



Buku Putih Google Cloud
Maret 2023

Undang-Undang Pelindungan Data Pribadi Indonesia



Daftar Isi

Pengantar	3
Ringkasan Undang-Undang Pelindungan Data Pribadi Indonesia	3
Ringkasan perlindungan data Google Cloud & Model Tanggung Jawab Bersama	4
Pendekatan Google Cloud terhadap keamanan dan perlindungan data	4
Pendekatan Google Cloud terhadap privasi dan perlindungan data	5
Model Tanggung Jawab Bersama	11
Cara Google Cloud membantu pelanggan memenuhi persyaratan Undang-Undang Pelindungan Data Pribadi	13
Kesimpulan	23

Pernyataan penyangkalan

Buku putih ini berkenaan dengan produk-produk Google Cloud yang dijelaskan di cloud.google.com. Isi laporan ini aktual per Maret 2023 dan menunjukkan keadaan sebenarnya pada saat penulisan. Kebijakan dan sistem keamanan Google dapat berubah pada masa mendatang, seiring upaya kami untuk terus meningkatkan perlindungan bagi pelanggan.

Pengantar

Bagi Google Cloud, privasi merupakan bagian penting dalam pengembangan dan pengoperasian produk serta layanan kami. Kami telah menetapkan standar tinggi dalam hal menghosting, menyajikan, dan melindungi data pelanggan dengan memusatkan keamanan dan perlindungan data sebagai inti dari cara kami mendesain dan membuat produk. Kami berangkat dari prinsip yang paling mendasar bahwa sebagai pelanggan Google Cloud, Anda¹ adalah pemilik data Anda sendiri. Kami menerapkan tindakan keamanan yang ketat untuk membantu mengamankan data pelanggan serta memberi Anda alat dan fitur untuk membantu mengontrolnya sesuai keinginan Anda.

Laporan resmi ini memberikan informasi kepada pelanggan kami tentang Undang-Undang Pelindungan Data Pribadi Indonesia dan cara Google Cloud menggunakan kemampuan keamanan dan privasi data terdepan di industri dari Google untuk membantu menyimpan, memproses, memelihara, dan mengamankan data pelanggan². Kami berkomitmen untuk bekerja sama dengan pelanggan kami agar mereka dapat men-deploy workload menggunakan layanan Google Cloud dan Google Workspace untuk kebutuhan produktivitas mereka dengan cara yang sesuai dengan persyaratan Undang-Undang Pelindungan Data Pribadi Indonesia. Kami menjelaskan fitur perlindungan data kami dan menguraikan cara fitur tersebut memenuhi persyaratan yang ditetapkan. Namun, perlu diperhatikan bahwa, sebagai penyedia layanan cloud, kami tidak berwenang untuk memberi Anda saran hukum. Hal tersebut hanya bisa Anda dapatkan dari penasihat hukum Anda.

Ringkasan Undang-Undang Pelindungan Data Pribadi Indonesia

[Undang-Undang Pelindungan Data Pribadi Indonesia](#) (“Undang-Undang PDP”), yang berlaku sejak tanggal 17 Oktober 2022, mengatur pengumpulan, penggunaan, pengungkapan, dan pemrosesan data pribadi lainnya oleh organisasi internasional serta entitas pemerintah dan swasta.

Serupa dengan undang-undang perlindungan data lainnya, Undang-Undang PDP memberikan kewajiban yang berbeda terkait “Pengontrol Data Pribadi” (“Pengontrol”) dan “Pemroses Data Pribadi” (“Pemroses”). Pengontrol adalah orang, lembaga publik, atau organisasi internasional yang bertindak sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kontrol terhadap pemrosesan data pribadi. Pemroses adalah orang, agensi publik, atau organisasi internasional yang bertindak sendiri atau bersama-sama dalam memproses data pribadi atas nama Pengontrol. Undang-undang ini memberlakukan kewajiban khusus terkait pemrosesan “Data Pribadi Spesifik”, yang mencakup kategori data yang lebih sensitif seperti data kesehatan, informasi biometrik, dan data anak-anak, misalnya dengan mewajibkan penilaian dampak perlindungan data tempat Pengontrol memproses Data Pribadi Spesifik.

¹ Dalam laporan resmi ini, “Anda” merujuk pada pelanggan Google Cloud dan Google Workspace serta partner Google Cloud. Kecuali jika dinyatakan lain, penyebutan “pelanggan” mencakup partner Google Cloud dan penyebutan “data pelanggan” mencakup data partner Google Cloud.

² Dalam laporan resmi ini, “data pelanggan” dan “data Anda” merujuk pada data pelanggan yang kami proses berdasarkan perjanjian Google Cloud Anda.

Undang-Undang PDP menetapkan tanggung jawab bagi organisasi dan hak privasi bagi individu. Undang-undang ini juga memiliki beberapa konsep yang sama dengan undang-undang perlindungan data lainnya, seperti persyaratan untuk memproses data pribadi yang hanya sesuai dengan dasar hukum serta kewajiban untuk mengadopsi kebijakan dan prosedur agar dapat bertanggung jawab terhadap kepatuhan. Selain itu, Undang-Undang PDP mewajibkan Pengontrol memproses data pribadi berdasarkan serangkaian prinsip pemrosesan yang dienumerasi, termasuk bahwa organisasi harus memberi tahu subjek data tentang tujuan dari pemrosesan data pribadi, memproses data pribadi secara terbatas, spesifik, transparan, dan sah, serta harus melindungi keamanan data pribadi dari akses tidak sah, pengungkapan tidak sah, perubahan tidak sah, penyalahgunaan, kerusakan, dan kehilangan.

Undang-Undang PDP berlaku untuk organisasi baik yang berada di Indonesia maupun di luar Indonesia, jika aktivitas pemrosesan data organisasi tersebut dapat menimbulkan konsekuensi hukum di Indonesia atau memengaruhi warga negara Indonesia di luar Indonesia. Dalam hal ini, Undang-Undang PDP memiliki cakupan penerapan yang lebih luas daripada sebagian besar undang-undang perlindungan data lainnya, yang sebagian besar hanya berlaku untuk aktivitas di dalam negara atau ditujukan kepada penduduk negara tersebut.

Penerapan undang-undang ini dimulai pada Oktober 2024, dua tahun setelah disahkan. Terdapat berbagai mekanisme penerapan dalam Undang-Undang PDP, termasuk hak pribadi atas tindakan melanggar hukum, denda administrasi, penyitaan keuntungan atau aset, dan hukuman pidana. Undang-Undang PDP mengatur pembentukan Otoritas Perlindungan Data untuk menjalankan UU tersebut dan menerbitkan peraturan pelaksanaannya pada masa mendatang.

Ringkasan perlindungan data Google Cloud & Model Tanggung Jawab Bersama

Kontrol privasi dan keamanan canggih Google Cloud dapat memberikan keyakinan kepada pelanggan untuk memanfaatkan layanan Google Cloud dan Google Workspace dengan cara yang sesuai dengan persyaratan Undang-Undang PDP. Selain itu, kami terus berupaya mengembangkan kemampuan privasi dan keamanan kami. Untuk membantu pelanggan dalam hal kepatuhan dan pelaporan, Google memberikan informasi dan praktik terbaik, serta menyediakan akses mudah ke dokumentasi. Di bagian ini, kami menjelaskan kemampuan privasi dan perlindungan data yang komprehensif serta fitur keamanan data canggih kami yang paling relevan dengan Undang-Undang PDP. Kemudian, kami menjelaskan cara kami berbagi tanggung jawab keamanan dan kepatuhan berdasarkan Model Tanggung Jawab Bersama.

Pendekatan Google Cloud terhadap keamanan dan perlindungan data

Fokus Google terhadap keamanan dan perlindungan informasi merupakan salah satu kriteria desain utama kami. Keamanan adalah inti dari segala hal yang kami lakukan. Keamanan tertanam dalam budaya serta arsitektur kami, dan kami berfokus untuk meningkatkannya setiap hari. Di bagian ini, kami memberikan ringkasan kontrol organisasi dan teknis yang kami gunakan untuk melindungi data Anda.

Untuk mempelajari lebih lanjut pendekatan kami terhadap keamanan dan kepatuhan, baca [laporan resmi keamanan Google](#) untuk layanan Google Cloud dan [laporan resmi keamanan Google Workspace](#).

Topik

Pendekatan Google Cloud terhadap privasi dan perlindungan data

- Prinsip kepercayaan privasi data
- Tim privasi khusus
- Kontrol pelanggan dan akses data
- Akses terbatas ke data pelanggan
- Permintaan data oleh penegak hukum

Pendekatan Google Cloud terhadap keamanan data

- Budaya keamanan yang kuat
- Tim keamanan
- Infrastruktur terpercaya
- Redundansi infrastruktur
- Keamanan pusat data yang canggih
- Enkripsi data
- Teknologi berbasis cloud
- Model Tanggung Jawab Bersama

Pendekatan Google Cloud terhadap privasi dan perlindungan data

Privasi dan perlindungan data sangat penting bagi Google. Kami mendesain produk dan layanan kami dari awal dengan kepercayaan dan privasi sebagai prinsip panduan. Google Cloud berupaya untuk membantu memastikan perlindungan dan privasi terhadap data pelanggan melalui tiga cara: 1) kami memberikan perlindungan data yang lebih unggul melalui infrastruktur inti aman yang didesain, dibangun, dan dioperasikan untuk membantu mencegah ancaman; 2) kami memberi pelanggan kontrol keamanan yang canggih untuk membantu mereka memenuhi tujuan kebijakan, peraturan, dan bisnis; dan 3) kami berupaya untuk memenuhi tanggung jawab kami terhadap kepatuhan serta mempermudah pelanggan kami memenuhi kepatuhan.

Prinsip kepercayaan privasi dan perlindungan data

Kami ingin pelanggan kami merasa yakin saat menggunakan produk Google Cloud dan Google Workspace. Kami yakin bahwa kepercayaan terbentuk melalui transparansi, dan kami ingin bersikap transparan terkait penawaran dan komitmen kami terhadap pelanggan dalam melindungi data mereka di cloud.

Komitmen kami kepada Anda terkait data Anda

Data sangat penting bagi bisnis Anda sehingga Anda pun menaruh perhatian besar untuk menjaganya tetap aman dan di bawah kendali Anda. Kami ingin Anda merasa yakin bahwa dengan memanfaatkan layanan Google Workspace dan Google Cloud, Anda tidak harus mengorbankan keamanan atau kendali atas data bisnis Anda.

Google Cloud percaya bahwa kepercayaan terbentuk melalui transparansi. Kami ingin bersikap transparan mengenai komitmen kami dan ekspektasi Anda terkait tanggung jawab bersama untuk melindungi dan mengelola data Anda di cloud.

Saat Anda menggunakan layanan Google Workspace atau Google Cloud, Anda dapat:

1. **Mengetahui bahwa keamanan Anda adalah prioritas utama dari semua hal yang kami lakukan.**

Kami akan segera memberitahu Anda jika kami mendeteksi pelanggaran keamanan yang membahayakan data Anda.

2. **Mengontrol apa yang terjadi dengan data Anda.**

Kami memproses data pelanggan berdasarkan instruksi Anda. Anda dapat mengakses data Anda atau mengambilnya kapan saja.

3. **Mengetahui bahwa data pelanggan tidak digunakan untuk iklan.**

Kami tidak memproses data pelanggan Anda untuk membuat profil iklan atau meningkatkan kualitas produk Google Ads.

4. **Mengetahui tempat Google menyimpan data dan mengandalkannya untuk menyediakan data saat Anda membutuhkan.**

Kami memublikasikan lokasi pusat data Google kami yang sangat tersedia, tangguh, dan aman.

5. **Bergantung pada praktik keamanan Google yang diverifikasi secara independen.**

Kepatuhan kami terhadap standar keamanan dan privasi internasional yang diakui, disertifikasi, dan divalidasi oleh auditor independen—di mana pun lokasi data Anda di Google Cloud.

6. **Yakinlah bahwa kami tidak pernah memberikan akses “backdoor” ke data Anda atau ke server kami yang menyimpan data Anda kepada entitas pemerintah mana pun.**

Kami menolak permintaan pemerintah yang tidak valid dan kami menerbitkan laporan transparansi untuk permintaan pemerintah.

Untuk mempelajari lebih lanjut komitmen kami dalam mengamankan informasi pelanggan, baca [halaman Privasi Google Cloud](#). Lihat persyaratan pemrosesan data untuk [Google Workspace](#) dan [Google Cloud](#).

Tim privasi khusus

Tim privasi Google beroperasi secara terpisah dari organisasi keamanan dan pengembangan produk, tetapi berpartisipasi dalam peluncuran produk Google dengan meninjau dokumentasi desain serta melakukan peninjauan kode untuk membantu memastikan bahwa persyaratan privasi dipatuhi. Mereka

Google Cloud

membantu merilis produk yang mencerminkan praktik privasi yang kuat: pengumpulan data pengguna yang transparan, yang membekali pengguna dan administrator dengan opsi konfigurasi privasi yang bermakna, dan terus menjadi penjaga yang baik atas informasi yang disimpan di platform kami. Untuk mempelajari lebih lanjut tim privasi kami, baca bagian tim privasi di [laporan resmi keamanan Google](#) untuk layanan Google Cloud dan [laporan resmi Keamanan Google Workspace](#).

Kontrol pelanggan dan akses data

Data pelanggan Google Cloud adalah milik mereka sendiri, bukan milik Google. Google hanya akan memproses data pelanggan sesuai dengan kewajiban kontrak. Kami juga memberi pelanggan solusi yang memungkinkan kontrol izin resource yang terperinci. Misalnya, dengan menggunakan Cloud Identity and Access Management, pelanggan dapat memetakan fungsi tugas pada grup dan peran, sehingga pengguna hanya mengakses data yang mereka perlukan untuk menyelesaikan tugas. Selain itu, pelanggan dapat menghapus data pelanggan dari sistem kami atau mengambilnya jika mereka memilih untuk berhenti menggunakan layanan kami.

Akses terbatas ke data pelanggan

Untuk menjaga privasi dan keamanan data, Google secara logis memisahkan setiap data pelanggan dari data pelanggan dan pengguna lain, bahkan saat data disimpan di server fisik yang sama. Hanya sekelompok kecil karyawan Google yang memiliki akses ke data pelanggan yang sesuai dengan alasan eksplisit berdasarkan peran dan fungsi tugas. Semua akses tambahan diberikan sesuai dengan prosedur yang ketat dan dilacak melalui data audit yang tersedia mendekati real-time melalui Transparansi Akses.

Pendekatan Google Cloud terhadap keamanan data

Di bagian ini, kami memberikan ringkasan kontrol organisasi dan teknis yang kami gunakan untuk melindungi data Anda di Google Cloud. Baca [laporan resmi keamanan Google](#), dan [laporan resmi Keamanan Google Workspace](#) untuk informasi tambahan mengenai praktik keamanan kami.

Budaya keamanan yang kuat

Keamanan adalah inti dari budaya Google. Budaya ini diperkuat dalam pelatihan keamanan karyawan dan acara di seluruh perusahaan untuk meningkatkan awareness serta mendorong inovasi pada keamanan dan privasi.

Untuk mempelajari lebih lanjut budaya keamanan kami, baca bagian budaya keamanan dalam [laporan resmi keamanan Google](#) dan [laporan resmi Keamanan Google Workspace](#) kami.

Tim keamanan

Google memiliki lebih dari 850 tenaga kerja profesional di bidang keamanan, termasuk sejumlah pakar ternama dunia. Tim ini mengelola sistem pertahanan perusahaan, mengembangkan proses peninjauan keamanan, membangun infrastruktur keamanan, menerapkan kebijakan keamanan Google, dan memindai ancaman keamanan secara aktif. Tim keamanan kami juga ikut berpartisipasi dalam aktivitas riset dan penjangkauan untuk melindungi komunitas pengguna Internet yang lebih luas, bukan

hanya orang yang memilih solusi Google. Makalah penelitian kami tersedia untuk publik. Sebagai bagian dari upaya penjangkauan kami, kami memiliki tim bernama Project Zero yang bertujuan mencegah serangan yang ditargetkan dengan melaporkan bug ke vendor software.

Selain itu, tim keamanan kami bekerja 24/7 untuk mendeteksi dan menyelesaikan potensi insiden keamanan dengan cepat. Program manajemen insiden keamanan kami disusun berdasarkan praktik terbaik di industri dan disesuaikan dalam program "Manajemen Insiden di Google (IMAG)" kami, yang dibuat dengan aspek unik Google beserta infrastrukturnya. Kami juga menguji rencana respons insiden secara rutin, sehingga kami selalu siap siaga.

Untuk mempelajari lebih lanjut, baca bagian tim keamanan, pengelolaan kerentanan, dan pemantauan dalam [laporan resmi keamanan Google](#). Selain itu, baca bagian tim keamanan, pengelolaan kerentanan, dan pemantauan dalam [laporan resmi Keamanan Google Workspace](#).

Infrastruktur tepercaya

Kami mengonsep, mendesain, dan membangun Google Cloud agar dapat beroperasi dengan aman. Google adalah inovator dalam teknologi pengelolaan hardware, software, jaringan, dan sistem. Kami mendesain khusus server, sistem operasi eksklusif, dan pusat data yang tersebar secara geografis. Dengan prinsip "defense in depth", kami telah menciptakan infrastruktur IT yang secara umum lebih aman dan mudah dikelola dibandingkan dengan sebagian besar opsi deployment lain. Infrastruktur kami dapat memberikan deployment layanan yang aman, penyimpanan data yang aman dengan pengamanan privasi pengguna akhir, komunikasi yang aman antar layanan, komunikasi yang aman dan pribadi dengan pelanggan melalui Internet, serta operasi yang aman oleh administrator. Kami menjaga keamanan infrastruktur ini dalam lapisan progresif, yang dimulai dari keamanan fisik pusat data kami, membangun solusi dengan hardware dan software inti yang dirancang untuk keamanan, melanjutkan dengan deployment layanan yang aman, penyimpanan data yang aman, dan komunikasi internet yang aman, dan terakhir, mengoperasikan infrastruktur dengan cara yang aman.

Untuk mempelajari lebih lanjut, baca [Ringkasan Desain Keamanan Infrastruktur Google Cloud](#), serta [Adendum Pemrosesan Data Cloud](#), Lampiran 2: Tindakan Keamanan.

Redundansi infrastruktur

Komponen infrastruktur Google didesain agar memiliki redundansi yang tinggi. Redundansi ini diterapkan pada desain dan deployment server, penyimpanan data, jaringan dan konektivitas Internet, serta layanan software itu sendiri. "Redundansi dari segalanya" ini menciptakan solusi andal yang tidak bergantung pada satu server, pusat data, atau koneksi jaringan. Pusat data kami tersebar secara geografis untuk meminimalkan dampak gangguan regional terhadap produk global, seperti bencana alam dan pemadaman layanan lokal. Jika terjadi kegagalan hardware, software, atau jaringan, layanan platform dan bidang kontrol dapat mengubah konfigurasi secara otomatis, sehingga pelanggan dapat terus bekerja tanpa gangguan. Infrastruktur kami yang sangat redundan juga membantu pelanggan terlindungi dari kehilangan data. Pelanggan dapat membuat dan men-deploy resource berbasis cloud kami di berbagai region dan zona, sehingga mereka dapat membangun sistem yang tangguh dan sangat tersedia. Untuk mempelajari lebih lanjut, baca solusi yang sangat tersedia dan latensi rendah dalam [laporan resmi keamanan Google](#) dan [laporan resmi Keamanan Google Workspace](#).

Keamanan pusat data yang canggih

Pusat data Google memiliki lapisan perlindungan keamanan fisik. Kami membatasi akses ke pusat data ini hanya untuk sebagian kecil karyawan dan memiliki berbagai kontrol keamanan fisik guna melindungi area pusat data kami, seperti identifikasi biometrik, deteksi logam, penghalang kendaraan, dan kartu akses elektronik yang didesain khusus. Kami memantau pusat data kami 24/7/365 untuk mendeteksi dan melacak penyusup. Patroli di pusat data secara rutin dilakukan oleh petugas keamanan berpengalaman yang telah melewati pemeriksaan latar belakang dan pelatihan yang ketat. Untuk mempelajari lebih lanjut, baca halaman [Inovasi Pusat Data](#) kami.

Enkripsi data

Google mengenkripsi data dalam penyimpanan dan mengenkripsi data dalam pengiriman secara default. Jenis enkripsi yang digunakan bergantung pada lapisan OSI, jenis layanan, dan komponen infrastruktur fisik. Secara default, kami mengenkripsi dan mengautentikasi data dalam pengiriman di satu atau beberapa lapisan jaringan saat data dipindahkan di luar batas fisik yang tidak dikontrol oleh atau atas nama Google. Untuk mempelajari lebih lanjut, baca halaman [Enkripsi dalam Pengiriman](#) dan [Enkripsi dalam Penyimpanan](#).

Teknologi berbasis cloud

Kami terus berinvestasi besar-besaran di bidang keamanan, baik dalam desain fitur baru maupun pengembangan alat canggih sehingga pelanggan dapat mengelola lingkungan mereka dengan lebih aman. Beberapa contoh adalah Cloud Security Command Center untuk Google Cloud dan Pusat Keamanan untuk Google Workspace yang menghadirkan hasil analisis yang bisa ditindaklanjuti kepada tim keamanan dengan memberikan analisis dan rekomendasi praktik terbaik keamanan dari Google, serta Kontrol Layanan VPC, yang membantu menetapkan perimeter keamanan virtual untuk data sensitif. Untuk mempelajari lebih lanjut teknologi keamanan kami, baca halaman [produk & kapabilitas keamanan](#).

Referensi Keamanan Tambahan

(1) [Keamanan infrastruktur Google](#)

Google mengelola keamanan infrastruktur kami (misalnya, hardware, software, jaringan, dan fasilitas yang mendukung layanan). Google memberikan informasi mendetail kepada pelanggan tentang praktik keamanan kami di:

- Halaman [keamanan infrastruktur](#) kami
- [Laporan resmi keamanan](#) kami
- [Laporan resmi keamanan berbasis cloud](#) kami
- Halaman [ringkasan desain keamanan infrastruktur](#) kami
- Halaman [referensi keamanan](#) kami
- Halaman [kepatuhan Cloud](#) kami

(2) [Produk keamanan](#)

Informasi terkait produk keamanan Google tersedia di halaman [Produk Keamanan Cloud](#) kami. Ilustrasi daftar layanan Google Cloud dan Google Workspace di bawah dapat digunakan untuk membantu memenuhi persyaratan penyimpanan dan keamanan:

Kontrol akses

- [Verifikasi 2 Langkah](#) - Memberikan lapisan keamanan tambahan bagi bisnis pelanggan dan mencegah pelaku kejahatan cyber yang mencoba mencuri nama serta sandi pengguna untuk mengakses data bisnis.
- [Identity and Access Management \(IAM\)](#) - Menetapkan peran dan izin ke grup administratif, yang menggabungkan prinsip hak istimewa terendah dan pemisahan tugas.
- [Kontrol Layanan VPC](#) - Mengontrol akses ke layanan tertentu oleh entitas tertentu secara ketat untuk mengurangi kehilangan data yang disengaja maupun tidak disengaja.

Log Akses

- [Cloud Logging](#) - Menyimpan, menelusuri, menganalisis, memantau, dan membuat pemberitahuan terkait data logging dan peristiwa dari Google Cloud serta Amazon Web Services.
- [Transparansi Akses](#) - Mempertahankan visibilitas akses orang dalam ke data Anda melalui log yang mendekati real-time dari Transparansi Akses.

Perlindungan dari Ancaman Eksternal

- [Cloud Security Command Center](#) - Memperkuat postur keamanan Anda dengan mengevaluasi keamanan dan permukaan serangan data Anda; menyediakan inventaris dan penemuan aset; mengidentifikasi kesalahan konfigurasi, kerentanan, dan ancaman; serta membantu Anda memitigasi dan memulihkan risiko.
- [Virtual Machine Threat Detection](#) - Mendeteksi ancaman melalui instrumentasi tingkat hypervisor.

Pemantauan

- [Dasbor Status Google Cloud](#) - Menyediakan informasi status pada layanan.
- [Dasbor Status Google Workspace](#) - Menyediakan informasi status pada layanan.
- [Google Cloud Operations](#) - Mendapatkan insight terkait aplikasi yang berjalan di Google Cloud, termasuk ketersediaan dan waktu beroperasi layanan tersebut.
- [Laporan Konsol Admin](#) - Memeriksa potensi risiko keamanan, mengukur kolaborasi pengguna, melacak siapa saja yang login beserta waktunya, menganalisis aktivitas administrator, dan masih banyak lagi.

(3) Referensi keamanan

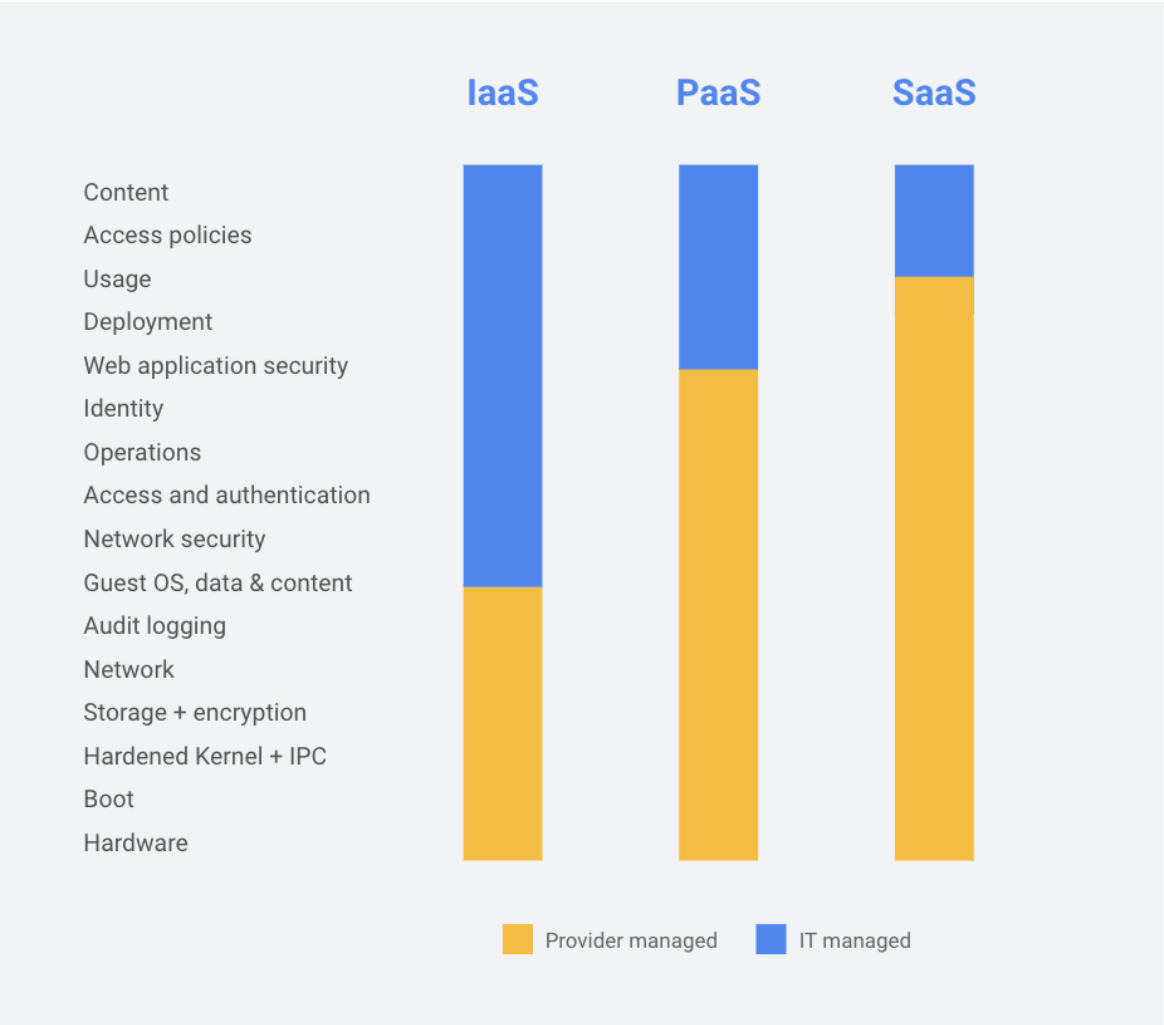
Google juga memublikasikan panduan tentang:

- [Praktik terbaik keamanan](#)
- [Kasus penggunaan keamanan](#)
- [Blueprint keamanan](#)

Model Tanggung Jawab Bersama

Berdasarkan Model Tanggung Jawab Bersama kami, pelanggan cloud beserta CSP-nya berbagi tanggung jawab dalam mengelola lingkungan IT, termasuk hal-hal yang terkait dengan keamanan dan kepatuhan. Sebagai partner terpercaya, peran Google Cloud dalam model ini meliputi penyediaan layanan pada platform yang sangat aman dan terkendali serta menawarkan berbagai fitur keamanan yang dapat dimanfaatkan oleh pelanggan. Tanggung jawab bersama memungkinkan pelanggan kami mengalokasikan resource secara lebih efektif ke kompetensi inti mereka dan berfokus pada hal yang mereka kuasai. Model tanggung jawab bersama tidak menghilangkan akuntabilitas dan risiko dari pelanggan yang menggunakan layanan Google Cloud, tetapi model ini akan membantu meringankan beban saat kami mengelola dan mengontrol komponen sistem dan pengawasan fisik fasilitas. Model ini juga mengalihkan sebagian biaya keamanan dan kepatuhan yang ditanggung oleh pelanggan ke Google Cloud. Gambar berikut menunjukkan contoh model tanggung jawab bersama pada penawaran lokal, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), dan Software as a Service (SaaS). Perlu diperhatikan bahwa mungkin terdapat perbedaan tanggung jawab tergantung layanan tertentu yang digunakan.

Untuk mengetahui informasi selengkapnya tentang konfigurasi keamanan dan produk Google Cloud, pelanggan sebaiknya melihat dokumentasi produk yang berlaku.



Cara Google Cloud membantu pelanggan memenuhi persyaratan Undang-Undang Pelindungan Data Pribadi

Kewajiban Perlindungan Data	Cara Google Mendukung Persyaratan Undang-Undang PDP
Pengumpulan, Penggunaan, dan Pengungkapan Data Pribadi	
Pemberitahuan Pengumpulan - Organisasi yang memproses data pribadi harus memberi tahu subjek data terkait tujuan pemrosesan dan memberikan informasi mengenai aktivitas pemrosesan. - Berdasarkan Undang-Undang PDP, Pengontrol harus memberikan informasi tertentu kepada individu saat memperoleh izin. Informasi ini mencakup konfirmasi bahwa pemrosesan data pribadi akan dilakukan untuk tujuan yang sah; tujuan pemrosesan data pribadi; jenis dan relevansi data pribadi yang akan diproses; periode retensi dokumen yang berisi data pribadi; detail terkait informasi yang dikumpulkan; durasi pemrosesan data pribadi yang akan dijalankan; dan hak-hak yang dimiliki subjek data pribadi. - Pengontrol juga harus memberi tahu subjek data jika Pengontrol mengalami penggabungan, spin-off, akuisisi, konsolidasi, atau pembubaran.	Tanggung Jawab Pelanggan: - Memastikan data pribadi dikumpulkan dengan cara yang sah. - Pelanggan juga harus mengungkapkan cara mereka mengumpulkan dan memproses data pribadi. Komentar Google Cloud: - Google berkomitmen untuk hanya mengakses atau menggunakan data Anda guna menyediakan layanan yang dipesan oleh Anda dan mematuhi persyaratan kontrak.
Batasan Tujuan Pengontrol harus memproses Data Pribadi secara spesifik dan terbatas, sah, dan transparan.	Tanggung Jawab Pelanggan: - Memastikan pengumpulan, penggunaan, dan pengungkapan data pribadi bersifat terbatas untuk tujuan sah yang ditentukan. Komentar Google Cloud: - Anda memutuskan informasi apa saja yang akan diberikan ke layanan dan layanan mana yang akan digunakan, cara

	menggunakannya, dan untuk tujuan apa. Google berkomitmen untuk hanya mengakses atau menggunakan data Anda guna menyediakan layanan yang dipesan oleh Anda dan mematuhi persyaratan kontrak. Google tidak akan menggunakan data Anda untuk produk lainnya atau untuk menayangkan iklan. Lihat bagian Penggunaan Data pada laporan resmi Keamanan Google.
Penggunaan Data Pribadi - Berdasarkan Undang-Undang PDP, Pengontrol berkewajiban melindungi data pribadi dari pemrosesan yang tidak sah. - Organisasi dilarang mengambil atau mengumpulkan data pribadi yang bukan milik mereka secara tidak sah dengan tujuan menguntungkan diri sendiri atau orang lain jika hal tersebut dapat menyebabkan kerugian pada subjek data. Organisasi juga dilarang mengungkapkan data pribadi yang bukan milik mereka secara tidak sah.	Tanggung Jawab Pelanggan: - Memastikan pengumpulan, penggunaan, atau pengungkapan data pribadi mematuhi hukum. Komentar Google Cloud: - Anda memutuskan informasi/data apa saja yang akan diberikan ke layanan dan layanan mana yang akan digunakan, cara menggunakannya, dan untuk tujuan apa. - Google berkomitmen untuk hanya mengakses atau menggunakan data Anda guna menyediakan layanan yang dipesan oleh Anda dan mematuhi persyaratan kontrak. Google tidak akan menggunakannya untuk produk lain atau untuk menayangkan iklan. Lihat bagian Penggunaan Data pada laporan resmi Keamanan Google.
Pengungkapan Data Pribadi - Berdasarkan Undang-Undang PDP, Pengontrol berkewajiban menjaga kerahasiaan data pribadi, kecuali jika ada pengecualian yang berlaku. - Organisasi dilarang mengungkapkan data pribadi yang bukan milik mereka secara tidak sah. - Berdasarkan undang-undang ini, jika Pengontrol melibatkan Pemroses untuk memproses data pribadi, Pemroses harus melaksanakan pemrosesan data pribadi sesuai dengan instruksi Pengontrol. - Undang-undang PDP juga menyatakan bahwa Pemroses dapat melibatkan Pemroses lain untuk memproses data pribadi jika Pengontrol telah memberikan persetujuan tertulis sebelumnya.	Tanggung Jawab Pelanggan: - Mengembangkan proses penanganan pengungkapan. Komentar Google Cloud: - Google Cloud membuat komitmen kerahasiaan, perlindungan data, dan keamanan yang kuat dalam kontrak kami. - Google berkomitmen untuk memproses data Anda guna memberikan layanan yang dipesan oleh Anda dan mematuhi persyaratan kontrak. Google tidak akan menggunakannya untuk produk lain atau untuk menayangkan iklan. Lihat bagian Penggunaan Data pada laporan resmi Keamanan Google.

Berdasarkan undang-undang ini, Pengontrol berkewajiban mengawasi pihak-pihak yang terlibat dalam pemrosesan data pribadi di bawah kendali Pengontrol.	
Pengungkapan Data Lintas Batas Negara - Saat mentransfer data pribadi, undang-undang mengharuskan Pengontrol memastikan bahwa negara domisili Pengontrol dan/atau negara domisili Pemroses yang menerima transfer data pribadi melindungi data pribadi setidaknya dengan memberikan perlindungan yang setara dengan Undang-Undang PDP. - Selain itu, Pengontrol bertanggung jawab untuk memastikan bahwa tindakan perlindungan data yang memadai dan bersifat mengikat diterapkan pada data pribadi yang ditransfer, atau untuk mendapatkan izin transfer dari subjek data.	Tanggung Jawab Pelanggan: - Pelanggan harus memastikan bahwa justifikasi dan izin yang sesuai (jika izin tidak diperlukan) telah tersedia untuk transfer lintas batas. Komentar Google Cloud: - Google menerapkan tindakan keamanan yang sama tangguhnya terhadap data pelanggan di mana pun data tersebut berada. Perjanjian pemrosesan data kami untuk layanan Google Workspace dan Google Cloud menyatakan dengan jelas komitmen privasi dan keamanan kami kepada pelanggan. - Layanan Google Workspace dan Google Cloud menjalani beberapa audit pihak ketiga independen secara rutin untuk memverifikasi kontrol keamanan, privasi, dan kepatuhan. Lihat laporan kepatuhan Cloud.
Akuntabilitas	
Penilaian dampak privasi Jika pemrosesan data pribadi tertentu berpotensi menimbulkan risiko tinggi bagi subjek data, Pengontrol harus melakukan penilaian terhadap dampak pemrosesan pada subjek data tersebut. Keadaan yang dianggap berisiko tinggi meliputi, tetapi tidak terbatas pada, pengambilan keputusan otomatis yang memiliki konsekuensi hukum atau dampak yang signifikan terhadap subjek data atau pemrosesan Data Pribadi yang bersifat spesifik (seperti data kesehatan, informasi biometrik, atau data anak), pemrosesan data pribadi berskala besar, pemrosesan data pribadi untuk tujuan mengevaluasi atau memantau subjek	Tanggung Jawab Pelanggan: - Pelanggan harus melakukan penilaian dampak privasi, jika diwajibkan. Komentar Google Cloud: - Google Cloud menyadari bahwa Anda memerlukan informasi tertentu agar dapat melakukan penilaian dampak privasi. Perjanjian pemrosesan data kami untuk layanan Google Workspace dan Google Cloud menyatakan dengan jelas komitmen privasi dan keamanan kami kepada pelanggan. - Selain itu, Anda dapat meninjau laporan sertifikasi dan audit terkini Google melalui laporan kepatuhan Cloud.

data secara sistematis, dan pemrosesan data pribadi untuk tujuan mencocokkan atau menggabungkan kelompok data.	
Permintaan untuk mengakses atau mengoreksi data pribadi • Undang-undang mengharuskan Pengontrol memberi subjek data akses ke data pribadi yang diproses sehubungan dengan mereka, dan bagaimana data tersebut diproses serta periode retensi data relevan yang diberikan untuk data pribadi tersebut. ◦ Akses harus diberikan paling lambat 72 jam sejak Pengontrol menerima permintaan subjek data, kecuali jika ada pengecualian yang berlaku. • Selain itu, Undang-Undang PDP mengharuskan Pengontrol memperbarui atau mengoreksi kesalahan atau ketidakakuratan dalam data pribadi. Hak ini tunduk pada pengecualian tertentu. ◦ Koreksi harus ditangani paling lambat 72 jam sejak Pengontrol menerima permintaan subjek data. ◦ Undang-Undang PDP mengharuskan Pengontrol memberi tahu subjek data pribadi tentang hasil permintaan koreksi.	Tanggung Jawab Pelanggan: • Mengembangkan prosedur dan kemampuan untuk memungkinkan individu mengakses serta mengoreksi data pribadi mereka. Komentar Google Cloud: • Pelanggan dapat mengakses data mereka di layanan Google Cloud kapan saja. • Jika Google menerima permintaan dari seseorang terkait data pribadinya, tim privasi kami akan memberikan saran kepada pemohon untuk mengirimkan permintaan tersebut kepada Anda, pelanggan Google Cloud. Pelanggan Google Cloud kemudian dapat mengambil alih untuk merespons permintaan ini sesuai persyaratan dan prosedur internal mereka. • Layanan dan konsol admin Google Cloud memiliki fungsi untuk mengakses data apa pun yang Anda atau pengguna Anda masukkan ke sistem kami.
Permintaan untuk membatasi pemrosesan data pribadi; Permintaan untuk menghapus data pribadi • Jika Pengontrol bergantung pada izin untuk memproses data pribadi, Pengontrol harus menghentikan pemrosesan jika subjek data mencabut izinnya, kecuali jika ada pengecualian yang berlaku. ◦ Pemrosesan tersebut harus dihentikan paling lambat 72 jam sejak Pengontrol menerima permintaan subjek data. • Pengontrol juga harus menghapus atau menghancurkan data pribadi atas permintaan dari subjek data, kecuali jika ada beberapa pengecualian. ◦ Pengontrol harus memberitahu	Tanggung Jawab Pelanggan: • Jika Anda ingin berhenti menggunakan layanan kami, Anda dapat melakukannya kapan saja. • Jika diperlukan, hapus data pribadi sebagai respons terhadap permintaan dari subjek data atau jika diwajibkan oleh undang-undang. Komentar Google Cloud: • Google menyediakan fungsionalitas untuk memungkinkan pelanggan mengakses, memperbaiki, dan membatasi pemrosesan data mereka serta mengambil atau menghapus data. • Anda dapat menggunakan fungsionalitas layanan Google Cloud berikut: ◦ Konsol Cloud: Antarmuka

subjek data saat ia menghapus atau menghancurkan data pribadi. • Berdasarkan Undang-Undang PDP, subjek data berhak menunda atau membatasi pemrosesan data pribadi secara proporsional dengan tujuan pemrosesan data pribadi, kecuali jika ada beberapa pengecualian. ◦ Pemrosesan tersebut harus dihentikan paling lambat 72 jam sejak Pengontrol menerima permintaan subjek data, dan subjek data harus diberitahu saat penundaan dan pembatasan pemrosesan tersebut diterapkan. • Berdasarkan Undang-Undang PDP, individu juga berhak menolak pemrosesan yang hanya didasarkan pada pengambilan keputusan otomatis, termasuk profiling, kecuali jika ada beberapa pengecualian. • Organisasi yang memproses Data Pribadi harus menghancurkan dan/atau menghapus data tersebut setelah periode retensi data berakhir atau atas permintaan subjek data, kecuali jika ditentukan lain oleh hukum dan peraturan.	pengguna grafis (GUI) berbasis web yang dapat digunakan pelanggan untuk mengelola resource Google Cloud mereka. ◦ Konsol Admin: Antarmuka pengguna grafis (GUI) berbasis web yang dapat digunakan pelanggan untuk mengelola resource Google Workspace mereka. ◦ Alat Command Line gcloud: Alat yang menyediakan antarmuka command line utama ke Google Cloud. Antarmuka command line adalah antarmuka pengguna pada sistem operasi komputer. ◦ Google API: Application programming interface (API) yang menyediakan akses ke Google Cloud.
Permintaan portabilitas data pribadi • Undang-Undang PDP memberi subjek data hak atas portabilitas data pribadi. Hak ini memiliki beberapa pengecualian terbatas. ◦ Individu berhak memperoleh informasi dari Pengontrol data dalam bentuk struktur atau format yang umum digunakan atau yang dapat dibaca oleh sistem elektronik.	Tanggung Jawab Pelanggan: • Memungkinkan subjek data memperoleh salinan data pribadi mereka dalam format yang umum digunakan. Komentar Google Cloud: • Google memungkinkan pelanggan mengakses dan mengekspor data mereka selama durasi kontrak mereka dan selama masa transisi pascapenghentian. • Anda dapat mengekspor data dari sejumlah layanan Google Cloud melalui sejumlah format standar industri: Contoh: ◦ Google Kubernetes Engine adalah lingkungan yang terkelola dan siap produksi yang memungkinkan portabilitas di berbagai lingkungan cloud serta di lingkungan lokal. ◦ Migrate for Anthos memungkinkan Anda

	memindahkan dan mengonversi workload secara langsung ke dalam container di Google Kubernetes Engine. - Anda dapat mengekspor/mengimpor seluruh image VM dalam format arsip .tar. Temukan informasi lebih lanjut terkait image di sini dan opsi penyimpanannya di sini. - Selain itu, Ekspor Data adalah fitur yang memudahkan Anda mengekspor dan mendownload salinan data Anda secara aman dari layanan kami.
Catatan Pemrosesan Undang-Undang PDP mengharuskan Pengontrol mencatat semua aktivitas pemrosesan data pribadi, kecuali jika ada pengecualian yang berlaku.	Komentar Google Cloud: - Google menyimpan catatan elektronik yang terkait dengan pemrosesan data pelanggan. - Hak, tanggung jawab, peran, kewajiban, dan tugas Google serta pelanggan diatur dalam kontrak Google Cloud.
Penanganan Data Pribadi	
Pemberitahuan Pelanggaran Data Jika terjadi pelanggaran data, Undang-Undang PDP menyatakan bahwa pengontrol harus menyampaikan pemberitahuan kepada subjek data yang terkena dampak dan otoritas perlindungan data Indonesia dalam waktu 72 jam, kecuali jika ada pengecualian yang berlaku.	Tanggung Jawab Pelanggan: - Pelanggan harus mengembangkan kebijakan dan prosedur untuk menangani dan merespons pelanggaran data secara efektif. Komentar Google Cloud: - Google menyadari bahwa untuk mengelola penggunaan Anda pada layanan secara efektif, termasuk menangani potensi pelanggaran data, Anda memerlukan informasi yang memadai tentang layanan tersebut secara rutin. Kami menyediakan sejumlah mekanisme untuk membantu Anda mengawasi layanan tersebut secara efektif dan berkelanjutan. - Google akan memberikan informasi terkait pengembangan yang terbukti mempengaruhi kemampuan Google untuk menyediakan layanan sesuai dengan SLA yang tersedia bagi Anda. Informasi

	selengkapnya tersedia di Dasbor Insiden & Google Cloud untuk Google Cloud dan Dasbor Status untuk Google Workspace. - Google juga akan segera memberitahu Anda jika terjadi insiden data, tanpa penundaan yang tidak semestinya. Informasi selengkapnya terkait proses respons insiden data Google tersedia di Laporan resmi respons insiden data kami. - Tim deteksi insiden Google menggunakan alat deteksi, sinyal, dan mekanisme peringatan canggih yang memberikan indikasi awal potensi insiden. Lihat Laporan resmi respons insiden data kami untuk mengetahui informasi selengkapnya.
Retensi - Undang-Undang PDP mewajibkan Pengontrol menghentikan pemrosesan data pribadi jika periode retensi data telah tercapai; tujuan pemrosesan tersebut telah tercapai; atau subjek data meminta Pengontrol menghentikan pemrosesan, kecuali jika ada pengecualian yang berlaku. - Di luar pengecualian tertentu, Pengontrol juga harus menghapus data pribadi apabila data pribadi tersebut tidak lagi diperlukan untuk mencapai tujuan pemrosesan; subjek data pribadi telah membatalkan persetujuannya; ada permintaan dari subjek data pribadi untuk menghapusnya; atau data pribadi diperoleh dan/atau diproses dengan cara yang melanggar hukum. - Selain itu, Undang-Undang PDP mewajibkan pengontrol menghancurkan data pribadi apabila: periode retensi data telah habis masa berlakunya; subjek data meminta penghancuran; data pribadi tidak terkait dengan penyelesaian proses hukum suatu perkara; dan/atau data pribadi diperoleh dan/atau diproses dengan cara yang melanggar hukum.	Tanggung Jawab Pelanggan: - Pelanggan harus menghapus data pribadi yang disimpan setelah tujuannya berakhir. Komentar Google Cloud: - Google akan mempertahankan, mengembalikan, menghancurkan, atau menghapus data pelanggan sesuai dengan kontrak. - Konsol dan layanan admin Google Workspace dan Google Cloud memberikan fungsionalitas untuk menghapus data pelanggan yang dimasukkan ke dalam sistem kami. Jika pelanggan menghapus data mereka, kami berkomitmen untuk menghapus data tersebut dari sistem kami dalam waktu 180 hari. Untuk mempelajari lebih lanjut penghapusan data di Google, lihat Laporan resmi penghapusan data di Google Cloud. - Kami juga menyediakan alat-alat yang memudahkan pelanggan untuk mengambil data mereka jika mereka memilih untuk berhenti menggunakan layanan kami, tanpa biaya tambahan.
Penyimpanan dan Keamanan Entitas yang memproses data pribadi memiliki kewajiban untuk melindungi keamanan data pribadi dari akses yang	Tanggung Jawab Pelanggan: Pelanggan harus mengimplementasikan kontrol keamanan yang memadai untuk melindungi data pribadi termasuk

tidak sah, pengungkapan yang tidak sah, perubahan yang tidak sah, penyalahgunaan, penghancuran, dan/atau kehilangan. ● Pengontrol harus menyiapkan dan mengimplementasikan langkah-langkah teknis operasional untuk melindungi pemrosesan data pribadi. Undang-Undang PDP mengamankan bahwa Pengontrol harus menentukan tingkat keamanan yang diperlukan dengan mempertimbangkan sifat dan risiko data pribadi. ● Pengontrol harus mencegah data pribadi diakses secara ilegal. Berdasarkan undang-undang tersebut, kewajiban ini dapat dilakukan melalui penggunaan sistem keamanan dan/atau dengan memproses data pribadi menggunakan sistem elektronik dengan cara yang andal, aman, dan bertanggung jawab.	konfigurasi fitur yang tepat di cloud di bawah pengelolaan pelanggan. Komentar Google: (1) <u>Keamanan infrastruktur Google</u> Google mengelola keamanan infrastruktur kami (misalnya, hardware, software, jaringan, dan fasilitas yang mendukung layanan). Google memberikan informasi mendetail kepada pelanggan tentang praktik keamanan kami di: ● Halaman keamanan infrastruktur kami ● Laporan resmi keamanan kami ● Laporan resmi keamanan berbasis cloud kami ● Halaman ringkasan desain keamanan infrastruktur kami ● Halaman referensi keamanan kami ● Halaman kepatuhan Cloud kami (2) <u>Keamanan data dan aplikasi Anda di cloud</u> (a) <u>Keamanan secara default</u> ● <u>Enkripsi dalam penyimpanan</u>. Google mengenkripsi data pelanggan yang tersimpan dalam keadaan nonaktif secara default, tanpa perlu tindakan tambahan dari Anda. Informasi selengkapnya tersedia di halaman Enkripsi dalam penyimpanan Google Cloud. ● <u>Enkripsi dalam pengiriman</u>. Google mengenkripsi dan mengautentikasi data dalam pengiriman di satu atau beberapa lapisan jaringan saat data dipindahkan ke luar batas fisik yang tidak dikontrol oleh Google atau atas nama Google. Informasi selengkapnya tersedia di halaman Enkripsi dalam pengiriman Google Cloud. (b) <u>Produk keamanan</u>
---	---

	Informasi terkait produk keamanan Google tersedia di halaman Produk Keamanan Cloud kami. Ilustrasi daftar layanan Google Cloud dan Google Workspace di bawah dapat digunakan untuk membantu memenuhi persyaratan penyimpanan dan keamanan: Kontrol akses Verifikasi 2 Langkah • Verifikasi 2 Langkah memberikan lapisan keamanan tambahan bagi bisnis pelanggan dan mencegah pelaku kejahatan cyber yang mencoba mencuri nama serta sandi pengguna untuk mengakses data bisnis. Dengan Verifikasi 2 Langkah, pengguna pelanggan dapat login ke akunnya dalam dua langkah, yaitu dengan sesuatu yang ia ketahui (sandi) dan sesuatu yang ia miliki (ponsel dengan aplikasi Google Authenticator). Identity and Access Management (IAM) • Identity and Access Management (IAM) dapat digunakan untuk menetapkan peran dan izin ke grup administratif, dengan menggabungkan prinsip hak istimewa terendah dan pemisahan tugas. Kontrol Layanan VPC • Kontrol Layanan VPC membantu pelanggan mengatasi ancaman, seperti pencurian data, kehilangan data secara tidak sengaja, serta akses berlebihan ke data yang disimpan di layanan multi-tenant Google Cloud. Dengan layanan ini, klien dapat secara ketat mengontrol akses ke layanan tertentu oleh entitas tertentu untuk mengurangi kerugian yang disengaja maupun tidak disengaja. • Kontrol Layanan VPC menyediakan akses model zero-trust ke layanan multi-tenant. Klien dapat membatasi akses ke IP, konteks klien, dan parameter perangkat yang diotorisasi saat terhubung ke
--	--

	layanan multi-tenant dari internet dan layanan lainnya. Contohnya mencakup GKE, BigQuery, dan lain-lain. Kontrol Layanan VPC membuat klien dapat menjaga keseluruhan pipeline pemrosesan data tetap bersifat pribadi. Log Akses Cloud Logging • Cloud Logging adalah layanan terkelola sepenuhnya yang dapat Anda gunakan untuk menyimpan, menelusuri, menganalisis, memantau, serta membuat pemberitahuan terkait data logging dan peristiwa dari Google Cloud serta Amazon Web Services. Anda dapat mengumpulkan data logging dari 150+ komponen aplikasi umum, sistem lokal, dan sistem hybrid cloud. Transparansi Akses • Transparansi Akses dapat mempertahankan visibilitas akses orang dalam ke data Anda melalui log yang mendekati real-time dari Transparansi Akses. Perlindungan dari Ancaman Eksternal Cloud Security Command Center • Security Command Center adalah layanan pelaporan kerentanan dan ancaman terpusat dari Google Cloud. Security Command Center membantu Anda memperkuat postur keamanan dengan mengevaluasi keamanan dan permukaan serangan data Anda; menyediakan inventaris dan penemuan aset; mengidentifikasi kesalahan konfigurasi, kerentanan, dan ancaman; serta membantu memitigasi dan memulihkan risiko. Virtual Machine Threat Detection
--	--

	• Virtual Machine Threat Detection adalah layanan bawaan dari Security Command Center Premium yang dapat memberikan deteksi ancaman melalui instrumentasi tingkat hypervisor. Pemantauan • Dasbor Status Google Cloud menyediakan informasi status pada layanan. • Dasbor Status Google Workspace menyediakan informasi status pada layanan. • Google Cloud Operations adalah solusi pemantauan, logging, dan diagnostik yang dihosting dan terintegrasi yang membantu Anda mendapatkan insight terkait aplikasi yang berjalan di Google Cloud, termasuk ketersediaan dan waktu beroperasi layanan tersebut. • Laporan Konsol Admin memungkinkan Anda memeriksa potensi risiko keamanan, mengukur kolaborasi pengguna, melacak siapa saja yang login beserta waktunya, menganalisis aktivitas administrator, dan banyak lagi. (c) <u>Referensi keamanan</u> Google juga memublikasikan panduan tentang: • Praktik terbaik keamanan • Kasus penggunaan keamanan • Blueprint keamanan
--	---

Kesimpulan

Di Google, kami menyadari bahwa data Anda tetap milik Anda dan menjamin integritas privasi data Anda adalah kuncinya. Perlindungan data Anda adalah pertimbangan desain utama untuk semua infrastruktur, produk, dan operasi kami. Kami yakin bahwa Google dapat menawarkan tingkat perlindungan yang tidak dapat ditandingi oleh hampir sebagian besar penyedia cloud publik atau tim IT perusahaan swasta. Karena melindungi data adalah inti dari bisnis Google, kami dapat melakukan investasi ekstensif dalam keamanan, resource, dan keahlian dengan skala yang tidak bisa dilakukan pihak lain. Investasi kami akan membebaskan Anda untuk berfokus pada bisnis dan inovasi.

Google Cloud

Perlindungan data dan privasi itu lebih dari sekadar keamanan. Komitmen kontraktual Google yang kuat membantu Anda menjaga kendali atas data Anda dan cara pemrosesannya, termasuk jaminan bahwa data Anda tidak digunakan untuk iklan atau tujuan apa pun selain untuk menyediakan layanan Google Cloud.

Informasi dalam laporan resmi ini sebaiknya digunakan untuk membantu pelanggan mempertimbangkan apakah produk atau layanan Google Cloud dan Google Workspace cocok untuk mereka sehubungan dengan Undang-Undang Pelindungan Data Pribadi Indonesia.