Sicherheitsmaßnahmen von ProcessMind

Gültig ab: 14. September 2026

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen („TOMs“), die ProcessMind B.V. zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Kundendaten aufrechterhält. ProcessMind verfolgt einen Defense-in-Depth-Ansatz, bei dem mehrere unabhängige Sicherheitsebenen Kundendaten auf jeder Ebene schützen — vom Netzwerk und der Infrastruktur über Identität, Autorisierung, Datenisolierung, Verschlüsselung und Überwachung bis hin zur Softwareentwicklung. Diese Maßnahmen ergänzen den Auftragsverarbeitungszusatz, die Datenschutzrichtlinie und die SaaS-Hosting-Richtlinie. ProcessMind überprüft und aktualisiert diese Maßnahmen mindestens jährlich.

Kundendaten werden niemals an Dritte verkauft, mit Dritten geteilt oder von Dritten für deren eigene Zwecke verwendet.

---

1. Infrastruktursicherheit

1.1 Cloud-Plattform. ProcessMind wird ausschließlich auf Amazon Web Services (AWS) in der EU (Frankfurt, Deutschland, `eu-central-1`) gehostet. AWS verfügt über Zertifizierungen nach ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3 und PCI DSS. Eine vollständige Liste finden Sie unter AWS Compliance Programs.

1.2 Serverlose Architektur. Die Anwendungslogik von ProcessMind läuft auf AWS Lambda und von AWS verwalteten Services. ProcessMind betreibt keine von Kunden verwalteten, langlebigen Anwendungsserver, wodurch ein großer Teil der Arbeiten zur Betriebssystem-Patchverwaltung und Serverhärtung entfällt.

1.3 Netzwerkgrenzen. ProcessMind unterhält eine AWS VPC für Datenbank- und Netzwerkkontrollen. Aurora PostgreSQL läuft in privaten Subnetzen ohne Internet-Egress, ist nicht öffentlich zugänglich, und VPC-Flow-Logs

sind aktiviert. ProcessMind platziert Anwendungs-Lambda-Funktionen standardmäßig nicht innerhalb der VPC. Lambdas greifen über die AWS RDS Data API über TLS unter Verwendung der Authentifizierung durch IAM und Secrets Manager auf Aurora zu.

1.4 Content Delivery und Edge-Kontrollen. Die kundenorientierte Website, die Frontend-SPA und der Datenverkehr öffentlicher Ressourcen werden über Amazon CloudFront bereitgestellt. Alle CloudFront-Distributionen erzwingen eine TLS-Mindestversion von TLS 1.2 (2021). Die Distributionen der Website und der Frontend-SPA fügen außerdem Sicherheits-Response-Header hinzu, einschließlich HTTP Strict Transport Security (HSTS), Content Security Policy (CSP), `frame-ancestors 'none'`, `X-Frame-Options: DENY`, `X-Content-Type-Options`, Referrer-Policy und Permissions-Policy. Die Distribution für öffentliche Ressourcen verwendet CloudFront Origin Access Control, um den Origin-Bucket privat zu halten. Der kundenorientierte API-Datenverkehr wird separat über Amazon API Gateway verarbeitet: HTTPS-Anfrage-/Antwortverkehr wird über eine HTTP API auf einer dedizierten API-Subdomain bereitgestellt, und Echtzeit-Clientverbindungen werden über eine separate API-Gateway-WebSocket-API auf einer dedizierten WebSocket-Subdomain bereitgestellt.

1.5 Trennung der Umgebungen. Produktions- und Entwicklungsumgebungen verwenden separate AWS-Konten, separate Datenbanken und separate Infrastruktur-Stacks. Entwicklerzugangsdaten ermöglichen keinen Zugriff auf Kundendaten der Produktionsumgebung.

---

2. Datenverschlüsselung

2.1 Verschlüsselung bei der Übertragung. Alle zwischen Clients und ProcessMind-Services übertragenen Daten werden mit TLS 1.2 oder höher verschlüsselt. Kundenorientierte Endpunkte werden über HTTPS bereitgestellt. Von ProcessMind direkt erstellte S3-Buckets, SNS-Themen und SQS-Warteschlangen erzwingen den ausschließlichen Zugriff über SSL.

Der Datenbankzugriff über die RDS Data API und andere AWS-Serviceaufrufe erfolgt über HTTPS/TLS.

2.2 Verschlüsselung im Ruhezustand. Aurora PostgreSQL wird im Ruhezustand unter Verwendung von kundenverwalteten AWS-KMS-Schlüsseln mit automatischer Schlüsselrotation verschlüsselt. Von ProcessMind direkt erstellte S3-Buckets für Kundendaten und den Betrieb, einschließlich Upload-, Ressourcen- und Zugriffsprotokoll-Buckets, verwenden kundenverwaltete KMS-Schlüssel. Von ProcessMind direkt erstellte CloudWatch-Loggruppen, SNS-Themen und SQS-Warteschlangen verwenden ebenfalls kundenverwaltete KMS-Schlüssel. Von SST verwaltete Website- und Frontend-Origin-Buckets verwenden die von AWS verwaltete serverseitige S3-Verschlüsselung (SSE-S3 / AES-256) anstelle kundenverwalteter KMS-Schlüssel.

2.3 Schlüsselverwaltung und Secrets.
Datenbankverschlüsselungsschlüssel werden zentral über AWS KMS verwaltet, und der Schlüsselzugriff wird durch IAM-Richtlinien nach dem Prinzip der geringsten Berechtigung geregelt. Datenbankzugangsdaten werden in AWS Secrets Manager gespeichert. Das Aurora-Master-Secret und das eingeschränkte Secret des Anwendungsbenutzers werden automatisch alle dreißig (30) Tage rotiert. Produktionsschlüssel und Secrets werden niemals im Quellcode gespeichert; ausschließlich für die Entwicklung bestimmte Zugangsdaten sind von der Produktionsumgebung isoliert. Einige von AWS/CDK/SST verwaltete unterstützende Ressourcen verwenden weiterhin die von AWS verwaltete Verschlüsselung, wenn der Service oder das Framework keine Konfiguration kundenverwalteter Schlüssel ermöglicht.

---

3. Datenisolierung und Datenresidenz

3.1 Mandantenisolierung. Jeder Kundenmandant erhält eine dedizierte, isolierte Datenbankinstanz. Kundendaten werden auf Datenbankebene niemals mit den Daten anderer Kunden vermischt. Gemeinsame

Metadaten (z. B. Kontodaten, Abrechnung, Zuordnungen von Benutzern zu Mandanten) werden in einer separaten mandantenfähigen Datenbank mit strengen Zugriffskontrollen gespeichert. Gemeinsame Tabellen mit Mandanten- und Organisationsbezug werden zusätzlich durch PostgreSQL-Richtlinien zur Sicherheit auf Zeilenebene (RLS) geschützt, die über einen anfragebezogenen Datenbankkontext durchgesetzt werden.

3.2 Datenresidenz. Alle Kundendaten, einschließlich Datenbanken, Datei-Uploads, Backups und Abfrageergebnisse, werden ausschließlich in der EU (Frankfurt, Deutschland) gespeichert. Wenn für eine bestimmte Verarbeitungstätigkeit ein außerhalb des EWR ansässiger Unterauftragsverarbeiter eingesetzt wird (beispielsweise für die Verarbeitung von KI-Modellen oder Zahlungen), wird die Übermittlung durch einen geeigneten Übermittlungsmechanismus abgedeckt, wie im Auftragsverarbeitungszusatz beschrieben; der Unterauftragsverarbeiter und sein Verarbeitungsstandort sind in der Liste der Unterauftragsverarbeiter aufgeführt.

3.3 Aufbewahrung und Löschung von Daten. Fristen für die Aufbewahrung und Löschung sind in Abschnitt 6 des Auftragsverarbeitungszusatzes festgelegt. Kunden können ihre Daten jederzeit über die Anwendung oder durch Kontaktaufnahme mit ProcessMind löschen. Sicherungskopien werden entfernt, sobald die jeweils geltenden Aufbewahrungsfristen für Backups ablaufen (Abschnitt 7.1).

---

4. Identitäts- und Zugriffsverwaltung

4.1 Authentifizierung. ProcessMind unterstützt Single Sign-On (SSO) über Microsoft Entra ID (Azure AD), Google OAuth 2.0/OIDC und LinkedIn OAuth 2.0/OIDC. ProcessMind fungiert als vertrauende Partei und speichert keine Benutzerpasswörter. Die Multi-Faktor-Authentifizierung wird vom Identitätsanbieter durchgesetzt — wenn eine Organisation beispielsweise Microsoft Entra ID (Azure AD) verbindet, gelten die eigenen MFA- und Zugriffsrichtlinien dieser Organisation.

4.2 Sitzungsverwaltung. Browsersitzungen verwenden signierte JSON Web Tokens (JWT), die über sichere HttpOnly-Cookies mit SameSite- und Secure-Flags übertragen werden. Die Tokensignaturen werden bei jeder authentifizierten Anfrage validiert.

4.3 Autorisierungsmodell. ProcessMind ist für seine zentralen Anwendungs-APIs nicht auf native Authorizer von API Gateway angewiesen. Die Autorisierung wird in gemeinsam genutzten Lambda-Handler-Wrappern durchgesetzt, die den Sitzungsstatus und den Mandantenbereich validieren, bevor die Geschäftslogik ausgeführt wird. Öffentliche Routen sind für nicht authentifizierte Abläufe, Webhooks, Ereigniserfassung und CORS-Preflight ausdrücklich als zulässig aufgeführt. Externe API-Endpunkte verwenden dedizierte Authentifizierungs-Handler. Der Zugriff auf Kundendaten ist auf den Kontext des authentifizierten Mandanten oder der authentifizierten Organisation beschränkt.

4.4 Geringste Berechtigung. Interne Systeme folgen dem Prinzip der geringsten Berechtigung. IAM-Rollen sind auf die mindestens erforderlichen Ressourcen beschränkt, soweit das Framework eine präzise Beschränkung ermöglicht. Einige von SST/CDK generierte Rollen verwenden für Bindings und den Laufzeitbetrieb umfassendere verwaltete oder Inline-Richtlinien; diese Fälle werden überprüft, soweit möglich auf Ressourcen beschränkt und als ausdrückliche Ausnahmen nachverfolgt.

4.5 Zugriffskontrollen für Mitarbeiter. Der Zugriff von Mitarbeitern auf interne Systeme wird über Active Directory mit SSO und verpflichtender MFA verwaltet. Die rollenbasierte Zugriffskontrolle (RBAC) stellt sicher, dass der Zugriff auf Kundendaten auf autorisiertes Personal nach dem Need-to-know-Prinzip beschränkt ist. Zugriffsrechte werden regelmäßig überprüft.

---

5. Protokollierung, Überwachung und Audit

5.1 Zentralisierte Protokollierung. Die Zugriffsprotokollierung der HTTP API und die Zugriffsprotokollierung von WebSockets sind mit strukturierten JSON-Feldern aktiviert und werden mit einer Aufbewahrungsfrist von einer

(1) Woche in Amazon CloudWatch Logs geschrieben. Diese Zugriffsloggruppen werden mit einem kundenverwalteten AWS-KMS-Schlüssel verschlüsselt. Anwendungsprotokolle werden in mit einem kundenverwalteten AWS-KMS-Schlüssel verschlüsselten Amazon-CloudWatch-Loggruppen zentralisiert und zehn (10) Jahre aufbewahrt. Separate Audit- und Telemetrie-Loggruppen werden ebenfalls mit einem kundenverwalteten AWS-KMS-Schlüssel verschlüsselt und zehn (10) Jahre aufbewahrt. Die Exportgruppe für Aurora-PostgreSQL-Engine-Protokolle wird eine (1) Woche aufbewahrt.

5.2 Was protokolliert wird und was nicht. ProcessMind protokolliert HTTP-API- und WebSocket-Zugriffsereignisse, einschließlich Anfragezeit, Anfragekennungen, Route oder Pfad, Antwortstatus, Latenz, Quell-IP und User-Agent. ProcessMind protokolliert außerdem Authentifizierungsereignisse, asynchrone Fehlerpfade und unterstützende Lambda-Aktivitäten der Anwendung in zentralisierten CloudWatch-Loggruppen. VPC-Flow-Logs sind aktiviert. ProcessMind aktiviert derzeit keine standardmäßige CloudFront-Zugriffsprotokollierung für die Website, die Frontend-SPA oder die Distributionen öffentlicher Ressourcen.

5.3 Überwachung und Alarmierung. CloudWatch-Alarme und Dashboards überwachen den Systemzustand, Dead-Letter-Queues und sicherheitsrelevante Fehler. Fehler bei der asynchronen Verarbeitung werden an verschlüsselte Dead-Letter-Queues weitergeleitet (Aufbewahrung von vierzehn (14) Tagen; zwei (2) Tage für die Thumbnail- und Suchindex-Warteschlangen), und DLQ-Alarme lösen SNS-Benachrichtigungen zur Untersuchung aus. Darüber hinaus verwendet ProcessMind Sentry zur Echtzeitverfolgung von Frontend-Fehlern, zur Leistungsüberwachung und zur Sitzungswiedergabe. Sitzungswiedergaben werden nur für Sitzungen aufgezeichnet, in denen ein Fehler auftritt; Text, Formulareingaben und Medien werden in den Wiedergaben maskiert oder blockiert. Sentry-Daten werden in der EU (Frankfurt) aufgenommen und sind auf ProcessMind-Nutzungsdaten beschränkt (Browserfehler, Leistungstraces, Gerätemetadaten und maskierte

Wiedergabeaufzeichnungen). Sentry ist in der Liste der Unterauftragsverarbeiter aufgeführt.

5.4 Schutz von Protokollen. Protokolle werden in dedizierten, zugriffskontrollierten CloudWatch-Loggruppen gespeichert und im Ruhezustand verschlüsselt. Produktions- und Entwicklungsprotokolle werden durch Umgebungs- und Kontogrenzen getrennt.

---

6. Automatisierte Kontrollvalidierung und Schwachstellenmanagement

6.1 Was ProcessMind tut. ProcessMind führt `cdk-nag` als Teil seines Workflows zur Infrastruktursynthese und -bereitstellung unter Verwendung mehrerer Regelpakete der Branche aus (einschließlich AWS Solutions, NIST 800-53 und PCI DSS). Berichte pro Stack werden im Rahmen des Infrastrukturänderungsmanagements erstellt und überprüft. Feststellungen werden als behoben, als akzeptiertes Risiko oder als geplante Verbesserung eingestuft.

6.2 Verwaltung von Ausnahmen. Unterdrückungen werden, soweit das Framework dies ermöglicht, in einem zentralen Register erfasst, auf die betroffenen Stacks beschränkt und erfordern eine schriftliche Begründung; wenn ein Stack eine Inline-Unterdrückung enthält, wird diese neben dem Stack dokumentiert. Wenn eine Feststellung behoben wurde, wird die entsprechende Unterdrückung aktualisiert oder entfernt. ProcessMind betrachtet eine Unterdrückung nicht als pauschalen Ausschluss von der Überprüfung.

6.3 Was ProcessMind derzeit nicht tut. ProcessMind verfolgt und überprüft wesentliche Ausnahmen von Infrastrukturkontrollen. Die wichtigsten sind:

- application Lambdas werden standardmäßig nicht innerhalb der VPC platziert; sie greifen über die RDS Data API über TLS mit IAM- und Secrets Manager-Authentifizierung auf Aurora zu
- die WebSocket API und statischen Distributionen sind nicht durch AWS WAF geschützt (WebSocket-Verbindungen verwenden

kurzlebige HMAC-Token; geografische Beschränkungen für Zahlungen werden im Zahlungssystem durchgesetzt), und statische Distributionen verfügen nicht über das standardmäßige CloudFront-Zugriffslogging

- die Datenbankwiederherstellung stützt sich auf automatisierte Aurora-Backups und Point-in-Time Recovery statt auf einen separaten AWS Backup-Plan oder Aurora Enhanced Monitoring
- es gibt keine regionsübergreifende S3-Replikation und kein S3 Object Lock für veränderliche Buckets
- einige von AWS/CDK/SST verwaltete unterstützende Ressourcen verwenden von AWS verwaltete Verschlüsselung oder umfassendere generierte IAM-Richtlinien, wenn der Dienst keine vom Kunden kontrollierbare Alternative bereitstellt

Das vollständige Unterdrückungsregister wird zusammen mit dem Infrastrukturcode geführt und ist auf Anfrage verfügbar. Die Verwendung von `cdk-nag` Rule Packs dient der technischen Kontrollvalidierung und stellt keine externe Zertifizierung, kein Prüfungsurteil und keine rechtliche Bescheinigung der HIPAA-, NIST- oder PCI-DSS-Konformität dar.

6.4 Verwaltung von Abhängigkeiten. Softwareabhängigkeiten werden kontinuierlich auf bekannte Schwachstellen überwacht. Kritische und hochgradige Schwachstellen werden mit dem Ziel behoben, dies innerhalb von sieben (7) Tagen zu tun. Abhängigkeiten werden regelmäßig aktualisiert.

6.5 Sicherer Softwareentwicklungslebenszyklus (SDLC). ProcessMind verfolgt bei der Softwareentwicklung einen Defense-in-Depth-Ansatz. Jede Änderung an der Produktionsumgebung muss vor der Bereitstellung mehrere unabhängige automatisierte Validierungsebenen durchlaufen:

- **Statische Analyse und Typsicherheit:** Der strikte Modus von TypeScript und ESLint erzwingen zur Kompilierzeit Typkorrektheit, Null-Sicherheit und sicherheitsrelevante Codierungsmuster.

- **KI-gestützte Codeprüfung:** Die KI-gestützte Analyse bietet eine zusätzliche Prüfungsperspektive für Pull Requests, um Sicherheitsrisiken, Logikfehler und Abweichungen von Konventionen zu erkennen, und ergänzt damit automatisierte Tests.
- **Unit- und Integrationstests:** Eine umfassende Vitest-Testsuite validiert Geschäftslogik, Datenzugriffsmuster, API-Verhalten und Fehlerbehandlung anhand aktiver AWS-Ressourcen in der Entwicklungsumgebung.
- **End-to-End-Tests:** Browsertests auf Basis von Playwright überprüfen kritische Benutzerabläufe, einschließlich Authentifizierung, Daten-Upload, Prozessmodellierung, Simulation und Mandantentrennung.
- **Infrastruktur-Compliance-Scanning:** `cdk-nag` validiert die Infrastruktur als Code bei jeder Änderung anhand mehrerer Compliance-Frameworks.
- **Scanning auf Schwachstellen in Abhängigkeiten:** Automatisierte Prüfungen von Abhängigkeiten verhindern, dass bekannte kritische und hochgradige Schwachstellen die Produktionsumgebung erreichen.

Die menschliche Prüfung konzentriert sich auf Architektur, Sicherheitsgrenzen und Entscheidungen auf Designebene und nicht auf die Inspektion einzelner Codezeilen. Bei strukturellen, sicherheitsrelevanten oder infrastrukturellen Änderungen ist zusätzlich zur automatisierten Validierung eine ausdrückliche Freigabe durch eine Person erforderlich.

Alle Validierungsebenen werden über CI als erforderliche Merge-Gates für Änderungen am Main-Branch durchgesetzt. Dringende Korrekturen in der Produktionsumgebung dürfen das CI-Gate umgehen, müssen jedoch innerhalb von vierundzwanzig (24) Stunden durch einen vollständigen Pipeline-Lauf und eine Überprüfung nach dem Vorfall nachbearbeitet werden.

---

7. Backup und Disaster Recovery

7.1 Automatisierte Backups. Amazon Aurora führt kontinuierliche, automatisierte Backups mit einer Aufbewahrungsfrist von sieben (7) Tagen durch. Backups werden mit denselben kundenseitig verwalteten KMS-Schlüsseln wie die Quelldatenbanken verschlüsselt.

7.2 Point-in-Time Recovery. Aurora unterstützt eine Point-in-Time Recovery auf jede Sekunde innerhalb des Backup-Aufbewahrungszeitraums und ermöglicht dadurch eine schnelle Wiederherstellung im Fall einer Datenbeschädigung oder versehentlichen Löschung.

7.3 S3-Dauerhaftigkeit und Versionierung. Datei-Uploads und betriebliche Artefakte werden in Amazon S3 gespeichert, das eine Dauerhaftigkeit von 99,999999999 % (11 Neunen) bietet. Die Versionierung ist für den Uploads-Bucket und Ressourcen-Buckets aktiviert, um Wiederherstellungen und Rollbacks zu unterstützen. Website- und Frontend-Bereitstellungs-Buckets sind reproduzierbare Build-Artefakte und werden nicht als Backup-System behandelt. ProcessMind aktiviert derzeit keine regionsübergreifende S3-Replikation.

7.4 Geschäftskontinuität. Verfahren zur Disaster Recovery sind dokumentiert und werden regelmäßig getestet. Eine Zusammenfassung ist im Dokument Disaster Recovery, Business Continuity & Incident Response verfügbar. Die Architektur stützt sich auf von AWS verwaltete Dienste innerhalb der `eu-central-1` Region, die AWS über mehrere Availability Zones hinweg betreibt; der Aurora-Cluster läuft derzeit mit einer einzelnen Writer-Instanz, sodass die Datenbankwiederherstellung auf automatisierten Backups und Point-in-Time Recovery statt auf einer Standby-Instanz innerhalb der Region beruht. Aurora-Backups, S3-Dauerhaftigkeit, Dead-Letter Queues und aus der Quelle neu erstellte statische Assets sind Bestandteil der Wiederherstellungsstrategie.

---

8. Reaktion auf Sicherheitsvorfälle

8.1 Benachrichtigung über Sicherheitsvorfälle. Im Fall eines Sicherheitsvorfalls (wie im DPA definiert) wird ProcessMind betroffene Kunden unverzüglich und, soweit möglich, innerhalb von zweiundsiebzig (72) Stunden nach Kenntniserlangung von dem Vorfall benachrichtigen.

8.2 Behandlung von Sicherheitsvorfällen. ProcessMind unterhält dokumentierte Verfahren zur Reaktion auf Sicherheitsvorfälle, die Identifizierung, Eindämmung, Beseitigung, Wiederherstellung und eine Überprüfung nach dem Vorfall abdecken. Eine Zusammenfassung ist im Dokument Disaster Recovery, Business Continuity & Incident Response verfügbar. Aus Sicherheitsvorfällen gewonnene Erkenntnisse werden in Sicherheitskontrollen und Prozesse integriert.

8.3 Kommunikation. Benachrichtigungen über Sicherheitsvorfälle enthalten Art und Umfang des Vorfalls, die betroffenen Datenkategorien, die zur Eindämmung des Vorfalls ergriffenen Maßnahmen und empfohlene Maßnahmen für den Kunden.

---

9. Organisatorische Maßnahmen

9.1 Management der Informationssicherheit. ProcessMind unterhält ein Informationssicherheits-Managementsystem, das an den Grundsätzen von ISO 27001 ausgerichtet ist. ProcessMind hat seinen Zertifizierungspfad für die ISO-27001-Zertifizierung und die SOC-2-Type-II-Bescheinigung ausgewählt; der formelle Zertifizierungsprozess hat noch nicht begonnen.

9.2 Sicherheitsbewusstsein. Alle Personen mit Zugriff auf Kundendaten erhalten eine Schulung zum Sicherheitsbewusstsein. Bewährte Sicherheitspraktiken sind in das Onboarding, die Entwicklungsabläufe und die betrieblichen Verfahren integriert.

9.3 Verwaltung von Anbietern und Unterauftragsverarbeitern. Unterauftragsverarbeiter sind vertraglich an Datenschutzstandards gebunden, die den in diesem Dokument beschriebenen Standards

gleichwertig sind. ProcessMind führt eine öffentliche Liste der Unterauftragsverarbeiter und informiert mindestens dreißig (30) Tage vor der Beauftragung eines neuen Unterauftragsverarbeiters. Unterauftragsverarbeiter werden jährlich auf Compliance überprüft.

9.4 Vertraulichkeit. Alle Personen, die zur Verarbeitung von Kundendaten berechtigt sind, sind durch schriftliche Vertraulichkeitsverpflichtungen gebunden.

---

10. Compliance und Zertifizierungen

Framework / Standard	Status
DSGVO (Datenschutz-Grundverordnung der EU)	Konform
Datenresidenz in der EU (Frankfurt, Deutschland)	Durchgesetzt
AWS-Infrastrukturzertifizierungen (ISO 27001, SOC 2, PCI DSS)	Über AWS übernommen
ISO 27001 (ProcessMind)	Geplant — Zertifizierungspfad ausgewählt; formeller Prozess noch nicht begonnen
SOC 2 Type II (ProcessMind)	Geplant — Zertifizierungspfad ausgewählt; formeller Prozess noch nicht begonnen

Framework / Standard	Status
Automatisierte Validierung von Infrastrukturkontrollen (`cdk-nag` über AWS Solutions, HIPAA Security, NIST 800-53 R4/R5, PCI DSS 3.2.1, Serverless)	Als technische Kontrollvalidierung implementiert, keine Zertifizierung
Standardvertragsklauseln (SCCs) für internationale Übermittlungen	Implementiert (siehe DPA)
Data Processing Addendum (DPA)	Öffentlich verfügbar

Die Verwendung von `cdk-nag` Rule Packs bedeutet nicht, dass ProcessMind formell nach HIPAA, NIST oder PCI DSS zertifiziert oder unabhängig geprüft ist. Diese Rule Packs werden als technische Leitplanken verwendet, um das Infrastrukturdesign zu validieren und Lücken ausdrücklich nachzuverfolgen.

Bei Fragen zu Sicherheit oder Compliance oder zur Anforderung von Unterlagen wie Prüfberichten oder ausgefüllten Sicherheitsfragebögen wenden Sie sich an **support@processmind.com**.