Erklärung zum Audit-Protokoll und SIEM von ProcessMind

Gültig ab: 12. November 2026

Diese Erklärung beschreibt, wie ProcessMind B.V. sicherheitsrelevante und administrative Aktionen protokolliert, die in Bezug auf Kundendaten ausgeführt werden (das „Audit-Protokoll“). Sie ergänzt die Sicherheitsmaßnahmen, den Nachtrag zur Auftragsverarbeitung, die Kundenvereinbarung und die Liste der Unterauftragsverarbeiter.

---

1. Geltungsbereich

1.1 Ein Audit-Protokoll. ProcessMind führt ein einziges Audit-Protokoll für sicherheitsrelevante und administrative Aktionen, die in Bezug auf Kundendaten und den ProcessMind-Dienst ausgeführt werden. Das Audit-Protokoll ist von der betrieblichen (Anwendungs-)Protokollierung, der HTTP-Zugriffsprotokollierung und dem Aktivitätsfeed des Produkts getrennt; diese Datenströme dienen anderen Zwecken und stellen keinen Audit-Trail dar.

1.2 Was es nicht ist. Das Audit-Protokoll erfasst nicht jeden Lesezugriff auf Kundendaten und ist auch nicht der Änderungsverlauf des Produkts für Prozessmodelle, Diagramme, Dokumentation oder Simulationen. Diese werden im innerhalb des Produkts verfügbaren Prozessänderungsverlauf erfasst.

---

2. Inhalt der einzelnen Audit-Aufzeichnungen

2.1 Felder. Jede Aufzeichnung enthält die nachstehend aufgeführten Felder. Die Menge der Felder ist durch das Aufzeichnungsschema festgelegt: Eine Aufzeichnung kann kein Feld enthalten, das nicht in dieser Liste aufgeführt ist, und eine Aktion kann kein Feld hinzufügen, das sie nicht im Register deklariert hat.

- *schemaVersion* (Zahl): Version des Aufzeichnungsschemas, derzeit 1.

- *eventId* (Zeichenfolge): eindeutige Kennung der Aufzeichnung. Neue Aufzeichnungen verwenden eine ULID; aus dem früheren Speicher migrierte Zeilen behalten ihre UUID.
- *occurredAt*, *ingestedAt* (Zeitstempel): Zeitpunkt der Aktion und Zeitpunkt, zu dem der Audit Writer die Aufzeichnung gespeichert hat. Beide in UTC.
- *eventClass* (Enum): security, auth, admin, data, api, ai oder platform.
- *action* (Enum): ein Code aus dem geschlossenen, geprüften Aktionsregister, zum Beispiel auth.login.blocked oder api.key.revoked.
- *outcome* (Enum): success, failure, denied oder error.
- *severity* (Enum): info, notice, warning oder critical, abgeleitet aus dem Ergebnis. Bei einer erfolgreichen Aktion wird der Standardwert des Registers verwendet (info, sofern für die Aktion nichts anderes festgelegt ist); ein Fehlschlag wird als notice und denied oder error als warning erfasst.
- *actor* (Objekt): wer gehandelt hat. type (user, apiKey, service, system oder anonymous), id, email, displayName sowie onBehalfOf und onBehalfOfEmail, wenn die Aktion für ein anderes Konto ausgeführt wurde.
- *actorContext* (Objekt): die Sitzung, in der gehandelt wurde. sessionId, authMethod (oidc, password, loginToken, apiKey oder none) und ein Kennzeichen für Support-Sitzungen.
- *organizationId*, *tenantId* (Kennungen, nullable): die Organisation und die Umgebung, zu denen die Aktion gehört. Null bei Aufzeichnungen, die keinen Kunden betreffen oder oberhalb der Umgebung angesiedelt sind.
- *resource* (Objekt, nullable): das betroffene Objekt. type, id und name, wobei type einen der folgenden Werte hat: apiKey, artifact, connection, database, datatable, export, lead, model, organization, process, role, session, setting, storage, tenant oder user.
- *source* (Objekt): wo die Aufzeichnung erstellt wurde. service (api, externalApi, superadminApi, worker, cron oder webSocket), function und version.

- *stage*, *region* (Zeichenfolgen): die Bereitstellungsstufe, in der die Aufzeichnung erstellt wurde (zum Beispiel prod), und die AWS-Region (eu-central-1 für Kundenaufzeichnungen).
- *correlation* (Objekt): requestId, traceId und parentEventId, die die Aufzeichnung mit der sie auslösenden Anfrage und den vorangegangenen Aufzeichnungen desselben Ablaufs verknüpfen.
- *network* (Objekt, nullable): sourceIp und userAgent. Werden nur für Aktionen erfasst, für die der entsprechende Eintrag im Register dies vorsieht: Anmeldung, Zugriffsentscheidungen, administrative Änderungen und Einstellungsänderungen, Daten-Uploads, Downloads und Exporte, Änderungen an API-Schlüsseln und Änderungen an KI-Richtlinien.
- *detail* (Objekt): die eigene Nutzlast der Aktion, validiert anhand des Schemas dieser Aktion. Werte sind ausschließlich primitive Datentypen (Zeichenfolge, Zahl, boolescher Wert, null), damit die Aufzeichnung abfragbar und redigierbar bleibt.

2.2 Ein geschlossenes Vokabular. Aktionen stammen aus einer festgelegten, geprüften Liste von Aktionscodes; eine Audit-Aufzeichnung enthält keine Freitextnachricht. Für jede Aktion ist außerdem festgelegt, welche zusätzlichen Felder sie enthalten darf, sodass eine Aufzeichnung nicht unbemerkt um eine neue Art von Inhalt erweitert werden kann.

---

3. Welche Aktionen protokolliert werden

3.1 Derzeit protokolliert. ProcessMind protokolliert unter anderem:

- **Authentifizierung:** erfolgreiche und fehlgeschlagene Anmeldungen, blockierte Anmeldungen (gesperrtes Konto, nicht zugelassene Domain, nicht verifizierte E-Mail-Adresse des Anbieters), Abmeldungen, Ausstellung und Übergabe von Anmeldetoken.
- **Autorisierung:** Zugriffsverweigerungen, einschließlich jeder abgelehnten Anmeldedaten für externe APIs, jedes abgelehnten

Umfangs und jedes abgelehnten Mandantenstatus sowie Ablehnungen aufgrund des Ursprungs (CORS).

- **Supportzugriff:** Beginn einer ProcessMind-Supportsitzung für ein Kundenkonto unter Angabe sowohl des Mitarbeiters als auch des betroffenen Kontos.
- **API-Anmeldedaten:** Erstellung, Änderung des Umfangs und Widerruf von API-Schlüsseln, einschließlich der gewährten Berechtigungsumfänge.
- **Konten- und Rollenverwaltung:** Erstellung von Benutzern, Einladungen, Änderungen an Administratorprofilen, Löschungen, Erteilung und Widerruf von Rollen sowie Änderungen der Mandanten- oder Organisationsmitgliedschaft.
- **Lebenszyklus von Organisationen:** Erstellung, Löschung, Wiederherstellung, Planung und Stornierung von Löschungen sowie abgeschlossene Löschung.
- **Daten-Upload, -Download und -Export:** Upload, Download und Löschung von Artefakten, Upload und Aktualisierung tabellarischer Daten, Export-Downloads, Löschung von Datentabellen sowie Erstellung, Änderung und Löschung von Webhooks (Verbindungen).
- **Abrechnungsstatus:** Tarifänderungen, durch Zahlungen bedingte Sperrungen und Wiederherstellungen sowie Kündigung von Abonnements.
- **Anbieterkonsole von ProcessMind:** Ausführung privilegierter Abfragen, Benutzer- und Organisationsverwaltung, Änderungen an Einstellungen und Funktionen, Anfragen zur Abrechnungssynchronisierung und Migrationen.
- **Administrative und destruktive Aktionen durch geplante Jobs von ProcessMind:** Löschungen von Mandanten, Organisationen, Benutzern und Leads, Aufbewahrungsbereinigungen und Pipeline-Fehler.
- **Integrität des Audit-Protokolls:** Fehler beim Schreibvorgang des Audit-Protokolls selbst.

3.2 Änderungen im Arbeitsbereich. Änderungen innerhalb eines Arbeitsbereichs (Prozessmodelle, Dokumentation, Simulationen, Dashboards, Kommentare und Lesezeichen) werden im eigenen Prozessänderungsverlauf des Produkts und nicht im Audit-Protokoll erfasst. Das Audit-Protokoll erfasst, wer Daten hochgeladen, heruntergeladen, exportiert oder gelöscht hat; der Änderungsverlauf erfasst, was in einem Modell geändert wurde. Die aktuelle Liste der protokollierten Aktionscodes ist auf Anfrage bei ProcessMind erhältlich.

---

4. Was niemals protokolliert wird

Passwörter, Authentifizierungstoken, API-Schlüsselwerte, Cookies, Autorisierungsheader, Anfrage- oder Antwortinhalte, Dateiinhalte, vorab signierte URLs sowie KI-Prompts oder -Vervollständigungen werden niemals in das Audit-Protokoll geschrieben. Audit-Aufzeichnungen können personenbezogene Daten enthalten, die zur Zuordnung erforderlich sind: die E-Mail-Adresse eines Akteurs sowie die Quell-IP-Adresse und den User-Agent für Aktionen, für die der entsprechende Eintrag im Register dies vorsieht (Anmeldungen, Zugriffsentscheidungen, administrative Änderungen und Einstellungsänderungen, Datenbewegungen, Änderungen an API-Schlüsseln und KI-Richtlinien). Die zulässigen Felder werden für jede Aktion festgelegt und bei deren Aufnahme überprüft.

---

5. Integrität

5.1 Nur anhängbar. Das Audit-Protokoll ist nur anhängbar. Keine Anwendungsrolle verfügt über Änderungs- oder Löschberechtigungen dafür, und eine Datenbankbeschränkung weist beide Vorgänge zurück.

5.2 Ein einziger Writer. Die Aufzeichnungen werden von einer einzelnen Komponente geschrieben, die den Aktionscode und dessen Nutzlast vor dem Schreiben validiert. Eine Aufzeichnung, die die Validierung nicht

besteht, wird zurückgewiesen und gemeldet, statt teilweise geschrieben zu werden.

5.3 Fehlerbehandlung. Ein fehlgeschlagener Audit-Schreibvorgang führt niemals zum Fehlschlagen der darin beschriebenen Geschäftsaktion. Er wird über einen überwachten betrieblichen Pfad erfasst, und die Aufzeichnung selbst wird in einer sekundären Kopie aufbewahrt, damit sie wiederhergestellt werden kann.

---

6. Aufbewahrung und Speicherort

6.1 Aufbewahrung. Audit-Aufzeichnungen werden ab dem Ereignisdatum mindestens zehn (10) Jahre lang aufbewahrt.

6.2 Speicherort und Verschlüsselung. Audit-Aufzeichnungen werden in der Europäischen Union (Frankfurt, Deutschland, `eu-central-1`) gespeichert und im Ruhezustand mit einem vom Kunden verwalteten AWS-KMS-Schlüssel verschlüsselt. Zusätzlich wird eine Live-Kopie in eine zugriffskontrollierte Amazon-CloudWatch-Loggruppe geschrieben, damit ein Vorfall während seines Auftretens untersucht werden kann.

6.3 Keine regionsübergreifende Replikation. Audit-Aufzeichnungen werden nicht außerhalb der Europäischen Union repliziert.

---

7. Zugriff auf Audit-Aufzeichnungen

7.1 Berechtigung. Das Audit-Protokoll in der Anwendung ist im Tarif Process Architecture und höheren Tarifen enthalten. Ein Organisationsadministrator kann die gesamte Organisation einsehen; ein auf einen Mandanten beschränkter Administrator kann den eigenen Mandanten einsehen. Der Umfang wird aus der authentifizierten Sitzung abgeleitet und vor der Abfrage geprüft, sodass eine Anfrage ihn nicht auf einen anderen Mandanten oder eine andere Organisation ausweiten kann.

7.2 Personal von ProcessMind. Das Personal von ProcessMind greift nur für Support, die Reaktion auf Vorfälle oder zur Erfüllung einer rechtlichen Verpflichtung und nach dem Erforderlichkeitsprinzip auf Audit-Aufzeichnungen zu. Der kundenübergreifende Zugriff ist auf eine spezielle Supportrolle beschränkt; ein solcher Zugriff ist selbst eine administrative Aktion.

7.3 Erhalt von Aufzeichnungen. Organisations- und Mandantenadministratoren können ihre Audit-Aufzeichnungen im Audit-Protokoll der Anwendung einsehen und über die externe API abrufen oder exportieren. Bei umfangreicheren oder unterstützten Anfragen stellt der ProcessMind-Support die Aufzeichnungen für eine angegebene Organisation, einen angegebenen Mandanten und einen angegebenen Zeitraum im CSV- oder JSON-Format bereit; bei einer Standardanfrage wird eine Bearbeitungszeit von fünf (5) Werktagen angestrebt.

---

8. Löschung von Audit-Aufzeichnungen

8.1 Auf Anfrage. Auf eine verifizierte schriftliche Anfrage hin löscht ProcessMind die zu einer Kundenorganisation gehörenden Audit-Aufzeichnungen aus dem Audit-Speicher und bestätigt die Löschung schriftlich. Die operative CloudWatch-Kopie kann nicht auf Ebene einzelner Aufzeichnungen bearbeitet werden; sie läuft gemäß ihrer eigenen Aufbewahrungsfrist ab.

8.2 Aufbewahrte Informationen. Die Aufzeichnung über die erfolgte Löschung (Organisationskennung, Datum, anfragende Person, Grund und Anzahl der entfernten Aufzeichnungen) wird als Audit-Aufzeichnung auf Plattformebene aufbewahrt und enthält keine Kundendaten. Aufzeichnungen, die keinem Kunden zuzuordnen sind (Ereignisse der ProcessMind-Plattform), sind von einem Löschantrag eines Kunden nicht betroffen.

8.3 Anträge auf Löschung einzelner Personen. Betrifft ein Antrag eine Person innerhalb eines Kunden, der weiterhin aktiv ist, wird die

Sicherheitsaufzeichnung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen aufbewahrt, soweit dies nach Artikel 17 Absatz 3 Buchstaben b und e DSGVO zulässig ist; diese Rechtsgrundlage wird im Verzeichnis der Verarbeitungstätigkeiten und in der Datenschutzerklärung festgehalten.

---

9. SIEM-Integration und Export

9.1 Verfügbarkeit. Das unveränderliche Audit-Archiv ist eine Enterprise-Option, die auf Anfrage für eine Kundenorganisation aktiviert wird. Es schreibt täglich komprimierte NDJSON-Objekte unter einem organisationsspezifischen Präfix in einen Object-Locked-(WORM-)S3-Bucket, zusammen mit einem Manifest und einem nächtlichen Abgleich.

9.2 Derzeitige Bereitstellung. ProcessMind bietet derzeit weder einen nativen SIEM-Connector noch einen Push-Feed an. Die Bereitstellung erfolgt per Abruf über drei Schnittstellen: die Lese-API (`GET /v1/tenant/{tenantId}/audit`), den begrenzten Exportauftrag (mit `POST /v1/tenant/{tenantId}/audit/exports` erstellen und das Ergebnis über dessen Statusaufruf abrufen, der eine kurzlebige Download-URL zurückgibt) sowie – mit dem Enterprise-Archiv – die täglichen Objekte unter dem organisationsspezifischen Präfix im Object-Locked-Bucket, die das SIEM des Kunden im Rahmen einer Zugriffsvereinbarung ausliest. ProcessMind stellt Aufzeichnungen nicht eigenständig nach einem eigenen Zeitplan an einem vom Kunden gewählten Speicherort bereit.

9.3 Eigene Überwachung von ProcessMind. Die Sicherheitsüberwachung von ProcessMind verarbeitet dieselben Aufzeichnungen: Fehler beim Schreiben des Audit-Protokolls, gehäufte Authentifizierungsfehler, Berechtigungsänderungen und destruktive administrative Aktionen lösen interne Alarme aus.

---

10. Kunden verfügbare Nachweise

Auf Anfrage und gegebenenfalls unter Vertraulichkeitsauflagen stellt ProcessMind diese Erklärung, die Sicherheitsmaßnahmen, den Nachtrag zur Auftragsverarbeitung, die Liste der Unterauftragsverarbeiter, ein redigiertes Muster von Audit-Aufzeichnungen sowie das Verfahren für Zugriffs- und Löschanträge bereit.

---

11. Einschränkungen

Zur Klarstellung: ProcessMind beansprucht für jede Organisation einen nur anhängbaren Audit-Speicher und, sofern die Berechtigung für das Audit-Archiv aktiviert ist, eine Object-Locked-(WORM-)Kopie mit nächtlichem Abgleich des Manifests. ProcessMind beansprucht derzeit weder eine Hash-Kette noch einen nativen SIEM-Push-Connector in Echtzeit, eine Redigierung von Audit-Aufzeichnungen auf Benutzerebene, eine ISO-27001- oder SOC-2-Bescheinigung für diese Kontrolle noch die Erfassung jedes Lesezugriffs auf Kundendaten. Kunden können Audit-Aufzeichnungen über das Audit-Protokoll in der Anwendung und die externe API selbst einsehen und exportieren.