Beveiligingsmaatregelen van ProcessMind

Ingangsdatum: 14 september 2026

Dit document beschrijft de technische en organisatorische maatregelen ("TOM's") die ProcessMind B.V. handhaaft om de vertrouwelijkheid, integriteit en beschikbaarheid van Klantgegevens te beschermen. ProcessMind hanteert een defense-in-depth-benadering waarbij meerdere onafhankelijke beveiligingslagen Klantgegevens op elk niveau beschermen — van netwerk en infrastructuur tot identiteit, autorisatie, gegevensisolatie, versleuteling, monitoring en softwareontwikkeling. Deze maatregelen vormen een aanvulling op het Addendum gegevensverwerking, het Privacybeleid en het SaaS-hostingbeleid. ProcessMind beoordeelt en actualiseert deze maatregelen ten minste jaarlijks.

Klantgegevens worden nooit verkocht aan, gedeeld met of gebruikt door derden voor hun eigen doeleinden.

---

1. Infrastructuurbeveiliging

1.1 Cloudplatform. ProcessMind wordt uitsluitend gehost op Amazon Web Services (AWS) in de EU (Frankfurt, Duitsland, `eu-central-1`). AWS beschikt over certificeringen voor ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3 en PCI DSS. Zie AWS Compliance Programs voor een volledige lijst.

1.2 Serverloze architectuur. De applicatielogica van ProcessMind draait op AWS Lambda en door AWS beheerde diensten. ProcessMind beheert geen langdurig actieve applicatieservers die door klanten worden beheerd, waardoor een groot deel van het patchen van besturingssystemen en het hardenen van servers vervalt.

1.3 Netwerkgrenzen. ProcessMind beheert een AWS VPC voor database- en netwerkcontroles. Aurora PostgreSQL draait in private subnetten zonder internet-egress, is niet publiek toegankelijk en VPC-flowlogs zijn

ingeschakeld. ProcessMind plaatst applicatie-Lambda-functies standaard niet binnen de VPC. Lambdas bereiken Aurora via de AWS RDS Data API over TLS met authenticatie via IAM en Secrets Manager.

1.4 Content delivery en edgecontroles. De klantgerichte website, frontend-SPA en het verkeer van publieke bronnen worden geleverd via Amazon CloudFront. Alle CloudFront-distributies dwingen een minimaal TLS-beleid van TLS 1.2 (2021) af. De distributies van de website en frontend-SPA voegen ook beveiligingsresponsheaders toe, waaronder HTTP Strict Transport Security (HSTS), Content Security Policy (CSP), `frame-ancestors 'none'`, `X-Frame-Options: DENY`, `X-Content-Type-Options`, referrer policy en permissions policy. De distributie van publieke bronnen gebruikt CloudFront Origin Access Control om de origin-bucket privé te houden. Klantgericht API-verkeer wordt afzonderlijk afgehandeld via Amazon API Gateway: HTTPS-aanvraag-/responsverkeer wordt geleverd via een HTTP API op een speciaal API-subdomein en realtime clientverbindingen worden geleverd via een afzonderlijke API Gateway WebSocket API op een speciaal WebSocket-subdomein.

1.5 Scheiding van omgevingen. Productie- en ontwikkelomgevingen gebruiken afzonderlijke AWS-accounts, afzonderlijke databases en afzonderlijke infrastructuurstacks. Inloggegevens van ontwikkelaars bieden geen toegang tot Klantgegevens in productie.

---

2. Gegevensversleuteling

2.1 Versleuteling tijdens overdracht. Alle gegevens die tussen clients en ProcessMind-diensten worden verzonden, worden versleuteld met TLS 1.2 of hoger. Klantgerichte endpoints zijn beschikbaar via HTTPS. S3-buckets, SNS-topics en SQS-queues die rechtstreeks door ProcessMind zijn aangemaakt, dwingen uitsluitend SSL-toegang af. Databasetoegang via de RDS Data API en andere AWS-serviceaanroepen gebruikt HTTPS/TLS.

2.2 Versleuteling in rust. Aurora PostgreSQL is in rust versleuteld met door de klant beheerde AWS KMS-sleutels met automatische sleutelrotatie. S3-

buckets voor klantgegevens en operationele gegevens die rechtstreeks door ProcessMind zijn aangemaakt, waaronder buckets voor uploads, bronnen en toegangslogs, gebruiken door de klant beheerde KMS-sleutels. CloudWatch-loggroepen, SNS-topics en SQS-queues die rechtstreeks door ProcessMind zijn aangemaakt, gebruiken eveneens door de klant beheerde KMS-sleutels. Door SST beheerde website- en frontend-origin-buckets gebruiken door AWS beheerde server-side encryptie van S3 (SSE-S3 / AES-256) in plaats van door de klant beheerde KMS-sleutels.

2.3 Sleutelbeheer en secrets. Databasaversleutelingssleutels worden centraal beheerd via AWS KMS en toegang tot sleutels wordt geregeld door IAM-beleidsregels volgens het beginsel van minimale bevoegdheden. Databasegegevens worden opgeslagen in AWS Secrets Manager. Het Aurora-mastersecret en het beperkte secret voor applicatiegebruikers worden automatisch elke dertig (30) dagen geroteerd. Productiesleutels en secrets worden nooit in broncode opgeslagen; uitsluitend voor ontwikkeling bestemde inloggegevens zijn gescheiden van productie. Sommige ondersteunende bronnen die door AWS/CDK/SST worden beheerd, blijven door AWS beheerde versleuteling gebruiken wanneer de dienst of het framework geen configuratie voor door de klant beheerde sleutels beschikbaar stelt.

---

3. Gegevensisolatie en verblijfplaats

3.1 Tenantisolatie. Elke klanttenant krijgt een toegewezen, geïsoleerde database-instantie. Klantgegevens worden op databaseniveau nooit vermengd met gegevens van andere klanten. Gedeelde metadata (bijvoorbeeld accountgegevens, facturering en toewijzingen van gebruikers aan tenants) wordt opgeslagen in een afzonderlijke multitenant-database met strikte toegangscontroles. Gedeelde tabellen met tenant- en organisatiebereik worden bovendien beschermd door PostgreSQL-beleid voor beveiliging op rijniveau (RLS), afgedwongen via databasecontext die aan het verzoek is gekoppeld.

3.2 Verblijfplaats van gegevens. Alle Klantgegevens, waaronder databases, bestandsuploads, back-ups en queryresultaten, worden uitsluitend opgeslagen in de EU (Frankfurt, Duitsland). Wanneer voor een specifieke verwerkingsactiviteit een subverwerker buiten de EER wordt ingeschakeld (bijvoorbeeld voor verwerking door een AI-model of betalingsverwerking), valt de doorgifte onder een passend doorgiftemechanisme zoals beschreven in het Addendum gegevensverwerking, en worden de subverwerker en de verwerkingslocatie vermeld in de Lijst van subverwerkers.

3.3 Bewaring en verwijdering van gegevens. Termijnen voor bewaring en verwijdering zijn vastgelegd in artikel 6 van het Addendum gegevensverwerking. Klanten kunnen hun gegevens op elk moment via de applicatie verwijderen of contact opnemen met ProcessMind. Back-upkopieën worden verwijderd wanneer de toepasselijke bewaartermijnen voor back-ups verstrijken (artikel 7.1).

---

4. Identiteits- en toegangsbeheer

4.1 Authenticatie. ProcessMind ondersteunt Single Sign-On (SSO) via Microsoft Entra ID (Azure AD), Google OAuth 2.0/OIDC en LinkedIn OAuth 2.0/OIDC. ProcessMind treedt op als relying party en slaat geen gebruikerswachtwoorden op. Multi-factor-authenticatie wordt afgedwongen door de identiteitsprovider — bijvoorbeeld: wanneer een organisatie Microsoft Entra ID (Azure AD) koppelt, zijn de eigen MFA- en toegangsbeleidsregels van die organisatie van toepassing.

4.2 Sessiebeheer. Browsersessies gebruiken ondertekende JSON Web Tokens (JWT) die via beveiligde, HttpOnly-cookies worden verzonden met SameSite- en Secure-flags. Tokensignaturen worden bij elk geauthenticeerd verzoek gevalideerd.

4.3 Autorisatiemodel. ProcessMind is voor zijn kern-API's niet afhankelijk van native authorizers van API Gateway. Autorisatie wordt afgedwongen in gedeelde Lambda-handlerwrappers die de sessiestatus en tenantscope

valideren voordat bedrijfslogica wordt uitgevoerd. Publieke routes zijn expliciet op een allowlist geplaatst voor niet-geauthenticeerde flows, webhooks, eventinname en CORS-preflight. Externe API-endpoints gebruiken speciale authenticatiehandlers. Toegang tot Klantgegevens is beperkt tot de geauthenticeerde tenant- of organisatiecontext.

4.4 Minimale bevoegdheden. Interne systemen volgen het beginsel van minimale bevoegdheden. IAM-rollen worden beperkt tot de minimaal vereiste bronnen wanneer het framework een nauwkeurige beperking mogelijk maakt. Sommige door SST/CDK gegenereerde rollen gebruiken bredere beheerde of inline-beleidsregels voor bindings en runtimewerking; deze gevallen worden beoordeeld, waar mogelijk beperkt tot specifieke bronnen en als expliciete uitzonderingen bijgehouden.

4.5 Toegangscontroles voor werknemers. Toegang van werknemers tot interne systemen wordt beheerd via Active Directory met SSO en verplichte MFA. Op rollen gebaseerd toegangsbeheer (RBAC) zorgt ervoor dat toegang tot Klantgegevens wordt beperkt tot geautoriseerd personeel op basis van need-to-know. Toegangsrechten worden periodiek beoordeeld.

---

5. Logging, monitoring en audit

5.1 Gecentraliseerde logging. HTTP API-toegangslogging en WebSocket-toegangslogging zijn ingeschakeld met gestructureerde JSON-velden en worden met een bewaartermijn van één (1) week naar Amazon CloudWatch Logs geschreven. Deze toegangsloggroepen zijn versleuteld met een door de klant beheerde AWS KMS-sleutel. Applicatielogs worden gecentraliseerd in Amazon CloudWatch-loggroepen die zijn versleuteld met een door de klant beheerde AWS KMS-sleutel en tien (10) jaar worden bewaard. Afzonderlijke audit- en telemetrieloggroepen zijn eveneens versleuteld met een door de klant beheerde AWS KMS-sleutel en worden tien (10) jaar bewaard. De exportgroep voor Aurora PostgreSQL-enginelogs wordt één (1) week bewaard.

5.2 Wat wel en niet wordt gelogd. ProcessMind logt HTTP API- en WebSocket-toegangsgebeurtenissen, waaronder aanvraagtijd, aanvraag-ID's, route of pad, responsstatus, latentie, bron-IP en user-agent. ProcessMind logt ook authenticatiegebeurtenissen, asynchrone foutpaden en ondersteunende Lambda-applicatieactiviteit naar gecentraliseerde CloudWatch-loggroepen. VPC-flowlogs zijn ingeschakeld. ProcessMind schakelt momenteel geen standaard CloudFront-toegangslogging in voor de distributies van de website, frontend-SPA of publieke bronnen.

5.3 Monitoring en waarschuwingen. CloudWatch-alarmen en dashboards monitoren systeemstatus, dead-letter-queues en beveiligingsrelevante fouten. Fouten in asynchrone verwerking worden doorgestuurd naar versleutelde dead-letter-queues (bewaartermijn van veertien (14) dagen; twee (2) dagen voor de thumbnail- en zoekindex-queues), en DLQ-alarmen activeren SNS-meldingen voor onderzoek. Daarnaast gebruikt ProcessMind Sentry voor realtime frontend-fouttracking, prestatiemonitoring en sessiereplay. Sessiereplays worden alleen opgenomen voor sessies waarin een fout optreedt, en tekst, formulierinvoer en media worden in replays gemaskeerd of geblokkeerd. Sentry-gegevens worden in de EU (Frankfurt) verwerkt en zijn beperkt tot ProcessMind Usage Data (browserfouten, performancetraces, apparaatgegevens en gemaskeerde replayopnamen). Sentry staat vermeld in de lijst van subverwerkers.

5.4 Logbeveiliging. Logs worden opgeslagen in speciale, toegangsgecontroleerde CloudWatch-loggroepen en in rust versleuteld. Productie- en ontwikkellogs worden gescheiden door omgevings- en accountgrenzen.

---

6. Geautomatiseerde validatie van controles en kwetsbaarheidsbeheer

6.1 Wat ProcessMind doet. ProcessMind voert `cdk-nag` uit als onderdeel van zijn workflow voor infrastructuursynthese en implementatie, met gebruik van meerdere regelpakketten uit de sector (waaronder AWS Solutions, NIST

800-53 en PCI DSS). Per stack worden rapporten gegenereerd en beoordeeld als onderdeel van het beheer van infrastructuurwijzigingen. Bevindingen worden getrieerd als opgelost, aanvaard risico of geplande verbetering.

6.2 Hoe uitzonderingen worden beheerd. Suppressions worden, waar het framework dit toestaat, vastgelegd in een centraal register, beperkt tot de betrokken stacks en vereisen een schriftelijke motivering; wanneer een stack een inline suppression bevat, wordt deze naast die stack gedocumenteerd. Wanneer een bevinding is verholpen, wordt de bijbehorende suppression bijgewerkt of verwijderd. ProcessMind beschouwt suppression niet als een algemene uitsluiting van beoordeling.

6.3 Wat ProcessMind momenteel niet doet. ProcessMind houdt wezenlijke uitzonderingen op infrastructuurcontroles bij en beoordeelt deze. De belangrijkste zijn:

- application Lambdas worden standaard niet binnen de VPC geplaatst; ze bereiken Aurora via de RDS Data API over TLS met IAM- en Secrets Manager-authenticatie
- de WebSocket API en statische distributies worden niet door AWS WAF beschermd (WebSocket-verbindingen gebruiken kortlevende HMAC-tokens; geografische beperkingen voor betalingen worden in het betalingssysteem afgedwongen), en statische distributies hebben geen standaardtoegangslogboekregistratie van CloudFront
- databaseherstel is gebaseerd op geautomatiseerde back-ups en point-in-time recovery van Aurora, in plaats van een afzonderlijk AWS Backup-plan of Aurora Enhanced Monitoring
- er is geen replicatie van S3 tussen regio's of S3 Object Lock voor veranderlijke buckets
- sommige ondersteunende bronnen die door AWS/CDK/SST worden beheerd, gebruiken door AWS beheerde versleuteling of bredere gegenereerde IAM-beleidsregels wanneer de service geen door de klant beheerd alternatief biedt

Het volledige register van onderdrukkingen wordt samen met de infrastructuurcode bijgehouden en is op verzoek beschikbaar. Het gebruik van `cdk-nag` rule packs is een technische controlevalidatie en geen externe certificering, auditopinie of juridische verklaring van naleving van HIPAA, NIST of PCI DSS.

6.4 Beheer van afhankelijkheden. Softwareafhankelijkheden worden voortdurend gecontroleerd op bekende kwetsbaarheden. Kritieke kwetsbaarheden en kwetsbaarheden met een hoge ernst worden gestopt met als doel dit binnen zeven (7) dagen te doen. Afhankelijkheden worden volgens een regelmatige cyclus bijgewerkt.

6.5 Veilige softwareontwikkelingslevenscyclus (SDLC). ProcessMind volgt bij softwareontwikkeling een defense-in-depth-benadering. Elke wijziging in productie moet vóór implementatie meerdere onafhankelijke geautomatiseerde validatielagen doorlopen:

- **Statische analyse en typeveiligheid:** TypeScript strict mode en ESLint handhaven typecorrectheid, null-veiligheid en beveiligingsrelevante codeerpatronen tijdens het compileren.
- **AI-ondersteunde codebeoordeling:** AI-ondersteunde analyse biedt een aanvullend beoordelingsperspectief op pull requests om beveiligingsrisico's, logische fouten en afwijkingen van conventies te identificeren, als aanvulling op geautomatiseerd testen.
- **Unit- en integratietests:** een uitgebreide Vitest-testsuite valideert bedrijfslogica, patronen voor gegevenstoegang, API-gedrag en foutafhandeling aan de hand van live AWS-bronnen in de ontwikkelomgeving.
- **End-to-endtests:** browsertests op basis van Playwright verifiëren kritieke gebruikersworkflows, waaronder authenticatie, het uploaden van gegevens, procesmodellering, simulatie en isolatie tussen tenants.
- **Scannen op naleving van infrastructuur:** `cdk-nag` valideert infrastructuur als code bij elke wijziging aan de hand van meerdere nalevingskaders.

- **Scannen op kwetsbaarheden in afhankelijkheden:** geautomatiseerde audits van afhankelijkheden verhinderen dat bekende kritieke kwetsbaarheden en kwetsbaarheden met een hoge ernst productie bereiken.

Menselijke beoordeling is gericht op architectuur, beveiligingsgrenzen en beslissingen op ontwerpniveau, en niet op inspectie van code op regelniveau. Wanneer structurele, beveiligingsgevoelige of infrastructuurwijzigingen aan de orde zijn, is naast geautomatiseerde validatie uitdrukkelijke goedkeuring door een persoon vereist.

Alle validatielagen worden via CI afgedwongen als verplichte samenvoegingspoorten voor wijzigingen in de hoofdbranch. Noodreparaties in productie mogen de CI-poort omzeilen, maar moeten binnen vierentwintig (24) uur worden gevolgd door een volledige pipeline-uitvoering en een evaluatie na het incident.

---

7. Back-up en herstel na calamiteiten

7.1 Geautomatiseerde back-ups. Amazon Aurora voert continue, geautomatiseerde back-ups uit met een bewaartermijn van zeven (7) dagen. Back-ups worden versleuteld met dezelfde door de klant beheerde KMS-sleutels als de brondatabases.

7.2 Point-in-time recovery. Aurora ondersteunt point-in-time recovery naar elke seconde binnen het back-upvenster, waardoor snel herstel mogelijk is in geval van beschadiging van gegevens of onbedoelde verwijdering.

7.3 S3-duurzaamheid en versiebeheer. Bestandsuploads en operationele artefacten worden opgeslagen in Amazon S3, dat een duurzaamheid van 99,999999999% (11 negens) biedt. Versiebeheer is ingeschakeld voor de uploadbucket en bronbuckets ter ondersteuning van herstel en terugdraaien. Website- en frontend-implementatiebuckets bevatten reproduceerbare buildartefacten en worden niet als back-upsysteem

behandeld. ProcessMind schakelt momenteel geen S3-replicatie tussen regio's in.

7.4 Bedrijfscontinuïteit. Procedures voor herstel na calamiteiten zijn gedocumenteerd en worden periodiek getest. Een samenvatting is beschikbaar in het document Disaster Recovery, Business Continuity & Incident Response. De architectuur is gebaseerd op door AWS beheerde services binnen de `eu-central-1`-regio, die AWS over meerdere Availability Zones exploiteert; het Aurora-cluster draait momenteel met één writer-instantie, waardoor databaseherstel afhankelijk is van geautomatiseerde back-ups en point-in-time recovery in plaats van een standby binnen de regio. Aurora-back-ups, S3-duurzaamheid, dead-letter queues en statische assets die vanuit de bron worden herbouwd, maken deel uit van de herstelstrategie.

---

8. Incidentrespons

8.1 Melding van incidenten. In geval van een Beveiligingsincident (zoals gedefinieerd in de DPA) stelt ProcessMind getroffen klanten zonder onnodige vertraging op de hoogte en, waar haalbaar, binnen tweeënzeventig (72) uur nadat ProcessMind kennis heeft gekregen van het incident.

8.2 Afhandeling van incidenten. ProcessMind onderhoudt gedocumenteerde incidentresponsprocedures voor identificatie, indamming, uitroeiing, herstel en evaluatie na het incident. Een samenvatting is beschikbaar in het document Disaster Recovery, Business Continuity & Incident Response. Geleerde lessen uit incidenten worden verwerkt in beveiligingscontroles en -processen.

8.3 Communicatie. Meldingen van incidenten bevatten de aard en omvang van het incident, de getroffen gegevenscategorieën, de maatregelen die zijn genomen om het incident in te dammen en aanbevolen acties voor de klant.

---

9. Organisatorische maatregelen

9.1. Beheer van informatiebeveiliging. ProcessMind onderhoudt een managementsysteem voor informatiebeveiliging dat is afgestemd op de beginselen van ISO 27001. ProcessMind heeft zijn certificeringstraject voor ISO 27001-certificering en SOC 2 Type II-attestatie geselecteerd; het formele certificeringsproces is nog niet gestart.

9.2 Bewustzijn van beveiliging. Al het personeel met toegang tot Klantgegevens ontvangt training in beveiligingsbewustzijn. Best practices op het gebied van beveiliging zijn ingebed in onboarding, ontwikkelingsworkflows en operationele procedures.

9.3 Beheer van leveranciers en subverwerkers. Subverwerkers zijn contractueel gebonden aan normen voor gegevensbescherming die gelijkwaardig zijn aan de in dit document beschreven normen. ProcessMind onderhoudt een openbare lijst van subverwerkers en geeft ten minste dertig (30) dagen voorafgaand aan de inschakeling van een nieuwe subverwerker kennis daarvan. Subverwerkers worden jaarlijks op naleving beoordeeld.

9.4 Vertrouwelijkheid. Al het personeel dat bevoegd is om Klantgegevens te verwerken, is gebonden aan schriftelijke geheimhoudingsverplichtingen.

---

10. Naleving en certificeringen

Kader / norm	Status
AVG (Algemene verordening gegevensbescherming van de EU)	Conform
EU-gegevensresidentie (Frankfurt, Duitsland)	Afgedwongen
AWS-infrastructuurcertificeringen (ISO 27001, SOC 2, PCI DSS)	Overgenomen via AWS

Kader / norm	Status
ISO 27001 (ProcessMind)	Gepland — certificeringstraject geselecteerd; formeel proces nog niet gestart
SOC 2 Type II (ProcessMind)	Gepland — certificeringstraject geselecteerd; formeel proces nog niet gestart
Geautomatiseerde validatie van infrastructuurcontroles (`cdk-nag` voor AWS Solutions, HIPAA Security, NIST 800-53 R4/R5, PCI DSS 3.2.1, Serverless)	Geïmplementeerd als technische controlevalidatie, niet als certificering
Standard Contractual Clauses (SCC's) voor internationale doorgiften	Geïmplementeerd (zie DPA)
Data Processing Addendum (DPA)	Openbaar beschikbaar

Het gebruik van `cdk-nag` rule packs betekent niet dat ProcessMind formeel is gecertificeerd of onafhankelijk is geaudit aan de hand van HIPAA, NIST of PCI DSS. Deze rule packs worden gebruikt als technische waarborgen om het infrastructuurontwerp te valideren en tekortkomingen expliciet bij te houden.

Neem voor vragen over beveiliging of naleving, of om documentatie zoals auditrapporten of ingevulde beveiligingsvragenlijsten op te vragen, contact op met **support@processmind.com**.