Dichiarazione di ProcessMind sul registro di audit e SIEM

Data di entrata in vigore: 12 novembre 2026

La presente dichiarazione descrive come ProcessMind B.V. registra le azioni rilevanti per la sicurezza e amministrative eseguite sui Dati del Cliente (il «registro di audit»). Essa integra le Misure di sicurezza, l'Addendum sul trattamento dei dati, il Contratto con il Cliente e l'Elenco dei sub-responsabili del trattamento.

---

1. Ambito di applicazione

1.1 Un unico registro di audit. ProcessMind mantiene un unico registro di audit per le azioni rilevanti per la sicurezza e amministrative eseguite sui Dati del Cliente e sul Servizio ProcessMind. Il registro di audit è distinto dalla registrazione operativa (dell'applicazione), dalla registrazione degli accessi HTTP e dal feed delle attività del prodotto; tali flussi hanno finalità diverse e non sono presentati come una traccia di audit.

1.2 Cosa non è. Il registro di audit non documenta ogni lettura dei Dati del Cliente e non costituisce la cronologia delle modifiche del prodotto per modelli di processo, diagrammi, documentazione o simulazioni. Queste modifiche sono registrate nella cronologia delle modifiche dei processi disponibile all'interno del prodotto.

---

2. Contenuto di ciascun record di audit

2.1 Campi. Ogni record contiene i campi indicati di seguito. L'insieme è definito dallo schema del record: un record non può includere un campo non presente in questo elenco e un'azione non può aggiungere un campo che non abbia dichiarato nel registro.

- *schemaVersion* (numero): versione dello schema del record, attualmente 1.

- *eventId* (stringa): identificativo univoco del record. I nuovi record utilizzano un ULID; le righe migrate dal precedente archivio mantengono il proprio UUID.
- *occurredAt*, *ingestedAt* (timestamp): quando si è verificata l'azione e quando il componente di scrittura dell'audit ha memorizzato il record. Entrambi in UTC.
- *eventClass* (enum): security, auth, admin, data, api, ai o platform.
- *action* (enum): un codice tratto dal registro chiuso e sottoposto a revisione delle azioni, ad esempio auth.login.blocked o api.key.revoked.
- *outcome* (enum): success, failure, denied o error.
- *severity* (enum): info, notice, warning o critical, determinata in base all'esito. Per un'azione riuscita si applica il valore predefinito del registro (info, salvo diversa indicazione per l'azione); un'azione non riuscita è registrata come notice e un'azione negata o con errore come warning.
- *actor* (oggetto): chi ha agito. type (user, apiKey, service, system o anonymous), id, email, displayName e onBehalfOf, oltre a onBehalfOfEmail quando l'azione è stata eseguita per un altro account.
- *actorContext* (oggetto): la sessione dell'autore dell'azione. sessionId, authMethod (oidc, password, loginToken, apiKey o none) e un flag relativo alla sessione di assistenza.
- *organizationId*, *tenantId* (identificativi, nullable): l'organizzazione e l'ambiente a cui appartiene l'azione. Null per i record che non riguardano alcun cliente o che si collocano al di sopra dell'ambiente.
- *resource* (oggetto, nullable): l'oggetto interessato. type, id e name, dove type è uno tra apiKey, artifact, connection, database, datatable, export, lead, model, organization, process, role, session, setting, storage, tenant o user.
- *source* (oggetto): dove è stato prodotto il record. service (api, externalApi, superadminApi, worker, cron o webSocket), function e

version.

- *stage*, *region* (stringhe): la fase di distribuzione che ha prodotto il record (ad esempio prod) e la regione AWS (eu-central-1 per i record dei clienti).
- *correlation* (oggetto): requestId, traceId e parentEventId, che collegano il record alla richiesta che lo ha generato e ai record che lo precedono nello stesso flusso.
- *network* (oggetto, nullable): sourceIp e userAgent. Acquisiti solo per le azioni per le quali la relativa voce del registro prevede tale acquisizione: accesso, decisioni di accesso, modifiche amministrative e alle impostazioni, caricamenti, download ed esportazioni di dati, modifiche delle chiavi API e modifiche delle policy AI.
- *detail* (oggetto): il payload specifico dell'azione, convalidato rispetto allo schema di tale azione. I valori sono esclusivamente primitivi (string, number, boolean, null), affinché il record resti consultabile e oscurabile.

2.2 Vocabolario chiuso. Le azioni sono selezionate da un elenco fisso e sottoposto a revisione di codici; un record di audit non contiene messaggi in testo libero. Ogni azione dichiara inoltre quali campi aggiuntivi può contenere, così che un record non possa acquisire silenziosamente una nuova tipologia di contenuto.

---

3. Quali azioni vengono registrate

3.1 Registrazioni attuali. ProcessMind registra, tra le altre, le seguenti azioni:

- **Autenticazione:** accessi riusciti e non riusciti, accessi bloccati (account bloccato, dominio non consentito, e-mail del provider non verificata), disconnessioni, emissione e trasferimento di token di accesso.
- **Autorizzazione:** dinieghi di accesso, comprese tutte le credenziali API esterne rifiutate, gli ambiti e gli stati del tenant, nonché i rifiuti

relativi all'origine (CORS).

- **Accesso per assistenza:** avvio di una sessione di assistenza ProcessMind su un account cliente, con indicazione sia dell'operatore sia dell'account interessato.
- **Credenziali API:** creazione, modifica degli ambiti e revoca delle chiavi API, compresi gli ambiti concessi.
- **Amministrazione di account e ruoli:** creazione di utenti, inviti, modifiche ai profili degli amministratori, eliminazioni, concessioni e revoche di ruoli e modifiche all'appartenenza a tenant o organizzazioni.
- **Ciclo di vita dell'organizzazione:** creazione, eliminazione, ripristino, pianificazione e annullamento dell'eliminazione e cancellazione completata.
- **Caricamento, download ed esportazione di dati:** caricamento, download ed eliminazione di artefatti, caricamento e aggiornamento di dati tabellari, download di esportazioni, eliminazione di tabelle di dati e creazione, modifica ed eliminazione di webhook (connessioni).
- **Stato di fatturazione:** modifiche del piano, sospensione e ripristino dovuti ai pagamenti e annullamento dell'abbonamento.
- **Console del provider di ProcessMind:** esecuzione di query con privilegi elevati, amministrazione di utenti e organizzazioni, modifiche alle impostazioni e alle funzionalità, richieste di sincronizzazione della fatturazione e migrazioni.
- **Azioni amministrative e distruttive eseguite dai processi pianificati di ProcessMind:** eliminazioni di tenant, organizzazioni, utenti e lead, operazioni di pulizia dei dati in base ai periodi di conservazione e errori delle pipeline.
- **Integrità del registro di audit:** errori del processo di scrittura del registro di audit.

3.2 Modifiche all'area di lavoro. Le modifiche all'interno di un'area di lavoro (modelli di processo, documentazione, simulazioni, dashboard, commenti e segnalibri) sono registrate nella cronologia delle modifiche dei processi

del prodotto, non nel registro di audit. Il registro di audit indica chi ha caricato, scaricato, esportato o eliminato i dati; la cronologia delle modifiche indica cosa è cambiato all'interno di un modello. L'elenco aggiornato dei codici delle azioni registrate è disponibile su richiesta presso ProcessMind.

---

4. Cosa non viene mai registrato

Le password, i token di autenticazione, i valori delle chiavi API, i cookie, le intestazioni di autorizzazione, i corpi delle richieste o delle risposte, i contenuti dei file, gli URL presigned e i prompt o le risposte dell'AI non vengono mai scritti nel registro di audit. I record di audit possono contenere dati personali necessari per l'attribuzione: l'indirizzo e-mail dell'autore dell'azione e l'indirizzo IP di origine e lo user agent per le azioni per le quali la relativa voce del registro prevede tale acquisizione (accesso, decisioni di accesso, modifiche amministrative e alle impostazioni, trasferimento di dati, modifiche delle chiavi API e delle policy AI). I campi consentiti sono definiti per ciascuna azione e sottoposti a revisione quando viene aggiunta un'azione.

---

5. Integrità

5.1 Solo aggiunta. Il registro di audit consente esclusivamente l'aggiunta di record. Nessun ruolo dell'applicazione dispone di privilegi di aggiornamento o eliminazione sul registro e un vincolo del database rifiuta entrambe le operazioni.

5.2 Un unico componente di scrittura. I record sono scritti da un unico componente che convalida il codice dell'azione e il relativo payload prima della scrittura. Un record che non supera la convalida viene rifiutato e segnalato, anziché essere scritto parzialmente.

5.3 Gestione degli errori. Un errore di scrittura dell'audit non causa mai il fallimento dell'azione aziendale che descrive. L'errore viene registrato

tramite un processo operativo soggetto ad allarme e il record stesso viene conservato in una copia secondaria, affinché possa essere recuperato.

---

6. Conservazione e ubicazione

6.1 Conservazione. I record di audit sono conservati per almeno dieci (10) anni dalla data dell'evento.

6.2 Ubicazione e cifratura. I record di audit sono conservati nell'Unione europea (Francoforte, Germania, `eu-central-1`) e sono cifrati a riposo con una chiave AWS KMS gestita dal cliente. Una copia aggiornata viene inoltre scritta in un gruppo di log Amazon CloudWatch con accesso controllato, affinché sia possibile indagare su un incidente mentre è in corso.

6.3 Nessuna replica tra regioni. I record di audit non vengono replicati al di fuori dell'Unione europea.

---

7. Accesso ai record di audit

7.1 Diritto di accesso. Il registro di audit in-app è incluso nel piano Process Architecture e nei piani superiori. Un amministratore dell'organizzazione può leggere i record dell'intera organizzazione; un amministratore con ambito limitato al tenant può leggere i record del proprio tenant. L'ambito è determinato dalla sessione autenticata e verificato prima dell'esecuzione della query, pertanto una richiesta non può estenderlo a un altro tenant o a un'altra organizzazione.

7.2 Personale di ProcessMind. Il personale di ProcessMind accede ai record di audit solo per assistenza, risposta agli incidenti o adempimento di un obbligo di legge, in base al principio della necessità di conoscere. L'accesso trasversale ai clienti è limitato a un ruolo di assistenza dedicato e tale accesso costituisce esso stesso un'azione amministrativa.

7.3 Come ottenere i record. Gli amministratori di organizzazioni e tenant possono leggere i propri record di audit nel registro di audit in-app e

recuperarli o esportarli tramite l'API esterna. Per richieste più ampie o che richiedono assistenza, il supporto di ProcessMind fornisce i record in formato CSV o JSON per un'organizzazione, un tenant e un intervallo temporale specificati, con l'obiettivo di evadere le richieste standard entro cinque (5) giorni lavorativi.

---

8. Eliminazione dei record di audit

8.1 Su richiesta. A seguito di una richiesta scritta verificata, ProcessMind cancella dall'archivio di audit i record appartenenti all'organizzazione cliente e conferma per iscritto l'avvenuta cancellazione. La copia operativa di CloudWatch non può essere modificata record per record; scade in base al proprio periodo di conservazione.

8.2 Dati conservati. Il record dell'avvenuta cancellazione (identificativo dell'organizzazione, data, richiedente, motivo e numero di record rimossi) è conservato come record di audit a livello di piattaforma e non contiene Dati del Cliente. I record che non appartengono ad alcun cliente (eventi della piattaforma ProcessMind) non sono interessati da una richiesta di cancellazione del cliente.

8.3 Richieste di cancellazione individuali. Se una richiesta riguarda una persona fisica appartenente a un cliente che rimane attivo, il record di sicurezza è conservato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, nei limiti consentiti dall'articolo 17, paragrafo 3, lettere b) ed e), del GDPR; tale base è indicata nel registro delle attività di trattamento e nell'Informativa sulla privacy.

---

9. Integrazione SIEM ed esportazione

9.1 Disponibilità. L'archivio di audit immutabile è un'opzione Enterprise, attivabile su richiesta per l'organizzazione cliente. Scrive ogni giorno oggetti NDJSON compressi con un prefisso specifico per organizzazione in un

bucket S3 con Object Lock (WORM), corredati di un manifest e di una riconciliazione notturna.

9.2 Modalità di fornitura attuale. Attualmente ProcessMind non offre un connettore SIEM nativo né un feed push. La fornitura avviene tramite pull da tre interfacce: l'API di lettura (`GET /v1/tenant/{tenantId}/audit`), il processo di esportazione con limiti (creato con `POST /v1/tenant/{tenantId}/audit/exports`, il cui risultato si recupera tramite la chiamata di stato, che restituisce un URL di download a breve scadenza) e, con l'archivio Enterprise, gli oggetti giornalieri nel prefisso specifico dell'organizzazione nel bucket con Object Lock, che il SIEM del cliente legge tramite un accordo di accesso. ProcessMind non invia i record a una destinazione scelta dal cliente secondo una propria pianificazione.

9.3 Monitoraggio interno di ProcessMind. Il monitoraggio della sicurezza di ProcessMind utilizza gli stessi record: gli errori di scrittura dell'audit, i picchi di errori di autenticazione, le modifiche dei privilegi e le azioni amministrative distruttive generano allarmi interni.

---

10. Documentazione disponibile ai clienti

Su richiesta e, ove applicabile, nel rispetto degli obblighi di riservatezza, ProcessMind fornisce la presente dichiarazione, le Misure di sicurezza, l'Addendum sul trattamento dei dati, l'Elenco dei sub-responsabili del trattamento, un esempio oscurato di record di audit e la procedura utilizzata per le richieste di accesso e cancellazione.

---

11. Limitazioni

A scanso di equivoci, ProcessMind dichiara di utilizzare un archivio di audit che consente esclusivamente l'aggiunta di record per ogni organizzazione e, ove sia abilitato il diritto all'archivio di audit, una copia con Object Lock (WORM) e riconciliazione notturna del manifest. Attualmente ProcessMind non dichiara di utilizzare una catena di hash, un connettore SIEM nativo con

invio in tempo reale, l'oscuramento dei record di audit per singolo utente, un'attestazione ISO 27001 o SOC 2 relativa a questo controllo, né la copertura di ogni lettura dei Dati del Cliente. I clienti possono leggere ed esportare autonomamente i dati tramite il registro di audit in-app e l'API esterna.