Adendum Pemrosesan Data Cloud (Mitra)

Adendum Pemrosesan Data Cloud ini (termasuk lampirannya, "*Adendum*") dimasukkan ke dalam Perjanjian(-Perjanjian) (sebagaimana didefinisikan di bawah) antara Google dan Mitra. Adendum ini sebelumnya dikenal sebagai "Ketentuan Pemrosesan dan Keamanan Data" untuk Google Cloud Platform atau "Ketentuan Pemrosesan dan Keamanan Data" untuk Looker (original) atau Layanan SecOps Google.

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 Mitra. 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 Mitra. 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 Mitra menerima, atau para pihak menyepakati Adendum ini.
- "*Pengendalian Keamanan Tambahan*" berarti sumber daya, fitur, fungsionalitas, dan pengendalian keamanan yang dapat digunakan oleh Mitra 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 Mitra.
- "*Hukum Privasi Yang Berlaku*" berarti sebagaimana berlaku pada pemrosesan Data Pribadi Mitra, setiap undang-undang atau peraturan nasional, federal, Uni Eropa, negara bagian, provinsi, atau undang-undang atau peraturan privasi atau keamanan data, atau perlindungan data Mitra.

- "*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).

- "*Insiden Data*" berarti pelanggaran keamanan Google yang mengakibatkan pemusnahan, kehilangan, perubahan, pengungkapan tidak sah dari, atau akses ke Data Mitra 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 Mitra); (b) hukum Inggris Raya atau bagian dari Inggris Raya (jika GDPR Inggris Raya berlaku pada pemrosesan Data Pribadi Mitra); atau (c) hukum Swiss (jika FADP Swiss berlaku pada pemrosesan Data Pribadi Mitra).

- "*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 Mitra.

- "*Instruksi*" memiliki arti yang diberikan dalam Bagian 5.2 (Kepatuhan terhadap Instruksi Mitra).

- "*Alamat Surel Pemberitahuan*" berarti alamat (-alamat) surel yang ditentukan oleh Mitra dalam Konsol Admin atau Formulir Pesanan untuk menerima pemberitahuan tertentu dari Google.

- "*Pengguna Akhir Mitra*" memiliki arti yang diberikan dalam Perjanjian atau, jika arti tersebut tidak diberikan, memiliki arti yang diberikan untuk "Pengguna Akhir" dalam Perjanjian.

- "*Data Pribadi Mitra*" berarti data pribadi yang terdapat dalam Data Mitra, termasuk seluruh kategori khusus data pribadi atau data sensitif yang didefinisikan dalam Hukum Privasi Yang Berlaku.

- "*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 Mitra dalam rangka menyediakan bagian Layanan dan TSS.

- "*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 Mitra sebagaimana dijelaskan dalam Adendum ini.

4. Peran; Kepatuhan Hukum

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

4.2 Ringkasan Pemrosesan. Pokok bahasan dan rincian pemrosesan Data Pribadi Mitra 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 Mitra berdasarkan Hukum Privasi Yang Berlaku.

4.4 Ketentuan Hukum Tambahan. Sepanjang pemrosesan Data Pribadi Mitra 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 Mitra. Jika Mitra adalah pemroses:*

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

i. Instruksi;

ii. Keterlibatan Mitra terhadap Google sebagai prosesor lain Mitra; dan

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

b. Mitra akan meneruskan kepada pengendali yang relevandengan 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. Mitra 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 Mitra. Mitra menginstruksikan Google untuk memproses Data Mitra sesuai dengan Perjanjian yang berlaku (termasuk Adendum ini) dan hukum yang berlaku hanya sebagai berikut:

a. untuk menyediakan, mengamankan, dan memantau Layanan dan TSS; dan

b. sebagaimana ditentukan lebih lanjut melalui:

i. penggunaan Layanan oleh Mitra (termasuk melalui Konsol Admin) dan TSS (jika berlaku); dan

ii. instruksi tertulis apa pun lainnya yang diberikan oleh Mitra 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 Mitra*. Google akan mengizinkan Mitra untuk menghapus Data Mitra selama Jangka Waktu dengan cara yang sesuai dengan fungsionalitas Layanan. Jika Mitra menggunakan Layanan untuk menghapus Data Mitra mana pun selama Jangka Waktu dan Data Mitra tersebut tidak dapat dipulihkan oleh Mitra, penggunaan ini akan dianggap sebagai Instruksi kepada Google untuk menghapus Data Mitra 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 Mitra ingin menyimpan Data Mitra apa pun setelah Jangka Waktu berakhir, Mitra dapat menginstruksikan Google sesuai dengan Bagian 9.1 (Akses; Perbaikan; Pemrosesan Yang Dibatasi; Portabilitas) untuk mengembalikan data tersebut selama Jangka Waktu. Mitra menginstruksikan Google untuk menghapus seluruh Data Mitra 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.

7. Keamanan Data

7.1 *Tindakan, Pengendalian, dan Bantuan Keamanan Google*.

7.1.1 *L*angkah-Langkah Keamanan Google. Google akan menerapkan dan memelihara tindakan teknis, organisasi, dan fisik untuk melindungi Data Mitra 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 Mitra; untuk membantu memastikan kerahasiaan, integritas, ketersediaan, dan ketahanan sistem dan layanan Google yang berkelanjutan; untuk membantu memulihkan akses tepat waktu ke Data Mitra 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 Mitra 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 Mitra berkewajiban menjaga kerahasiaan.

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

a. mengizinkan Mitra untuk mengambil langkah pengamanan Data Mitra; dan

b. memberikan informasi kepada Mitra mengenai cara mengamankan, mengakses, dan menggunakan Data Mitra.

7.1.4 Bantuan Keamanan Google. Google akan (dengan mempertimbangkan sifat pemrosesan Data Pribadi Mitra dan informasi yang tersedia untuk Google) membantu Mitra dalam memastikan kepatuhan terhadap kewajibannya (atau, jika Mitra 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 Mitra (atau pengendali yang relevan) untuk mematuhi kewajiban tersebut, atas permintaan Mitra, memberikan kerja sama dan bantuan tambahan yang wajar kepada Mitra.

7.2 *Insiden Data*.

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

7.2.2 *Rincian Insiden Data*. Pemberitahuan Google mengenai Insiden Data akan menjelaskan: sifat Insiden Data termasuk sumber daya Mitra 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 Mitra 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 Mitra oleh Google*. Google tidak berkewajiban menilai Data Mitra 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 Mitra.

7.3.1 *Tanggung Jawab Keamanan Mitra*. 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, Mitra bertanggung jawab atas penggunaan Layanan oleh Mitra serta penyimpanan salinan Data Mitra 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 Mitra;

b. mengamankan kredensial autentikasi akun, sistem dan perangkat yang digunakan Mitra dan Pelanggannya untuk mengakses Layanan; dan

c. mencadangkan Data Pelanggannya sebagaimana mestinya.

7.3.2 *Penilaian Keamanan Mitra*. Mitra 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 Mitra (dengan mempertimbangkan keadaan terkini, biaya penerapan, dan sifat, ruang lingkup, konteks, dan tujuan pemrosesan Data Mitra 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 Mitra dan, jika Mitra adalah pemroses, mengizinkan Mitra 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 Mitra*.

a. *Audit Mitra*. Google akan, jika diwajibkan berdasarkan Hukum Privasi Yang Berlaku, mengizinkan Mitra atau auditor independen yang ditunjuk oleh Mitra 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 Mitra atau auditornya sebagaimana dijelaskan dalam Bagian 7.5 (Peninjauan dan Audit Kepatuhan).

b. *Peninjauan Independen Mitra*. Mitra 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. Mitra 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 Mitra).

b. Berdasarkan permintaan Mitra berdasarkan Bagian 7.5.3(a), Google dan Mitra 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 Mitra).

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

d. Google dapat mengajukan keberatan secara tertulis kepada auditor yang ditunjuk oleh Mitra untuk melakukan audit apa pun berdasarkan Bagian 7.5.2(a) (Audit Mitra) 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 Mitra menunjuk auditor lain atau melakukan audit sendiri.

e. Setiap permintaan MitraMitra 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 Mitra dalam memastikan kepatuhan terhadap kewajibannya (atau, jika Mitra 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 Mitra (atau pengendali yang relevan) untuk mematuhi kewajiban tersebut, atas permintaan Mitra, memberikan kerja sama dan bantuan tambahan yang wajar kepada Mitra.

9. Akses dan lain-lain; Hak Subjek Data; Ekspor Data

9.1 *Akses; Perbaikan; Pemrosesan Yang Dibatasi; Portabilitas*. Selama Jangka Waktu, Google akan memperbolehkan Mitra, dengan cara yang sesuai dengan fungsionalitas Layanan, untuk mengakses, memperbaiki, dan membatasi pemrosesan Data Mitra, termasuk melalui fungsionalitas penghapusan yang disediakan oleh Google sebagaimana dijelaskan dalam Bagian 6.1 (Penghapusan oleh Mitra), dan untuk mengekspor Data Mitra. Jika Mitra mengetahui bahwa Data Pribadi Mitra mana pun tidak akurat atau bukan yang terbaru (*outdated*), Mitra 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 Mitra dan mengidentifikasi Mitra, Google akan:

a. menyarankan subjek data untuk menyampaikan permintaannya kepada Mitra;

b. segera memberitahukan Mitra; dan

c. sebaliknya tidak akan menanggapi permintaan subjek data tersebut tanpa izin dari Mitra.

Mitra 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 Mitra) membantu Mitra dalam memenuhi kewajibannya (atau, jika Mitra 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 Mitra (atau pengendali yang relevan) untuk mematuhi kewajiban tersebut, atas permintaan Mitra, memberikan kerja sama dan bantuan tambahan yang wajar kepada Mitra.

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 Mitra 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*. Mitra 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), Mitra 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 Mitra sejauh diperlukan untuk melaksanakan kewajiban yang disubkontrakkan padanya, dan melakukannya sesuai dengan Perjanjian (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 Mitra apa pun, memberitahukan Mitra mengenai keterlibatan tersebut (termasuk nama, lokasi, dan aktivitas Subprosesor Baru).

b. Mitra 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 Mitra terkait pemrosesan Data Mitra berdasarkan Perjanjian dan dapat dihubungi sebagaimana dijelaskan di bagian Pemberitahuan Perjanjian 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 Mitra, Mitra 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 Mitra, Google akan menyarankan pihak ketiga tersebut untuk menghubungi Mitra.

13. Pemberitahuan

Pemberitahuan berdasarkan Adendum ini (termasuk pemberitahuan mengenai Insiden Data apa pun) akan dikirimkan ke Alamat Surel Pemberitahuan. Mitra bertanggung jawab menggunakan Konsol Admin untuk memastikan Alamat MitraSurel Pemberitahuannya 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.

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

14.3 *Mitra*. Untuk menghindari keraguan, Mitra bukan merupakan penerima manfaat pihak ketiga Adendum ini.

Lampiran 1: Pokok Bahasan dan Rincian Pemrosesan Data

Pokok Bahasan

Penyediaan Layanan dan TSS oleh Google kepada Mitra.

Durasi Pemrosesan

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

Sifat dan Tujuan Pemrosesan

Google akan memproses Data Pribadi Mitra untuk tujuan penyediaan Layanan dan TSS kepada Mitra sesuai dengan Adendum ini.

Kategori Data

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

Subjek Data

Subjek data mencakup individu yang datanya diberikan kepada Google melalui Layanan oleh (atau atas arahan dari) Mitra 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 Mitra dan Pengguna Akhir Mitraharus 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 Mitra. Google merancang sistemnya untuk (i) hanya mengizinkan orang yang berwenang untuk mengakses data yang diperbolehkan untuk mereka akses; dan (ii) memastikan bahwa Data Mitra 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 Mitra di beberapa pusat data yang tersebar secara geografis. Google juga secara logis mengisolasi Data Mitra. Mitra akan diberikan kendali atas kebijakan berbagi data tertentu. Kebijakan tersebut, sesuai dengan fungsionalitas Layanan, akan memungkinkan Mitra untuk menentukan pengaturan berbagi produk yang berlaku bagi Pengguna Akhir Mitra untuk tujuan tertentu. Mitra 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 Mitra diharuskan melengkapi persyaratan tambahan yang sesuai dengan peran mereka (misalnya sertifikasi). Personel Google tidak akan memproses Data Mitra 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 Mitra.

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 Komisaris 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 Mitra" berarti SCC (Pengendali-ke-Prosesor), SCC (Prosesor-ke-Prosesor), atau SCC (Prosesor-ke-Pengendali), sebagaimana berlaku.

- "SCC" berarti SCC Mitra 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 Mitra) atau hak atau kewajiban lain apa pun dari salah satu pihak berdasarkan Perjanjian yang berlaku, Google akan segera memberitahukan Mitra 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 Mitra adalah prosesor, Mitra akan segera meneruskan kepada pengendali yang relevan setiap pemberitahuan yang diberikan oleh Google berdasarkan bagian ini.

3. Hak Audit Mitra. Google akan mengizinkan Mitra atau auditor independen yang ditunjuk oleh Mitra untuk melakukan audit (termasuk inspeksi) sebagaimana dijelaskan dalam Bagian 7.5.2(a) (Audit Mitra). 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 Mitra dapat diproses atau ditransfer ke Negara Yang Memadai. Jika Data Pribadi Mitra ditransfer ke negara lain mana pun dan Hukum Perlindungan Data Eropa berlaku untuk transfer tersebut (sebagaimana disertifikasi oleh Mitra berdasarkan Bagian 4.2 (Sertifikasi oleh Mitra Non-EMEA) dari ketentuan Hukum Perlindungan Data Eropa ini, jika alamat Mitrapenagihannya 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 Mitra mengenai solusi yang relevan Mitradan 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 Mitra 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 Mitra tidak berada di Negara Yang Memadai, SCC (Prosesor-ke Pengendali) akan berlaku (terlepas dari apakah Mitra adalah pengendali atau prosesor) sehubungan dengan Transfer Yang Dibatasi antara Google dan Mitra; atau

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

4.2 *Sertifikasi oleh Mitra Non-EMEA*. Jika alamat penagihan Mitra berada di luar EMEA, dan pemrosesan Data Pribadi Mitra tunduk pada Hukum Perlindungan Data Eropa, maka kecuali Lampiran 4 (Produk Khusus) dari Adendum ini menyatakan sebaliknya, Mitra 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 Mitra 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 Mitra berlaku sebagaimana dijelaskan dalam Bagian 4.1 (Transfer Yang Dibatasi) dari ketentuan Hukum Perlindungan Data Eropa ini, Google akan mengizinkan Mitra (atau auditor independen yang ditunjuk oleh Mitra) 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*. Mitra 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 Mitra menyimpulkan, berdasarkan penggunaan Layanan saat ini atau yang dimaksudkan, bahwa perlindungan yang sesuai tidak diberikan untuk Data Pribadi Mitra yang ditransfer, maka Mitra 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 Mitra mana pun (yang dimasukkan sebagai referensi ke dalam Adendum ini) dan bagian lain dalam Perjanjian (termasuk Adendum ini), SCC Mitra 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 Mitra"* 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 Mitra), sehubungan dengan pemrosesan Data Pribadi Mitra sesuai dengan CCPA, Google tidak akan, kecuali diizinkan berdasarkan CCPA:

a. menjual atau membagikan Data Pribadi Mitra;

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

i. selain untuk tujuan bisnis berdasarkan CCPA atas nama Mitra dan untuk tujuan khusus dalam melaksanakan Layanan dan TSS; atau

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

c. menggabungkan atau memperbarui Data Pribadi Mitra 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 Mitra) atau hak atau kewajiban lain apa pun dari salah satu pihak berdasarkan Perjanjian yang berlaku, Google akan memberitahukan Mitra jika, menurut pendapat Google, Google tidak dapat memenuhi kewajibannya berdasarkan CCPA, kecuali jika pemberitahuan tersebut dilarang oleh hukum yang berlaku.

4. Intervensi Mitra. Jika Google memberitahukan Mitra mengenai setiap penggunaan Data Pribadi Mitra yang tidak sah, termasuk berdasarkan Bagian 3 (Kepatuhan) sub-bagian ini atau Bagian 7.2.1 (Pemberitahuan Insiden), Mitra 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 Mitra) 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 Mitra berada di Turki dan Google menyediakan ketentuan tambahan opsional apa pun (termasuk SCC Turki) untuk disetujui oleh Mitra sehubungan dengan transfer Data Pribadi Mitra 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) Mitra.

2.2 *Pemberitahuan kepada Pejabat Yang Berwenang*. Jika Mitra 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, Mitra akan bertanggung jawab untuk memberikan pemberitahuan tersebut dalam waktu lima (5) hari sejak penandatanganan SCC Turki.

2.3 *Audit SCC*. Jika Mitra menandatangani SCC Turki berdasarkan Bagian 2 (Transfer Data) ini, Google akan mengizinkan Mitra (atau auditor independen yang ditunjuk oleh Mitra) 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 Mitra menyimpulkan, berdasarkan penggunaan Layanan saat ini atau yang dimaksudkan, bahwa perlindungan yang sesuai tidak diberikan untuk Data Pribadi Mitra yang ditransfer, maka Mitra 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 Mitra) 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 Mitra. Google akan mengizinkan Mitra atau auditor independen yang ditunjuk oleh Mitra untuk melakukan audit (termasuk inspeksi) sebagaimana dijelaskan dalam Bagian 7.5.2(a) (Audit Mitra).

Lampiran 4: Produk Khusus

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

Google Cloud Platform

1. Definisi Tambahan.

- *"Akun"*, jika tidak didefinisikan dalam Perjanjian, berarti akun Google Cloud Platform Mitra.

- *"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 Mitra berdasarkan permintaan.

- Ketentuan berikut dihapus:

    - Dari Bagian 7.1.1 (Langkah-Langkah Keamanan Google), frasa "Mitraenkripsi 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 Mitra yang menyatakan sebaliknya (misalnya, dalam bentuk pemilihan lokasi data), Google mereplikasi Data Mitra 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 Mitra dan, jika Mitra adalah prosesor, mengizinkan Mitra 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 Mitra. Tanpa membatasi kewajiban tersurat Google terkait dengan Solusi Bare Metal, Mitra akan mengambil langkah-langkah yang wajar untuk melindungi dan menjaga keamanan Data Mitra 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.

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

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 Mitra) 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 Mitra.

Google Distributed Cloud Edge (Google Cloud Platform)

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

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

- 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*. Mitra menginstruksikan Google untuk menghapus seluruh Data Mitra yang tersisa (termasuk salinan yang ada) dari Peralatan di akhir Jangka Waktu sesuai dengan hukum yang berlaku. Jika Mitra ingin menyimpan Data Mitra apa pun setelah Jangka Waktu berakhir, Mitra 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 Mitra 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 Mitra hanya disimpan pada Peralatan untuk ditempatkan di Lokasi Mitra.

      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 GDCE dan meningkatkan keamanan produk di lingkungan produksi GDCE.

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. GDCE memiliki integrasi CMEK; informasi lebih lanjut dapat ditemukan di https://cloud.google.com/kms/docs/cmek.

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

Penyimpanan Terikat. Penyimpanan data MitraMitra 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 GDCE.

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 Mitra atau tidak dapat mengenkripsi data pribadi di lingkungan VMware Mitra.

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 Mitra 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 Mitra di antara beberapa pusat data yang tersebar secara geografis. Google juga mengisolasi Data Mitra secara logis. Mitra akan diberikan kendali atas kebijakan berbagi data tertentu. Kebijakan tersebut, sesuai dengan fungsionalitas Layanan, akan memungkinkan Mitra untuk menentukan pengaturan berbagi produk yang berlaku bagi Pengguna Akhir Mitra untuk tujuan tertentu. Mitra 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 Mitra dan, jika Mitra adalah pemroses, mengizinkan Mitra untuk meminta akses ke Laporan SOC NetApp kepada pengendali yang relevan sesuai dengan Bagian 7.5.3 (Ketentuan Bisnis Tambahan untuk Peninjauan dan Audit).

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 Mitra 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 Mitra 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 Mitra 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 Eksportir)" 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 Mitra. Mitra bertanggung jawab atas keamanan lingkungan, basis data, dan konfigurasi Mitra untuk Looker (Mitra 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 Mitra Non-EMEA. Mitra tidak berkewajiban untuk mensertifikasi atau mengidentifikasi Otoritas Pengawasnya yang berwenang sebagaimana dijelaskan dalam Bagian 4.2 (Sertifikasi oleh Mitra 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:

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

b. 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 Processingmelengkapi 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 Mitra atau Pelanggannya, Mitra 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 Mitra 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 Mitra mengendalikan akses ke aplikasi oleh personel Google untuk memberikan dukungan teknis yang diminta oleh Mitra atau Pengguna Akhir.

Layanan SecOps

1. Definisi Tambahan.

- *"Akun"*, jika tidak didefinisikan dalam Perjanjian, berarti Layanan SecOps Mitra atau akun Google Cloud Platform Mitra, sebagaimana berlaku.

- "*Layanan SecOps*" berarti Chronicle SIEM, Chronicle SOAR, dan Mandiant Solutions, yang masing-masing dijelaskan dalam https://cloud.google.com/terms/secops/services, yang tidak termasuk Penawaran Pihak Ketiga mana pun. Untuk menghindari keraguan, Layanan SecOps tidak mencakup Mandiant Managed Services dan Mandiant Consulting Services.

- *"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 LunakSecOps, 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 Mitra sesuai pilihannya dan/atau sebagaimana Mitra 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 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.

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

4. Tidak Ada Sertifikasi oleh Mitra Non-EMEA. Mitra tidak berkewajiban untuk mengesahkan atau mengidentifikasi Otoritas Pengawasnya yang berwenang sebagaimana dijelaskan dalam Bagian 4.2 (Sertifikasi oleh Mitra 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 Mitra, Mitra 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 Mitra menyediakan dan memperbarui informasi tersebut melalui cara lain.

Versi sebelumnya dari Ketentuan Pemrosesan dan Keamanan Data (Mitra):

30 Juni 2022 24 September 2021 20 Agustus 2020 10 Agustus 2020 17 Juli 2020 1 Oktober 2019 28 Februari 2019 25 Mei 2018 13 Maret 2018

Versi sebelumnya dari Ketentuan Pemrosesan dan Keamanan Data Layanan SecOps (Mitra):

6 Februari 2023 31 Oktober 2022 27 September 2021

VERSI SEBELUMNYA *(Terakhir diubah pada tanggal 30 Oktober 2024)*

15 Oktober 2024 26 September 2024 9 September 2024 9 April 2024 8 November 2023 15 Agustus 2023 20 September 2022