A ProcessMind auditnapló- és SIEM-nyilatkozata

Hatálybalépés dátuma: 2026. november 12.

Ez a nyilatkozat ismerteti, hogyan rögzíti a ProcessMind B.V. az Ügyféladatokon végzett, biztonsági szempontból releváns és adminisztratív műveleteket (az „auditnapló"). Kiegészíti a Biztonsági intézkedéseket, az Adatfeldolgozási kiegészítést, az Ügyfélszerződést és az Alfeldolgozók listáját.

---

1. Hatály

1.1 Egyetlen auditnapló. A ProcessMind egyetlen auditnaplót vezet az Ügyféladatokon és a ProcessMind Szolgáltatáson végzett, biztonsági szempontból releváns és adminisztratív műveletekről. Az auditnapló elkülönül a működési (alkalmazás-)naplózástól, a HTTP-hozzáférési naplózástól és a termék tevékenységfolyamától; ezek az adatfolyamok eltérő célokat szolgálnak, és nem minősülnek auditnyomvonalnak.

1.2 Mi nem tartozik ide. Az auditnapló nem rögzíti az Ügyféladatok minden egyes olvasását, és nem a termék folyamatmodellekre, diagramokra, dokumentációra vagy szimulációkra vonatkozó változástörténete. Ezeket a terméken belül elérhető folyamatváltozási előzmények rögzítik.

---

2. Mit tartalmaznak az egyes auditbejegyzések

2.1 Mezők. Minden bejegyzés az alábbi mezőket tartalmazza. A mezőkészletet a bejegyzésséma rögzíti: a bejegyzés nem tartalmazhat a listán nem szereplő mezőt, és egy művelet sem adhat hozzá olyan mezőt, amelyet a nyilvántartásban nem deklaráltak.

- *schemaVersion* (szám): a bejegyzésséma verziója, jelenleg 1.
- *eventId* (karakterlánc): egyedi bejegyzésazonosító. Az új bejegyzések ULID-t használnak; a korábbi tárolóból migrált sorok megtartják UUID-jukat.

- *occurredAt*, *ingestedAt* (időbélyegek): a művelet időpontja, illetve az időpont, amikor az auditíró eltárolta a bejegyzést. Mindkettő UTC szerint.
- *eventClass* (felsorolás): security, auth, admin, data, api, ai vagy platform.
- *action* (felsorolás): egy kód a zárt, felülvizsgált művelet-nyilvántartásból, például auth.login.blocked vagy api.key.revoked.
- *outcome* (felsorolás): success, failure, denied vagy error.
- *severity* (felsorolás): info, notice, warning vagy critical, az eredményből levezetve. A sikeres művelet a nyilvántartásban meghatározott alapértelmezett értéket használja (info, kivéve, ha a művelet másként rendelkezik), a sikertelenség notice értékként, a denied vagy error pedig warning értékként kerül rögzítésre.
- *actor* (objektum): ki végezte a műveletet. type (user, apiKey, service, system vagy anonymous), id, email, displayName, valamint onBehalfOf és onBehalfOfEmail, ha a műveletet egy másik fiók nevében hajtották végre.
- *actorContext* (objektum): a műveletet végrehajtó munkamenet. sessionId, authMethod (oidc, password, loginToken, apiKey vagy none), valamint egy támogatási munkamenetet jelző érték.
- *organizationId*, *tenantId* (azonosítók, null értéket is felvehetnek): a szervezet és a környezet, amelyhez a művelet tartozik. Az érték null azoknál a bejegyzéseknél, amelyek nem érintenek ügyfelet, vagy a környezet feletti szinten helyezkednek el.
- *resource* (objektum, null értéket is felvehet): az érintett objektum. type, id és name, ahol a type értéke apiKey, artifact, connection, database, datatable, export, lead, model, organization, process, role, session, setting, storage, tenant vagy user lehet.
- *source* (objektum): a bejegyzés létrehozásának helye. service (api, externalApi, superadminApi, worker, cron vagy webSocket), function és version.
- *stage*, *region* (karakterláncok): a bejegyzést létrehozó telepítési szakasz (például prod) és az AWS-régió (ügyfélrekordok esetén eu-

central-1).

- *correlation* (objektum): requestId, traceId és parentEventId, amelyek a bejegyzést az azt kiváltó kérelemhez, valamint az ugyanabban az adatfolyamban előtte keletkezett bejegyzésekhez kapcsolják.
- *network* (objektum, null értéket is felvehet): sourceIp és userAgent. Csak azoknál a műveleteknél kerül rögzítésre, amelyek nyilvántartási bejegyzése ezt engedélyezi: bejelentkezés, hozzáférési döntések, adminisztratív és beállítási módosítások, adatfeltöltések, letöltések és exportok, API-kulcsok módosítása, valamint AI-szabályzatok módosítása.
- *detail* (objektum): a művelet saját adattartalma, az adott művelet sémája szerint ellenőrizve. Az értékek kizárólag primitív típusúak (karakterlánc, szám, logikai érték, null), így a bejegyzés lekérdezhető és kitakarható marad.

2.2 Zárt szókészlet. A műveletek kódjai egy rögzített, felülvizsgált listából származnak; az auditbejegyzés nem tartalmaz szabad szöveges üzenetet. Minden művelet azt is meghatározza, hogy milyen további mezőket tartalmazhat, így a bejegyzés nem bővülhet észrevétlenül új típusú tartalommal.

---

3. Mely műveletek kerülnek rögzítésre

3.1 Jelenleg rögzített műveletek. A ProcessMind többek között az alábbiakat rögzíti:

- **Hitelesítés:** sikeres és sikertelen bejelentkezés, blokkolt bejelentkezés (zárolt fiók, nem engedélyezett tartomány, nem ellenőrzött szolgáltatói e-mail-cím), kijelentkezés, bejelentkezési token kibocsátása és átadása.
- **Engedélyezés:** hozzáférés megtagadása, beleértve minden elutasított külső API-hitelesítő adatot, hatókört és bérlői állapotot, valamint a forrás (CORS) miatti elutasításokat.

- **Támogatási hozzáférés:** a ProcessMind támogatási munkamenetének megkezdése egy ügyfélfiókban, megnevezve mind az ügyintézőt, mind az érintett fiókot.
- **API-hitelesítő adatok:** API-kulcsok létrehozása, hatókörének módosítása és visszavonása, beleértve a megadott hatóköröket.
- **Fiók- és szerepkör-adminisztráció:** felhasználók létrehozása, meghívása, rendszergazdai profilok szerkesztése, törlése, szerepkörök megadása és visszavonása, valamint a bérlői vagy szervezeti tagság módosítása.
- **Szervezeti életciklus:** létrehozás, törlés, visszaállítás, törlés ütemezése és megszakítása, valamint a végleges törlés végrehajtása.
- **Adatok feltöltése, letöltése és exportálása:** artefaktumok feltöltése, letöltése és törlése, táblázatos adatok feltöltése és frissítése, exportok letöltése, adattáblák törlése, valamint webhookok (kapcsolatok) létrehozása, módosítása és törlése.
- **Számlázási állapot:** csomagváltások, fizetés miatti felfüggesztés és helyreállítás, valamint az előfizetés lemondása.
- **A ProcessMind szolgáltatói konzolja:** kiemelt jogosultságú lekérdezések végrehajtása, felhasználók és szervezetek adminisztrációja, beállítások és funkciók módosítása, számlázási szinkronizálási kérelmek és migrációk.
- **A ProcessMind ütemezett feladatai által végzett adminisztratív és romboló műveletek:** bérlők, szervezetek, felhasználók és érdeklődők törlése, megőrzési időszak szerinti törlési műveletek, valamint folyamatfeldolgozási hibák.
- **Az auditnapló integritása:** az auditnapló saját írási folyamatának hibái.

3.2 Munkaterületen végzett szerkesztések. A munkaterületen belüli szerkesztéseket (folyamatmodellek, dokumentáció, szimulációk, dashboardok, megjegyzések és könyvjelzők) a termék saját folyamatváltozási előzményei rögzítik, nem az auditnapló. Az auditnapló azt rögzíti, hogy ki töltött fel, töltött le, exportált vagy törölt adatokat; a változási

előzmények pedig azt, hogy mi változott egy modellen belül. A rögzített műveleti kódok aktuális listája kérésre elérhető a ProcessMindtől.

---

4. Mi nem kerül rögzítésre

Jelszavak, hitelesítési tokenek, API-kulcsok értékei, cookie-k, engedélyezési fejlécek, kérések vagy válaszok törzse, fájltartalmak, előre aláírt URL-ek, valamint AI-promptok vagy -kiegészítések soha nem kerülnek az auditnaplóba. Az auditbejegyzések tartalmazhatnak a hozzárendeléshez szükséges személyes adatokat: a műveletet végző személy e-mail-címét, valamint a forrás IP-címét és user agentjét azoknál a műveleteknél, amelyek nyilvántartási bejegyzése ezt engedélyezi (bejelentkezés, hozzáférési döntések, adminisztratív és beállítási módosítások, adatmozgatás, API-kulcsok és AI-szabályzatok módosítása). Az engedélyezett mezőket műveletenként határozzák meg, és a művelet felvételekor felülvizsgálják.

---

5. Integritás

5.1 Csak hozzáfűzés. Az auditnapló csak hozzáfűzhető. Egyetlen alkalmazásszerepkör sem rendelkezik módosítási vagy törlési jogosultsággal, és adatbázis-korlátozás utasítja el mindkét műveletet.

5.2 Egyetlen író. A bejegyzéseket egyetlen komponens írja, amely írás előtt ellenőrzi a műveleti kódot és annak adattartalmát. Az ellenőrzésen át nem menő bejegyzést elutasítja és jelenti, nem pedig részlegesen írja be.

5.3 Hibakezelés. A sikertelen auditírás soha nem hiúsítja meg az általa leírt üzleti műveletet. A hibát riasztással ellátott működési útvonalon rögzítik, magát a bejegyzést pedig egy másodlagos példányban is megőrzik, hogy helyreállítható legyen.

---

6. Megőrzés és helyszín

6.1 Megőrzés. Az auditbejegyzéseket az esemény dátumától számított legalább tíz (10) évig őrzik meg.

6.2 Helyszín és titkosítás. Az auditbejegyzéseket az Európai Unióban (Frankfurt, Németország, `eu-central-1`) tárolják, és nyugalmi állapotban az ügyfél által kezelt AWS KMS-kulccsal titkosítják. Egy élő példányt emellett egy hozzáférés-vezérelt Amazon CloudWatch naplócsoportba is írnak, hogy az incidensek bekövetkezésük közben kivizsgálhatók legyenek.

6.3 Nincs régiók közötti replikáció. Az auditbejegyzéseket nem replikálják az Európai Unión kívülre.

---

7. Hozzáférés az auditbejegyzésekhez

7.1 Jogosultság. Az alkalmazáson belüli auditnapló a Process Architecture csomagban és az annál magasabb csomagokban érhető el. A szervezeti rendszergazda a teljes szervezet adatait olvashatja; a bérlőre korlátozott rendszergazda a saját bérlője adatait olvashatja. A hatókör a hitelesített munkamenetből származik, és a lekérdezés előtt ellenőrzik, így a kérelem nem terjesztheti ki azt másik bérlőre vagy szervezetre.

7.2 A ProcessMind személyzete. A ProcessMind személyzete kizárólag támogatás, incidenskezelés vagy jogi kötelezettség teljesítése céljából, a szükséges ismeret elve alapján fér hozzá az auditbejegyzésekhez. Az ügyfelek közötti hozzáférés egy erre kijelölt támogatási szerepkörre korlátozódik, és az ilyen hozzáférés maga is adminisztratív műveletnek minősül.

7.3 A bejegyzések beszerzése. A szervezeti és bérlői rendszergazdák az alkalmazáson belüli auditnaplóban olvashatják auditbejegyzéseiket, és a külső API-n keresztül lekérhetik vagy exportálhatják azokat. Nagyobb vagy támogatást igénylő kérelem esetén a ProcessMind támogatási csapata CSV- vagy JSON-formátumban biztosítja a bejegyzéseket a megadott

szervezetre, bérlőre és időszakra vonatkozóan; a szokásos kérelmek esetében öt (5) munkanapos teljesítési céllal.

---

8. Az auditbejegyzések törlése

8.1 Kérelemre. Ellenőrzött írásbeli kérelem alapján a ProcessMind törli az ügyfélszervezethez tartozó auditbejegyzéseket az auditadat-tárolóból, és írásban megerősíti a törlést. A működési CloudWatch-példány bejegyzésenként nem szerkeszthető; a saját megőrzési időszakának lejártakor törlődik.

8.2 Mi marad meg. A törlés tényét rögzítő bejegyzést (szervezetazonosító, dátum, kérelmező, indok és az eltávolított bejegyzések száma) platformszintű auditbejegyzésként őrzik meg, és az nem tartalmaz Ügyféladatokat. Az ügyfélhez nem tartozó bejegyzéseket (a ProcessMind platformeseményeit) az ügyfél törlési kérelme nem érinti.

8.3 Egyéni törlési kérelmek. Ha a kérelem olyan személyre vonatkozik, aki egy továbbra is aktív ügyfélnél dolgozik, a biztonsági bejegyzést a jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez szükséges mértékben megőrzik, a GDPR 17. cikke (3) bekezdésének b) és e) pontja által megengedettek szerint; ezt a jogalapot az adatkezelési tevékenységek nyilvántartásában és az Adatvédelmi szabályzatban rögzítik.

---

9. SIEM-integráció és exportálás

9.1 Elérhetőség. A megváltoztathatatlan auditarchívum Enterprise-opció, amelyet kérelemre engedélyeznek az ügyfélszervezet számára. Naponta tömörített NDJSON-objektumokat ír szervezetenkénti előtag alatt egy Object-Locked (WORM) S3-tárolóba, jegyzékkel és éjszakai egyeztetéssel.

9.2 Jelenlegi kézbesítés. A ProcessMind jelenleg nem kínál natív SIEM-csatlakozót vagy push-adatfolyamot. Az adatok lekéréssel érhetők el, három felületen keresztül: az olvasási API-n (`GET /v1/tenant/{tenantId}/audit`), a korlátozott exportfeladaton keresztül (hozza

létre a `POST /v1/tenant/{tenantId}/audit/exports` használatával, majd kérje le az eredményt az állapotlekérdezésből, amely rövid élettartamú letöltési URL-t ad vissza), valamint Enterprise-archívum esetén a szervezet saját előtagja alatt lévő napi objektumokon keresztül az Object-Locked tárolóban, amelyeket az ügyfél SIEM-rendszere hozzáférési megállapodás alapján olvas. A ProcessMind nem kézbesít bejegyzéseket az ügyfél által választott helyre, saját ütemezése szerint.

9.3 A ProcessMind saját felügyelete. A ProcessMind biztonsági felügyelete ugyanezeket a bejegyzéseket használja: az auditírási hibák, a hitelesítési hibák megugrásai, a jogosultságváltozások és a romboló adminisztratív műveletek belső riasztásokat váltanak ki.

---

10. Az ügyfelek számára elérhető bizonyítékok

Kérésre, és adott esetben titoktartási kötelezettség mellett a ProcessMind rendelkezésre bocsátja ezt a nyilatkozatot, a Biztonsági intézkedéseket, az Adatfeldolgozási kiegészítést, az Alfeldolgozók listáját, az auditbejegyzések kitakart mintáját, valamint a hozzáférési és törlési kérelmekre alkalmazott eljárást.

---

11. Korlátozások

A kétségek elkerülése érdekében a ProcessMind minden szervezet esetében csak hozzáfűzhető auditadat-tárolót, továbbá – ha az auditarchívumra vonatkozó jogosultság engedélyezett – Object-Locked (WORM) példányt és éjszakai jegyzékegyeztetést biztosít. A ProcessMind jelenleg nem állítja, hogy hash-láncot, natív, valós idejű SIEM-push-csatlakozót, auditbejegyzések felhasználónkénti kitakarását, e kontrollra kiterjedő ISO 27001- vagy SOC 2-tanúsítást, illetve az Ügyféladatok minden olvasására kiterjedő lefedettséget biztosít. Az ügyfelek önkiszolgáló olvasási és exportálási lehetősége az alkalmazáson belüli auditnaplón és a külső API-n keresztül érhető el.