Anggota UE (jika GDPR UE berlaku untuk pemrosesan Data Pribadi Pelanggan); (b) hukum Inggris Raya atau bagian dari Inggris Raya (jika GDPR Inggris Raya berlaku pada pemrosesan Data Pribadi Pelanggan); atau (c) hukum Swiss (jika FADP Swiss berlaku pada pemrosesan Data Pribadi Pelanggan).
- “*GDPR*” berarti, sebagaimana berlaku: (a) GDPR UE; atau (b) GDPR Inggris Raya.
- “*Auditor Pihak Ketiga Google*” berarti auditor pihak ketiga yang ditunjuk Google, memenuhi syarat, dan independen, yang identitasnya saat itu akan diungkapkan oleh Google kepada Pelanggan.
- “*Instruksi*” memiliki arti yang diberikan dalam Bagian 5.2 (Kepatuhan terhadap Instruksi Pelanggan).

- “*Alamat Surel Pemberitahuan*” berarti alamat(-alamat) surel yang ditentukan oleh Pelanggan dalam Konsol Admin atau Formulir Pesanan untuk menerima pemberitahuan tertentu dari Google.
- “*Dokumentasi Keamanan*” berarti Sertifikasi Kepatuhan dan Laporan SOC.
- “*Langkah-Langkah Keamanan*” memiliki arti yang diberikan dalam Bagian 7.1.1 (Langkah-Langkah Keamanan Google).
- “*Layanan*” berarti layanan yang berlaku sebagaimana dijelaskan dalam Lampiran 4 (Produk Khusus).
- “*Laporan SOC*” memiliki arti yang diberikan dalam Bagian 7.4 (Sertifikasi Kepatuhan dan Laporan SOC).
- “*Subprosesor*” berarti pihak ketiga yang berwenang sebagai prosesor lain berdasarkan Adendum ini untuk memproses Data Pelanggan dalam rangka menyediakan bagian Layanan dan TSS (jika berlaku).
- “*Otoritas Pengawas*” berarti, sebagaimana berlaku: (a) “otoritas pengawas” sebagaimana didefinisikan dalam GDPR UE; atau (b) “Komisaris” sebagaimana didefinisikan dalam GDPR Inggris Raya atau FADP Swiss.
- “*FADP Swiss*” berarti, sebagaimana berlaku, Undang-Undang Federal tentang Perlindungan Data (Federal Act on Data Protection) tanggal 19 Juni 1992 (Swiss) (dengan Ordonansi Undang-Undang Federal tentang Perlindungan Data (*Ordinance to the Federal Act on Data Protection*) tanggal 14 Juni 1993) atau Undang-Undang Federal tentang Perlindungan Data (*Federal Act on Data Protection*) yang direvisi tanggal 25 September 2020 (Swiss) (dengan Ordonansi Undang-Undang Federal tentang Perlindungan Data (*Ordinance to the Federal Act on Data Protection*) tanggal 31 Agustus 2022).
- “*Jangka Waktu*” berarti jangka waktu sejak Tanggal Efektif Adendum hingga berakhirnya penyediaan Layanan oleh Google, termasuk, jika berlaku, jangka waktu apa pun di mana penyediaan Layanan dapat ditangguhkan dan setiap periode pasca-pengakhiran apa pun di mana Google dapat terus menyediakan Layanan untuk tujuan transisi.
- “*GDPR Inggris Raya*” berarti GDPR UE sebagaimana diubah dan dimasukkan ke dalam undang-undang Inggris Raya berdasarkan Undang-Undang (Penarikan) Uni Eropa Inggris (UK European Union (Withdrawal) Act) Tahun 2018, dan peraturan perundang-undangan sekunder yang berlaku yang dibuat berdasarkan Undang-Undang tersebut.

2.2 Istilah “data pribadi”, “subjek data”, “pemrosesan”, “pengendali”, dan “prosesor” sebagaimana digunakan dalam Adendum ini memiliki arti sebagaimana ditentukan oleh Hukum Privasi Yang Berlaku atau, jika tidak ada arti atau hukum tersebut, oleh GDPR UE.

2.3 Istilah “subjek data”, “pengendali”, dan “pemroses” masing-masing mencakup “konsumen”, “bisnis”, dan “penyedia layanan”, masing-masingnya, sebagaimana diwajibkan oleh Hukum Privasi Yang Berlaku.

3. Durasi

Terlepas dari apakah Perjanjian yang berlaku telah diakhiri atau kedaluwarsa, Adendum ini akan tetap berlaku hingga, dan secara otomatis berakhir ketika, Google menghapus seluruh Data Pelanggan sebagaimana dijelaskan dalam Adendum ini.

4. Peran; Kepatuhan Hukum

4.1 Peran Para Pihak. Google adalah prosesor dan Pelanggan adalah pengendali atau pemroses, sebagaimana berlaku, dari Data Pribadi Pelanggan.

4.2 Ringkasan Pemrosesan. Pokok bahasan dan rincian pemrosesan Data Pribadi Pelanggan dijelaskan dalam Lampiran 1 (Pokok Bahasan dan Rincian Pemrosesan Data).

4.3 Kepatuhan terhadap Hukum. Masing-masing pihak akan mematuhi kewajibannya terkait pemrosesan Data Pribadi Pelanggan berdasarkan Hukum Privasi Yang Berlaku.

4.4 Ketentuan Hukum Tambahan. Sepanjang pemrosesan Data Pribadi Pelanggan tunduk pada Hukum Privasi Yang Berlaku yang dijelaskan dalam Lampiran 3 (Hukum Privasi Khusus), ketentuan terkait dalam Lampiran 3 akan berlaku sebagai tambahan terhadap Ketentuan Umum ini dan berlaku sebagaimana dijelaskan dalam Bagian 14.1 (Prioritas).

5. Pemrosesan Data

5.1 *Prosesor Pelanggan. Jika Pelanggan adalah pemroses:*

a. Pelanggan menjamin secara berkelanjutan bahwa pengendali yang relevan telah mengizinkan:

i. Instruksi;

ii. Keterlibatan Pelanggan terhadap Google sebagai prosesor lain; dan

iii. Keterlibatan Google terhadap Subprosesor sebagaimana dijelaskan dalam Bagian 11 (Subprosesor);

b. Pelanggan akan meneruskan kepada pengendali yang relevan dengan segera dan tanpa penundaan yang tidak semestinya, setiap pemberitahuan yang diberikan oleh Google berdasarkan Bagian 7.2.1 (Pemberitahuan Insiden), 9.2.1 (Tanggung Jawab atas Permintaan), atau 11.4 (Kesempatan untuk Menolak Subprosesor); dan

c. Pelanggan dapat menyediakan kepada pengendali informasi lain apa pun yang disediakan oleh Google berdasarkan Adendum ini mengenai lokasi pusat data Google atau nama, lokasi, dan aktivitas Subprosesor.

5.2 Kepatuhan terhadap Instruksi Pelanggan. Pelanggan menginstruksikan Google untuk memproses Data Pelanggan sesuai dengan Perjanjian yang berlaku (termasuk Adendum ini) dan hukum yang berlaku hanya sebagai berikut:

- a. untuk menyediakan, mengamankan, dan memantau Layanan dan TSS (jika berlaku); dan
- b. sebagaimana ditentukan lebih lanjut melalui:
 - i. penggunaan Layanan oleh Pelanggan (termasuk melalui Konsol Admin) dan TSS (jika berlaku); dan
 - ii. instruksi tertulis apa pun lainnya yang diberikan oleh Pelanggan dan diakui oleh Google sebagai instruksi berdasarkan Adendum ini

(secara bersama-sama, "*Instruksi*").

Google akan mematuhi Instruksi kecuali dilarang oleh Hukum Eropa, jika Hukum Perlindungan Data Eropa berlaku, atau dilarang oleh hukum yang berlaku, jika Hukum Privasi Yang Berlaku lainnya berlaku.

6. Penghapusan Data

6.1 Penghapusan oleh Pelanggan. Google akan mengizinkan Pelanggan untuk menghapus Data Pelanggan selama Jangka Waktu dengan cara yang sesuai dengan fungsionalitas Layanan. Jika Pelanggan menggunakan Layanan untuk menghapus Data Pelanggan mana pun selama Jangka Waktu dan Data Pelanggan tersebut tidak dapat dipulihkan oleh Pelanggan, penggunaan ini akan dianggap sebagai Instruksi kepada Google untuk menghapus Data Pelanggan yang relevan dari sistem Google sesuai dengan hukum yang berlaku. Google akan mematuhi Instruksi ini sesegera mungkin dan dalam jangka waktu paling lama 180 hari, kecuali Hukum Eropa mewajibkan penyimpanan, di mana Hukum Perlindungan Data Eropa berlaku, atau hukum yang berlaku mewajibkan penyimpanan, di mana Hukum Privasi Yang Berlaku lainnya berlaku.

6.2 Pengembalian atau Penghapusan Saat Jangka Waktu Berakhir. Jika Pelanggan ingin menyimpan Data Pelanggan apa pun setelah Jangka Waktu berakhir, Pelanggan dapat menginstruksikan Google sesuai dengan Bagian 9.1 (Akses; Perbaikan; Pemrosesan Yang Dibatasi; Portabilitas) untuk mengembalikan data tersebut selama Jangka Waktu. Tunduk pada Bagian 6.3 (Instruksi Penghapusan Yang Ditunda), Pelanggan menginstruksikan Google untuk menghapus seluruh Data Pelanggan yang tersisa (termasuk salinan yang ada) dari sistem Google pada akhir Jangka Waktu sesuai dengan hukum yang berlaku. Setelah masa pemulihan sampai dengan 30 hari sejak tanggal tersebut, Google akan mematuhi Instruksi ini sesegera mungkin dan dalam jangka waktu paling lama 180 hari, kecuali Hukum Eropa mewajibkan penyimpanan, di mana Hukum Perlindungan Data Eropa berlaku, atau hukum yang berlaku mewajibkan penyimpanan, di mana Hukum Privasi Yang Berlaku lainnya berlaku.

6.3. Instruksi Penghapusan Yang Ditunda. Sepanjang Data Pelanggan yang tercakup dalam instruksi penghapusan yang dijelaskan dalam Bagian 6.2 (Pengembalian atau Penghapusan Saat Jangka Waktu Berakhir) juga diproses, saat Jangka Waktu yang berlaku berdasarkan Bagian 6.2 berakhir, sehubungan dengan Perjanjian dengan Jangka Waktu yang berkelanjutan, instruksi penghapusan tersebut akan berlaku sehubungan dengan Data Pelanggan tersebut hanya saat Jangka Waktu yang berkelanjutan berakhir. Untuk kejelasan, Adendum ini akan terus berlaku untuk Data Pelanggan tersebut hingga Data Pelanggan tersebut dihapus oleh Google.

7. Keamanan Data

7.1 Tindakan, Pengendalian, dan Bantuan Keamanan Google.

7.1.1 Langkah-Langkah Keamanan Google. Google akan menerapkan dan memelihara tindakan teknis, organisasi, dan fisik untuk melindungi Data Pelanggan dari pemusnahan, kehilangan, perubahan, pengungkapan atau akses yang tidak disengaja atau melanggar hukum sebagaimana dijelaskan dalam Lampiran 2 (Langkah-Langkah Keamanan) ("**Langkah-Langkah Keamanan**"). Langkah-Langkah Keamanan mencakup tindakan untuk mengenkripsi Data Pelanggan; untuk membantu memastikan kerahasiaan, integritas, ketersediaan, dan ketahanan sistem dan layanan Google yang berkelanjutan; untuk membantu memulihkan akses tepat waktu ke Data Pelanggan setelah terjadi insiden; dan untuk pengujian efektivitas secara berkala. Google dapat memperbarui Langkah-Langkah Keamanan dari waktu ke waktu dengan ketentuan bahwa pembaruan tersebut tidak mengakibatkan penurunan Layanan secara material.

7.1.2 Akses dan Kepatuhan. Google akan:

- a. memberi wewenang kepada karyawan, kontraktor, dan Subprosesornya untuk mengakses Data Pelanggan hanya jika diperlukan untuk mematuhi Instruksi;
- b. mengambil langkah-langkah yang tepat untuk memastikan kepatuhan terhadap Langkah-Langkah Keamanan oleh karyawannya, kontraktornya, dan Subprosesornya sejauh berlaku pada lingkup kinerja mereka; dan
- c. memastikan bahwa seluruh orang yang berwenang untuk memproses Data Pelanggan berkewajiban menjaga kerahasiaan.

7.1.3 Pengendalian Keamanan Tambahan. Google akan menyediakan Pengendalian Keamanan Tambahan untuk:

- a. mengizinkan Pelanggan untuk mengambil langkah pengamanan Data Pelanggan; dan
- b. memberikan informasi kepada Pelanggan mengenai cara mengamankan, mengakses, dan menggunakan Data Pelanggan.

7.1.4 Bantuan Keamanan Google. Google akan (dengan mempertimbangkan sifat pemrosesan Data Pribadi Pelanggan dan informasi yang tersedia untuk Google) membantu Pelanggan dalam memastikan kepatuhan terhadap kewajibannya (atau, jika Pelanggan adalah pemroses, pengendali yang relevan) terkait dengan pelanggaran keamanan dan data pribadi berdasarkan Hukum Privasi Yang Berlaku, dengan:

- a. menerapkan dan melakukan Langkah-Langkah Keamanan sesuai dengan Bagian 7.1.1 (Langkah-Langkah Keamanan Google);
- b. menyediakan Pengendalian Keamanan Tambahan sesuai dengan Bagian 7.1.3 (Pengendalian Keamanan Tambahan);
- c. mematuhi ketentuan Bagian 7.2 (Insiden Data);
- d. menyediakan Dokumentasi Keamanan sesuai dengan Bagian 7.5.1 (Peninjauan Dokumentasi Keamanan) dan memberikan informasi yang terdapat dalam Perjanjian yang berlaku (termasuk Adendum ini); dan

e. jika sub-bagian (a)-(d) di atas tidak cukup bagi Pelanggan (atau pengendali yang relevan) untuk mematuhi kewajiban tersebut, atas permintaan Pelanggan, memberikan kerja sama dan bantuan tambahan yang wajar kepada Pelanggan.

7.2 Insiden Data.

7.2.1 Pemberitahuan Insiden. Google akan segera memberitahukan Pelanggan dan tanpa penundaan yang tidak semestinya setelah mengetahui adanya Insiden Data, dan segera mengambil langkah-langkah yang wajar untuk meminimalkan kerugian dan mengamankan Data Pelanggan.

7.2.2 Rincian Insiden Data. Pemberitahuan Google mengenai Insiden Data akan menjelaskan: sifat Insiden Data termasuk sumber daya Pelanggan yang terkena dampak; tindakan yang telah diambil atau direncanakan oleh Google untuk mengatasi Insiden Data dan memitigasi potensi risikonya; tindakan, jika ada, yang direkomendasikan oleh Google agar Pelanggan ambil untuk mengatasi Insiden Data; dan rincian titik kontak di mana informasi lebih lanjut dapat diperoleh. Jika tidak memungkinkan untuk memberikan seluruh informasi tersebut pada saat yang sama, pemberitahuan awal Google akan berisi informasi yang tersedia saat itu dan informasi lebih lanjut akan diberikan tanpa penundaan setelah informasi tersebut tersedia.

7.2.3 Tidak Ada Penilaian Data Pelanggan oleh Google. Google tidak berkewajiban menilai Data Pelanggan untuk mengidentifikasi informasi yang tunduk pada persyaratan hukum tertentu.

7.2.4 Tidak Ada Pengakuan Kesalahan oleh Google. Pemberitahuan atau tanggapan Google terhadap Insiden Data berdasarkan Bagian 7.2 (Insiden Data) ini tidak akan ditafsirkan sebagai pengakuan Google atas kesalahan atau liabilitas apa pun sehubungan dengan Insiden Data.

7.3 Tanggung Jawab dan Penilaian Keamanan Pelanggan.

7.3.1 Tanggung Jawab Keamanan Pelanggan. Tanpa mengurangi kewajiban Google berdasarkan Bagian 7.1 (Tindakan, Pengendalian, dan Bantuan Keamanan Google) dan 7.2 (Insiden Data), dan bagian lain dalam Perjanjian yang berlaku, Pelanggan bertanggung jawab atas penggunaan Layanan oleh Pelanggan serta penyimpanan salinan Data Pelanggan apa pun di luar sistem Google atau Subprosesor Google, termasuk:

- a. menggunakan Layanan dan Pengendalian Keamanan Tambahan untuk memastikan tingkat keamanan yang sesuai dengan risiko terhadap Data Pelanggan;
- b. mengamankan kredensial autentikasi akun, sistem dan perangkat yang digunakan Pelanggannya untuk mengakses Layanan; dan
- c. mencadangkan atau menyimpan salinan Data Pelanggannya sebagaimana mestinya.

7.3.2 Penilaian Keamanan Pelanggan. Pelanggan setuju bahwa Layanan, Langkah-Langkah Keamanan, Pengendalian Keamanan Tambahan, dan komitmen Google berdasarkan Bagian 7 (Keamanan Data) ini memberikan tingkat keamanan yang sesuai dengan risiko Data Pelanggan (dengan mempertimbangkan keadaan terkini, biaya penerapan, dan sifat, ruang lingkup, konteks, dan tujuan pemrosesan Data Pelanggan serta risiko terhadap individu).

7.4 *Sertifikasi Kepatuhan dan Laporan SOC*. Google akan mempertahankan setidaknya hal-hal berikut untuk Layanan Yang Diaudit dalam rangka memverifikasi efektivitas Langkah-Langkah Keamanan yang berkelanjutan:

a. sertifikat ISO 27001 dan sertifikasi tambahan apa pun yang dijelaskan dalam Lampiran 4 (Produk Khusus) ("*Sertifikasi Kepatuhan*"); dan

b. Laporan SOC 2 dan SOC 3 dibuat oleh Auditor Pihak Ketiga Google dan diperbarui secara tahunan berdasarkan suatu audit yang dilakukan setidaknya sekali setiap 12 bulan ("*Laporan SOC*").

Google dapat menambahkan standar kapan pun. Google dapat mengganti suatu Sertifikasi Kepatuhan atau Laporan SOC dengan alternatif yang setara atau lebih baik.

7.5 *Peninjauan dan Audit Kepatuhan*.

7.5.1 *Peninjauan Dokumentasi Keamanan*. Untuk menunjukkan kepatuhan Google terhadap kewajibannya berdasarkan Adendum ini, Google akan menyediakan Dokumentasi Keamanan untuk ditinjau oleh Pelanggan dan, jika Pelanggan adalah pemroses, mengizinkan Pelanggan untuk meminta akses ke Laporan SOC kepada pengendali yang relevan sesuai dengan Bagian 7.5.3 (Ketentuan Bisnis Tambahan untuk Peninjauan dan Audit).

7.5.2 *Hak Audit Pelanggan*.

a. *Audit Pelanggan*. Google akan, jika diwajibkan berdasarkan Hukum Privasi Yang Berlaku, mengizinkan Pelanggan atau auditor independen yang ditunjuk oleh Pelanggan untuk melakukan audit (termasuk inspeksi) untuk memverifikasi kepatuhan Google terhadap kewajibannya berdasarkan Adendum ini sesuai dengan Bagian 7.5.3 (Ketentuan Bisnis Tambahan untuk Peninjauan dan Audit). Selama audit, Google akan bekerja sama secara wajar dengan Pelanggan atau auditornya sebagaimana dijelaskan dalam Bagian 7.5 (Peninjauan dan Audit Kepatuhan).

b. *Peninjauan Independen Pelanggan*. Pelanggan dapat melakukan audit untuk memverifikasi kepatuhan Google terhadap kewajibannya berdasarkan Adendum ini dengan meninjau Dokumentasi Keamanan (yang mencerminkan hasil audit yang dilakukan oleh Auditor Pihak Ketiga Google).

7.5.3 *Ketentuan Bisnis Tambahan untuk Peninjauan dan Audit*.

a. Pelanggan harus menghubungi Tim Perlindungan Data Google Cloud untuk meminta:

i. akses ke Laporan SOC untuk pengendali yang relevan berdasarkan Bagian 7.5.1 (Peninjauan Dokumentasi Keamanan); atau

ii. audit berdasarkan Bagian 7.5.2(a) (Audit Pelanggan).

b. Berdasarkan permintaan Pelanggan berdasarkan Bagian 7.5.3(a), Google dan Pelanggan akan mendiskusikan dan menyepakati terlebih dahulu mengenai:

i. pengendalian keamanan dan kerahasiaan yang berlaku untuk setiap akses ke Laporan SOC oleh pengendali yang relevan berdasarkan Bagian 7.5.1 (Peninjauan Dokumentasi Keamanan); dan

ii. tanggal mulai yang wajar, ruang lingkup dan durasi serta pengendalian keamanan dan kerahasiaan yang berlaku untuk audit apa pun berdasarkan Bagian 7.5.2(a) (Audit Pelanggan).

c. Google dapat mengenakan suatu biaya (berdasarkan biaya yang wajar dari Google) untuk audit apa pun berdasarkan Bagian 7.5.2(a) (Audit Pelanggan). Google akan memberikan rincian lebih lanjut kepada Pelanggan mengenai biaya yang berlaku, dan dasar penghitungannya, sebelum audit tersebut dilakukan. Pelanggan akan bertanggung jawab atas segala biaya yang dibebankan oleh auditor mana pun yang ditunjuk oleh Pelanggan untuk melaksanakan audit tersebut.

d. Google dapat mengajukan keberatan secara tertulis kepada auditor yang ditunjuk oleh Pelanggan untuk melakukan audit apa pun berdasarkan Bagian 7.5.2(a) (Audit Pelanggan) jika auditor tersebut, menurut pendapat yang wajar dari Google, tidak memenuhi syarat atau independen, merupakan pesaing Google, atau secara nyata tidak sesuai. Keberatan apa pun dari Google akan mengharuskan Pelanggan menunjuk auditor lain atau melakukan audit sendiri.

e. Setiap permintaan Pelanggan berdasarkan Lampiran 3 (Hukum Privasi Khusus) atau Lampiran 4 (Produk Khusus) untuk mengakses laporan SOC apa pun untuk pengendali yang relevan atau untuk audit juga akan tunduk pada Bagian 7.5.3 ini (Ketentuan Bisnis Tambahan untuk Peninjauan dan Audit).

8. Penilaian Dampak dan Konsultasi

Google akan (dengan mempertimbangkan sifat pemrosesan dan informasi yang tersedia untuk Google) membantu Pelanggan dalam memastikan kepatuhan terhadap kewajibannya (atau, jika Pelanggan adalah pemroses, pengendali yang relevan) terkait dengan penilaian perlindungan data, penilaian risiko, konsultasi peraturan sebelumnya atau prosedur serupa berdasarkan Hukum Privasi Yang Berlaku, dengan:

a. menyediakan Pengendalian Keamanan Tambahan sesuai dengan Bagian 7.1.3 (Pengendalian Keamanan Tambahan) dan Dokumentasi Keamanan yang tersedia sesuai dengan Bagian 7.5.1 (Peninjauan Dokumentasi Keamanan);

b. memberikan informasi yang terdapat dalam Perjanjian yang berlaku (termasuk Adendum ini); dan

c. jika sub-bagian (a) dan (b) di atas tidak cukup bagi Pelanggan (atau pengendali yang relevan) untuk mematuhi kewajiban tersebut, atas permintaan Pelanggan, memberikan kerja sama dan bantuan tambahan yang wajar kepada Pelanggan.

9. Akses; Hak Subjek Data; Ekspor Data

9.1 Akses; Perbaikan; Pemrosesan Yang Dibatasi; Portabilitas. Selama Jangka Waktu, Google akan memperbolehkan Pelanggan, dengan cara yang sesuai dengan fungsionalitas Layanan, untuk mengakses, memperbaiki, dan membatasi pemrosesan Data Pelanggan, termasuk melalui fungsionalitas penghapusan yang disediakan oleh Google sebagaimana dijelaskan dalam Bagian 6.1 (Penghapusan oleh Pelanggan), dan untuk mengeksport Data Pelanggan. Jika Pelanggan mengetahui bahwa Data Pribadi Pelanggan mana pun tidak akurat atau bukan yang terbaru (*outdated*), Pelanggan akan bertanggung jawab untuk menggunakan fungsionalitas tersebut untuk memperbaiki atau menghapus data tersebut jika diwajibkan oleh Hukum Privasi Yang Berlaku.

9.2 *Permintaan Subjek Data.*

9.2.1 *Tanggung Jawab atas Permintaan.* Selama Jangka Waktu, jika Tim Perlindungan Data Google Cloud menerima permintaan dari subjek data yang berkaitan dengan Data Pribadi Pelanggan dan mengidentifikasi Pelanggan, Google akan:

- a. menyarankan subjek data untuk menyampaikan permintaannya kepada Pelanggan;
- b. segera memberitahukan Pelanggan; dan
- c. sebaliknya tidak akan menanggapi permintaan subjek data tersebut tanpa izin dari Pelanggan.

Pelanggan akan bertanggung jawab untuk menanggapi setiap permintaan tersebut termasuk, jika diperlukan, dengan menggunakan fungsionalitas Layanan.

9.2.2 *Bantuan Permintaan Subjek Data Google.* Google akan (dengan mempertimbangkan sifat pemrosesan Data Pribadi Pelanggan) membantu Pelanggan dalam memenuhi kewajibannya (atau, jika Pelanggan adalah prosesor, pengendali yang relevan) berdasarkan Hukum Privasi Yang Berlaku untuk menanggapi permintaan pelaksanaan hak subjek data dengan:

- a. menyediakan Pengendalian Keamanan Tambahan sesuai dengan Bagian 7.1.3 (Pengendalian Keamanan Tambahan);
- b. mematuhi Bagian 9.1 (Akses; Perbaikan; Pemrosesan Yang Dibatasi; Portabilitas) dan 9.2.1 (Tanggung Jawab atas Permintaan); dan
- c. jika sub-bagian (a) dan (b) di atas tidak cukup bagi Pelanggan (atau pengendali yang relevan) untuk mematuhi kewajiban tersebut, atas permintaan Pelanggan, memberikan kerja sama dan bantuan tambahan yang wajar kepada Pelanggan.

10. **Lokasi Pemrosesan Data**

10.1 *Fasilitas Penyimpanan dan Pemrosesan Data.* Tunduk pada komitmen lokasi data Google berdasarkan Ketentuan Khusus Layanan dan komitmen transfer data berdasarkan Lampiran 3 (Hukum Privasi Khusus), jika berlaku, Data Pelanggan dapat diproses di negara mana pun tempat Google atau Subprosesornya mengelola fasilitasnya.

10.2 *Informasi Pusat Data.* Lokasi pusat data Google dijelaskan dalam Lampiran 4 (Produk Khusus).

11. **Subprosesor**

11.1 *Persetujuan Keterlibatan Subprosesor.* Pelanggan secara khusus mengizinkan keterlibatan Google sebagai Subprosesor dari entitas yang diungkapkan sebagaimana dijelaskan dalam Bagian 11.2 (Informasi Mengenai Subprosesor) sejak Tanggal Efektif Adendum. Selain itu, tanpa mengesampingkan Bagian 11.4 (Kesempatan untuk Menolak Subprosesor), Pelanggan secara umum mengizinkan Google untuk melibatkan pihak ketiga lainnya sebagai Subprosesor ("*Subprosesor Baru*").

11.2 *Informasi Mengenai Subprosesor.* Nama, lokasi, dan aktivitas Subprosesor dijelaskan dalam Lampiran 4 (Produk Khusus).

11.3 Persyaratan untuk Keterlibatan Subprosesor. Saat melibatkan Subprosesor mana pun, Google akan:

a. memastikan melalui suatu kontrak tertulis bahwa:

i. Subprosesor hanya mengakses dan menggunakan Data Pelanggan sejauh diperlukan untuk melaksanakan kewajiban yang disubkontrakkan padanya, dan melakukannya sesuai dengan Perjanjian yang berlaku (termasuk Adendum ini); dan

ii. jika diwajibkan berdasarkan Hukum Privasi Yang Berlaku, kewajiban perlindungan data yang dijelaskan dalam Adendum ini diberlakukan pada Subprosesor (sebagaimana dapat dijelaskan lebih lanjut dalam Lampiran 3 (Hukum Privasi Khusus)); dan

b. tetap bertanggung jawab penuh atas seluruh kewajiban yang disubkontrakkan kepada, dan seluruh tindakan dan kelalaian dari, Subprosesor.

11.4 *Kesempatan untuk Menolak Subprosesor.*

a. Ketika Google melibatkan Subprosesor Baru mana pun selama Jangka Waktu, Google akan, setidaknya 30 hari sebelum Subprosesor Baru mulai memproses Data Pelanggan apa pun, memberitahukan Pelanggan mengenai keterlibatan tersebut (termasuk nama, lokasi, dan aktivitas Subprosesor Baru).

b. Pelanggan dapat, dalam waktu 90 hari setelah menerima pemberitahuan mengenai keterlibatan Subprosesor Baru, mengajukan keberatan dengan segera mengakhiri Perjanjian yang berlaku tanpa alasan:

i. sesuai dengan ketentuan pengakhiran tanpa alasan dari Perjanjian; atau

ii. jika tidak ada ketentuan tersebut, dengan memberitahukan Google.

12. Tim Perlindungan Data Cloud; Memproses Catatan

12.1 *Tim Perlindungan Data Cloud.* Tim Perlindungan Data Google Cloud akan memberikan bantuan yang cepat dan wajar terhadap pertanyaan apa pun dari Pelanggan terkait pemrosesan Data Pelanggan berdasarkan Perjanjian yang berlaku dan dapat dihubungi sebagaimana dijelaskan di bagian Pemberitahuan Perjanjian yang berlaku atau di Lampiran 4 (Produk Khusus).

12.2 *Catatan Pemrosesan Google.* Google akan menyimpan dokumentasi yang sesuai mengenai aktivitas pemrosesannya sebagaimana diwajibkan oleh Hukum Privasi Yang Berlaku. Sepanjang Hukum Privasi Yang Berlaku mewajibkan Google untuk mengumpulkan dan menyimpan catatan informasi tertentu yang berkaitan dengan Pelanggan, Pelanggan akan menggunakan Konsol Admin atau cara lain yang disebutkan dalam Lampiran 4 (Produk Khusus) untuk menyediakan informasi tersebut dan menjaganya tetap akurat dan terkini. Google dapat menyediakan informasi tersebut kepada regulator yang berwenang, termasuk Otoritas Pengawas, jika diwajibkan oleh Hukum Privasi Yang Berlaku.

12.3 *Permintaan Pengendali.* Selama Jangka Waktu, jika Tim Perlindungan Data Google Cloud menerima permintaan atau instruksi dari pihak ketiga yang mengaku sebagai pengendali Data Pribadi Pelanggan, Google akan menyarankan pihak ketiga tersebut untuk menghubungi Pelanggan.

13. Pemberitahuan

Pemberitahuan berdasarkan Adendum ini (termasuk pemberitahuan mengenai Insiden Data apa pun) akan dikirimkan ke Alamat Surel Pemberitahuan. Pelanggan bertanggung jawab menggunakan Konsol Admin untuk memastikan Alamat Surel Pemberituannya tetap terkini dan sah.

14. Penafsiran

14.1 *Prioritas*. Sepanjang terdapat pertentangan apa pun antara:

- a. Lampiran 3 (Hukum Privasi Khusus) dan sisa dari Adendum (termasuk Lampiran 4 (Produk Khusus)), Lampiran akan berlaku; dan
- b. Lampiran 4 (Produk Khusus) dan sisa dari Adendum (tidak termasuk Lampiran 3), Lampiran 4 akan berlaku; dan
- c. Adendum ini dan sisa Perjanjian ini, maka Adendum ini yang akan berlaku.

Untuk kejelasan, jika Pelanggan memiliki lebih dari satu Perjanjian, Adendum ini akan mengubah masing-masing Perjanjian secara terpisah.

14.2 *Referensi Bagian*. Kecuali dinyatakan lain, referensi bagian dalam Lampiran apa pun pada Adendum ini merujuk pada bagian dari Ketentuan Umum Adendum.

Lampiran 1: Pokok Bahasan dan Rincian Pemrosesan Data

Pokok Bahasan

Penyediaan Layanan dan TSS (jika berlaku) oleh Google kepada Pelanggan.

Durasi Pemrosesan

Jangka Waktu ditambah jangka waktu sejak akhir Jangka Waktu hingga penghapusan seluruh Data Pelanggan oleh Google sesuai dengan Adendum ini.

Sifat dan Tujuan Pemrosesan

Google akan memproses Data Pribadi Pelanggan untuk tujuan penyediaan Layanan dan TSS (jika berlaku) kepada Pelanggan sesuai dengan Adendum ini.

Kategori Data

Data terkait individu yang diberikan kepada Google melalui Layanan, oleh (atau atas arahan dari) Pelanggan, atau oleh Pengguna Akhirnya.

Subjek Data

Subjek data mencakup individu yang datanya diberikan kepada Google melalui Layanan oleh (atau atas arahan dari) Pelanggan atau oleh Pengguna Akhirnya.

Lampiran 2: Langkah-Langkah Keamanan

Sejak Tanggal Mulai Berlaku Adendum, Google akan menerapkan dan mengelola Prosedur Keamanan yang dijelaskan dalam Lampiran 2 ini.

1. Pusat Data dan Keamanan Jaringan

(a) Pusat Data.

Infrastruktur. Google mengelola pusat data yang tersebar secara geografis. Google menyimpan seluruh data produksi di pusat data yang aman secara fisik.

Redundansi. Sistem infrastruktur telah dirancang untuk menghilangkan titik kegagalan tunggal dan meminimalkan dampak risiko lingkungan yang diantisipasi. Sirkuit ganda, sakelar, jaringan, atau perangkat lain yang diperlukan membantu menyediakan redundansi ini. Layanan dirancang untuk memungkinkan Google melakukan jenis pemeliharaan preventif dan korektif tertentu tanpa gangguan. Seluruh peralatan dan fasilitas lingkungan telah mendokumentasikan prosedur pemeliharaan preventif yang merinci proses dan frekuensi kinerja sesuai dengan spesifikasi manufaktur atau internal. Pemeliharaan preventif dan korektif pada peralatan pusat data dijadwalkan melalui proses perubahan standar sesuai prosedur yang terdokumentasi.

Daya. Sistem tenaga listrik pusat data dirancang agar bersifat berulang dan dapat dikelola tanpa berdampak pada pengoperasian berkelanjutan, 24 jam sehari, 7 hari seminggu. Dalam banyak kasus, sumber daya primer dan alternatif, masing-masing dengan kapasitas yang sama, disediakan untuk komponen infrastruktur penting di pusat data. Daya cadangan disediakan oleh berbagai mekanisme seperti baterai uninterruptible power supplies (UPS), yang memberikan perlindungan daya yang andal secara konsisten selama pemadaman listrik, pemadaman listrik, tegangan berlebih, tegangan rendah, dan kondisi frekuensi di luar batas toleransi. Jika daya listrik terputus, daya cadangan dirancang untuk menyediakan daya sementara ke pusat data, dengan kapasitas penuh, hingga 10 menit hingga sistem generator cadangan mengambil alih. Generator cadangan mampu menyala secara otomatis dalam hitungan detik untuk menyediakan daya listrik darurat yang cukup untuk menjalankan pusat data dengan kapasitas penuh, biasanya untuk jangka waktu beberapa hari.

Sistem Operasi Server. Server Google menggunakan implementasi berbasis Linux yang disesuaikan untuk lingkungan aplikasi. Data disimpan menggunakan algoritma kepemilikan untuk meningkatkan keamanan dan redundansi data.

Kualitas Kode. Google menerapkan proses peninjauan kode untuk meningkatkan keamanan kode yang digunakan untuk menyediakan Layanan dan meningkatkan keamanan produk di lingkungan produksi.

Keberlanjutan Bisnis. Google telah merancang dan secara rutin merencanakan serta menguji program perencanaan keberlanjutan bisnis/pemulihan bencana.

(b) Jaringan dan Transmisi.

Transmisi Data. Pusat data umumnya terhubung melalui tautan pribadi berkecepatan tinggi untuk menyediakan transfer data yang aman dan cepat antar pusat data. Hal ini dirancang untuk mencegah

data dibaca, disalin, diubah atau dihapus tanpa izin selama transfer atau pengangkutan elektronik atau ketika direkam ke media penyimpanan data. Google mentransfer data melalui protokol standar Internet.

Permukaan Serangan Eksternal. Google menggunakan beberapa lapisan perangkat jaringan dan deteksi intrusi untuk melindungi permukaan serangan eksternalnya. Google mempertimbangkan potensi vektor serangan dan menggabungkan teknologi yang dibuat khusus ke dalam sistem yang berhadapan dengan pihak eksternal.

Deteksi Intrusi. Deteksi intrusi dimaksudkan untuk memberikan wawasan mengenai aktivitas serangan yang sedang berlangsung dan memberikan informasi yang memadai untuk merespons insiden. Deteksi intrusi Google mencakup: (i) secara ketat mengendalikan ukuran dan komposisi permukaan serangan Google melalui tindakan pencegahan; (ii) menggunakan pengendalian deteksi cerdas pada titik masuk data; dan (iii) menggunakan teknologi yang secara otomatis memperbaiki situasi berbahaya tertentu.

Respons Insiden. Google memantau berbagai saluran komunikasi untuk mengetahui adanya insiden keamanan, dan personel keamanan Google akan segera bereaksi terhadap insiden yang diketahui.

Teknologi Enkripsi. Google menyediakan enkripsi HTTPS (juga disebut sebagai koneksi SSL atau TLS). Server Google mendukung pertukaran kunci kriptografi Diffie-Hellman elliptic curve ephemeral yang ditandatangani dengan RSA dan ECDSA. Metode perfect forward secrecy (PFS) ini membantu melindungi lalu lintas dan meminimalkan dampak kunci yang disusupi, atau pembobolan kriptografi.

2. Pengendalian Situs dan Akses

(a) Pengendalian Lokasi.

Operasi Keamanan Pusat Data di Lokasi. Pusat data Google menjalankan operasi keamanan di lokasi yang bertanggung jawab atas seluruh fungsi keamanan fisik pusat data 24 jam sehari, 7 hari seminggu. Personel operasi keamanan di lokasi memantau kamera TV sirkuit tertutup (closed circuit TV) (CCTV) dan seluruh sistem alarm. Personel operasi keamanan di lokasi melakukan patroli internal dan eksternal pusat data secara teratur.

Prosedur Akses Pusat Data. Google menerapkan prosedur akses formal untuk mengizinkan akses fisik ke pusat data. Pusat data ditempatkan di fasilitas yang memerlukan akses kunci kartu elektronik, dengan alarm yang terhubung dengan operasi keamanan di lokasi. Seluruh orang yang masuk ke pusat data diharuskan untuk mengidentifikasi diri mereka sendiri serta menunjukkan bukti identitas untuk operasi keamanan di lokasi. Hanya karyawan, kontraktor, dan pengunjung yang berwenang yang diizinkan masuk ke pusat data. Hanya karyawan dan kontraktor yang berwenang yang diizinkan untuk meminta akses kunci kartu elektronik ke fasilitas ini. Permintaan akses kunci kartu elektronik pusat data harus dilakukan melalui surel, dan memerlukan persetujuan dari manajer pemohon dan direktur pusat data. Seluruh pengunjung lain yang memerlukan akses pusat data sementara harus: (i) mendapatkan persetujuan terlebih dahulu dari manajer pusat data untuk pusat data tertentu dan area internal yang ingin mereka kunjungi; (ii) masuk pada operasi keamanan di lokasi; dan (iii) merujuk pada catatan akses pusat data yang disetujui yang mengidentifikasi individu tersebut sebagai orang yang disetujui.

Perangkat Keamanan Pusat Data di Lokasi. Pusat data Google menggunakan sistem pengendalian akses autentikasi ganda yang terhubung dengan alarm sistem. Sistem pengendalian akses memantau

dan mencatat kunci kartu elektronik setiap individu dan ketika mereka mengakses pintu perimeter, pengiriman dan penerimaan, serta area penting lainnya. Aktivitas yang tidak sah dan upaya akses yang gagal dicatat oleh sistem pengendalian akses dan diselidiki, sebagaimana mestinya. Akses resmi di seluruh operasi bisnis dan pusat data dibatasi berdasarkan zona dan tanggung jawab pekerjaan individu. Pintu darurat di pusat diberikan alarm. Kamera CCTV beroperasi baik di dalam maupun di luar pusat data. Penempatan kamera telah dirancang untuk mencakup area strategis antara lain perimeter, pintu gedung pusat data, dan pengiriman/penerimaan. Personel operasi keamanan di lokasi mengelola pemantauan, perekaman, dan pengendalian keamanan CCTV. Kabel yang aman di seluruh pusat data menghubungkan peralatan CCTV. Kamera merekam di lokasi melalui perekam video digital 24 jam sehari, 7 hari seminggu. Catatan pengawasan disimpan hingga 30 hari berdasarkan aktivitas.

(b) Pengendalian Akses.

Personel Keamanan Infrastruktur. Google memiliki, dan memelihara, kebijakan keamanan untuk personelnya, dan mewajibkan pelatihan keamanan sebagai bagian dari program pelatihan untuk personelnya. Personel keamanan infrastruktur Google bertanggung jawab atas pemantauan infrastruktur keamanan Google yang berkelanjutan, peninjauan Layanan, dan respons terhadap insiden keamanan.

Pengendalian Akses dan Manajemen Hak Istimewa. Administrator Pelanggan dan Pengguna Akhir harus mengautentikasi diri mereka melalui sistem autentikasi pusat atau melalui sistem masuk tunggal untuk menggunakan Layanan.

Proses dan Kebijakan Akses Data Internal – Kebijakan Akses. Proses dan kebijakan akses data internal Google dirancang untuk mencegah orang dan sistem yang tidak berwenang memperoleh akses ke sistem yang digunakan untuk memproses Data Pelanggan. Google merancang sistemnya untuk (i) hanya mengizinkan orang yang berwenang untuk mengakses data yang diperbolehkan untuk mereka akses; dan (ii) memastikan bahwa Data Pelanggan tidak dapat dibaca, disalin, diubah, atau dihapus tanpa izin selama pemrosesan, penggunaan, dan setelah pencatatan. Sistem dirancang untuk mendeteksi akses apa pun yang tidak sesuai. Google menggunakan sistem pengelolaan akses terpusat untuk mengendalikan akses personel ke server produksi, dan hanya memberikan akses kepada personel resmi dalam jumlah terbatas. Sistem autentikasi dan otorisasi Google menggunakan sertifikat SSH dan kunci keamanan, serta dirancang untuk memberikan mekanisme akses yang aman dan fleksibel kepada Google. Mekanisme ini dirancang untuk hanya memberikan hak akses yang disetujui ke host situs, log, data, dan informasi konfigurasi. Google mewajibkan penggunaan ID pengguna yang unik, sandi yang kuat, autentikasi dua faktor, dan daftar akses yang dipantau secara hati-hati untuk meminimalkan potensi penggunaan akun yang tidak sah. Pemberian atau perubahan hak akses didasarkan pada: tanggung jawab pekerjaan personel yang berwenang; persyaratan tugas pekerjaan yang diperlukan untuk melakukan tugas resmi; dan dengan dasar kebutuhan untuk mengetahui (need to know). Pemberian atau modifikasi hak akses juga harus sesuai dengan kebijakan dan pelatihan akses data internal Google. Persetujuan dikelola oleh alat alur kerja yang menyimpan catatan audit seluruh perubahan. Akses ke sistem dicatat untuk membuat jejak audit demi akuntabilitas. Jika kata sandi digunakan untuk autentikasi (misalnya login ke stasiun kerja), kebijakan kata sandi yang setidaknya mengikuti praktik standar industri akan diterapkan. Standar ini mencakup pembatasan penggunaan kembali kata sandi dan kekuatan kata sandi yang memadai. Untuk akses ke informasi yang sangat sensitif (misalnya data kartu kredit), Google menggunakan token perangkat keras.

3. Data

(a) *Penyimpanan Data, Isolasi dan Pencatatan.* Google menyimpan data dalam lingkungan multi-penyewa di server milik Google. Tunduk pada Instruksi apa pun yang bertentangan (misalnya dalam bentuk pemilihan lokasi data), Google mereplikasi Data Pelanggan di beberapa pusat data yang tersebar secara geografis. Google juga secara logis mengisolasi Data Pelanggan. Pelanggan akan diberikan kendali atas kebijakan berbagi data tertentu. Kebijakan tersebut, sesuai dengan fungsionalitas Layanan, akan memungkinkan Pelanggan untuk menentukan pengaturan berbagi produk yang berlaku bagi Pengguna Akhirnya untuk tujuan tertentu. Pelanggan dapat memilih untuk menggunakan fungsionalitas pencatatan yang disediakan Google melalui Layanan.

(b) *Kebijakan Disk Yang Dinonaktifkan dan Penghapusan Disk.* Disk yang berisi data mungkin mengalami masalah kinerja, kesalahan, atau kegagalan perangkat keras yang menyebabkan disk tersebut dinonaktifkan (“Disk Yang Dinonaktifkan”). Setiap Disk Yang Dinonaktifkan harus melalui serangkaian proses pemusnahan data (“Kebijakan Penghapusan Disk”) sebelum meninggalkan lokasi Google untuk digunakan kembali atau dimusnahkan. Disk Yang Dinonaktifkan akan dihapus dalam proses beberapa langkah dan diverifikasi selesai oleh setidaknya dua validator independen. Hasil penghapusan dicatat berdasarkan nomor seri Disk Yang Dinonaktifkan untuk pelacakan. Terakhir, Disk Yang Dinonaktifkan yang telah dihapus dikembalikan ke inventaris untuk digunakan kembali dan dipindahkan. Jika, karena kegagalan perangkat keras, Disk Yang Dinonaktifkan tidak dapat dihapus, maka Disk tersebut akan disimpan dengan aman hingga dapat dimusnahkan. Setiap fasilitas diaudit secara berkala untuk memantau kepatuhan terhadap Kebijakan Penghapusan Disk.

4. Keamanan Personel

Personel Google diwajibkan berperilaku sesuai dengan pedoman perusahaan mengenai kerahasiaan, etika bisnis, penggunaan yang pantas, dan standar profesional. Google melakukan pemeriksaan latar belakang yang wajar sejauh diizinkan secara hukum dan sesuai dengan undang-undang ketenagakerjaan setempat serta peraturan perundang-undangan yang berlaku.

Personel Google diwajibkan untuk menandatangani perjanjian kerahasiaan dan harus mengakui penerimaan dari, dan kepatuhan terhadap, kebijakan kerahasiaan dan privasi Google. Personel diberikan pelatihan keamanan. Personel yang menangani Data Pelanggan diharuskan melengkapi persyaratan tambahan yang sesuai dengan peran mereka (misalnya sertifikasi). Personel Google tidak akan memproses Data Pelanggan tanpa izin.

5. Keamanan Subprosesor

Sebelum merekrut Subprosesor, Google melakukan audit terhadap praktik keamanan dan privasi Subprosesor untuk memastikan Subprosesor memberikan tingkat keamanan dan privasi yang sesuai dengan akses mereka ke data dan ruang lingkup layanan yang mereka sediakan. Setelah Google telah menilai risiko yang ditunjukkan oleh Subprosesor, maka tunduk pada persyaratan yang dijelaskan dalam Bagian 11.3 (Persyaratan untuk Keterlibatan Subprosesor), Subprosesor wajib menandatangani ketentuan kontrak keamanan, kerahasiaan, dan privasi yang sesuai.

Lampiran 3: Hukum Privasi Khusus

Ketentuan dalam setiap sub-bagian dari Lampiran 3 ini hanya berlaku jika hukum terkait berlaku pada pemrosesan Data Pribadi Pelanggan.

Hukum Perlindungan Data Eropa

1. Definisi Tambahan.

- “Negara Yang Memadai” berarti:

(a) untuk data yang diproses sesuai dengan GDPR UE: Wilayah Ekonomi Eropa (European Economic Area), atau negara atau wilayah yang diakui menjamin perlindungan yang memadai berdasarkan GDPR UE;

(b) untuk data yang diproses sesuai dengan GDPR Inggris Raya: Inggris Raya, atau negara atau wilayah yang diakui menjamin perlindungan yang memadai berdasarkan GDPR Inggris Raya dan Undang-Undang Perlindungan Data 2018 (Data Protection Act 2018); atau

(c) untuk data yang diproses sesuai dengan FADP Swiss: Swiss, atau negara atau wilayah yang: (i) termasuk dalam daftar negara bagian yang undang-undangnya menjamin perlindungan yang memadai sebagaimana diterbitkan oleh Komisararis Perlindungan Data dan Informasi Federal Swiss (Swiss Federal Data Protection and Information Commissioner), jika berlaku; atau (ii) diakui menjamin perlindungan yang memadai oleh Dewan Federal Swiss (Swiss Federal Council) berdasarkan FADP Swiss;

dalam setiap hal, selain berdasarkan kerangka perlindungan data opsional.

- “Solusi Transfer Alternatif” berarti solusi, selain SCC, yang memungkinkan transfer data pribadi secara sah ke negara ketiga sesuai dengan Hukum Perlindungan Data Eropa, misalnya kerangka perlindungan data yang diakui untuk memastikan bahwa entitas yang berpartisipasi memberikan perlindungan yang memadai.
- “SCC Pelanggan” berarti SCC (Pengendali-ke-Prosesor), SCC (Prosesor-ke-Prosesor), atau SCC (Prosesor-ke-Pengendali), sebagaimana berlaku.
- “SCC” berarti SCC Pelanggan atau SCC (Prosesor-ke-Prosesor, Google Eksportir), sebagaimana berlaku.
- “SCC (Pengendali-ke-Prosesor)” berarti ketentuan di:
<https://cloud.google.com/terms/sccs/eu-c2p>
- “SCC (Prosesor-ke-Pengendali)” berarti ketentuan di:
<https://cloud.google.com/terms/sccs/eu-p2c>
- “SCC (Prosesor-ke-Prosesor)” berarti ketentuan di:
<https://cloud.google.com/terms/sccs/eu-p2p>

- “SCC (Prosesor-ke-Prosesor, Google Eksportir)” berarti ketentuan di:
<https://cloud.google.com/terms/sccs/eu-p2p-google-exporter>

2. Pemberitahuan Instruksi. Tanpa mengesampingkan kewajiban Google berdasarkan Bagian 5.2 (Kepatuhan terhadap Instruksi Pelanggan) atau hak atau kewajiban lain apa pun dari salah satu pihak berdasarkan Perjanjian yang berlaku, Google akan segera memberitahukan Pelanggan jika, menurut pendapat Google:

- a. Hukum Eropa melarang Google mematuhi Instruksi;
- b. suatu Instruksi tidak mematuhi Hukum Perlindungan Data Eropa; atau
- c. Google tidak dapat mematuhi Instruksi,

dalam setiap hal kecuali pemberitahuan tersebut dilarang oleh Hukum Eropa.

Jika Pelanggan adalah prosesor, Pelanggan akan segera meneruskan kepada pengendali yang relevan setiap pemberitahuan yang diberikan oleh Google berdasarkan bagian ini.

3. Hak Audit Pelanggan. Google akan mengizinkan Pelanggan atau auditor independen yang ditunjuk oleh Pelanggan untuk melakukan audit (termasuk inspeksi) sebagaimana dijelaskan dalam Bagian 7.5.2(a) (Audit Pelanggan). Selama audit tersebut, Google akan menyediakan seluruh informasi yang diperlukan untuk menunjukkan kepatuhan terhadap kewajibannya berdasarkan Adendum ini dan berkontribusi pada audit sebagaimana dijelaskan dalam Bagian 7.5 (Peninjauan dan Audit Kepatuhan) dan bagian ini.

4. Transfer Data.

4.1 Transfer Yang Dibatasi. Para pihak mengakui bahwa Hukum Perlindungan Data Eropa tidak mewajibkan SCC atau Solusi Transfer Alternatif agar Data Pribadi Pelanggan dapat diproses atau ditransfer ke Negara Yang Memadai. Jika Data Pribadi Pelanggan ditransfer ke negara lain mana pun dan Hukum Perlindungan Data Eropa berlaku untuk transfer tersebut (sebagaimana disertifikasi oleh Pelanggan berdasarkan Bagian 4.2 (Sertifikasi oleh Pelanggan Non-EMEA) dari ketentuan Hukum Perlindungan Data Eropa ini, jika alamat penagihannya berada di luar EMEA) (“Transfer Yang Dibatasi”), maka:

- a. jika Google telah menerapkan Solusi Transfer Alternatif untuk Transfer Yang Dibatasi apa pun, Google akan memberitahukan Pelanggan mengenai solusi yang relevan dan memastikan bahwa Transfer Yang Dibatasi tersebut dilakukan sesuai dengan solusi tersebut; atau
- b. jika Google belum menerapkan Solusi Transfer Alternatif untuk Transfer Yang Dibatasi apa pun, atau memberitahukan Pelanggan bahwa Google tidak lagi menerapkan Solusi Transfer Alternatif untuk Transfer Yang Dibatasi apa pun (tanpa menggunakan Solusi Transfer Alternatif pengganti):
 - i. jika alamat Google berada di Negara Yang Memadai:

- a. SCC (Prosesor-ke-Prosesor, Google Eksportir) akan berlaku sehubungan dengan Transfer Yang Dibatasi tersebut dari Google ke Subprosesor; dan

b. selain itu, jika alamat penagihan Pelanggan tidak berada di Negara Yang Memadai, SCC (Prosesor-ke-Pengendali) akan berlaku (terlepas dari apakah Pelanggan adalah pengendali atau prosesor) sehubungan dengan Transfer Yang Dibatasi antara Google dan Pelanggan; atau

ii. jika alamat Google tidak berada di Negara Yang Memadai, SCC (Pengendali-ke-Prosesor) atau SCC (Prosesor-keProsesor) akan berlaku (sesuai dengan apakah Pelanggan adalah pengendali atau prosesor) sehubungan dengan Transfer Yang Dibatasi tersebut antara Google dan Pelanggan.

4.2 Sertifikasi oleh Pelanggan Non-EMEA. Jika alamat penagihan Pelanggan berada di luar EMEA, dan pemrosesan Data Pribadi Pelanggan tunduk pada Hukum Perlindungan Data Eropa, maka kecuali Lampiran 4 (Produk Khusus) dari Adendum ini menyatakan sebaliknya, Pelanggan akan menyatakan hal tersebut dan mengidentifikasi Otoritas Pengawasnya yang kompeten melalui Konsol Admin untuk Layanan yang berlaku.

4.3 Informasi Mengenai Transfer Yang Dibatasi. Google akan memberikan informasi yang relevan kepada Pelanggan mengenai Transfer Yang Dibatasi, Pengendalian Keamanan Tambahan, dan tindakan perlindungan tambahan lainnya:

a. sebagaimana dijelaskan dalam Bagian 7.5.1 (Peninjauan Dokumentasi Keamanan);

b. di lokasi tambahan mana pun yang dijelaskan dalam Lampiran 4 (Produk Khusus); dan

c. sehubungan dengan penerapan Solusi Transfer Alternatif oleh Google, di <https://cloud.google.com/terms/alternative-transfer-solution>.

4.4 Audit SCC. Jika SCC Pelanggan berlaku sebagaimana dijelaskan dalam Bagian 4.1 (Transfer Yang Dibatasi) dari ketentuan Hukum Perlindungan Data Eropa ini, Google akan mengizinkan Pelanggan (atau auditor independen yang ditunjuk oleh Pelanggan) untuk melakukan audit sebagaimana dijelaskan dalam SCC tersebut dan, selama audit, menyediakan seluruh informasi yang diperlukan oleh SCC tersebut, keduanya sesuai dengan Bagian 7.5.3 (Ketentuan Bisnis Tambahan untuk Peninjauan dan Audit).

4.5 Pemberitahuan SCC. Pelanggan akan meneruskan kepada pengendali yang relevan dengan segera dan tanpa penundaan, pemberitahuan apa pun yang merujuk pada SCC mana pun.

4.6 Pengakhiran Karena Risiko Transfer Data. Jika Pelanggan menyimpulkan, berdasarkan penggunaan Layanan saat ini atau yang dimaksudkan, bahwa perlindungan yang sesuai tidak diberikan untuk Data Pribadi Pelanggan yang ditransfer, maka Pelanggan dapat segera mengakhiri Perjanjian sesuai dengan ketentuan pengakhiran tanpa alasan dari Perjanjian yang berlaku atau, jika tidak terdapat ketentuan tersebut, dengan memberitahukan Google.

4.7 Tidak Ada Modifikasi SCC. Tidak ada ketentuan dalam Perjanjian ini (termasuk Adendum ini) yang dimaksudkan untuk mengubah atau bertentangan dengan SCC atau mengurangi hak-hak dasar atau kebebasan subjek data berdasarkan Hukum Perlindungan Data Eropa.

4.8 Prioritas SCC. Apabila terdapat pertentangan atau ketidakkonsistenan antara SCC Pelanggan mana pun (yang dimasukkan sebagai referensi ke dalam Adendum ini) dan bagian lain dalam Perjanjian (termasuk Adendum ini), SCC Pelanggan adalah yang akan berlaku.

5. Persyaratan untuk Keterlibatan Subprosesor. Hukum Perlindungan Data Eropa mewajibkan Google untuk memastikan melalui kontrak tertulis bahwa kewajiban perlindungan data yang dijelaskan dalam Adendum ini, sebagaimana dimaksud dalam Pasal 28(3) GDPR, jika berlaku, diberlakukan pada Subprosesor mana pun yang dilibatkan oleh Google.

CCPA

1. Definisi Tambahan.

- *“CCPA”* berarti Undang-Undang Privasi Konsumen California Tahun 2018 (California Consumer Privacy Act of 2018), sebagaimana diubah, termasuk sebagaimana diubah oleh Undang-Undang Hak Privasi California Tahun 2020 (California Privacy Rights Act of 2020), beserta seluruh peraturan pelaksanaannya.
- *“Data Pribadi Pelanggan”* mencakup *“informasi pribadi”*.
- Istilah *“bisnis”, “tujuan bisnis”, “konsumen”, “informasi pribadi”, “pemrosesan”, “penjualan”, “menjual”, “penyedia layanan”, dan “berbagi”* memiliki arti yang diberikan dalam CCPA.

2. Larangan. Tanpa mengesampingkan kewajiban Google berdasarkan Bagian 5.2 (Kepatuhan terhadap Instruksi Pelanggan), sehubungan dengan pemrosesan Data Pribadi Pelanggan sesuai dengan CCPA, Google tidak akan, kecuali diizinkan berdasarkan CCPA:

a. menjual atau membagikan Data Pribadi Pelanggan;

b. menyimpan, menggunakan, atau mengungkapkan Data Pribadi Pelanggan:

i. selain untuk tujuan bisnis berdasarkan CCPA atas nama Pelanggan dan untuk tujuan khusus dalam melaksanakan Layanan dan TSS (jika berlaku); atau

ii. di luar hubungan bisnis langsung antara Google dan Pelanggan; atau

c. menggabungkan atau memperbarui Data Pribadi Pelanggan dengan informasi pribadi yang diterima Google dari atau atas nama pihak ketiga atau dikumpulkan dari interaksinya sendiri dengan konsumen.

3. Kepatuhan. Tanpa mengesampingkan kewajiban Google berdasarkan Bagian 5.2 (Kepatuhan terhadap Instruksi Pelanggan) atau hak atau kewajiban lain apa pun dari salah satu pihak berdasarkan Perjanjian yang berlaku, Google akan memberitahukan Pelanggan jika, menurut pendapat Google, Google tidak dapat memenuhi kewajibannya berdasarkan CCPA, kecuali jika pemberitahuan tersebut dilarang oleh hukum yang berlaku.

4. Intervensi Pelanggan. Jika Google memberitahukan Pelanggan mengenai setiap penggunaan Data Pribadi Pelanggan yang tidak sah, termasuk berdasarkan Bagian 3 (Kepatuhan) sub-bagian ini atau Bagian 7.2.1 (Pemberitahuan Insiden), Pelanggan dapat mengambil langkah-langkah yang wajar dan sesuai untuk menghentikan atau memulihkan setiap penggunaan tidak sah tersebut dengan:

a. mengambil tindakan apa pun yang direkomendasikan oleh Google sesuai dengan Bagian 7.2.2 (Rincian Insiden Data), jika berlaku; atau

b. melaksanakan haknya berdasarkan Bagian 7.5.2(a) (Audit Pelanggan) atau 9.1 (Akses; Perbaikan; Pemrosesan Yang Dibatasi; Portabilitas).

Turki

1. Definisi Tambahan.

- *“Hukum Perlindungan Data Turki”* berarti Undang-Undang Turki tentang Perlindungan Data Pribadi No. 6698 (Turkish Law on the Protection of Personal Data No. 6698) tanggal 7 April 2016.
- *“Otoritas Perlindungan Data Pribadi Turki”* berarti Kişisel Verileri Koruma Kurumu.
- *“SCC Turki”* berarti klausul kontrak standar berdasarkan Hukum Perlindungan Data Turki.

2. Transfer Data.

2.1 Ketentuan Tambahan. Jika alamat penagihan Pelanggan berada di Turki dan Google menyediakan ketentuan tambahan opsional apa pun (termasuk SCC Turki) untuk disetujui oleh Pelanggan sehubungan dengan transfer Data Pribadi Pelanggan berdasarkan Hukum Perlindungan Data Turki, ketentuan tersebut akan melengkapi Adendum ini sejak tanggal ketentuan tersebut diberitahukan oleh Otoritas Perlindungan Data Pribadi Turki sesuai dengan Bagian 2.2 (Pemberitahuan kepada Otoritas Yang Berwenang).

2.2 Pemberitahuan kepada Pejabat Yang Berwenang. Jika Pelanggan menandatangani SCC Turki berdasarkan Bagian 2 (Transfer Data) ini dan Hukum Perlindungan Data Turki mewajibkan pemberitahuan kepada Otoritas Perlindungan Data Pribadi Turki mengenai penggunaan SCC Turki, Pelanggan akan bertanggung jawab untuk memberikan pemberitahuan tersebut dalam waktu lima (5) hari sejak penandatanganan SCC Turki.

2.3 Audit SCC. Jika Pelanggan menandatangani SCC Turki berdasarkan Bagian 2 (Transfer Data) ini, Google akan mengizinkan Pelanggan (atau auditor independen yang ditunjuk oleh Pelanggan) untuk melakukan audit seperti yang dijelaskan dalam SCC tersebut dan, selama audit, menyediakan seluruh informasi yang diperlukan oleh SCC tersebut, keduanya sesuai dengan Bagian 7.5.3 (Ketentuan Bisnis Tambahan untuk Peninjauan dan Audit).

2.4 Pengakhiran Karena Risiko Transfer Data. Jika Pelanggan menyimpulkan, berdasarkan penggunaan Layanan saat ini atau yang dimaksudkan, bahwa perlindungan yang sesuai tidak diberikan untuk Data Pribadi Pelanggan yang ditransfer, maka Pelanggan dapat segera mengakhiri Perjanjian yang berlaku sesuai dengan ketentuan pengakhiran tanpa alasan dari Perjanjian tersebut atau, jika tidak terdapat ketentuan tersebut, dengan memberitahukan Google.

2.5 Tidak Ada Modifikasi SCC Turki. Tidak ada ketentuan apa pun dalam Perjanjian ini (termasuk Adendum ini) yang dimaksudkan untuk mengubah atau bertentangan dengan SCC Turki atau mengurangi hak-hak dasar atau kebebasan subjek data berdasarkan Hukum Perlindungan Data Turki.

2.6 Prioritas SCC. Apabila terdapat pertentangan atau ketidakkonsistenan antara SCC Turki (yang akan dimasukkan melalui referensi ke dalam Adendum ini jika disepakati oleh Pelanggan) dan bagian lain Perjanjian (termasuk Adendum ini), SCC Turki akan berlaku.

Israel

1. Definisi Tambahan.

- *"Hukum Perlindungan Privasi Israel"* berarti Undang-Undang Perlindungan Privasi Israel tahun 1981 (Israeli Privacy Protection Law, 1981) dan setiap peraturan yang diundangkan berdasarkan undang-undang tersebut.

2. Istilah Setara. Istilah apa pun yang setara dengan "pengendali", "data pribadi", "pemrosesan", dan "prosesor", sebagaimana digunakan dalam Adendum ini, memiliki arti sebagaimana ditentukan dalam Hukum Perlindungan Privasi Israel.

3. Hak Audit Pelanggan. Google akan mengizinkan Pelanggan atau auditor independen yang ditunjuk oleh Pelanggan untuk melakukan audit (termasuk inspeksi) sebagaimana dijelaskan dalam Bagian 7.5.2(a) (Audit Pelanggan).

Lampiran 4: Produk Khusus

Ketentuan dalam setiap sub-bagian Lampiran 4 ini hanya berlaku sehubungan dengan pemrosesan Data Pelanggan oleh Layanan(-Layanan) terkait.

Google Cloud Platform

1. Definisi Tambahan.

- *"Akun"*, jika tidak didefinisikan dalam Perjanjian, berarti akun Google Cloud Platform Pelanggan.
- *"Data Pelanggan"*, jika tidak didefinisikan dalam Perjanjian, berarti data yang diberikan kepada Google oleh Pelanggan atau Pengguna Akhir melalui Google Cloud Platform dalam Akun, dan data yang diperoleh Pelanggan atau Pengguna Akhir dari data tersebut melalui penggunaan Google Cloud Platform.
- *"Google Cloud Platform"* berarti layanan Google Cloud Platform yang dijelaskan di <https://cloud.google.com/terms/services>, tidak termasuk Penawaran Pihak Ketiga mana pun.
- *"Penawaran Pihak Ketiga"*, jika tidak didefinisikan dalam Perjanjian, berarti (a) layanan, perangkat lunak, produk, dan penawaran pihak ketiga lainnya yang tidak dimasukkan ke dalam Google Cloud Platform atau Perangkat Lunak, (b) penawaran yang diidentifikasi dalam bagian "Persyaratan Pihak Ketiga" dari Ketentuan Khusus Layanan dalam Perjanjian, dan (c) sistem operasi pihak ketiga.

2. Sertifikasi Kepatuhan. Sertifikasi Kepatuhan untuk Layanan Audit Google Cloud Platform juga akan mencakup sertifikat ISO 27017 dan ISO 27018 serta Pengesahan Kepatuhan PCI DSS.

3. Lokasi Pusat Data. Lokasi pusat data Google Cloud Platform dijelaskan di <https://cloud.google.com/about/locations/>.

4. Informasi Mengenai Subprosesor. Nama, lokasi dan aktivitas Subprosesor Google Cloud Platform dijelaskan di <https://cloud.google.com/terms/subprocessors>.

5. Tim Perlindungan Data Cloud. Tim Perlindungan Data untuk Google Cloud Platform dapat dihubungi di <https://support.google.com/cloud/contact/dpo>.

6. Informasi mengenai Transfer yang Dibatasi. Informasi tambahan terkait dengan Transfer Yang Dibatasi, Pengendalian Keamanan Tambahan, dan langkah-langkah perlindungan tambahan lainnya tersedia di cloud.google.com/privacy/.

7. Ketentuan Khusus Layanan.

Solusi Bare Metal (Google Cloud Platform)

Solusi Bare Metal memberikan akses yang tidak di-virtualisasi ke sumber daya infrastruktur yang mendasarinya dan, secara desain, memiliki karakteristik tertentu yang berbeda.

1. Amendemen. Adendum ini diamendemen sebagai berikut sehubungan dengan Solusi Bare Metal:

- Definisi “Auditor Pihak Ketiga Google” diganti dengan yang berikut:
 - “Auditor Pihak Ketiga Google” berarti auditor pihak ketiga yang memenuhi syarat dan independen yang ditunjuk oleh Google atau Subprosesor Solusi Bare Metal, yang identitasnya saat itu akan diungkapkan oleh Google kepada Pelanggan berdasarkan permintaan.
- Ketentuan berikut dihapus:
 - Dari Bagian 7.1.1 (Langkah-Langkah Keamanan Google), frasa “enkripsi data pribadi”;
 - Dari Lampiran 2 (Langkah-Langkah Keamanan), sub-bagian Bagian 1(a) berjudul “Sistem Operasi Server” dan “Kelangsungan Bisnis”;
 - Dari Lampiran 2, sub-bagian Bagian 1(b) berjudul “Permukaan Serangan Eksternal”, “Deteksi Intrusi”, dan “Teknologi Enkripsi”; dan
 - Dari Lampiran 2, kalimat-kalimat Bagian 3(a) berikut ini:
 - Google menyimpan data dalam lingkungan beberapa penyewa di server milik Google. Tunduk pada instruksi Pelanggan yang menyatakan sebaliknya (misalnya, dalam bentuk pemilihan lokasi data), Google mereplikasi Data Pelanggan di beberapa pusat data yang tersebar secara geografis.

2. Sertifikasi Kepatuhan dan Laporan SOC. Google atau Subprosesornya akan mempertahankan setidaknya hal-hal berikut (atau alternatif yang setara atau lebih baik) untuk Solusi Bare Metal untuk memverifikasi efektivitas berkelanjutan dari Langkah-Langkah Keamanan:

a. sertifikat ISO 27001 dan Pengesahan Kepatuhan PCI DSS (“Sertifikasi Kepatuhan BMS”); dan

b. SOC 1 dan laporan SOC 2 diperbarui setiap tahun berdasarkan audit yang dilakukan setidaknya sekali setiap 12 bulan (“Laporan SOC BMS”).

3. Peninjauan Dokumentasi Keamanan. Untuk menunjukkan kepatuhan Google terhadap kewajibannya berdasarkan Adendum ini, Google akan menyediakan Sertifikasi Kepatuhan BMS dan Laporan SOC BMS untuk ditinjau oleh Pelanggan dan, jika Pelanggan adalah prosesor, mengizinkan Pelanggan untuk meminta akses ke Laporan SOC BMS kepada pengendali yang relevan sesuai dengan Bagian 7.5.3 (Ketentuan Bisnis Tambahan untuk Peninjauan dan Audit).

4. Kewajiban Pelanggan. Tanpa membatasi kewajiban tersurat Google terkait dengan Solusi Bare Metal, Pelanggan akan mengambil langkah-langkah yang wajar untuk melindungi dan menjaga keamanan Data Pelanggan dan setiap konten lainnya yang disimpan dalam atau diproses melalui Solusi Bare Metal.

5. Penafian. Tanpa mengesampingkan ketentuan apa pun yang bertentangan dalam Perjanjian (termasuk Adendum ini), Google tidak bertanggung jawab atas hal-hal berikut sehubungan dengan Solusi Bare Metal:

- a. keamanan non-fisik, seperti pengendalian akses, enkripsi, firewall, perlindungan antivirus, deteksi ancaman, dan pemindaian keamanan;
- b. pencatatan dan pemantauan;
- c. pemeliharaan atau dukungan non-perangkat keras;
- d. pencadangan data, termasuk setiap redundansi atau konfigurasi ketersediaan yang tinggi; atau
- e. keberlanjutan bisnis dan kebijakan atau prosedur pemulihan bencana.

Pelanggan sepenuhnya bertanggung jawab untuk mengamankan (selain keamanan fisik server Solusi Bare Metal), mencatat dan memantau, memelihara dan mendukung, serta mencadangkan Sistem Operasi, Data Pelanggan, perangkat lunak, dan aplikasi apa pun yang Pelanggan gunakan, unggah ke, atau host di Solusi Bare Metal.

Cloud NGFW (Google Cloud Platform)

Edisi Cloud NGFW dengan judul “Cloud NGFW Enterprise” (“CNE”) dirancang untuk memitigasi risiko keamanan siber dan, dengan demikian, memiliki karakteristik tertentu yang berbeda.

1. Amendemen. Adendum ini diamendemen sebagai berikut sehubungan dengan CNE:

- Bagian 6.1 (Penghapusan oleh Pelanggan) dan 6.2 (Pengembalian atau Penghapusan Saat Jangka Waktu Berakhir) tidak akan mencegah Google atau Subprosesor untuk menyimpan file atau paket lalu lintas jaringan apa pun yang dikirimkan untuk tujuan TSS dan ditetapkan oleh CNE sebagai ancaman keamanan, dengan ketentuan bahwa file atau pengambilan paket lalu lintas jaringan tidak termasuk Data Pribadi Pelanggan.

Google Distributed Cloud terhubung (Google Cloud Platform)

Google Distributed Cloud connected (“GDCE”) tidak ditempatkan di pusat data Google dan, secara desain, memiliki karakteristik tertentu yang berbeda.

1. Amendemen. Amendemen ini diubah sebagai berikut sehubungan dengan Google Distributed Cloud connected:

- Rujukan ke “sistem Google” diganti dengan “Peralatan”.
- Bagian 6.2 (Pengembalian atau Penghapusan Saat Jangka Waktu Berakhir) diganti dengan ketentuan berikut:
 - *6.2 Pengembalian atau Penghapusan pada akhir Jangka Waktu.* Pelanggan menginstruksikan Google untuk menghapus seluruh Data Pelanggan yang tersisa (termasuk salinan yang ada) dari Peralatan di akhir Jangka Waktu sesuai dengan hukum yang berlaku. Jika Pelanggan ingin menyimpan Data Pelanggan apa pun setelah Jangka Waktu berakhir, Pelanggan dapat mengekspor atau membuat salinan data tersebut sebelum Jangka Waktu berakhir. Google akan mematuhi Instruksi dalam Bagian 6.2 ini sesegera mungkin dan dalam jangka waktu maksimum 180 hari, kecuali Hukum Eropa mewajibkan penyimpanan, jika Hukum Perlindungan Data Eropa berlaku, atau hukum yang berlaku mengharuskan penyimpanan, jika Hukum Privasi Yang Berlaku lainnya berlaku.
- Kata-kata berikut ditambahkan pada akhir Bagian 10.1 (Penyimpanan Data dan Fasilitas Pemrosesan): “atau di mana Lokasi Pelanggan berada.”
- Bagian 1 (Pusat Data dan Keamanan Jaringan) dari Lampiran 2 (Langkah-Langkah Keamanan) diganti dengan ketentuan berikut:
 - **1. Mesin Setempat dan Keamanan Jaringan**

Mesin Setempat. Data Pelanggan hanya disimpan pada Peralatan untuk ditempatkan di Lokasi Pelanggan.

Sistem Operasi Server. Server Google menggunakan implementasi berbasis Linux yang disesuaikan untuk lingkungan aplikasi. Google menggunakan proses peninjauan kode untuk meningkatkan keamanan kode yang digunakan untuk menyediakan Google Distributed Cloud connected dan meningkatkan keamanan produk di lingkungan produksi Google Distributed Cloud connected.

Teknologi Enkripsi. Google menyediakan enkripsi HTTPS (juga disebut sebagai koneksi SSL atau TLS) dan memungkinkan enkripsi data pada saat transit. Server Google mendukung pertukaran kunci kriptografi Diffie-Hellman ephemeral elliptic curve sementara yang ditandatangani dengan RSA dan ECDSA. Metode perfect forward secrecy (PFS) ini membantu melindungi lalu lintas dan meminimalkan dampak kunci yang disusupi, atau pembobolan kriptografi. Google juga menyediakan enkripsi data pada saat tidak digunakan, menggunakan setidaknya AES128 atau yang serupa. Google Distributed Cloud connected memiliki integrasi CMEK; informasi lebih lanjut dapat ditemukan di <https://cloud.google.com/kms/docs/cmek>.

Koneksi ke Cloud VPN. Google mengizinkan Pelanggan untuk mengaktifkan dan mengonfigurasi interkoneksi terenkripsi yang kuat antara Peralatan dan Virtual Private Cloud Pelanggan menggunakan Cloud VPN melalui koneksi IPSEC VPN.

Penyimpanan Terikat. Penyimpanan data Pelanggan terikat pada server. Jika disk dicuri atau disalin saat tidak digunakan, konten disk tersebut tidak dapat dipulihkan di luar server.

- Bagian 2 (Akses dan Pengendalian Situs) dan 3 (Data) dari Lampiran 2 (Langkah-Langkah Keamanan) dihapus.

2. Ketentuan yang Tidak Berlaku. Setiap kewajiban Google dalam Perjanjian (termasuk Adendum ini) atau pernyataan dalam dokumentasi keamanan terkait (termasuk *whitepaper*) yang bergantung pada pengoperasian pusat data Google tidak berlaku untuk Google Distributed Cloud connected.

Google-Managed Multi-Cloud (Google Cloud Platform)

Layanan Google-Managed Multi-Cloud melibatkan infrastruktur pihak ketiga dan, secara desain, memiliki karakteristik tertentu yang berbeda.

1. Definisi Tambahan.

- “Amendemen Google-Managed MCS Data Processing” berarti ketentuan di <https://cloud.google.com/terms/mcs-data-processing-terms>.

2. Ketentuan Multi-Cloud Data Processing. Amandemen Pemrosesan Data MCS yang Dikelola Google melengkapi dan mengubah Adendum ini sehubungan dengan Layanan Google-Managed Multi-Cloud Services untuk Google Cloud Platform.

Google Cloud VMware Engine (Google Cloud Platform)

Google mungkin tidak memiliki akses ke lingkungan VMware Pelanggan atau tidak dapat mengenkripsi data pribadi di lingkungan VMware Pelanggan.

NetApp Volumes (Google Cloud Platform)

1. Amendemen. Adendum ini diamendemen sebagai berikut sehubungan dengan NetApp Volumes:

- Definisi “Auditor Pihak Ketiga Google” diganti sebagai berikut:
 - “*Auditor Pihak Ketiga Google*” berarti auditor pihak ketiga yang memenuhi syarat dan independen yang ditunjuk oleh Google atau Subprosesor NetApp Volumes, yang identitasnya akan diungkapkan oleh Google kepada Pelanggan berdasarkan permintaan.
- Bagian 3(a) (Penyimpanan Data, Isolasi dan Pencatatan) dari Lampiran 2 (Langkah-Langkah Keamanan) diganti dengan yang berikut ini:
 - (a) *Penyimpanan Data, Isolasi dan Pencatatan.* Google menyimpan data dalam lingkungan beberapa penyewa di server milik NetApp, Inc. Dengan tunduk pada

Instruksi apa pun yang bertentangan (misalnya dalam bentuk pemilihan lokasi data), Google mereplikasi Data Pelanggan di antara beberapa pusat data yang tersebar secara geografis. Google juga mengisolasi Data Pelanggan secara logis. Pelanggan akan diberikan kendali atas kebijakan berbagi data tertentu. Kebijakan tersebut, sesuai dengan fungsionalitas Layanan, akan memungkinkan Pelanggan untuk menentukan pengaturan berbagi produk yang berlaku bagi Pengguna Akhirnya untuk tujuan tertentu. Pelanggan dapat memilih untuk menggunakan fungsionalitas pencatatan yang disediakan Google melalui Layanan.

2. Sertifikasi Kepatuhan dan Laporan SOC. Google atau Subprosesornya akan mendapatkan setidaknya hal berikut (atau alternatif yang setara atau lebih baik) untuk NetApp Volumes:

- a. sertifikat ISO 27001 dan Pengesahan Kepatuhan PCI DSS ("*Sertifikasi Kepatuhan NetApp*"); dan
- b. Laporan SOC 1 dan SOC 2 diperbarui setiap tahun berdasarkan audit yang dilakukan setidaknya sekali setiap 12 bulan ("*Laporan SOC NetApp*").

3. Peninjauan Dokumentasi Keamanan. Untuk menunjukkan kepatuhan Google terhadap kewajibannya berdasarkan Adendum ini, Google akan menyediakan Sertifikasi Kepatuhan NetApp dan Laporan SOC NetApp untuk ditinjau oleh Pelanggan dan, jika Pelanggan adalah pemroses, mengizinkan Pelanggan untuk meminta akses ke Laporan SOC NetApp kepada pengendali yang relevan sesuai dengan Bagian 7.5.3 (Ketentuan Bisnis Tambahan untuk Peninjauan dan Audit).

Google Workspace dan Cloud Identity

1. Definisi Tambahan.

- "*Akun*", jika tidak didefinisikan dalam Perjanjian, berarti akun Google Workspace atau Cloud Identity milik Pelanggan.
- "*Cloud Identity*" jika dibeli berdasarkan Perjanjian yang berdiri sendiri dan bukan sebagai bagian dari Google Cloud Platform atau Google Workspace, berarti Layanan Cloud Identity yang dijelaskan di <https://cloud.google.com/terms/identity/user-features>.
- "*Data Pelanggan*", jika tidak didefinisikan dalam Perjanjian, berarti data yang diajukan, disimpan, dikirim, atau diterima oleh atau atas nama Pelanggan atau Pengguna Akhirnya melalui Google Workspace atau Cloud Identity dalam Akun.
- "*Google Workspace*" berarti layanan Google Workspace atau Google Workspace for Education yang dijelaskan di https://workspace.google.com/terms/user_features.html, sebagaimana berlaku.

2. Produk Tambahan. Jika Google atas pilihannya sendiri menyediakan Produk Tambahan bagi Pelanggan untuk digunakan dengan Google Workspace atau Cloud Identity sesuai dengan Ketentuan Produk Tambahan yang berlaku:

a. Pelanggan dapat mengaktifkan atau menonaktifkan Produk Tambahan melalui Konsol Admin dan tidak perlu menggunakan Produk Tambahan untuk menggunakan Google Workspace atau Cloud Identity; dan

b. jika Pelanggan memilih untuk memasang Produk Tambahan apa pun atau menggunakannya dengan Google Workspace atau Cloud Identity, Produk Tambahan tersebut dapat mengakses Data Pelanggan sebagaimana diperlukan untuk interoperasi dengan Google Workspace atau Cloud Identity, sebagaimana berlaku.

Untuk kejelasan, Adendum ini tidak berlaku untuk pemrosesan data pribadi sehubungan dengan penyediaan Produk Tambahan yang dipasang atau digunakan oleh Pelanggan, termasuk data pribadi yang dikirimkan ke atau dari Produk Tambahan tersebut.

3. Sertifikasi Kepatuhan. Sertifikasi Kepatuhan untuk Google Workspace dan Layanan Cloud Identity Audited juga akan mencakup sertifikat untuk ISO 27017 dan ISO 27018.

4. Lokasi Pusat Data. Lokasi pusat data Google Workspace dan Cloud Identity dijelaskan di <https://www.google.com/about/datacenters/locations/>.

5. Informasi Mengenai Subprosesor. Nama, lokasi, dan aktivitas Subprosesor Google Workspace dan Cloud Identity dijelaskan di <https://workspace.google.com/intl/en/terms/subprocessors.html>.

6. Tim Perlindungan Data Cloud. Tim Perlindungan Data untuk Google Workspace dan Cloud Identity (saat Administrator masuk ke Akun Admin mereka) dapat dihubungi di https://support.google.com/a/contact/googlecloud_dpr.

7. Langkah-Langkah Keamanan Tambahan. Untuk Google Workspace dan Cloud Identity:

a. Google secara logis memisahkan data setiap Pengguna Akhir dari data Pengguna Akhir lainnya; dan

b. data untuk Pengguna Akhir yang diautentikasi tidak akan ditampilkan kepada Pengguna Akhir lainnya (kecuali Pengguna Akhir sebelumnya atau Administrator mengizinkan data tersebut untuk dibagikan).

8. Informasi Mengenai Transfer Yang Dibatasi. Informasi tambahan yang relevan dengan Transfer Yang Dibatasi, Pengendalian Keamanan Tambahan, dan tindakan perlindungan tambahan lainnya tersedia di cloud.google.com/privacy/.

9. Adendum Data Layanan. Jika Google menyediakan Adendum Data Layanan opsional untuk diterima oleh Pelanggan sehubungan dengan Adendum ini, ketersediaan Adendum opsional tersebut akan dianggap sebagai "Pembaruan DPA" jika istilah tersebut didefinisikan dalam Adendum Data Layanan yang sebelumnya ditandatangani oleh Pelanggan.

10. Ketentuan Khusus Layanan.

AppSheet (Google Workspace)

1. Amendemen. Adendum ini diubah sebagai berikut sehubungan dengan AppSheet:

- Paragraf berjudul “Sistem Operasi Server” di Bagian 1(a) Lampiran 2 (Langkah-Langkah Keamanan) diganti dengan yang berikut ini:
 - *Sistem Operasi Server*. Server Google menggunakan implementasi berbasis Linux yang disesuaikan untuk lingkungan aplikasi.

2. Lokasi Pusat Data Tambahan. Lokasi pusat data tambahan untuk AppSheet dijelaskan di <https://cloud.google.com/about/locations/>.

Looker (original)

1. Definisi Tambahan.

- “*Konsol Admin*” berarti konsol admin apa pun yang berlaku untuk setiap Instance.
- “*Amendemen Google-Managed MCS Data Processing*” berarti, jika berlaku, ketentuan di <https://cloud.google.com/terms/mcs-data-processing-terms>.
- “*Layanan Google-Managed Multi-Cloud*” berarti, jika berlaku, layanan, produk, dan fitur Google tertentu yang di hosting di infrastruktur penyedia cloud pihak ketiga.
- “*Looker (original)*” berarti platform terintegrasi (termasuk infrastruktur berbasis cloud, jika berlaku, dan komponen perangkat lunak termasuk API terkait) yang memungkinkan bisnis menganalisis data dan menentukan metrik bisnis di berbagai sumber data yang disediakan oleh Google kepada Pelanggan berdasarkan Perjanjian. Looker (original) tidak termasuk Penawaran Pihak Ketiga.
- “*Penyedia Pihak Ketiga Multi-Cloud Service*” memiliki arti sebagaimana tercantum dalam Amendemen Google-Managed MCS Data Processing.
- “*Formulir Pesanan*” memiliki arti yang diberikan dalam Perjanjian, kecuali Pelanggan telah membeli melalui reseller atau marketplace online atau menggunakan Looker hanya untuk tujuan uji coba atau evaluasi berdasarkan perjanjian uji coba atau evaluasi, dalam hal ini Formulir Pesanan dapat berarti bentuk tertulis lainnya (surel atau sarana elektronik lainnya yang diizinkan) sebagaimana diizinkan oleh Google.

2. Amendemen. Adendum ini diamendemen sebagai berikut sehubungan dengan Looker (original):

- Definisi “*Alamat Surel Pemberitahuan*” diganti dengan yang berikut:
 - “*Alamat Surel Pemberitahuan*” berarti alamat(-alamat) surel yang ditentukan oleh Pelanggan dalam Formulir Pesanan atau melalui Looker (sebagaimana berlaku) untuk menerima pemberitahuan tertentu dari Google.
- Definisi “*SCC (Pengendali-ke-Prosesor)*”, “*SCC (Prosesor-ke-Pengendali)*”, “*SCC (Pemroses-ke-Pemroses)*” dan “*SCC (Prosesor-ke-Prosesor, Google Eksporir)*” dalam Lampiran 3 (Hukum Privasi Khusus) diganti dengan:

- “SCC (Pengendali-ke-Prosesor)” berarti ketentuan di: <https://cloud.google.com/terms/looker/legal/sccs/eu-c2p>;
 - “SCC (Prosesor-ke-Pengendali)” berarti ketentuan di: <https://cloud.google.com/terms/looker/legal/sccs/eu-p2c>;
 - “SCC (Prosesor-ke-Prosesor)” berarti ketentuan di: <https://cloud.google.com/terms/looker/legal/sccs/eu-p2p>; dan
 - “SCC (Prosesor-ke-Prosesor, Google Eksportir)” berarti ketentuan di: <https://cloud.google.com/terms/looker/legal/sccs/eu-p2p-intra-group>.
- Kata-kata berikut ditambahkan akhir Bagian 10.1 (Penyimpanan Data dan Fasilitas Pemrosesan):
“atau apabila Penyedia Pihak Ketiga Layanan Multi-Cloud memelihara fasilitas.”

3. Tanggung Jawab Tambahan Keamanan Pelanggan. Pelanggan bertanggung jawab atas keamanan lingkungan, basis data, dan konfigurasi Pelanggan untuk Looker (original) tidak termasuk sistem yang dikelola dan dikendalikan oleh Google.

4. Sertifikasi Kepatuhan dan Laporan SOC. Sertifikasi Kepatuhan dan Laporan SOC untuk Layanan Yang Diaudit Looker (original) asli dapat bervariasi sesuai dengan lingkungan hosting di mana Layanan terkait digunakan. Google akan memberikan rincian Sertifikasi Kepatuhan dan Laporan SOC yang tersedia untuk lingkungan hosting tertentu berdasarkan permintaan.

5. Lokasi Pusat Data. Lokasi pusat data Looker (original) akan dijelaskan pada Formulir Pesanan yang berlaku atau diidentifikasi oleh Google.

6. Tidak Ada Sertifikasi oleh Pelanggan Non-EMEA. Pelanggan tidak berkewajiban untuk mensertifikasi atau mengidentifikasi Otoritas Pengawasnya yang berwenang sebagaimana dijelaskan dalam Bagian 4.2 (Sertifikasi oleh Pelanggan Non-EMEA) ketentuan Perlindungan Data Eropa dalam Lampiran 3 (Hukum Privasi Khusus) untuk Looker (original).

7. Informasi Mengenai Transfer Yang Dibatasi. Informasi tambahan yang relevan dengan Transfer Yang Dibatasi, Pengendalian Keamanan Tambahan, dan tindakan perlindungan tambahan lainnya untuk Looker (original) tersedia di <https://docs.looker.com>.

8. Informasi Mengenai Subprosesor. Nama, lokasi, dan aktivitas Subprosesor untuk Looker (original) dijelaskan di:

- <https://cloud.google.com/terms/looker/privacy/lookeroriginal-subprocessors> dan
- <https://cloud.google.com/terms/subprocessors>.

9. Google-Managed Multi-Cloud (Looker (original))

Layanan Google-Managed Multi-Cloud melibatkan infrastruktur pihak ketiga dan, secara desain, memiliki karakteristik tertentu yang berbeda.

9.1 *Ketentuan Pemrosesan Multi-Cloud Data*. Amendemen Google-Managed MCS Data Processing melengkapi dan mengubah Adendum ini sehubungan dengan Layanan Google-Managed Multi-Cloud untuk Looker (original).

10. Tim Perlindungan Data Cloud. Tim Perlindungan Data untuk Looker (original) dapat dihubungi di <https://support.google.com/cloud/contact/dpo>.

11. Catatan Pemrosesan Google. Sepanjang Hukum Privasi Yang Berlaku mewajibkan Google untuk mengumpulkan dan menyimpan catatan informasi tertentu yang berkaitan dengan Pelanggan, Pelanggan akan memberikan informasi tersebut kepada Google berdasarkan permintaan, dan memberitahukan Google mengenai pembaruan apa pun yang diperlukan untuk menjaga informasi tersebut tetap akurat dan terkini, kecuali Google meminta Pelanggan menyediakan dan memperbarui informasi tersebut melalui cara lain.

12. Langkah-Langkah Tambahan Keamanan Aplikasi. Google akan menerapkan dan mempertahankan Langkah-Langkah Keamanan tambahan yang dijelaskan di bawah untuk Looker (original):

a. Google setidaknya mengikuti praktik standar industri untuk arsitektur keamanan. Server proxy yang digunakan untuk aplikasi Google membantu mengamankan akses ke Looker dengan menyediakan satu titik untuk menyaring serangan melalui penolakan IP dan pembatasan kecepatan koneksi.

b. Administrator Pelanggan mengendalikan akses ke aplikasi oleh personel Google untuk memberikan dukungan teknis yang diminta oleh Pelanggan atau Pengguna Akhir.

Layanan SecOps

1. Definisi Tambahan.

- *"Akun"*, jika tidak didefinisikan dalam Perjanjian, berarti Layanan SecOps Pelanggan atau akun Google Cloud Platform, sebagaimana berlaku.
- *"Data Pelanggan"*, jika tidak didefinisikan dalam Perjanjian, berarti data yang diberikan kepada Google oleh Pelanggan atau Pengguna Akhir melalui Layanan SecOps dalam Akun atau, untuk Mandiant Consulting Services and Managed Services, sehubungan dengan penerimaan Layanan SecOps.
- *"Penyedia Yang Dilibatkan oleh Pelanggan"* berarti penyedia layanan (yang dapat mencakup prosesor atau subprosesor) yang secara langsung dilibatkan oleh Pelanggan berdasarkan perjanjian terpisah antara Pelanggan dan penyedia tersebut.
- *"Layanan SecOps"* berarti Layanan SecOps sebagaimana dijelaskan di <https://cloud.google.com/terms/secops/services>, tidak termasuk Penawaran Pihak Ketiga apa pun.
- *"Penawaran Pihak Ketiga"*, jika tidak didefinisikan dalam Perjanjian, berarti (a) layanan, perangkat lunak, produk, dan penawaran pihak ketiga lainnya yang tidak dimasukkan ke dalam Layanan atau Perangkat Lunak SecOps, dan (b) sistem operasi pihak ketiga.

2. Amendemen. Adendum ini diamendemen sebagai berikut sehubungan dengan Layanan SecOps:

- Definisi “Pengendalian Keamanan Tambahan” diganti dengan definisi berikut:
 - “*Pengendalian Keamanan Tambahan*” berarti sumber daya keamanan, fitur, fungsionalitas dan/atau pengendalian (jika ada) yang dapat digunakan oleh Pelanggan sesuai pilihannya dan/atau sebagaimana ditentukannya, termasuk (jika ada) enkripsi, pencatatan dan pemantauan, identitas dan manajemen akses, dan pemindaian keamanan.
- Definisi “Layanan Yang Diaudit” diganti dengan definisi berikut:
 - “*Layanan Yang Diaudit*” berarti Layanan SecOps yang berlaku saat itu diindikasikan berada dalam ruang lingkup sertifikasi atau laporan terkait di <https://cloud.google.com/security/compliance/secops/services-in-scope>. Google tidak boleh menghapus Layanan SecOps apa pun dari LSS ini kecuali layanan tersebut telah dihentikan sesuai dengan Perjanjian yang berlaku.
- Definisi “SCC (Pengendali-ke-Prosesor)”, “SCC (Prosesor-ke-Pengendali)”, “SCC (Prosesor-ke-Prosesor)” dan “SCC (Pemroses-ke-Prosesor, Google Eksportir)” dalam Lampiran 3 (Hukum Privasi Khusus) diganti dengan yang berikut:
 - “SCC (Pengendali-ke-Prosesor)” berarti ketentuan di: <https://cloud.google.com/terms/secops/sccs/eu-c2p>;
 - “SCC (Prosesor-ke-Pengendali)” berarti ketentuan di: <https://cloud.google.com/terms/secops/sccs/eu-p2c>;
 - “SCC (Prosesor-ke-Prosesor)” berarti ketentuan di: <https://cloud.google.com/terms/secops/sccs/eu-p2p>; dan
 - “SCC (Prosesor-ke-Prosesor, Google Eksportir)” berarti ketentuan di: <https://cloud.google.com/terms/secops/sccs/eu-p2p-google-exporter>.
- Bagian 6.1 (Penghapusan oleh Pelanggan) diubah menjadi sebagai berikut:
 - **6.1 Penghapusan oleh Pelanggan.** Google akan memungkinkan Pelanggan untuk menghapus Data Pelanggan selama Jangka Waktu dengan cara yang konsisten dengan fungsionalitas Layanan atau atas permintaan. Jika Pelanggan menggunakan Layanan untuk menghapus Data Pelanggan mana pun selama Jangka Waktu dan Data Pelanggan tersebut tidak dapat dipulihkan oleh Pelanggan, atau jika Pelanggan meminta penghapusan Data Pelanggan apa pun selama Jangka Waktu, penggunaan atau permintaan ini (sebagaimana berlaku) akan dianggap sebagai Instruksi kepada Google untuk menghapus Data Pelanggan yang relevan dari sistem Google sesuai dengan hukum yang berlaku. Google akan mematuhi Instruksi ini sesegera mungkin dan dalam jangka waktu paling lama 180 hari, kecuali Hukum Eropa mengharuskan penyimpanan, jika Hukum Perlindungan Data Eropa berlaku, atau hukum yang berlaku

mengharuskan penyimpanan, jika Hukum Privasi Yang Berlaku lainnya berlaku.

- Bagian 7.4 (Sertifikasi Kepatuhan dan Laporan SOC) Adendum diubah menjadi sebagai berikut:
 - 7.4 Sertifikasi Kepatuhan dan Laporan SOC. Google akan mempertahankan setidaknya sertifikasi dan laporan sebagaimana diidentifikasi di <https://cloud.google.com/security/compliance/secops/services-in-scope> untuk Layanan Yang Diaudit untuk memverifikasi efektivitas berkelanjutan dari Langkah-Langkah Keamanan (“Sertifikasi Kepatuhan” dan “Laporan SOC”).

Google dapat menambahkan standar kapan saja. Google dapat mengganti Sertifikasi Kepatuhan atau Laporan SOC dengan alternatif yang setara atau lebih baik.

- Bagian 9.1 (Akses; Perbaikan; Pemrosesan Yang Dibatasi; Portabilitas) diubah menjadi sebagai berikut:

9.1 Akses; Perbaikan; Pemrosesan Yang Dibatasi; Portabilitas. Selama Jangka Waktu, Google akan memungkinkan Pelanggan, dengan cara yang konsisten dengan fungsionalitas Layanan, untuk mengakses, memperbaiki, dan membatasi pemrosesan Data Pelanggan, termasuk sebagaimana dijelaskan dalam Bagian 6.1 (Penghapusan oleh Pelanggan), dan untuk mengeksport Data Pelanggan berdasarkan permintaan. Jika Pelanggan menyadari bahwa Data Pribadi Pelanggan tidak akurat atau kedaluwarsa, Pelanggan akan bertanggung jawab untuk memberitahukan Google dan Google akan membantu Pelanggan dalam memperbaiki data tersebut jika diwajibkan oleh Hukum Privasi Yang Berlaku.

3. Lokasi Pusat Data. Lokasi pusat data Layanan SecOps dijelaskan di <https://cloud.google.com/terms/secops/data-residency>.

4. Tidak Ada Sertifikasi oleh Pelanggan Non-EMEA. Pelanggan tidak berkewajiban untuk mengesahkan atau mengidentifikasi Otoritas Pengawasnya yang berwenang sebagaimana dijelaskan dalam Bagian 4.2 (Sertifikasi oleh Pelanggan Non-EMEA) persyaratan Perlindungan Data Eropa dalam Lampiran 3 (Hukum Privasi Khusus) untuk Layanan SecOps.

5. Informasi Mengenai Subprosesor. Nama, lokasi, dan aktivitas Subprosesor untuk Layanan SecOps dijelaskan di <https://cloud.google.com/terms/secops/subprocessors>.

6. Tim Perlindungan Data Cloud. Tim Perlindungan Data untuk Layanan SecOps dapat dihubungi di <https://support.google.com/cloud/contact/dpo> (dan/atau melalui cara lain yang mungkin disediakan oleh Google dari waktu ke waktu).

7. Catatan Pemrosesan Google. Sepanjang Hukum Privasi Yang Berlaku mewajibkan Google untuk mengumpulkan dan menyimpan catatan informasi tertentu yang berkaitan dengan Pelanggan, Pelanggan akan memberikan informasi tersebut kepada Google berdasarkan permintaan, dan memberitahukan Google mengenai pembaruan apa pun yang diperlukan untuk menjaga informasi tersebut tetap akurat dan terkini, kecuali Google meminta Pelanggan menyediakan dan memperbarui informasi tersebut melalui cara lain.

8. Ketentuan Khusus Layanan.

Mandiant Consulting Services dan Mandiant Managed Services

Mandiant Consulting Services and Managed Services menyediakan layanan konsultasi dan implementasi (termasuk respons insiden, kesiapan strategis, dan jaminan teknis untuk mengurangi ancaman dan risiko terkait insiden) serta layanan deteksi dan respons terkelola dan secara desain, memiliki karakteristik tertentu yang berbeda.

1. Amendemen. Adendum ini diubah sebagai berikut semata-mata sehubungan dengan Mandiant Consulting Services and Managed Services:

- Definisi “Insiden Data” dilengkapi sebagai berikut:
 - Untuk kejelasan, Insiden Data mengecualikan insiden yang menjadi subjek Mandiant Consulting Services and/or Managed Services, sebagaimana berlaku.
- Bagian 5.2(b)(i) (Kepatuhan terhadap Instruksi Pelanggan) diganti dengan yang berikut ini:
 - i. Penggunaan Layanan oleh Pelanggan; dan
- Kalimat kedua dari Bagian 7.1.1 (Tindakan Keamanan Google) dimodifikasi menjadi sebagai berikut:
 - Langkah-Langkah Keamanan dapat mencakup (sebagaimana sesuai) langkah-langkah untuk mengenkripsi Data Pelanggan; untuk membantu memastikan kerahasiaan, integritas, ketersediaan, dan ketahanan sistem dan layanan Google yang berkelanjutan; untuk membantu memulihkan akses tepat waktu ke Data Pelanggan setelah suatu insiden; dan untuk pengujian efektivitas secara berkala.
- Bagian 7.3.1(b) dimodifikasi menjadi sebagai berikut:
 - b. mengadministrasikan, mengelola akses ke, dan mengamankan kredensial autentikasi akun, sistem, perangkat lunak, jaringan, dan perangkat yang digunakan Pelanggan untuk menerima, atau memberi kewenangan kepada Google untuk mengakses untuk menyediakan Mandiant Consulting Services and/or Mandiant Services, sebagaimana berlaku;
- Bagian 7.3.1(d) dan (e) berikut ditambahkan sebagai bagian baru:
 - d. meminimalkan jumlah Data Pelanggan yang diberikan oleh atau atas nama Pelanggan kepada Google; dan
 - e. sepanjang akses Google ke Data Pelanggan berada dalam kendali Pelanggan, mencabut akses tersebut setelah Google menyelesaikan Mandiant Consulting Services and/or Managed Services, sebagaimana berlaku.
- Lampiran 2 (Langkah-Langkah Keamanan) diganti sebagai berikut:

- Lampiran 2: Langkah-Langkah Teknis dan Organisasi Tambahan

1. Lingkungan Yang Dikendalikan Pelanggan. Google hanya akan mengakses dan memproses Data Pelanggan yang diberikan oleh atau atas nama Pelanggan kepada Google melalui akun atau lingkungan yang dikendalikan atau disetujui Pelanggan.

2. Proses dan Kebijakan Akses Data – Kebijakan Akses. Proses dan kebijakan akses data Google dirancang untuk mencegah orang dan/atau sistem yang tidak berwenang memperoleh akses ke sistem yang digunakan untuk memproses Data Pelanggan. Google (i) hanya mengizinkan orang untuk mengakses data yang mereka berwenang untuk mengaksesnya; dan (ii) mengambil langkah-langkah untuk memastikan bahwa data pribadi tidak dapat dibaca, disalin, diubah, atau dihapus tanpa izin selama pemrosesan dan penggunaan. Pemberian atau modifikasi hak akses oleh Google didasarkan pada ketentuan Pelanggan kepada Google mengenai akses pengguna akhir ke akun atau lingkungannya.

3. Keamanan Personel. Personel Google diharuskan untuk berperilaku sesuai dengan pedoman perusahaan mengenai kerahasiaan, etika bisnis, penggunaan yang tepat, dan standar profesional. Google melakukan pemeriksaan latar belakang yang wajar dan sesuai dengan hukum ketenagakerjaan setempat dan peraturan perundang-undangan yang berlaku.

Personel diharuskan untuk melaksanakan perjanjian kerahasiaan dan harus mengakui penerimaan atas, dan kepatuhan terhadap, kebijakan kerahasiaan dan privasi Google. Personel diberikan pelatihan keamanan. Personel yang menangani Data Pelanggan diharuskan untuk melengkapi persyaratan tambahan yang sesuai dengan peran mereka (misalnya, sertifikasi). Personel Google tidak akan memproses Data Pelanggan tanpa otorisasi.

4. Langkah-Langkah Keamanan Tambahan. Google dan Pelanggan dapat menyepakati langkah-langkah keamanan tambahan dalam Formulir Pesanan yang berlaku, termasuk Pernyataan Pekerjaan yang terlampir, untuk Mandiant Consulting Services and/or Managed Services, sebagaimana berlaku.

2. Penyedia yang Digunakan Pelanggan. Untuk kejelasan, dan tanpa membatasi kewajiban Google berdasarkan Bagian 7 (Keamanan Data) atau 11 (Subprosesor), Lampiran 2 (Langkah-langkah Keamanan) tidak menjelaskan Langkah-langkah keamanan atau pengendalian yang diterapkan atau disediakan oleh Pelanggan atau Penyedia Layanan Yang Dilibatkan oleh Pelanggan.

Layanan Implementasi

1. Definisi Tambahan.

- *“Data Pelanggan”* berarti data yang diizinkan Pelanggan untuk diakses oleh Personel Google pada Sistem Yang Dikelola Pelanggan.
- *“Sistem Yang Dikelola Pelanggan”* berarti hal-hal berikut, sebagaimana digunakan oleh Pelanggan untuk menerima Layanan Implementasi: (a) Instance Layanan Google Cloud atau layanan cloud pihak ketiga yang dikelola Pelanggan; dan (b) perangkat keras atau perangkat lunak apa pun yang di hosting atau dikelola di lingkungan lokal Pelanggan.

- “*Layanan Google Cloud*” berarti Layanan apa pun yang dijelaskan dalam Lampiran 4 ini (Produk Tertentu), selain Layanan Implementasi, Mandiant Consulting Services, dan Mandiant Managed Services.
- “*Personel Google*” berarti karyawan dan kontraktor Google yang terlibat dalam penyediaan Layanan Implementasi.
- “*Layanan Implementasi*” berarti layanan penasihat, konsultasi, dan implementasi yang diberikan oleh karyawan dan kontraktor Google untuk mendukung Layanan Google Cloud sebagaimana dijelaskan dalam Perjanjian, termasuk dalam Formulir Pesanan atau Pernyataan Pekerjaan.

2. Amendemen. Adendum ini diamendemen sebagai berikut sehubungan dengan Layanan Implementasi:

- Definisi “Pengendalian Keamanan Tambahan” dihapus.
- Definisi “Insiden Data” diganti dengan yang berikut:
 - “*Insiden Data*” berarti pelanggaran Bagian 7.1 (Langkah-Langkah Keamanan, Pengendalian, dan Bantuan Google) oleh Personel Google, yang mengakibatkan penghancuran, kehilangan, perubahan, pengungkapan yang tidak sah dari, atau akses ke Data Pribadi Pelanggan secara tidak sengaja atau melanggar hukum.
- Tunduk pada ketentuan lain dalam bagian ini, istilah “Data Pelanggan” diganti dengan “Data Pribadi Pelanggan” jika digunakan (a) di Bagian 2 (Definisi) dalam definisi “Subprosesor”, dan (b) di bagian lain dari Adendum ini. Untuk kejelasan, definisi lain dalam Bagian 2 (Definisi) tetap tidak diubah.
- Bagian 3 (Durasi) diganti sebagai berikut:
 - **3. Durasi.** Terlepas dari apakah Perjanjian yang berlaku telah berakhir atau kedaluwarsa, Adendum ini akan tetap berlaku hingga, dan secara otomatis kedaluwarsa ketika, Google tidak lagi memiliki akses ke Data Pribadi dari Pelanggan mana pun.
- Bagian 6 (Penghapusan Data) diganti sebagai berikut:
 - **6. Penghapusan Data.** Pada akhir Jangka Waktu, Pelanggan akan (a) menentukan apakah akan menghapus Data Pribadi dari Pelanggan mana pun, dan (b) bertanggung jawab atas penghapusan tersebut.
- Kalimat kedua pada Bagian 7.1.1 (Langkah-Langkah Keamanan Google) diganti sebagai berikut:
 - “Langkah-langkah Keamanan dapat mencakup (sebagaimana sesuai) langkah-langkah untuk mengenkripsi Data Pelanggan; untuk membantu memastikan kerahasiaan, integritas, ketersediaan, dan ketahanan sistem dan layanan Google yang berkelanjutan;

untuk membantu memulihkan akses tepat waktu ke Data Pelanggan setelah suatu insiden; dan untuk pengujian efektivitas secara berkala.”

- Bagian 7.1.3 (Pengendalian Keamanan Tambahan) dihapus, bersama dengan seluruh rujukan lain ke bagian tersebut.
- Bagian 9.1 (Akses; Perbaikan; Pemrosesan Yang Dibatasi; Portabilitas) diganti dengan berikut:
 - 9.1 *Akses; Perbaikan; Pemrosesan Yang Dibatasi; Portabilitas*. Pelanggan akan bertanggung jawab untuk menggunakan fungsionalitas Sistem Yang Dikelola Pelanggan untuk mengakses, memperbaiki, dan membatasi pemrosesan Data Pribadi Pelanggan, termasuk jika Pelanggan menyadari bahwa Data Pribadi Pelanggan tidak akurat atau sudah kedaluwarsa dan diwajibkan oleh Hukum Privasi Yang Berlaku untuk memperbaiki atau menghapus data tersebut.
- Bagian 11.4 (Kesempatan untuk Menolak Subprosesor) diganti dengan yang berikut ini:
 - 11.4 *Kesempatan untuk Menolak Subprosesor*. Jika terdapat Subprosesor Baru yang dilibatkan selama Jangka Waktu, Google akan memberitahukan Pelanggan mengenai keterlibatan Subprosesor Baru tersebut sebelum memproses Data Pribadi Pelanggan. Pelanggan dapat menolak Subprosesor Baru dengan memberitahukan Google dan, jika Pelanggan melakukannya, para pihak akan bekerja dengan itikad baik untuk menentukan alternatif yang dapat diterima bersama.
- Lampiran 1 (Pokok Pembahasan dan Rincian Pengolahan Data) diubah sebagai berikut:
 - Bagian “*Durasi Pemrosesan*” diganti sebagai berikut:
 - “*Durasi Pemrosesan*. Jangka Waktu ditambah (jika berlaku) periode dari akhir Jangka Waktu hingga berakhirnya akses Google terhadap Data Pribadi Pelanggan.”
 - Kata-kata “disediakan kepada Google melalui Layanan” dalam bagian “Kategori Data” dan “Subjek Data” diganti dengan “disediakan bagi Google sehubungan dengan Layanan”.
- Lampiran 2 (Langkah-Langkah Keamanan) diganti sebagai berikut:
 - **Lampiran 2: Langkah-Langkah Keamanan**

1. Sistem Yang Dikelola Pelanggan. Personel Google hanya akan mengakses dan memproses Data Pribadi Pelanggan pada Sistem Yang Dikelola Pelanggan. Jika sistem tersebut mencakup Layanan Google Cloud, penggunaan Layanan Google Cloud oleh Pelanggan tetap diatur oleh perjanjian yang berlaku untuk layanan tersebut.

2. Pengendalian Akses. Proses dan kebijakan akses data internal Google dirancang untuk mencegah orang dan sistem yang tidak berwenang memperoleh akses ke Layanan Google Cloud yang digunakan

untuk memproses data pribadi. Kebijakan Google (i) hanya mengizinkan Personel Google untuk mengakses data yang diperbolehkan untuk mereka akses; dan (ii) mengharuskan Personel Google untuk tidak membaca, menyalin, mengubah, atau menghapus Data Pribadi Pelanggan tanpa izin selama pemrosesan, penggunaan, dan setelah perekaman. Pelanggan mengendalikan penyediaan atau modifikasi hak akses pengguna akhir ke Sistem Yang Dikelola Pelanggan. Jika sistem tersebut menyertakan Layanan Google Cloud, perincian mengenai alat alur kerja yang menyimpan catatan audit perubahan dan log akses sistem dibahas dalam perjanjian untuk Layanan Google Cloud yang berlaku.

3. Keamanan Personel. Personel Google diharuskan untuk berperilaku sesuai dengan pedoman perusahaan mengenai kerahasiaan, etika bisnis, penggunaan yang tepat, dan standar profesional. Google melakukan pemeriksaan latar belakang yang wajar dan sesuai dengan hukum ketenagakerjaan setempat dan peraturan perundang-undangan yang berlaku.

Personel Google diharuskan untuk menandatangani perjanjian kerahasiaan dan harus mengakui penerimaan atas dan kepatuhan terhadap kebijakan kerahasiaan dan privasi Google. Personel Google diberikan pelatihan keamanan. Personel Google yang menangani Data Pribadi Pelanggan diharuskan untuk melengkapi persyaratan tambahan yang sesuai dengan peran mereka (misalnya, sertifikasi).

4. Langkah-Langkah Keamanan Tambahan. Google dan Pelanggan dapat menyetujui langkah-langkah keamanan tambahan dalam Perjanjian, termasuk dalam Formulir Pesanan atau Pernyataan Pekerjaan.

5. Keamanan Subprosesor. Sebelum merekrut Subprosesor, Google melakukan audit praktik keamanan dan privasi Subprosesor untuk memastikan Subprosesor memberikan tingkat keamanan dan privasi yang sesuai dengan akses mereka ke data dan ruang lingkup layanan yang mereka berikan. Setelah Google menilai risiko yang ditimbulkan oleh Subprosesor, maka sesuai dengan persyaratan yang dijelaskan dalam Bagian 11.3 (Persyaratan untuk Keterlibatan Subprosesor), Subprosesor diharuskan untuk menyetujui persyaratan kontrak keamanan, kerahasiaan, dan privasi yang sesuai.

3. Tanggung Jawab Keamanan Pelanggan. Selain kewajibannya berdasarkan Bagian 7.3.1 (Tanggung Jawab Keamanan Pelanggan), Pelanggan bertanggung jawab atas hal-hal berikut:

- mengelola, mengatur akses ke, dan mengamankan Sistem Yang Dikelola Pelanggan, termasuk meminimalkan akses Personel Google ke Data Pribadi Pelanggan sejauh yang dapat dilaksanakan secara wajar dan menghentikan akses tersebut setelah Layanan Implementasi selesai; dan
- menerapkan rekomendasi keamanan apa pun yang diberikan secara tertulis oleh Google kepada Pelanggan sehubungan dengan Sistem Yang Dikelola Pelanggan.

4. Sertifikasi Kepatuhan. Google akan memelihara sertifikat untuk ISO 27001, ISO 27017, dan ISO 27018 yang mencakup Layanan Implementasi yang diberikan untuk mendukung Google Cloud Platform dan Google Workspace (*"Sertifikasi Kepatuhan Layanan Implementasi"*). Google dapat menambahkan standar kapan saja. Google dapat mengganti Sertifikasi Kepatuhan Layanan Implementasi dengan alternatif yang setara atau lebih baik.

5. Peninjauan Sertifikasi Kepatuhan. Untuk menunjukkan kepatuhan Google terhadap kewajibannya berdasarkan Adendum ini, Google akan menyediakan Sertifikasi Kepatuhan Layanan Implementasi untuk ditinjau oleh Pelanggan dan, jika Pelanggan adalah prosesor, mengizinkan Pelanggan untuk meminta akses kepada pengontrol terkait ke Sertifikasi Kepatuhan Layanan Implementasi.

6. Lokasi Pemrosesan Data. Data Pribadi Pelanggan dapat diproses di negara mana pun tempat Google menyediakan Layanan Implementasi atau tempat Pelanggan mengelola Sistem Yang Dikelola Pelanggan.

7. Tidak Ada Sertifikasi oleh Pelanggan di Luar EMEA. Pelanggan tidak berkewajiban untuk menyertifikasi atau mengidentifikasi Otoritas Pengawas yang berwenang sebagaimana dijelaskan dalam Bagian 4.2 (Sertifikasi oleh Pelanggan di Luar EMEA) dari ketentuan Perlindungan Data Eropa dalam Lampiran 3 (Hukum Privasi Khusus) untuk Layanan Implementasi.

8. Informasi Mengenai Subprosesor. Subprosesor untuk Layanan Implementasi akan diidentifikasi (sebagai subkontraktor) dalam Formulir Pesanan yang berlaku, Pernyataan Pekerjaan, atau konfirmasi lain yang diberikan kepada Pelanggan sebelum dimulainya Layanan Implementasi atau akan menjadi Afiliasi Google. Google juga akan menyediakan nama, lokasi, dan aktivitas Subprosesor untuk Layanan Implementasi kepada Pelanggan atas permintaan.

9. Catatan Pemrosesan Google. Sejauh Hukum Privasi Yang Berlaku mengharuskan Google untuk mengumpulkan dan menyimpan catatan informasi tertentu yang berkaitan dengan Pelanggan, Pelanggan akan memberikan informasi tersebut kepada Google atas permintaan, dan memberitahukan Google mengenai pembaruan apa pun yang diperlukan untuk menjaga keakuratan dan kekinian informasi tersebut, kecuali Google meminta Pelanggan untuk memberikan dan memperbarui informasi tersebut melalui cara lain.

Google Cloud Skills Boost for Organizations

1. Definisi Tambahan.

- “Akun”, jika tidak didefinisikan dalam Perjanjian, berarti Akun Pelanggan untuk Google Cloud Skills Boost for Organizations.
- “GCSBO” berarti layanan dan konten edukasi, pelatihan, dan pembelajaran yang disediakan melalui <https://www.cloudskillsboost.google/> (atau situs web lain yang dioperasikan atau dikendalikan oleh Google dan digunakan untuk tujuan Google Cloud Skills Boost for Organizations).
- “TSS” berarti layanan dukungan teknis yang dapat diberikan oleh Google kepada Pelanggan atas kebijakannya sendiri.

2. Amendemen. Adendum ini diamandemen sebagai berikut sehubungan dengan GCSBO:

- Definisi “Pengendalian Keamanan Tambahan” diganti sebagai berikut:
 - “Pengendalian Keamanan Tambahan” berarti sumber daya, fitur, fungsionalitas, dan pengendalian keamanan yang dapat digunakan oleh Pelanggan sesuai pilihannya

dan sebagaimana ditentukannya, termasuk Konsol Admin, enkripsi, pencatatan dan pemantauan, manajemen identitas dan akses, dan pemindaian keamanan.

- Definisi “SCC (Pengendali-ke-Prosesor)”, “SCC (Prosesor-ke-Pengendali)”, “SCC (Prosesor-ke-Prosesor)” dan “SCC (Pemroses-ke-Prosesor, Google Eksportir)” dalam Lampiran 3 (Hukum Privasi Khusus) diganti dengan yang berikut:
 - “SCC (Pengendali-ke-Prosesor)” berarti ketentuan di: <https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-c2p>
 - “SCC (Prosesor-ke-Pengendali)” berarti ketentuan di: <https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-p2c>
 - “SCC (Prosesor-ke-Prosesor)” berarti ketentuan di: <https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-p2p>; dan
 - “SCC (Prosesor-ke-Prosesor, Google Eksportir)” berarti ketentuan di: <https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-p2p-intragroup>.

3. Lokasi Pusat Data. Lokasi pusat data GCSBO dijelaskan di <https://cloud.google.com/about/locations/>.

4. Tidak Ada Sertifikasi oleh Pelanggan Non-EMEA. Pelanggan tidak diwajibkan untuk menyatakan atau mengidentifikasi Otoritas Badan Pengawas yang berwenang sebagaimana dijelaskan dalam Bagian 4.2 (Sertifikasi oleh Pelanggan Non-EMEA) dari ketentuan Perlindungan Data Eropa yang tercantum dalam Lampiran 3 (Hukum Privasi Tertentu) untuk GCSBO.

5. Informasi Mengenai Subprosesor. Nama, lokasi, dan aktivitas Subprosesor GCSBO dijelaskan di:

- <https://cloud.google.com/terms/skillsboost-organizations/subprocessors>; dan
- <https://cloud.google.com/terms/subprocessors>.

6. Tim Perlindungan Data Cloud. Tim Perlindungan Data untuk GCSBO dapat dihubungi di <https://support.google.com/qwiklabs> (dan/atau melalui cara lain yang mungkin disediakan oleh Google dari waktu ke waktu).

7. Catatan Pemrosesan Google. Sepanjang Hukum Privasi Yang Berlaku mewajibkan Google untuk mengumpulkan dan menyimpan catatan informasi tertentu yang berkaitan dengan Pelanggan, Pelanggan akan memberikan informasi tersebut kepada Google berdasarkan permintaan, dan memberitahukan Google mengenai pembaruan apa pun yang diperlukan untuk menjaga informasi tersebut tetap akurat dan terkini, kecuali Google meminta Pelanggan menyediakan dan memperbarui informasi tersebut melalui cara lain.

Versi sebelumnya dari Ketentuan Pemrosesan dan Keamanan Data:

[9 April 2024](#) [30 Juni 2022](#) [24 September 2021](#) [19 Agustus 2020](#) [10 Agustus 2020](#) [17 Juli 2020](#)
[11 Oktober 2019](#) [1 Oktober 2019](#) [25 Mei 2018](#) [13 Maret 2018](#) [9 November 2017](#) [11 Oktober 2017](#)
[7 Februari 2017](#) [6 Oktober 2016](#)

Versi sebelumnya dari Amendemen Pemrosesan Data:

[7 Juli 2022](#) [24 September 2021](#) [27 Mei 2021](#) [29 Oktober 2019](#) [25 Mei 2018](#) [25 April 2018](#) [11 Juli 2017](#) [28 November 2016](#)
[7 Januari 2016](#) [24 April 2015](#) [1 April 2014](#) [14 November 2012](#)

Versi sebelumnya dari Adendum Pemrosesan Data untuk Layanan Looker (original) (Pelanggan):

[14 Februari 2023](#) [4 Januari 2023](#) [20 September 2022](#) [30 Juni 2022](#) [16 Maret 2022](#) [24 September 2021](#)
[1 April 2021](#) [15 Januari 2021](#) [17 Desember 2020](#) [28 Agustus 2020](#) [1 Juni 2020](#) [9 Maret 2020](#)

Versi sebelumnya dari DPST Layanan SecOps (Pelanggan):

[6 Februari 2023](#) [28 November 2022](#) [27 September 2021](#) [1 Oktober 2020](#)

Versi sebelumnya dari Adendum Pemrosesan Data untuk Layanan Konsultasi SecOps dan Layanan Terkelola:

[5 Oktober 2023](#) [19 September 2023](#) [15 Juni 2023](#) [22 Februari 2023](#) [6 Februari 2023](#)

VERSI SEBELUMNYA (Terakhir diubah pada tanggal 15 Oktober 2024)

[26 September 2024](#) [9 September 2024](#) [5 Agustus 2024](#) [23 Mei 2024](#) [9 April 2024](#) [8 November 2023](#)
[15 Agustus 2023](#) [20 September 2022](#)