

Langkah-Langkah Keamanan ProcessMind

Tanggal berlaku: 14 September 2026

Dokumen ini menjelaskan langkah-langkah teknis dan organisasional ("TOM") yang diterapkan ProcessMind B.V. untuk melindungi kerahasiaan, integritas, dan ketersediaan Data Pelanggan. ProcessMind menerapkan pendekatan pertahanan berlapis, dengan beberapa lapisan keamanan independen yang melindungi Data Pelanggan di setiap tingkat — mulai dari jaringan dan infrastruktur hingga identitas, otorisasi, isolasi data, enkripsi, pemantauan, dan pengembangan perangkat lunak. Langkah-langkah ini melengkapi [Adendum Pemrosesan Data](#), [Kebijakan Privasi](#), dan [Kebijakan Hosting SaaS](#). ProcessMind meninjau dan memperbarui langkah-langkah ini setidaknya setiap tahun.

Data Pelanggan tidak pernah dijual kepada, dibagikan dengan, atau digunakan oleh pihak ketiga untuk tujuan mereka sendiri.

1. Keamanan Infrastruktur

1.1 Platform Cloud. ProcessMind dihosting secara eksklusif di Amazon Web Services (AWS) di UE (Frankfurt, Jerman, eu-central-1). AWS memiliki sertifikasi ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3, dan PCI DSS. Lihat [Program Kepatuhan AWS](#) untuk daftar lengkap.

1.2 Arsitektur Tanpa Server. Logika aplikasi ProcessMind berjalan di AWS Lambda dan layanan terkelola AWS. ProcessMind tidak mengoperasikan server aplikasi berumur panjang yang dikelola pelanggan, sehingga menghilangkan sebagian besar pekerjaan penambalan sistem operasi dan penguatan keamanan server.

1.3 Batas Jaringan. ProcessMind memelihara AWS VPC untuk kontrol basis data dan jaringan. Aurora PostgreSQL berjalan di subnet privat tanpa akses keluar ke internet, tidak dapat diakses secara publik, dan log alur VPC diaktifkan. Secara default, ProcessMind tidak menempatkan fungsi

Lambda aplikasi di dalam VPC. Lambda mengakses Aurora melalui AWS RDS Data API melalui TLS dengan autentikasi IAM dan Secrets Manager.

1.4 Pengiriman Konten dan Kontrol Edge. Situs web yang ditujukan kepada pelanggan, SPA frontend, dan lalu lintas sumber daya publik disajikan melalui Amazon CloudFront. Semua distribusi CloudFront menerapkan kebijakan TLS minimum TLS 1.2 (2021). Distribusi situs web dan SPA frontend juga menambahkan header respons keamanan, termasuk HTTP Strict Transport Security (HSTS), Content Security Policy (CSP), frame-ancestors 'none', X-Frame-Options: DENY, X-Content-Type-Options, kebijakan perujuk, dan kebijakan izin. Distribusi sumber daya publik menggunakan CloudFront Origin Access Control untuk menjaga bucket asal tetap privat. Lalu lintas API yang ditujukan kepada pelanggan ditangani secara terpisah melalui Amazon API Gateway: lalu lintas permintaan/respons HTTPS disajikan melalui HTTP API pada subdomain API khusus, dan koneksi klien real-time disajikan melalui API WebSocket API Gateway terpisah pada subdomain WebSocket khusus.

1.5 Pemisahan Lingkungan. Lingkungan produksi dan pengembangan menggunakan akun AWS, basis data, dan tumpukan infrastruktur yang terpisah. Kredensial pengembang tidak memberikan akses ke Data Pelanggan produksi.

2. Enkripsi Data

2.1 Enkripsi Saat Transit. Semua data yang dikirimkan antara klien dan layanan ProcessMind dienkripsi menggunakan TLS 1.2 atau yang lebih tinggi. Endpoint yang diakses pelanggan tersedia melalui HTTPS. Bucket S3, topik SNS, dan antrian SQS yang dibuat langsung oleh ProcessMind menerapkan akses SSL saja. Akses basis data melalui RDS Data API dan panggilan layanan AWS lainnya menggunakan HTTPS/TLS.

2.2 Enkripsi Saat Disimpan. Aurora PostgreSQL dienkripsi saat disimpan menggunakan kunci AWS KMS yang dikelola pelanggan dengan rotasi kunci otomatis. Bucket S3 untuk data pelanggan dan operasional yang

dibuat langsung oleh ProcessMind, termasuk bucket unggahan, sumber daya, dan log akses, menggunakan kunci KMS yang dikelola pelanggan. Grup log CloudWatch, topik SNS, dan antrean SQS yang dibuat langsung oleh ProcessMind juga menggunakan kunci KMS yang dikelola pelanggan. Bucket asal situs web dan frontend yang dikelola SST menggunakan enkripsi sisi server S3 yang dikelola AWS (SSE-S3 / AES-256), bukan kunci KMS yang dikelola pelanggan.

2.3 Manajemen Kunci dan Rahasia. Kunci enkripsi basis data dikelola secara terpusat melalui AWS KMS, dan akses kunci diatur oleh kebijakan IAM yang mengikuti prinsip hak akses minimum. Kredensial basis data disimpan di AWS Secrets Manager. Rahasia master Aurora dan rahasia pengguna aplikasi terbatas dirotasi secara otomatis setiap tiga puluh (30) hari. Kunci dan rahasia produksi tidak pernah disimpan dalam kode sumber; kredensial khusus pengembangan diisolasi dari produksi. Sejumlah sumber daya pendukung yang dikelola AWS/CDK/SST tetap menggunakan enkripsi yang dikelola AWS jika layanan atau kerangka kerja tidak menyediakan konfigurasi kunci yang dikelola pelanggan.

3. Isolasi dan Lokasi Data

3.1 Isolasi Penyewa. Setiap penyewa pelanggan memperoleh instans basis data khusus yang terisolasi. Data Pelanggan tidak pernah dicampur dengan data pelanggan lain pada tingkat basis data. Metadata bersama (misalnya, catatan akun, penagihan, pemetaan pengguna ke penyewa) disimpan dalam basis data multi-penyewa yang terpisah dengan kontrol akses ketat. Tabel bersama yang cakupannya terbatas pada penyewa dan organisasi juga dilindungi oleh kebijakan keamanan tingkat baris (RLS) PostgreSQL yang diterapkan melalui konteks basis data yang dicakup per permintaan.

3.2 Lokasi Data. Semua Data Pelanggan, termasuk basis data, unggahan berkas, cadangan, dan hasil kueri, disimpan secara eksklusif di UE (Frankfurt, Jerman). Jika sub-pemroses yang berlokasi di luar EEA

dilibatkan untuk aktivitas pemrosesan tertentu (misalnya, pemrosesan model AI atau pemrosesan pembayaran), transfer tersebut dilindungi oleh mekanisme transfer yang sesuai sebagaimana dijelaskan dalam Adendum Pemrosesan Data, dan sub-pemroses serta lokasi pemrosesannya tercantum dalam Daftar Sub-pemroses.

3.3 Retensi dan Penghapusan Data. Jangka waktu retensi dan penghapusan ditetapkan dalam Bagian 6 [Adendum Pemrosesan Data](#). Pelanggan dapat menghapus data mereka kapan saja melalui aplikasi atau dengan menghubungi ProcessMind. Salinan cadangan dihapus setelah berakhirnya periode retensi cadangan yang berlaku (Bagian 7.1).

4. Manajemen Identitas dan Akses

4.1 Autentikasi. ProcessMind mendukung Single Sign-On (SSO) melalui Microsoft Entra ID (Azure AD), Google OAuth 2.0/OIDC, dan LinkedIn OAuth 2.0/OIDC. ProcessMind bertindak sebagai pihak yang mengandalkan penyedia identitas dan tidak menyimpan kata sandi pengguna. Autentikasi multifaktor diterapkan oleh penyedia identitas – misalnya, jika suatu organisasi menghubungkan Microsoft Entra ID (Azure AD), MFA dan kebijakan akses organisasi itu sendiri yang berlaku.

4.2 Manajemen Sesi. Sesi browser menggunakan JSON Web Token (JWT) bertanda tangan yang dikirim melalui cookie aman beratribut HttpOnly, SameSite, dan Secure. Tanda tangan token divalidasi pada setiap permintaan terautentikasi.

4.3 Model Otorisasi. ProcessMind tidak mengandalkan authorizer native API Gateway untuk API aplikasi intinya. Otorisasi diberlakukan dalam wrapper handler Lambda bersama yang memvalidasi status sesi dan cakupan tenant sebelum logika bisnis dijalankan. Rute publik secara eksplisit dimasukkan ke daftar yang diizinkan untuk alur non-terautentikasi, webhook, pemasukan peristiwa, dan preflight CORS. Endpoint API eksternal menggunakan handler autentikasi khusus. Akses ke Data Pelanggan dibatasi pada konteks tenant atau organisasi yang terautentikasi.

4.4 Hak Akses Minimum. Sistem internal mengikuti prinsip hak akses minimum. Peran IAM dibatasi pada sumber daya minimum yang diperlukan jika kerangka kerja memungkinkan pembatasan yang tepat. Beberapa peran yang dibuat SST/CDK menggunakan kebijakan terkelola atau inline yang lebih luas untuk binding dan operasi runtime; kasus-kasus ini ditinjau, dibatasi pada sumber daya jika memungkinkan, dan dicatat sebagai pengecualian eksplisit.

4.5 Kontrol Akses Karyawan. Akses karyawan ke sistem internal dikelola melalui Active Directory dengan SSO dan MFA wajib. Kontrol akses berbasis peran (RBAC) memastikan bahwa akses ke Data Pelanggan dibatasi bagi personel berwenang yang memerlukannya untuk menjalankan tugas. Hak akses ditinjau secara berkala.

5. Pencatatan Log, Pemantauan, dan Audit

5.1 Pencatatan Log Terpusat. Pencatatan log akses HTTP API dan WebSocket diaktifkan dengan bidang JSON terstruktur dan ditulis ke Amazon CloudWatch Logs dengan retensi satu (1) tahun. Grup log akses tersebut dienkrpsi dengan kunci AWS KMS yang dikelola pelanggan. Log aplikasi dipusatkan dalam grup log Amazon CloudWatch yang dienkrpsi dengan kunci AWS KMS yang dikelola pelanggan dan disimpan selama sepuluh (10) tahun. Grup log audit dan telemetry terpisah juga dienkrpsi dengan kunci AWS KMS yang dikelola pelanggan dan disimpan selama sepuluh (10) tahun. Grup ekspor log mesin Aurora PostgreSQL disimpan selama satu (1) minggu.

5.2 Hal yang Dicatat dan Tidak Dicatat. ProcessMind mencatat peristiwa akses HTTP API dan WebSocket — waktu permintaan, pengenalan permintaan, rute atau jalur, status respons, dan latensi. Log akses tidak mencakup alamat IP sumber atau agen pengguna pemanggil. ProcessMind juga mencatat peristiwa autentikasi, jalur kegagalan asinkron, dan aktivitas aplikasi Lambda pendukung ke grup log CloudWatch terpusat. Log alur VPC diaktifkan. Saat ini, ProcessMind tidak mengaktifkan pencatatan log

akses standar CloudFront pada distribusi situs web, SPA frontend, atau sumber daya publik.

5.3 Pemantauan dan Peringatan. Alarm dan dasbor CloudWatch memantau kesehatan sistem, antrean surat mati, dan kegagalan yang relevan dengan keamanan. Kegagalan pemrosesan asinkron diarahkan ke antrean surat mati terenkripsi (retensi empat belas (14) hari; dua (2) hari untuk antrean gambar mini dan indeks pencarian), dan alarm DLQ memicu notifikasi SNS untuk penyelidikan. Selain itu, ProcessMind menggunakan Sentry untuk pelacakan kesalahan frontend waktu nyata, pemantauan kinerja, dan pemutaran ulang sesi. Pemutaran ulang sesi hanya direkam untuk sesi yang mengalami kesalahan, dan teks, masukan formulir, serta media disamarkan atau diblokir dalam rekaman pemutaran ulang. Data Sentry diterima di UE (Frankfurt) dan terbatas pada Data Penggunaan ProcessMind (kesalahan browser, jejak kinerja, metadata perangkat, dan rekaman pemutaran ulang yang disamarkan). Sentry tercantum dalam [daftar sub-pemroses](#).

5.4 Perlindungan Log. Log disimpan dalam grup log CloudWatch khusus dengan kontrol akses dan dienkripsi saat disimpan. Log produksi dan pengembangan dipisahkan berdasarkan lingkungan dan batas akun.

6. Validasi Kontrol Otomatis dan Manajemen Kerentanan

6.1 Hal yang Dilakukan ProcessMind. ProcessMind menjalankan cdk-nag sebagai bagian dari sintesis infrastruktur dan alur kerja penerapannya dengan menggunakan beberapa paket aturan industri (termasuk AWS Solutions, NIST 800-53, dan PCI DSS). Laporan per tumpukan dibuat dan ditinjau sebagai bagian dari manajemen perubahan infrastruktur. Temuan ditriase sebagai telah diperbaiki, risiko yang diterima, atau peningkatan yang direncanakan.

6.2 Cara Pengecualian Dikelola. Penekanan temuan dicatat dalam registri pusat jika kerangka kerja memungkinkan, dibatasi pada tumpukan yang terdampak, dan memerlukan justifikasi tertulis; jika suatu tumpukan

memuat penekanan inline, hal itu didokumentasikan bersama tumpukan tersebut. Ketika suatu temuan diperbaiki, penekanan terkait diperbarui atau dihapus. ProcessMind tidak memperlakukan penekanan sebagai pengecualian menyeluruh dari peninjauan.

6.3 Hal yang Saat Ini Tidak Dilakukan ProcessMind. ProcessMind melacak dan meninjau pengecualian kontrol infrastruktur yang material.

Pengecualian utamanya adalah:

- Lambda aplikasi secara default tidak ditempatkan di dalam VPC; Lambda tersebut mengakses Aurora melalui RDS Data API menggunakan TLS dengan autentikasi IAM dan Secrets Manager
- tidak ada bagian layanan yang dilindungi oleh AWS WAF: AWS WAF tidak mendukung API Gateway HTTP APIs, dan titik masuk lainnya juga tidak dilindungi WAF (koneksi WebSocket menggunakan token HMAC berumur pendek; pembatasan geografis terkait pembayaran diberlakukan dalam sistem pembayaran); distribusi statis juga tidak memiliki pencatatan akses standar CloudFront
- pemulihan basis data mengandalkan pencadangan otomatis Aurora dan pemulihan titik waktu, bukan paket AWS Backup terpisah atau Aurora Enhanced Monitoring
- tidak ada replikasi S3 lintas wilayah atau S3 Object Lock untuk bucket yang dapat diubah
- sejumlah sumber daya pendukung yang dikelola AWS/CDK/SST menggunakan enkripsi yang dikelola AWS atau kebijakan IAM yang dihasilkan dengan cakupan lebih luas apabila layanan tidak menyediakan alternatif yang dapat dikendalikan pelanggan

Registri penekanan lengkap dipelihara bersama kode infrastruktur dan tersedia berdasarkan permintaan. Penggunaan `cdk-nag` paket aturan merupakan validasi kontrol rekayasa, bukan sertifikasi eksternal, opini audit, atau atestasi hukum atas kepatuhan terhadap HIPAA, NIST, atau PCI DSS.

6.4 Manajemen Dependensi. Dependensi perangkat lunak dipantau secara berkelanjutan untuk mengetahui kerentanan yang telah diketahui. Kerentanan kritis dan berkeparahan tinggi ditambah dengan target tujuh (7) hari. Dependensi diperbarui secara berkala.

6.5 Siklus Hidup Pengembangan Perangkat Lunak yang Aman (SDLC).

ProcessMind menerapkan pendekatan pertahanan berlapis dalam pengembangan perangkat lunak. Setiap perubahan pada produksi harus melewati beberapa lapisan validasi otomatis yang independen sebelum penerapan:

- **Analisis statis dan keamanan tipe:** Mode ketat TypeScript dan ESLint menerapkan ketepatan tipe, keamanan nilai null, dan pola pengodean yang relevan dengan keamanan pada waktu kompilasi.
- **Tinjauan kode berbantuan AI:** Analisis berbantuan AI memberikan perspektif tinjauan tambahan pada pull request untuk mengidentifikasi risiko keamanan, kesalahan logika, dan penyimpangan dari konvensi, sebagai pelengkap pengujian otomatis.
- **Pengujian unit dan integrasi:** rangkaian pengujian Vitest yang komprehensif memvalidasi logika bisnis, pola akses data, perilaku API, dan penanganan kesalahan terhadap sumber daya AWS aktif di lingkungan pengembangan.
- **Pengujian menyeluruh:** Pengujian browser berbasis Playwright memverifikasi alur kerja pengguna yang penting, termasuk autentikasi, pengunggahan data, pemodelan proses, simulasi, dan isolasi multi-penyewa.
- **Pemindaian kepatuhan infrastruktur:** cdk-nag memvalidasi infrastruktur sebagai kode terhadap beberapa kerangka kerja kepatuhan pada setiap perubahan.
- **Pemindaian kerentanan dependensi:** audit dependensi otomatis mencegah kerentanan kritis dan berkeparahan tinggi yang telah diketahui mencapai lingkungan produksi.

Tinjauan manusia berfokus pada arsitektur, batas keamanan, dan keputusan pada tingkat desain, bukan pemeriksaan kode baris demi baris. Jika terdapat perubahan struktural, yang sensitif terhadap keamanan, atau infrastruktur, persetujuan eksplisit dari manusia diwajibkan selain validasi otomatis.

Semua lapisan validasi diterapkan melalui CI sebagai gerbang penggabungan wajib untuk perubahan aplikasi dan infrastruktur ke cabang utama. Konten situs web dan rilis aset statis mengikuti proses rilis terpisah yang terdokumentasi dengan pemeriksaan pada waktu penerapan — termasuk pemeriksaan otomatis bahwa dokumen hukum telah diperbarui — bukan gerbang CI aplikasi. Perbaikan darurat produksi dapat melewati gerbang CI, tetapi harus ditindaklanjuti dengan pelaksanaan pipeline lengkap dan tinjauan pascainsiden dalam waktu dua puluh empat (24) jam.

7. Penceadangan dan Pemulihan Bencana

7.1 Penceadangan Otomatis. Amazon Aurora melakukan pencadangan otomatis berkelanjutan dengan masa retensi tujuh (7) hari. Cadangan dienkrpsi menggunakan kunci KMS yang dikelola pelanggan yang sama dengan basis data sumber.

7.2 Pemulihan Titik Waktu. Aurora mendukung pemulihan titik waktu ke detik mana pun dalam periode retensi cadangan, sehingga memungkinkan pemulihan cepat jika terjadi kerusakan data atau penghapusan yang tidak disengaja.

7.3 Ketahanan dan Pembuatan Versi S3. Unggahan berkas dan artefak operasional disimpan di Amazon S3, yang menyediakan ketahanan 99.999999999% (11 angka sembilan). Pembuatan versi diaktifkan pada bucket unggahan dan bucket sumber daya untuk mendukung pemulihan dan pengembalian ke versi sebelumnya. Bucket penerapan situs web dan frontend merupakan artefak build yang dapat direproduksi dan tidak

diperlakukan sebagai sistem pencadangan. Saat ini, ProcessMind tidak mengaktifkan replikasi S3 lintas wilayah.

7.4 Kelangsungan Bisnis. Prosedur pemulihan bencana didokumentasikan dan diuji secara berkala. Ringkasannya tersedia dalam dokumen [Pemulihan Bencana, Kelangsungan Bisnis & Respons Insiden](#). Arsitektur ini mengandalkan layanan terkelola AWS di wilayah eu-central-1, yang dioperasikan AWS di beberapa Availability Zone; kluster Aurora saat ini menjalankan satu instans penulis, sehingga pemulihan basis data mengandalkan pencadangan otomatis dan pemulihan titik waktu, bukan instans siaga dalam wilayah yang sama. Cadangan Aurora, ketahanan S3, antrean surat mati, dan aset statis yang dibangun ulang dari sumber merupakan bagian dari strategi pemulihan.

8. Respons Insiden

8.1 Pemberitahuan Insiden. Jika terjadi Insiden Keamanan (sebagaimana didefinisikan dalam DPA), ProcessMind akan memberi tahu pelanggan yang terdampak tanpa penundaan yang tidak semestinya dan, jika memungkinkan, dalam waktu tujuh puluh dua (72) jam sejak mengetahui insiden tersebut.

8.2 Penanganan Insiden. ProcessMind memelihara prosedur respons insiden terdokumentasi yang mencakup identifikasi, pembatasan, pemberantasan, pemulihan, dan tinjauan pascainsiden. Ringkasannya tersedia dalam dokumen [Pemulihan Bencana, Kelangsungan Bisnis & Respons Insiden](#). Pembelajaran dari insiden dimasukkan ke dalam kontrol dan proses keamanan.

8.3 Komunikasi. Pemberitahuan insiden mencakup sifat dan cakupan insiden, kategori data yang terdampak, langkah-langkah yang diambil untuk membatasi insiden, dan tindakan yang direkomendasikan bagi pelanggan.

9. Langkah-Langkah Organisasional

9.1. Manajemen Keamanan Informasi. ProcessMind memelihara sistem manajemen keamanan informasi yang selaras dengan prinsip ISO 27001. ProcessMind telah memilih jalur sertifikasinya untuk sertifikasi ISO 27001 dan atestasi SOC 2 Tipe II; proses sertifikasi formal belum dimulai.

9.2 Kesadaran Keamanan. Semua personel yang memiliki akses ke Data Pelanggan menerima pelatihan kesadaran keamanan. Praktik terbaik keamanan diterapkan dalam orientasi karyawan baru, alur kerja pengembangan, dan prosedur operasional.

9.3 Manajemen Vendor dan Sub-pemroses. Sub-pemroses terikat secara kontraktual untuk mematuhi standar perlindungan data yang setara dengan yang dijelaskan dalam dokumen ini. ProcessMind memelihara [daftar sub-pemroses](#) publik dan memberikan pemberitahuan setidaknya tiga puluh (30) hari sebelum menggunakan sub-pemroses baru. Sub-pemroses ditinjau setiap tahun untuk memastikan kepatuhan.

9.4 Kerahasiaan. Semua personel yang berwenang memproses Data Pelanggan terikat oleh kewajiban kerahasiaan tertulis.

10. Kepatuhan dan Sertifikasi

Kerangka Kerja / Standar	Status
GDPR (Peraturan Perlindungan Data Umum UE)	Patuh
Lokasi Data UE (Frankfurt, Jerman)	Diterapkan
Sertifikasi Infrastruktur AWS (ISO 27001, SOC 2, PCI DSS)	Diwarisi melalui AWS
ISO 27001 (ProcessMind)	Direncanakan — jalur sertifikasi telah dipilih; proses formal belum dimulai

Kerangka Kerja / Standar	Status
SOC 2 Tipe II (ProcessMind)	Direncanakan — jalur sertifikasi telah dipilih; proses formal belum dimulai
Validasi kontrol infrastruktur otomatis (cdk-nag di AWS Solutions, HIPAA Security, NIST 800-53 R4/R5, PCI DSS 3.2.1, Serverless)	Diterapkan sebagai validasi kontrol rekayasa, bukan sertifikasi
Klausul Kontraktual Standar (SCC) untuk transfer internasional	Diterapkan (lihat DPA)
Adendum Pemrosesan Data (DPA)	Tersedia untuk umum

Penggunaan cdk-nag paket aturan tidak berarti ProcessMind secara resmi tersertifikasi atau diaudit secara independen terhadap HIPAA, NIST, atau PCI DSS. Paket aturan tersebut digunakan sebagai pedoman rekayasa untuk memvalidasi desain infrastruktur dan melacak kesenjangan secara eksplisit.

Untuk pertanyaan mengenai keamanan atau kepatuhan, atau untuk meminta dokumentasi seperti laporan audit atau kuesioner keamanan yang telah diisi, hubungi support@processmind.com.