Verklaring van ProcessMind over auditlog en SIEM

Ingangsdatum: 12 november 2026

Deze verklaring beschrijft hoe ProcessMind B.V. beveiligingsrelevante en administratieve handelingen met betrekking tot Klantgegevens registreert (de "auditlog"). Deze verklaring vormt een aanvulling op de Beveiligingsmaatregelen, het Addendum inzake gegevensverwerking, de Klantovereenkomst en de Lijst van subverwerkers.

---

1. Reikwijdte

1.1 Eén auditlog. ProcessMind houdt één auditlog bij voor beveiligingsrelevante en administratieve handelingen met betrekking tot Klantgegevens en de ProcessMind-dienst. De auditlog staat los van operationele logging (applicatielogging), HTTP-toegangslogging en de activiteitenfeed van het product; deze gegevensstromen dienen andere doeleinden en worden niet voorgesteld als een audittrail.

1.2 Wat het niet is. De auditlog is geen registratie van elke raadpleging van Klantgegevens en vormt niet de wijzigingsgeschiedenis van het product voor procesmodellen, diagrammen, documentatie of simulaties. Deze worden vastgelegd in de proceswijzigingsgeschiedenis die in het product beschikbaar is.

---

2. Wat elk auditrecord bevat

2.1 Velden. Elk record bevat de onderstaande velden. De set wordt bepaald door het recordschema: een record kan geen veld bevatten dat niet op deze lijst staat, en een handeling kan geen veld toevoegen dat niet in het register is opgenomen.

- *schemaVersion* (getal): versie van het recordschema, momenteel 1.
- *eventId* (tekenreeks): unieke recordidentificatie. Nieuwe records gebruiken een ULID; rijen die uit de eerdere opslag zijn gemigreerd,

behouden hun UUID.

- *occurredAt*, *ingestedAt* (tijdstempels): het tijdstip waarop de handeling plaatsvond en het tijdstip waarop de auditwriter het record heeft opgeslagen. Beide in UTC.
- *eventClass* (enum): security, auth, admin, data, api, ai of platform.
- *action* (enum): één code uit het gesloten, beoordeelde actieregister, bijvoorbeeld auth.login.blocked of api.key.revoked.
- *outcome* (enum): success, failure, denied of error.
- *severity* (enum): info, notice, warning of critical, afgeleid van de uitkomst. Voor een geslaagde handeling geldt de standaardwaarde uit het register (info, tenzij bij de handeling anders is aangegeven), een mislukking wordt geregistreerd als notice en denied of error als warning.
- *actor* (object): wie de handeling heeft verricht. type (user, apiKey, service, system of anonymous), id, email, displayName en onBehalfOf plus onBehalfOfEmail wanneer de handeling voor een andere account is uitgevoerd.
- *actorContext* (object): de sessie waarin de handeling is verricht. sessionId, authMethod (oidc, password, loginToken, apiKey of none) en een vlag voor een supportsessie.
- *organizationId*, *tenantId* (identificaties, nullable): de organisatie en de omgeving waartoe de handeling behoort. Null voor records die geen klant betreffen of die boven de omgeving staan.
- *resource* (object, nullable): het getroffen object. type, id en name, waarbij type een van de volgende waarden heeft: apiKey, artifact, connection, database, datatable, export, lead, model, organization, process, role, session, setting, storage, tenant of user.
- *source* (object): waar het record is aangemaakt. service (api, externalApi, superadminApi, worker, cron of webSocket), function en version.
- *stage*, *region* (tekenreeksen): de implementatiefase waarin het record is aangemaakt (bijvoorbeeld prod) en de AWS-regio (eu-central-1 voor klantrecords).

- *correlation* (object): requestId, traceId en parentEventId, die het record koppelen aan het verzoek dat ertoe heeft geleid en aan de voorgaande records in dezelfde stroom.
- *network* (object, nullable): sourceIp en userAgent. Alleen vastgelegd voor handelingen waarvoor de registervermelding dit toestaat: aanmelden, toegangsbeslissingen, administratieve wijzigingen en wijzigingen van instellingen, gegevensuploads, downloads en exports, wijzigingen van API-sleutels en wijzigingen van AI-beleid.
- *detail* (object): de eigen payload van de handeling, gevalideerd aan de hand van het schema voor die handeling. Waarden zijn uitsluitend primitieve waarden (string, number, boolean, null), zodat het record doorzoekbaar en redigeerbaar blijft.

2.2 Een gesloten vocabulaire. Handelingen komen uit een vaste, beoordeelde lijst met actiecodes; een auditrecord bevat geen vrije tekst. Elke handeling vermeldt ook welke aanvullende velden deze mag bevatten, zodat een record niet ongemerkt een nieuw soort inhoud kan krijgen.

---

3. Welke handelingen worden geregistreerd

3.1 Huidige registratie. ProcessMind registreert onder meer:

- **Authenticatie:** geslaagde en mislukte aanmeldingen, geblokkeerde aanmeldingen (vergrendelde account, niet-toegestaan domein, niet-geverifieerd e-mailadres van de identiteitsprovider), afmeldingen, uitgifte en overdracht van inlogtokens.
- **Autorisatie:** geweigerde toegang, waaronder elke afgewezen aanmeldingsgegeven voor de externe API, scope en tenantstatus, en afwijzingen op basis van de oorsprong (CORS).
- **Supporttoegang:** het starten van een ProcessMind-supportsessie op een klantaccount, met vermelding van zowel de medewerker als de getroffen account.
- **API-aanmeldingsgegevens:** aanmaak, wijziging van scope en intrekking van API-sleutels, met inbegrip van de toegekende scopes.

- **Account- en rolbeheer:** aanmaak en uitnodiging van gebruikers, wijzigingen van beheerdersprofielen, verwijdering, toekenning en intrekking van rollen, en wijzigingen van tenant- of organisatielidmaatschap.
- **Levenscyclus van organisaties:** aanmaak, verwijdering, herstel, planning en annulering van verwijdering, en voltooide wissing.
- **Upload, download en export van gegevens:** upload, download en verwijdering van artefacten, upload en bijwerking van tabelgegevens, downloads van exports, verwijdering van gegevenstabellen en aanmaak, wijziging en verwijdering van webhooks (verbindingen).
- **Factureringsstatus:** wijzigingen van abonnementen, opschorting en herstel wegens betaling, en annulering van abonnementen.
- **Providerconsole van ProcessMind:** uitvoering van bevoorrechte query's, beheer van gebruikers en organisaties, wijzigingen van instellingen en functies, verzoeken om factureringssynchronisatie en migraties.
- **Administratieve en destructieve handelingen door geplande taken van ProcessMind:** verwijdering van tenants, organisaties, gebruikers en leads, opschoning op basis van bewaartermijnen en fouten in pipelines.
- **Integriteit van de auditlog:** fouten in het eigen schrijfproces van de auditlog.

3.2 Wijzigingen in werkruimten. Wijzigingen binnen een werkruimte (procesmodellen, documentatie, simulaties, dashboards, opmerkingen en bladwijzers) worden vastgelegd in de eigen proceswijzigingsgeschiedenis van het product, niet in de auditlog. De auditlog registreert wie gegevens heeft geüpload, gedownload, geëxporteerd of verwijderd; de wijzigingsgeschiedenis registreert wat er in een model is gewijzigd. De actuele lijst met geregistreerde actiecodes is op verzoek verkrijgbaar bij ProcessMind.

---

4. Wat nooit wordt geregistreerd

Wachtwoorden, authenticatietokens, waarden van API-sleutels, cookies, autorisatieheaders, verzoek- of antwoordinhoud, bestandsinhoud, vooraf ondertekende URL's en AI-prompts of -antwoorden worden nooit in de auditlog opgenomen. Auditrecords kunnen persoonsgegevens bevatten die nodig zijn voor toerekening: het e-mailadres van een actor en het bron-IP-adres en de user agent voor handelingen waarvoor de registervermelding dit toestaat (aanmelden, toegangsbeslissingen, administratieve wijzigingen en wijzigingen van instellingen, gegevensverplaatsing, wijzigingen van API-sleutels en AI-beleid). De toegestane velden worden per handeling bepaald en beoordeeld wanneer een handeling wordt toegevoegd.

---

5. Integriteit

5.1 Alleen toevoegen. Aan de auditlog kunnen uitsluitend records worden toegevoegd. Geen enkele applicatierol heeft rechten om deze bij te werken of te verwijderen, en een databasebeperking weigert beide bewerkingen.

5.2 Eén schrijver. Records worden geschreven door één component die de actiecode en de payload valideert voordat deze worden opgeslagen. Een record dat niet aan de validatie voldoet, wordt geweigerd en gemeld in plaats van gedeeltelijk opgeslagen.

5.3 Afhandeling van fouten. Een mislukte auditregistratie laat de zakelijke handeling die deze beschrijft nooit mislukken. De fout wordt geregistreerd via een operationeel proces met alarmmelding en het record zelf wordt bewaard in een secundaire kopie, zodat het kan worden hersteld.

---

6. Bewaartermijn en locatie

6.1 Bewaartermijn. Auditrecords worden vanaf de datum van de gebeurtenis ten minste tien (10) jaar bewaard.

6.2 Locatie en versleuteling. Auditrecords worden opgeslagen in de Europese Unie (Frankfurt, Duitsland, `eu-central-1`) en worden in rust versleuteld met een door de klant beheerde AWS KMS-sleutel. Daarnaast wordt een actuele kopie geschreven naar een toegangsbeperkte Amazon CloudWatch-loggroep, zodat een incident tijdens het plaatsvinden ervan kan worden onderzocht.

6.3 Geen replicatie tussen regio's. Auditrecords worden niet buiten de Europese Unie gerepliceerd.

---

7. Toegang tot auditrecords

7.1 Toegangsrechten. De auditlog in de app is inbegrepen bij het abonnement Process Architecture en hogere abonnementen. Een organisatiebeheerder kan de volledige organisatie inzien; een tenantbeheerder kan de eigen tenant inzien. De reikwijdte wordt afgeleid van de geauthenticeerde sessie en vóór de query gecontroleerd, zodat een verzoek deze niet kan uitbreiden naar een andere tenant of organisatie.

7.2 Medewerkers van ProcessMind. Medewerkers van ProcessMind hebben alleen toegang tot auditrecords voor support, incidentrespons of een wettelijke verplichting, op basis van noodzakelijke kennis. Toegang tot gegevens van andere klanten is beperkt tot een specifieke supportrol; dergelijke toegang is zelf een administratieve handeling.

7.3 Auditrecords verkrijgen. Organisatie- en tenantbeheerders kunnen hun auditrecords inzien in de auditlog in de app en deze ophalen of exporteren via de externe API. Voor een groter verzoek of een verzoek waarvoor ondersteuning nodig is, verstrekt ProcessMind Support de records in CSV- of JSON-formaat voor een opgegeven organisatie, tenant en periode; voor een standaardverzoek geldt een streeftermijn van vijf (5) werkdagen.

---

8. Verwijdering van auditrecords

8.1 Op verzoek. Na een geverifieerd schriftelijk verzoek wist ProcessMind de auditrecords van een klantorganisatie uit de auditopslag en bevestigt het de wissing schriftelijk. De operationele CloudWatch-kopie kan niet record voor record worden bewerkt; deze verloopt volgens de eigen bewaartermijn.

8.2 Wat wordt bewaard. Het record waaruit blijkt dat de wissing heeft plaatsgevonden (organisatie-identificatie, datum, verzoeker, reden en het aantal verwijderde records) wordt bewaard als een auditrecord op platformniveau en bevat geen Klantgegevens. Records die niet aan een klant toebehoren (gebeurtenissen op het ProcessMind-platform) worden niet beïnvloed door een verzoek tot wissing van een klant.

8.3 Verzoeken tot wissing van personen. Wanneer een verzoek betrekking heeft op een persoon binnen een klant die actief blijft, wordt het beveiligingsrecord bewaard voor de instelling, uitoefening of onderbouwing van rechtsvorderingen, zoals toegestaan op grond van artikel 17(3)(b) en (e) AVG; die grondslag wordt vastgelegd in het register van verwerkingsactiviteiten en in het Privacybeleid.

---

9. SIEM-integratie en export

9.1 Beschikbaarheid. Het onveranderlijke auditarchief is een Enterprise-optie die op verzoek voor een klantorganisatie wordt ingeschakeld. Het schrijft dagelijks gecomprimeerde NDJSON-objecten onder een prefix per organisatie in een S3-bucket met Object Lock (WORM), met een manifest en nachtelijke afstemming.

9.2 Huidige levering. ProcessMind biedt momenteel geen native SIEM-connector of pushfeed. Levering vindt plaats via pull, vanaf drie locaties: de lees-API (`GET /v1/tenant/{tenantId}/audit`), de begrensde exporttaak (aanmaken met `POST /v1/tenant/{tenantId}/audit/exports` en het resultaat ophalen via de statusaanroep, die een tijdelijke download-URL retourneert)

en, met het Enterprise-archief, de dagelijkse objecten onder de eigen prefix van de organisatie in de bucket met Object Lock, die het SIEM van de klant via een toegangsregeling uitleest. ProcessMind levert niet zelfstandig records volgens een eigen schema af op een door de klant gekozen locatie.

9.3 Eigen monitoring van ProcessMind. De beveiligingsmonitoring van ProcessMind gebruikt dezelfde records: mislukte auditregistraties, pieken in mislukte authenticaties, wijzigingen van bevoegdheden en destructieve administratieve handelingen leiden tot interne alarmmeldingen.

---

10. Bewijsstukken die beschikbaar zijn voor klanten

Op verzoek en, waar van toepassing, onder geheimhouding verstrekt ProcessMind deze verklaring, de Beveiligingsmaatregelen, het Addendum inzake gegevensverwerking, de Lijst van subverwerkers, een geredigeerd voorbeeld van auditrecords en de procedure voor verzoeken om toegang en wissing.

---

11. Beperkingen

Voor alle duidelijkheid: ProcessMind stelt dat er voor elke organisatie een auditopslag is waaraan uitsluitend records kunnen worden toegevoegd en dat, wanneer het recht op het auditarchief is ingeschakeld, er een kopie met Object Lock (WORM) is met nachtelijke afstemming van het manifest. ProcessMind stelt momenteel niet dat er sprake is van een hashketen, een native SIEM-pushconnector in realtime, redactie van auditrecords per gebruiker, een ISO 27001- of SOC 2-verklaring die deze beheersmaatregel omvat, of dekking van elke raadpleging van Klantgegevens. Klanten kunnen zelf records inzien en exporteren via de auditlog in de app en de externe API.