Pernyataan Log Audit dan SIEM ProcessMind

Tanggal berlaku: 12 November 2026

Pernyataan ini menjelaskan cara ProcessMind B.V. mencatat tindakan administratif dan tindakan yang relevan dengan keamanan yang dilakukan terhadap Data Pelanggan ("log audit"). Pernyataan ini melengkapi Langkah-Langkah Keamanan, Adendum Pemrosesan Data, Perjanjian Pelanggan, dan Daftar Subprosesor.

---

1. Cakupan

1.1 Satu log audit. ProcessMind memelihara satu log audit untuk tindakan administratif dan tindakan yang relevan dengan keamanan yang dilakukan terhadap Data Pelanggan dan Layanan ProcessMind. Log audit terpisah dari pencatatan operasional (aplikasi), pencatatan akses HTTP, dan umpan aktivitas produk; aliran tersebut memiliki tujuan yang berbeda dan tidak dinyatakan sebagai jejak audit.

1.2 Hal yang bukan merupakan log audit. Log audit bukan catatan setiap pembacaan Data Pelanggan, dan bukan riwayat perubahan produk untuk model proses, diagram, dokumentasi, atau simulasi. Hal-hal tersebut dicatat dalam riwayat perubahan proses yang tersedia di dalam produk.

---

2. Isi setiap catatan audit

2.1 Kolom. Setiap catatan memuat kolom-kolom di bawah ini. Kumpulan kolom ditetapkan oleh skema catatan: catatan tidak dapat memiliki kolom yang tidak tercantum dalam daftar ini, dan suatu tindakan tidak dapat menambahkan kolom yang tidak dideklarasikannya dalam registri.

- *schemaVersion* (angka): versi skema catatan, saat ini 1.
- *eventId* (string): pengenal catatan unik. Catatan baru menggunakan ULID; baris yang dimigrasikan dari penyimpanan sebelumnya tetap menggunakan UUID.

- *occurredAt*, *ingestedAt* (stempel waktu): waktu tindakan terjadi dan waktu penulis audit menyimpan catatan. Keduanya dalam UTC.
- *eventClass* (enum): security, auth, admin, data, api, ai, atau platform.
- *action* (enum): satu kode dari registri tindakan tertutup yang telah ditinjau, misalnya auth.login.blocked atau api.key.revoked.
- *outcome* (enum): success, failure, denied, atau error.
- *severity* (enum): info, notice, warning, atau critical, yang ditentukan berdasarkan hasil. Tindakan yang berhasil menggunakan nilai bawaan registrinya (info kecuali jika tindakan menyatakan lain), kegagalan dicatat sebagai notice, dan denied atau error sebagai warning.
- *actor* (objek): pihak yang bertindak. type (user, apiKey, service, system, atau anonymous), id, email, displayName, serta onBehalfOf dan onBehalfOfEmail jika tindakan dilakukan untuk akun lain.
- *actorContext* (objek): sesi yang melakukan tindakan. sessionId, authMethod (oidc, password, loginToken, apiKey, atau none), dan penanda sesi dukungan.
- *organizationId*, *tenantId* (pengenal, dapat bernilai null): organisasi dan lingkungan tempat tindakan tersebut berada. Bernilai null untuk catatan yang tidak berkaitan dengan pelanggan, atau yang berada di atas lingkungan tersebut.
- *resource* (objek, dapat bernilai null): objek yang terdampak. type, id, dan name, dengan type berupa salah satu dari apiKey, artifact, connection, database, datatable, export, lead, model, organization, process, role, session, setting, storage, tenant, atau user.
- *source* (objek): tempat catatan dibuat. service (api, externalApi, superadminApi, worker, cron, atau webSocket), function, dan version.
- *stage*, *region* (string): tahap penerapan yang menghasilkan catatan (misalnya prod) dan wilayah AWS (eu-central-1 untuk catatan pelanggan).
- *correlation* (objek): requestId, traceId, dan parentEventId, yang mengaitkan catatan dengan permintaan yang menyebabkannya

dan dengan catatan sebelumnya dalam alur yang sama.

- *network* (objek, dapat bernilai null): sourceIp dan userAgent. Hanya direkam untuk tindakan yang memilih untuk menyertakannya dalam entri registrinya: masuk, keputusan akses, perubahan administratif dan pengaturan, unggahan, unduhan, dan ekspor data, perubahan kunci API, serta perubahan kebijakan AI.
- *detail* (objek): muatan khusus tindakan tersebut, divalidasi berdasarkan skema tindakan itu. Nilainya hanya berupa nilai primitif (string, angka, boolean, null), sehingga catatan tetap dapat dikueri dan disunting.

2.2 Kosakata tertutup. Tindakan diambil dari daftar kode tindakan tetap yang telah ditinjau; tidak ada pesan teks bebas dalam catatan audit. Setiap tindakan juga menyatakan kolom tambahan yang boleh dimuatnya, sehingga catatan tidak dapat secara diam-diam menambahkan jenis konten baru.

---

3. Tindakan yang dicatat

3.1 Yang dicatat saat ini. ProcessMind mencatat, antara lain:

- **Autentikasi:** keberhasilan dan kegagalan masuk, masuk yang diblokir (akun terkunci, domain tidak diizinkan, email penyedia yang belum diverifikasi), keluar, penerbitan dan pengalihan token masuk.
- **Otorisasi:** penolakan akses, termasuk setiap kredensial API eksternal, cakupan, dan status tenant yang ditolak, serta penolakan asal (CORS).
- **Akses dukungan:** dimulainya sesi dukungan ProcessMind pada akun pelanggan, dengan menyebutkan operator dan akun yang terdampak.
- **Kredensial API:** pembuatan, perubahan cakupan, dan pencabutan kunci API, termasuk cakupan yang diberikan.
- **Administrasi akun dan peran:** pembuatan pengguna, undangan, penyuntingan profil administrator, penghapusan, pemberian dan

pencabutan peran, serta perubahan keanggotaan tenant atau organisasi.

- **Siklus hidup organisasi:** pembuatan, penghapusan, pemulihan, penjadwalan dan pembatalan penghapusan, serta penghapusan menyeluruh yang telah diselesaikan.
- **Unggahan, unduhan, dan ekspor data:** unggahan, unduhan, dan penghapusan artefak, unggahan dan pembaruan data tabular, unduhan ekspor, penghapusan tabel data, serta pembuatan, perubahan, dan penghapusan webhook (koneksi).
- **Status penagihan:** perubahan paket, penangguhan dan pemulihan akibat pembayaran, serta pembatalan langganan.
- **Konsol penyedia ProcessMind:** pelaksanaan kueri dengan hak istimewa, administrasi pengguna dan organisasi, perubahan pengaturan dan fitur, permintaan sinkronisasi penagihan, serta migrasi.
- **Tindakan administratif dan destruktif oleh tugas terjadwal ProcessMind:** penghapusan tenant, organisasi, pengguna, dan prospek, penyisiran retensi, serta kegagalan pipeline.
- **Integritas log audit:** kegagalan jalur penulisan log audit itu sendiri.

3.2 Penyuntingan ruang kerja. Penyuntingan di dalam ruang kerja (model proses, dokumentasi, simulasi, dasbor, komentar, dan penanda) dicatat dalam riwayat perubahan proses milik produk, bukan dalam log audit. Log audit mencatat siapa yang mengunggah, mengunduh, mengekspor, atau menghapus data; riwayat perubahan mencatat apa yang berubah di dalam model. Daftar kode tindakan yang dicatat saat ini tersedia dari ProcessMind berdasarkan permintaan.

---

4. Hal yang tidak pernah dicatat

Kata sandi, token autentikasi, nilai kunci API, cookie, header otorisasi, isi permintaan atau respons, konten berkas, URL yang telah ditandatangani sebelumnya, serta prompt atau hasil AI tidak pernah ditulis ke dalam log audit. Catatan audit dapat memuat data pribadi yang diperlukan untuk

atribusi: alamat email pelaku, serta alamat IP sumber dan user agent untuk tindakan yang memilih untuk menyertakannya dalam entri registrinya (masuk, keputusan akses, perubahan administratif dan pengaturan, perpindahan data, perubahan kunci API dan kebijakan AI). Kolom yang diizinkan ditetapkan untuk setiap tindakan dan ditinjau saat suatu tindakan ditambahkan.

---

5. Integritas

5.1 Hanya dapat ditambahkan. Log audit hanya dapat ditambahkan. Tidak ada peran aplikasi yang memiliki hak istimewa untuk memperbarui atau menghapusnya, dan batasan basis data menolak kedua operasi tersebut.

5.2 Satu penulis. Catatan ditulis oleh satu komponen yang memvalidasi kode tindakan dan muatannya sebelum menulis. Catatan yang tidak lolos validasi ditolak dan dilaporkan, bukan ditulis sebagian.

5.3 Penanganan kegagalan. Kegagalan penulisan audit tidak pernah menyebabkan kegagalan tindakan bisnis yang dijelaskannya. Kegagalan tersebut dicatat melalui jalur operasional yang dilengkapi alarm, dan catatan itu sendiri disimpan dalam salinan sekunder agar dapat dipulihkan.

---

6. Retensi dan lokasi

6.1 Retensi. Catatan audit disimpan setidaknya selama sepuluh (10) tahun sejak tanggal peristiwa.

6.2 Lokasi dan enkripsi. Catatan audit disimpan di Uni Eropa (Frankfurt, Jerman, `eu-central-1`) dan dienkripsi saat tersimpan dengan kunci AWS KMS yang dikelola pelanggan. Salinan langsung juga ditulis ke grup log Amazon CloudWatch yang aksesnya dikendalikan agar insiden dapat diselidiki saat sedang terjadi.

6.3 Tidak ada replikasi lintas wilayah. Catatan audit tidak direplikasi ke luar Uni Eropa.

---

7. Akses ke catatan audit

7.1 Hak akses. Log audit dalam aplikasi termasuk dalam paket Process Architecture dan paket di atasnya. Administrator organisasi dapat membaca seluruh organisasi; administrator dengan cakupan tenant dapat membaca tenantnya sendiri. Cakupan ditentukan berdasarkan sesi yang telah diautentikasi dan diperiksa sebelum kueri, sehingga permintaan tidak dapat memperluas cakupan ke tenant atau organisasi lain.

7.2 Personel ProcessMind. Personel ProcessMind mengakses catatan audit hanya untuk dukungan, penanganan insiden, atau kewajiban hukum, berdasarkan kebutuhan untuk mengetahui. Akses lintas pelanggan dibatasi pada peran dukungan khusus, dan akses tersebut merupakan tindakan administratif yang dicatat.

7.3 Cara memperoleh catatan. Administrator organisasi dan tenant dapat membaca catatan audit mereka di log audit dalam aplikasi, serta mengambil atau mengekspornya melalui API eksternal. Untuk permintaan yang lebih besar atau memerlukan bantuan, dukungan ProcessMind menyediakan catatan dalam format CSV atau JSON untuk organisasi, tenant, dan rentang waktu tertentu, dengan sasaran lima (5) hari kerja untuk permintaan standar.

---

8. Penghapusan catatan audit

8.1 Atas permintaan. Setelah menerima permintaan tertulis yang telah diverifikasi, ProcessMind menghapus catatan audit milik organisasi pelanggan dari penyimpanan audit dan mengonfirmasi penghapusan tersebut secara tertulis. Salinan operasional CloudWatch tidak dapat

disunting satu per satu; salinan tersebut kedaluwarsa sesuai periode retensinya sendiri.

8.2 Hal yang disimpan. Catatan bahwa penghapusan telah dilakukan (pengenal organisasi, tanggal, pemohon, alasan, dan jumlah catatan yang dihapus) disimpan sebagai catatan audit tingkat platform dan tidak memuat Data Pelanggan. Catatan yang bukan milik pelanggan mana pun (peristiwa platform ProcessMind) tidak terpengaruh oleh permintaan penghapusan pelanggan.

8.3 Permintaan penghapusan individu. Jika permintaan berkaitan dengan individu dalam suatu pelanggan yang tetap aktif, catatan keamanan disimpan untuk penetapan, pelaksanaan, atau pembelaan klaim hukum sebagaimana diizinkan oleh Pasal 17(3)(b) dan (e) GDPR; dasar tersebut dicatat dalam catatan kegiatan pemrosesan dan dalam Kebijakan Privasi.

---

9. Integrasi dan ekspor SIEM

9.1 Ketersediaan. Arsip audit yang tidak dapat diubah merupakan opsi Enterprise, yang diaktifkan untuk organisasi pelanggan berdasarkan permintaan. Arsip ini menulis objek NDJSON terkompresi setiap hari dengan prefiks per organisasi di bucket S3 Object-Locked (WORM), beserta manifes dan rekonsiliasi setiap malam.

9.2 Pengiriman saat ini. Saat ini ProcessMind tidak menawarkan konektor SIEM bawaan atau umpan push. Pengiriman dilakukan dengan cara pull dari tiga sarana: API baca (`GET /v1/tenant/{tenantId}/audit`), tugas ekspor terbatas (buat dengan `POST /v1/tenant/{tenantId}/audit/exports` dan ambil hasilnya melalui panggilan status, yang mengembalikan URL unduhan berjangka pendek), dan, dengan arsip Enterprise, objek harian di bawah prefiks milik organisasi sendiri dalam bucket Object-Locked, yang dibaca SIEM pelanggan melalui pengaturan akses. ProcessMind tidak mengirimkan catatan ke lokasi pilihan pelanggan berdasarkan jadwalnya sendiri.

9.3 Pemantauan internal ProcessMind. Pemantauan keamanan ProcessMind menggunakan catatan yang sama: kegagalan penulisan audit, lonjakan kegagalan autentikasi, perubahan hak istimewa, dan tindakan administratif destruktif memicu alarm internal.

---

10. Bukti yang tersedia bagi pelanggan

Atas permintaan, dan dengan tunduk pada kerahasiaan jika berlaku, ProcessMind menyediakan pernyataan ini, Langkah-Langkah Keamanan, Adendum Pemrosesan Data, Daftar Subprosesor, contoh catatan audit yang telah disunting, dan prosedur yang digunakan untuk permintaan akses dan penghapusan.

---

11. Batasan

Untuk menghindari keraguan, ProcessMind menyatakan bahwa setiap organisasi memiliki penyimpanan audit yang hanya dapat ditambahkan dan, jika hak akses arsip audit diaktifkan, salinan Object-Locked (WORM) dengan rekonsiliasi manifes setiap malam. Saat ini ProcessMind tidak menyatakan memiliki rantai hash, konektor push SIEM real-time bawaan, penyuntingan catatan audit per pengguna, pengesahan ISO 27001 atau SOC 2 yang mencakup kontrol ini, atau cakupan atas setiap pembacaan Data Pelanggan. Pelanggan dapat membaca dan mengekspor sendiri melalui log audit dalam aplikasi dan API eksternal.