Prohlášení ProcessMind o protokolu auditu a SIEM

Datum účinnosti: 12. listopadu 2026

Toto prohlášení popisuje, jak společnost ProcessMind B.V. zaznamenává bezpečnostně relevantní a administrativní činnosti prováděné ve vztahu k zákaznickým datům (dále jen „protokol auditu“). Doplňuje Bezpečnostní opatření, Dodatek o zpracování údajů, Zákaznickou smlouvu a Seznam dílčích zpracovatelů.

---

1. Rozsah

1.1 Jeden protokol auditu. ProcessMind vede jediný protokol auditu bezpečnostně relevantních a administrativních činností prováděných ve vztahu k zákaznickým datům a službě ProcessMind. Protokol auditu je oddělen od provozního (aplikačního) protokolování, protokolování přístupu HTTP a kanálu aktivit produktu; tyto datové toky slouží jiným účelům a nejsou prezentovány jako auditní stopa.

1.2 Co protokol auditu není. Protokol auditu není záznamem každého přístupu ke čtení zákaznických dat ani historií změn produktu pro procesní modely, diagramy, dokumentaci nebo simulace. Tyto změny se zaznamenávají v historii změn procesů dostupné v produktu.

---

2. Obsah jednotlivých auditních záznamů

2.1 Pole. Každý záznam obsahuje níže uvedená pole. Jejich soubor je pevně stanoven schématem záznamu: záznam nemůže obsahovat pole, které není na tomto seznamu, a činnost nemůže přidat pole, které nebylo deklarováno v registru.

- *schemaVersion* (číslo): verze schématu záznamu, aktuálně 1.
- *eventId* (řetězec): jedinečný identifikátor záznamu. Nové záznamy používají ULID; řádky migrované z dřívějšího úložiště si zachovávají své UUID.

- *occurredAt*, *ingestedAt* (časová razítka): kdy k činnosti došlo a kdy zapisovací komponenta auditu záznam uložila. Obojí v UTC.
- *eventClass* (výčtový typ): security, auth, admin, data, api, ai nebo platform.
- *action* (výčtový typ): jeden kód z uzavřeného a prověřeného registru činností, například auth.login.blocked nebo api.key.revoked.
- *outcome* (výčtový typ): success, failure, denied nebo error.
- *severity* (výčtový typ): info, notice, warning nebo critical, odvozené od výsledku. U úspěšné činnosti se použije výchozí hodnota z registru (info, pokud není u činnosti uvedeno jinak), neúspěch se zaznamená jako notice a denied nebo error jako warning.
- *actor* (objekt): kdo činnost provedl. type (user, apiKey, service, system nebo anonymous), id, email, displayName a onBehalfOf spolu s onBehalfOfEmail, pokud byla činnost provedena za jiný účet.
- *actorContext* (objekt): relace, v níž byla činnost provedena. sessionId, authMethod (oidc, password, loginToken, apiKey nebo none) a příznak relace podpory.
- *organizationId*, *tenantId* (identifikátory, mohou být null): organizace a prostředí, k nimž činnost náleží. Hodnota null u záznamů, které se netýkají žádného zákazníka nebo se vztahují k úrovni nad prostředím.
- *resource* (objekt, může být null): dotčený objekt. type, id a name, přičemž type je jedna z hodnot apiKey, artifact, connection, database, datatable, export, lead, model, organization, process, role, session, setting, storage, tenant nebo user.
- *source* (objekt): místo, kde byl záznam vytvořen. service (api, externalApi, superadminApi, worker, cron nebo webSocket), function a version.
- *stage*, *region* (řetězce): fáze nasazení, ve které byl záznam vytvořen (například prod), a oblast AWS (eu-central-1 pro zákaznické záznamy).
- *correlation* (objekt): requestId, traceId a parentEventId, které propojují záznam s požadavkem, jenž jej vyvolal, a s předchozími

záznamy v témže toku.

- *network* (objekt, může být null): sourceIp a userAgent. Zachycují se pouze u činností, u nichž to příslušná položka registru povoluje: přihlášení, rozhodnutí o přístupu, administrativní změny a změny nastavení, nahrávání, stahování a export dat, změny klíčů API a změny zásad AI.
- *detail* (objekt): vlastní údaje dané činnosti, ověřené podle jejího schématu. Hodnoty jsou pouze primitivní (řetězec, číslo, logická hodnota, null), aby bylo možné záznamy dotazovat a redigovat.

2.2 Uzavřený slovník. Činnosti se vybírají z pevného, prověřeného seznamu kódů; auditní záznam neobsahuje žádnou volně psanou zprávu. Každá činnost také deklaruje, která další pole může obsahovat, takže záznam nemůže bez upozornění získat nový druh obsahu.

---

3. Které činnosti se zaznamenávají

3.1 Aktuálně zaznamenávané činnosti. ProcessMind zaznamenává mimo jiné:

- **Ověřování:** úspěšná a neúspěšná přihlášení, zablokovaná přihlášení (uzamčený účet, nepovolená doména, neověřený e-mail poskytovatele), odhlášení, vydání přihlašovacího tokenu a jeho předání.
- **Autorizace:** zamítnutí přístupu, včetně každého odmítnutého přihlašovacího údaje pro externí API, rozsahu oprávnění a stavu tenanta, a odmítnutí na základě původu (CORS).
- **Přístup podpory:** zahájení relace podpory ProcessMind v zákaznickém účtu, včetně uvedení operátora i dotčeného účtu.
- **Přihlašovací údaje API:** vytvoření, změna rozsahu oprávnění a odvolání klíčů API, včetně udělených rozsahů oprávnění.
- **Správa účtů a rolí:** vytvoření uživatele, pozvání, úpravy profilu správce, odstranění, udělení a odvolání rolí a změny členství v tenantu nebo organizaci.

- **Životní cyklus organizace:** vytvoření, odstranění, obnovení, naplánování odstranění a jeho zrušení a dokončené vymazání.
- **Nahrávání, stahování a export dat:** nahrání, stažení a odstranění artefaktů, nahrání a aktualizace tabulkových dat, stažení exportů, odstranění datových tabulek a vytvoření, změna a odstranění webhooků (připojení).
- **Fakturační stav:** změny plánu, pozastavení a obnovení z důvodu platby a zrušení předplatného.
- **Konzole poskytovatele ProcessMind:** provádění privilegovaných dotazů, správa uživatelů a organizací, změny nastavení a funkcí, požadavky na synchronizaci fakturace a migrace.
- **Administrativní a destruktivní činnosti plánovaných úloh ProcessMind:** odstraňování tenantů, organizací, uživatelů a potenciálních zákazníků, úlohy hromadného mazání podle retenčních lhůt a selhání zpracovatelských toků.
- **Integrita protokolu auditu:** selhání vlastního procesu zápisu protokolu auditu.

3.2 Úpravy pracovního prostoru. Úpravy v pracovním prostoru (procesní modely, dokumentace, simulace, dashboardy, komentáře a záložky) se zaznamenávají ve vlastní historii změn procesů produktu, nikoli v protokolu auditu. Protokol auditu zaznamenává, kdo data nahrál, stáhl, exportoval nebo odstranil; historie změn zaznamenává, co se změnilo v modelu. Aktuální seznam zaznamenávaných kódů činností poskytne ProcessMind na vyžádání.

---

4. Co se nikdy nezaznamenává

Hesla, ověřovací tokeny, hodnoty klíčů API, soubory cookie, autorizační hlavičky, těla požadavků nebo odpovědí, obsah souborů, předem podepsané adresy URL a výzvy nebo dokončení AI se do protokolu auditu nikdy nezapisují. Auditní záznamy mohou obsahovat osobní údaje nezbytné k určení původu činnosti: e-mailovou adresu aktéra a zdrojovou IP adresu a user agent u činností, u nichž to příslušná položka registru

povoluje (přihlášení, rozhodnutí o přístupu, administrativní změny a změny nastavení, přesun dat, změny klíčů API a zásad AI). Povolená pole jsou definována pro každou činnost a při jejím přidání se prověřují.

---

5. Integrita

5.1 Pouze připojování. Do protokolu auditu lze pouze připojovat záznamy. Žádná aplikační role nemá oprávnění k jeho aktualizaci ani odstranění a databázové omezení obě operace odmítá.

5.2 Jediný zapisovatel. Záznamy zapisuje jediná komponenta, která před zápisem ověřuje kód činnosti a její údaje. Záznam, který ověřením neprojde, se odmítne a nahlásí, místo aby byl zapsán pouze částečně.

5.3 Řešení selhání. Selhání zápisu do auditu nikdy nezpůsobí selhání obchodní činnosti, kterou popisuje. Zaznamená se prostřednictvím provozního procesu s aktivovaným alarmem a samotný záznam se uchová v sekundární kopii, aby jej bylo možné obnovit.

---

6. Uchovávání a umístění

6.1 Uchovávání. Auditní záznamy se uchovávají po dobu nejméně deseti (10) let od data události.

6.2 Umístění a šifrování. Auditní záznamy se ukládají v Evropské unii (Frankfurt, Německo, `eu-central-1`) a jsou šifrovány v klidovém stavu pomocí klíče AWS KMS spravovaného zákazníkem. Živá kopie se navíc zapisuje do skupiny protokolů Amazon CloudWatch s řízeným přístupem, aby bylo možné vyšetřovat incident v průběhu jeho řešení.

6.3 Bez replikace mezi oblastmi. Auditní záznamy se nereplikují mimo Evropskou unii.

---

7. Přístup k auditním záznamům

7.1 Oprávnění. Protokol auditu v aplikaci je zahrnut v plánu Process Architecture a vyšších plánech. Správce organizace může číst záznamy celé organizace; správce s rozsahem oprávnění omezeným na tenanta může číst záznamy svého tenanta. Rozsah se odvozuje z ověřené relace a kontroluje před provedením dotazu, takže požadavek jej nemůže rozšířit na jiného tenanta nebo organizaci.

7.2 Pracovníci ProcessMind. Pracovníci ProcessMind přistupují k auditním záznamům pouze za účelem podpory, reakce na incident nebo splnění právní povinnosti, a to na základě nezbytné znalosti. Přístup napříč zákazníky je omezen na vyhrazenou roli podpory a takový přístup je sám o sobě administrativní činností.

7.3 Jak získat záznamy. Správci organizace a tenanta mohou číst své auditní záznamy v protokolu auditu v aplikaci a získávat je nebo exportovat prostřednictvím externího API. U rozsáhlejšího požadavku nebo požadavku vyžadujícího asistenci poskytne podpora ProcessMind záznamy ve formátu CSV nebo JSON pro určenou organizaci, tenanta a časové období; u standardního požadavku je cílová lhůta pět (5) pracovních dnů.

---

8. Odstranění auditních záznamů

8.1 Na žádost. Na základě ověřené písemné žádosti ProcessMind vymaže z úložiště auditu auditní záznamy náležející zákaznické organizaci a písemně potvrdí jejich vymazání. Provozní kopii v CloudWatch nelze upravovat po jednotlivých záznamech; její platnost skončí podle její vlastní retenční lhůty.

8.2 Co se uchovává. Záznam o provedeném vymazání (identifikátor organizace, datum, žadatel, důvod a počet odstraněných záznamů) se uchovává jako auditní záznam na úrovni platformy a neobsahuje žádná zákaznická data. Záznamy, které nenáleží žádnému zákazníkovi (události platformy ProcessMind), nejsou žádostí zákazníka o vymazání dotčeny.

8.3 Žádosti o vymazání jednotlivých osob. Pokud se žádost týká jednotlivce u zákazníka, který zůstává aktivní, bezpečnostní záznam se uchovává pro určení, výkon nebo obhajobu právních nároků, jak povoluje čl. 17 odst. 3 písm. b) a e) GDPR; tento právní základ se zaznamenává v záznamu o činnostech zpracování a v Zásadách ochrany osobních údajů.

---

9. Integrace SIEM a export

9.1 Dostupnost. Neměnný archiv auditu je volitelnou funkcí tarifu Enterprise, kterou lze na žádost aktivovat pro zákaznickou organizaci. Denně zapisuje komprimované objekty NDJSON pod prefixem příslušné organizace do bucketu S3 s uzamčením objektů (WORM), včetně manifestu a nočního odsouhlasení.

9.2 Aktuální způsob doručování. ProcessMind v současnosti nenabízí nativní konektor SIEM ani push kanál. Záznamy se získávají prostřednictvím tří rozhraní: API pro čtení (`GET /v1/tenant/{tenantId}/audit`), omezená úloha exportu (vytvořte ji pomocí `POST /v1/tenant/{tenantId}/audit/exports` a výsledek získejte prostřednictvím volání jejího stavu, které vrací krátkodobou adresu URL ke stažení) a v případě archivu Enterprise denní objekty pod vlastním prefixem organizace v bucketu s uzamčením objektů, které SIEM zákazníka čte na základě dohody o přístupu. ProcessMind nedoručuje záznamy podle vlastního harmonogramu do umístění zvoleného zákazníkem.

9.3 Vlastní monitorování ProcessMind. Bezpečnostní monitorování ProcessMind využívá stejné záznamy: selhání zápisu do auditu, nárůsty počtu selhání ověřování, změny oprávnění a destruktivní administrativní činnosti vyvolávají interní alarmy.

---

10. Podklady dostupné zákazníkům

Na vyžádání a případně za podmínek důvěrnosti poskytne ProcessMind toto prohlášení, Bezpečnostní opatření, Dodatek o zpracování údajů,

Seznam dílčích zpracovatelů, redigovaný vzor auditních záznamů a postup používaný pro žádosti o přístup a vymazání.

---

11. Omezení

Pro vyloučení pochybností ProcessMind uvádí, že pro každou organizaci používá úložiště auditu, do něhož lze pouze připojovat záznamy, a pokud je aktivováno oprávnění k archivu auditu, také kopii s uzamčením objektů (WORM) a nočním odsouhlasením manifestu. ProcessMind v současnosti netvrdí, že používá hashovací řetězec, nativní konektor SIEM pro přenos v reálném čase, redigování auditních záznamů pro jednotlivé uživatele, osvědčení podle ISO 27001 nebo SOC 2 vztahující se na tuto kontrolu ani že pokrývá každý přístup ke čtení zákaznických dat. Zákazníci mohou sami číst a exportovat záznamy prostřednictvím protokolu auditu v aplikaci a externího API.