Misure di sicurezza di ProcessMind

Data di entrata in vigore: 14 settembre 2026

Il presente documento descrive le misure tecniche e organizzative («TOM») che ProcessMind B.V. mantiene per proteggere la riservatezza, l'integrità e la disponibilità dei Customer Data. ProcessMind segue un approccio di difesa in profondità, nel quale più livelli di sicurezza indipendenti proteggono i Customer Data a ogni livello — dalla rete e dall'infrastruttura fino all'identità, all'autorizzazione, all'isolamento dei dati, alla crittografia, al monitoraggio e allo sviluppo del software. Tali misure integrano il Data Processing Addendum, la Privacy Policy e la SaaS Hosting Policy. ProcessMind riesamina e aggiorna tali misure almeno una volta all'anno.

I Customer Data non vengono mai venduti a terzi, condivisi con terzi né utilizzati da terzi per finalità proprie.

---

1. Sicurezza dell'infrastruttura

1.1 Piattaforma cloud. ProcessMind è ospitata esclusivamente su Amazon Web Services (AWS) nell'UE (Francoforte, Germania, `eu-central-1`). AWS mantiene le certificazioni ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3 e PCI DSS. Per un elenco completo, consulti AWS Compliance Programs.

1.2 Architettura serverless. La logica applicativa di ProcessMind viene eseguita su AWS Lambda e sui servizi gestiti da AWS. ProcessMind non gestisce server applicativi di lunga durata amministrati dai clienti, eliminando così un'ampia categoria di attività di applicazione delle patch al sistema operativo e di hardening dei server.

1.3 Confini di rete. ProcessMind mantiene una AWS VPC per i controlli del database e della rete. Aurora PostgreSQL viene eseguito in subnet private senza egress verso Internet, non è accessibile pubblicamente e i log di flusso VPC sono abilitati. Per impostazione predefinita, ProcessMind non colloca le funzioni Lambda applicative all'interno della VPC. Le funzioni

Lambda raggiungono Aurora tramite l'AWS RDS Data API su TLS, utilizzando l'autenticazione IAM e Secrets Manager.

1.4 Distribuzione dei contenuti e controlli edge. Il sito web rivolto ai clienti, la SPA frontend e il traffico verso le risorse pubbliche vengono serviti tramite Amazon CloudFront. Tutte le distribuzioni CloudFront impongono una policy TLS minima di TLS 1.2 (2021). Le distribuzioni del sito web e della SPA frontend aggiungono inoltre intestazioni di risposta di sicurezza, tra cui HTTP Strict Transport Security (HSTS), Content Security Policy (CSP), `frame-ancestors 'none'`, `X-Frame-Options: DENY`, `X-Content-Type-Options`, referrer policy e permissions policy. La distribuzione delle risorse pubbliche utilizza CloudFront Origin Access Control per mantenere privato il bucket di origine. Il traffico API rivolto ai clienti è gestito separatamente tramite Amazon API Gateway: il traffico HTTPS di richiesta/risposta viene servito tramite un'HTTP API su un sottodominio API dedicato e le connessioni client in tempo reale vengono servite tramite una WebSocket API separata di API Gateway su un sottodominio WebSocket dedicato.

1.5 Separazione degli ambienti. Gli ambienti di produzione e sviluppo utilizzano account AWS separati, database separati e stack infrastrutturali separati. Le credenziali degli sviluppatori non consentono l'accesso ai Customer Data di produzione.

---

2. Crittografia dei dati

2.1 Crittografia in transito. Tutti i dati trasmessi tra i client e i servizi ProcessMind sono crittografati utilizzando TLS 1.2 o superiore. Gli endpoint rivolti ai clienti sono esposti tramite HTTPS. I bucket S3, gli argomenti SNS e le code SQS creati direttamente da ProcessMind impongono l'accesso esclusivamente tramite SSL. L'accesso al database tramite RDS Data API e le altre chiamate ai servizi AWS utilizzano HTTPS/TLS.

2.2 Crittografia a riposo. Aurora PostgreSQL è crittografato a riposo utilizzando chiavi AWS KMS gestite dal cliente con rotazione automatica delle chiavi. I bucket S3 relativi ai dati dei clienti e alle operazioni creati

direttamente da ProcessMind, inclusi i bucket per upload, risorse e log di accesso, utilizzano chiavi KMS gestite dal cliente. Anche i gruppi di log CloudWatch, gli argomenti SNS e le code SQS creati direttamente da ProcessMind utilizzano chiavi KMS gestite dal cliente. I bucket di origine del sito web e del frontend gestiti da SST utilizzano la crittografia lato server S3 gestita da AWS (SSE-S3 / AES-256) anziché chiavi KMS gestite dal cliente.

2.3 Gestione delle chiavi e dei segreti. Le chiavi di crittografia del database sono gestite centralmente tramite AWS KMS e l'accesso alle chiavi è disciplinato dalle policy IAM secondo i principi del privilegio minimo. Le credenziali del database sono conservate in AWS Secrets Manager. Il segreto master di Aurora e il segreto dell'utente applicativo con accesso limitato ruotano automaticamente ogni trenta (30) giorni. Le chiavi e i segreti di produzione non vengono mai conservati nel codice sorgente; le credenziali utilizzate esclusivamente per lo sviluppo sono isolate dalla produzione. Alcune risorse di supporto gestite da AWS/CDK/SST continuano a utilizzare la crittografia gestita da AWS quando il servizio o il framework non espone una configurazione per chiavi gestite dal cliente.

---

3. Isolamento e residenza dei dati

3.1 Isolamento dei tenant. A ciascun tenant cliente viene assegnata un'istanza di database dedicata e isolata. I Customer Data non vengono mai mescolati con i dati di altri clienti a livello di database. I metadati condivisi (ad es. record degli account, fatturazione, mappature tra utenti e tenant) sono conservati in un database multi-tenant separato con rigorosi controlli degli accessi. Le tabelle condivise con ambito tenant e organizzazione sono inoltre protette da policy di sicurezza a livello di riga (RLS) di PostgreSQL, applicate tramite il contesto del database definito per la richiesta.

3.2 Localizzazione dei dati. Tutti i Dati del Cliente, inclusi database, caricamenti di file, backup e risultati delle query, sono archiviati esclusivamente nell'UE (Francoforte, Germania). Qualora un sub-

responsabile del trattamento situato al di fuori del SEE venga incaricato per una specifica attività di trattamento (ad esempio, il trattamento dei modelli AI o l'elaborazione dei pagamenti), il trasferimento è coperto da un meccanismo di trasferimento adeguato, come descritto nell'Addendum sul trattamento dei dati, e il sub-responsabile del trattamento e il relativo luogo del trattamento sono elencati nell'Elenco dei sub-responsabili del trattamento.

3.3 Conservazione e cancellazione dei dati. I termini di conservazione e cancellazione sono stabiliti nella Sezione 6 del Data Processing Addendum. I clienti possono cancellare i propri dati in qualsiasi momento tramite l'applicazione o contattando ProcessMind. Le copie di backup vengono rimosse alla scadenza delle finestre di conservazione dei backup applicabili (Sezione 7.1).

---

4. Gestione delle identità e degli accessi

4.1 Autenticazione. ProcessMind supporta il Single Sign-On (SSO) tramite Microsoft Entra ID (Azure AD), Google OAuth 2.0/OIDC e LinkedIn OAuth 2.0/OIDC. ProcessMind agisce in qualità di relying party e non conserva le password degli utenti. L'autenticazione a più fattori è applicata dal provider di identità — ad esempio, quando un'organizzazione collega Microsoft Entra ID (Azure AD), si applicano le policy di accesso e MFA proprie di tale organizzazione.

4.2 Gestione delle sessioni. Le sessioni del browser utilizzano JSON Web Token (JWT) firmati, trasmessi tramite cookie sicuri con flag SameSite e Secure e con attributo HttpOnly. Le firme dei token vengono convalidate a ogni richiesta autenticata.

4.3 Modello di autorizzazione. ProcessMind non dipende dagli authorizer nativi di API Gateway per le proprie API applicative principali. L'autorizzazione è applicata in wrapper condivisi degli handler Lambda che convalidano lo stato della sessione e l'ambito del tenant prima dell'esecuzione della logica aziendale. Le route pubbliche sono

esplicitamente inserite in una allowlist per flussi non autenticati, webhook, acquisizione di eventi e preflight CORS. Gli endpoint API esterni utilizzano handler di autenticazione dedicati. L'accesso ai Customer Data è limitato al contesto del tenant o dell'organizzazione autenticato.

4.4 Privilegio minimo. I sistemi interni seguono il principio del privilegio minimo. I ruoli IAM sono limitati alle risorse minime necessarie ove il framework consenta una limitazione precisa. Alcuni ruoli generati da SST/CDK utilizzano policy gestite o inline più ampie per i binding e il funzionamento in fase di esecuzione; tali casi vengono riesaminati, limitati alle risorse ove possibile e registrati come eccezioni esplicite.

4.5 Controlli degli accessi dei dipendenti. L'accesso dei dipendenti ai sistemi interni è gestito tramite Active Directory con SSO e MFA obbligatoria. Il controllo degli accessi basato sui ruoli (RBAC) garantisce che l'accesso ai Customer Data sia limitato al personale autorizzato secondo il principio della necessità di sapere. I diritti di accesso vengono riesaminati periodicamente.

---

5. Registrazione dei log, monitoraggio e audit

5.1 Registrazione centralizzata dei log. La registrazione degli accessi all'HTTP API e degli accessi WebSocket è abilitata con campi JSON strutturati e viene scritta nei log Amazon CloudWatch con una conservazione di una (1) settimana. Tali gruppi di log degli accessi sono crittografati con una chiave AWS KMS gestita dal cliente. I log applicativi sono centralizzati in gruppi di log Amazon CloudWatch crittografati con una chiave AWS KMS gestita dal cliente e conservati per dieci (10) anni. Anche i gruppi di log separati per audit e telemetria sono crittografati con una chiave AWS KMS gestita dal cliente e conservati per dieci (10) anni. Il gruppo di esportazione dei log del motore Aurora PostgreSQL è conservato per una (1) settimana.

5.2 Cosa viene registrato e cosa no. ProcessMind registra gli eventi di accesso all'HTTP API e WebSocket, inclusi ora della richiesta, identificativi

della richiesta, route o percorso, stato della risposta, latenza, indirizzo IP di origine e user agent. ProcessMind registra inoltre gli eventi di autenticazione, i percorsi di errore asincroni e l'attività applicativa di supporto Lambda nei gruppi di log CloudWatch centralizzati. I log di flusso VPC sono abilitati. Attualmente ProcessMind non abilita la registrazione standard degli accessi CloudFront sulle distribuzioni del sito web, della SPA frontend o delle risorse pubbliche.

5.3 Monitoraggio e avvisi. Gli allarmi e i dashboard CloudWatch monitorano lo stato del sistema, le dead-letter queue e gli errori rilevanti per la sicurezza. Gli errori di elaborazione asincrona vengono indirizzati a dead-letter queue crittografate (conservazione di quattordici (14) giorni; due (2) giorni per le code delle miniature e dell'indice di ricerca) e gli allarmi DLQ attivano notifiche SNS per l'analisi. Inoltre, ProcessMind utilizza Sentry per il monitoraggio degli errori frontend in tempo reale, il monitoraggio delle prestazioni e la riproduzione delle sessioni. Le riproduzioni delle sessioni vengono registrate solo per le sessioni in cui si verifica un errore e il testo, gli input dei moduli e i contenuti multimediali sono mascherati o bloccati nelle riproduzioni. I dati Sentry vengono acquisiti nell'UE (Francoforte) e sono limitati ai ProcessMind Usage Data (errori del browser, tracce delle prestazioni, metadati del dispositivo e registrazioni delle riproduzioni mascherate). Sentry è indicato nell'elenco dei sub-responsabili.

5.4 Protezione dei log. I log sono conservati in gruppi di log CloudWatch dedicati e soggetti a controllo degli accessi e sono crittografati a riposo. I log di produzione e sviluppo sono separati mediante confini di ambiente e di account.

---

6. Convalida automatizzata dei controlli e gestione delle vulnerabilità

6.1 Cosa fa ProcessMind. ProcessMind esegue `cdk-nag` nell'ambito del proprio flusso di sintesi e distribuzione dell'infrastruttura, utilizzando più pacchetti di regole del settore (inclusi AWS Solutions, NIST 800-53 e PCI

DSS). I report per stack vengono generati e riesaminati nell'ambito della gestione delle modifiche all'infrastruttura. I risultati vengono classificati come corretti, rischio accettato o miglioramento pianificato.

6.2 Gestione delle eccezioni. Le soppressioni vengono registrate in un registro centrale ove il framework lo consente, limitate agli stack interessati e richiedono una motivazione scritta; qualora uno stack contenga una soppressione inline, questa viene documentata insieme a tale stack. Quando un risultato viene risolto, la soppressione corrispondente viene aggiornata o rimossa. ProcessMind non considera la soppressione come un'esclusione generale dal riesame.

6.3 Cosa ProcessMind attualmente non fa. ProcessMind tiene traccia e riesamina le eccezioni sostanziali ai controlli dell'infrastruttura. Le principali sono:

- Le application Lambdas non sono collocate all'interno della VPC per impostazione predefinita; accedono ad Aurora tramite RDS Data API su TLS con autenticazione IAM e Secrets Manager
- la WebSocket API e le distribuzioni statiche non sono protette da AWS WAF (le connessioni WebSocket utilizzano token HMAC di breve durata; le restrizioni geografiche relative ai pagamenti sono applicate nel sistema di pagamento) e le distribuzioni statiche non dispongono della registrazione standard degli accessi CloudFront
- il ripristino dei database si basa sui backup automatici e sul ripristino point-in-time di Aurora, anziché su un piano AWS Backup separato o su Aurora Enhanced Monitoring
- non è prevista la replica S3 tra regioni né S3 Object Lock per i bucket modificabili
- alcune risorse di supporto gestite da AWS/CDK/SST utilizzano la crittografia gestita da AWS o policy IAM generate più ampie laddove il servizio non esponga un'alternativa controllabile dal cliente

Il registro completo delle soppressioni è mantenuto insieme al codice dell'infrastruttura ed è disponibile su richiesta. L'uso dei `cdk-nag` pacchetti di

regole costituisce una validazione dei controlli ingegneristici, non una certificazione esterna, un giudizio di audit o un'attestazione legale della conformità HIPAA, NIST o PCI DSS.

6.4 Gestione delle dipendenze. Le dipendenze software sono monitorate continuamente per individuare vulnerabilità note. Le vulnerabilità critiche e ad alta gravità vengono corrette con un obiettivo di sette (7) giorni. Le dipendenze vengono aggiornate secondo un ciclo regolare.

6.5 Ciclo di vita dello sviluppo software sicuro (SDLC). ProcessMind adotta un approccio di difesa in profondità allo sviluppo software. Ogni modifica alla produzione deve superare più livelli indipendenti di validazione automatizzata prima della distribuzione:

- **Analisi statica e sicurezza dei tipi:** La modalità strict di TypeScript e ESLint impongono la correttezza dei tipi, la sicurezza rispetto ai valori null e i pattern di codifica rilevanti per la sicurezza in fase di compilazione.
- **Revisione del codice assistita dall'AI:** L'analisi assistita dall'AI fornisce un'ulteriore prospettiva di revisione sulle pull request per identificare rischi per la sicurezza, errori logici e deviazioni dalle convenzioni, integrando i test automatizzati.
- **Test unitari e di integrazione:** una suite completa di test Vitest convalida la logica aziendale, i pattern di accesso ai dati, il comportamento delle API e la gestione degli errori rispetto a risorse AWS attive nell'ambiente di sviluppo.
- **Test end-to-end:** i test del browser basati su Playwright verificano i flussi di lavoro critici degli utenti, inclusi autenticazione, caricamento dei dati, modellazione dei processi, simulazione e isolamento multi-tenant.
- **Scansione della conformità dell'infrastruttura:** `cdk-nag` convalida l'infrastruttura come codice rispetto a molteplici framework di conformità a ogni modifica.
- **Scansione delle vulnerabilità delle dipendenze:** gli audit automatizzati delle dipendenze impediscono alle vulnerabilità

critiche e ad alta gravità note di raggiungere la produzione.

La revisione umana si concentra sull'architettura, sui confini di sicurezza e sulle decisioni a livello di progettazione, anziché sull'ispezione del codice riga per riga. Quando sono coinvolte modifiche strutturali, sensibili sotto il profilo della sicurezza o relative all'infrastruttura, è richiesta un'approvazione umana esplicita in aggiunta alla validazione automatizzata.

Tutti i livelli di validazione sono applicati tramite CI come gate obbligatori per il merge delle modifiche al branch principale. Le correzioni urgenti in produzione possono bypassare il gate CI, ma devono essere seguite da un'esecuzione completa della pipeline e da una revisione post-incidente entro ventiquattro (24) ore.

---

7. Backup e ripristino di emergenza

7.1 Backup automatici. Amazon Aurora esegue backup continui e automatici con un periodo di conservazione di sette (7) giorni. I backup sono crittografati utilizzando le stesse chiavi KMS gestite dal cliente dei database di origine.

7.2 Ripristino point-in-time. Aurora supporta il ripristino point-in-time a qualsiasi secondo all'interno del periodo di conservazione dei backup, consentendo un ripristino rapido in caso di corruzione dei dati o cancellazione accidentale.

7.3 Durabilità e versioning di S3. I caricamenti di file e gli artefatti operativi sono archiviati in Amazon S3, che offre una durabilità del 99.999999999% (11 nines). Il versioning è abilitato nel bucket dei caricamenti e nei bucket delle risorse per supportare il ripristino e i rollback. I bucket di distribuzione del sito web e del frontend contengono artefatti di build riproducibili e non sono trattati come un sistema di backup. ProcessMind attualmente non abilita la replica S3 tra regioni.

7.4 Continuità operativa. Le procedure di ripristino di emergenza sono documentate e testate periodicamente. Un riepilogo è disponibile nel documento Disaster Recovery, Business Continuity & Incident Response. L'architettura si basa sui servizi gestiti AWS all'interno della regione `eu-central-1`, che AWS gestisce attraverso più Availability Zones; il cluster Aurora attualmente esegue una singola istanza writer, pertanto il ripristino del database si basa sui backup automatici e sul ripristino point-in-time anziché su un'istanza standby nella regione. I backup Aurora, la durabilità S3, le code dead-letter e gli asset statici ricostruibili dall'origine fanno parte della strategia di ripristino.

---

8. Risposta agli incidenti

8.1 Notifica degli incidenti. In caso di Incidente di sicurezza (come definito nel DPA), ProcessMind informerà i clienti interessati senza indebito ritardo e, ove possibile, entro settantadue (72) ore dal momento in cui viene a conoscenza dell'incidente.

8.2 Gestione degli incidenti. ProcessMind mantiene procedure documentate di risposta agli incidenti che riguardano identificazione, contenimento, eradicazione, ripristino e revisione post-incidente. Un riepilogo è disponibile nel documento Disaster Recovery, Business Continuity & Incident Response. Le lezioni apprese dagli incidenti sono integrate nei controlli e nei processi di sicurezza.

8.3 Comunicazione. Le notifiche degli incidenti includono la natura e la portata dell'incidente, le categorie di dati interessate, le misure adottate per contenere l'incidente e le azioni raccomandate al cliente.

---

9. Misure organizzative

9.1. Gestione della sicurezza delle informazioni. ProcessMind mantiene un sistema di gestione della sicurezza delle informazioni allineato ai principi della ISO 27001. ProcessMind ha selezionato il proprio percorso di

certificazione per la certificazione ISO 27001 e l'attestazione SOC 2 Type II; il processo formale di certificazione non è ancora iniziato.

9.2 Consapevolezza della sicurezza. Tutto il personale con accesso ai Dati del Cliente riceve una formazione sulla consapevolezza della sicurezza. Le migliori pratiche di sicurezza sono integrate nell'onboarding, nei flussi di sviluppo e nelle procedure operative.

9.3 Gestione dei fornitori e dei Sub-processors. I Sub-processors sono contrattualmente vincolati a standard di protezione dei dati equivalenti a quelli descritti nel presente documento. ProcessMind mantiene un elenco pubblico dei Sub-processors e fornisce un preavviso di almeno trenta (30) giorni prima di incaricare un nuovo Sub-processor. I Sub-processors sono sottoposti annualmente a revisione ai fini della conformità.

9.4 Riservatezza. Tutto il personale autorizzato a trattare i Dati del Cliente è vincolato da obblighi scritti di riservatezza.

---

10. Conformità e certificazioni

Framework / Standard	Stato
GDPR (Regolamento generale sulla protezione dei dati dell'UE)	Conforme
Residenza dei dati nell'UE (Francoforte, Germania)	Applicata
Certificazioni dell'infrastruttura AWS (ISO 27001, SOC 2, PCI DSS)	Ereditate tramite AWS
ISO 27001 (ProcessMind)	Pianificata — percorso di certificazione selezionato; processo formale non ancora iniziato

Framework / Standard	Stato
SOC 2 Type II (ProcessMind)	Pianificata — percorso di certificazione selezionato; processo formale non ancora iniziato
Validazione automatizzata dei controlli dell'infrastruttura (`cdk-nag` tra AWS Solutions, HIPAA Security, NIST 800-53 R4/R5, PCI DSS 3.2.1, Serverless)	Implementata come validazione dei controlli ingegneristici, non come certificazione
Clausole contrattuali standard (SCC) per i trasferimenti internazionali	Implementate (vedere DPA)
Addendum sul trattamento dei dati (DPA)	Disponibile pubblicamente

L'uso dei `cdk-nag` pacchetti di regole non significa che ProcessMind sia formalmente certificata o sottoposta ad audit indipendente rispetto a HIPAA, NIST o PCI DSS. Tali pacchetti di regole sono utilizzati come misure di salvaguardia ingegneristiche per convalidare la progettazione dell'infrastruttura e tracciare esplicitamente le lacune.

Per domande relative alla sicurezza, alla conformità o per richiedere documentazione, come rapporti di audit o questionari di sicurezza compilati, contatti **support@processmind.com**.