Notfallwiederherstellung, Geschäftskontinuität und Reaktion auf Sicherheitsvorfälle bei ProcessMind

Gültig ab: 14. September 2026

Dieses Dokument enthält eine allgemeine Zusammenfassung der Verfahren der ProcessMind B.V. zur Notfallwiederherstellung („DR“), Geschäftskontinuität („BCP“) und Reaktion auf Sicherheitsvorfälle für ihren Cloud-Dienst. Es ergänzt die Sicherheitsmaßnahmen, die SaaS-Hosting-Richtlinie, die Service-Level-Vereinbarung und den Nachtrag zur Datenverarbeitung.

Es erläutert unseren derzeitigen Ansatz und begründet keine gesonderten vertraglichen Wiederherstellungszeitziele, Wiederherstellungspunktziele, Garantien für die Dauerhaftigkeit von Daten, Fristen für Benachrichtigungen, Service-Level oder Haftungsmaßstäbe, die über die ausdrücklich in der anwendbaren Vereinbarung, dem DPA oder dem SLA festgelegten hinausgehen.

---

1. Ziele und Geltungsbereich

ProcessMind unterhält diese Verfahren, um:

- die Vertraulichkeit, Integrität und Verfügbarkeit von Kundendaten während eines störenden Ereignisses zu schützen
- kritische Komponenten des Produktionsdienstes nach Ausfällen in von ProcessMind kontrollierten Systemen wiederherzustellen
- das Vorfallmanagement, die Kundenkommunikation und die betriebliche Entscheidungsfindung während Dienstunterbrechungen fortzuführen
- Ausfälle der Infrastruktur-, Bereitstellungs-, Anwendungs- oder Datenebene mithilfe dokumentierter Verfahren und quellcodeverwalteter Infrastrukturdefinitionen zu beheben
- Sicherheitsvorfälle zu identifizieren und zu bewerten, Bedrohungen einzudämmen, Ursachen zu beseitigen, betroffene Systeme

wiederherzustellen, erforderliche Mitteilungen vorzunehmen und gewonnene Erkenntnisse festzuhalten

Diese Verfahren gelten für den produktiven ProcessMind-Cloud-Dienst sowie für Sicherheitsereignisse, an denen Unterauftragsverarbeiter oder Cloud-Dienste beteiligt sind, soweit sie den Service betreffen und innerhalb der angemessenen Untersuchungs- und Verwaltungsmöglichkeiten von ProcessMind liegen. Entwicklungs- und Testumgebungen sind getrennt und werden für Verpflichtungen zur Wiederherstellung der kundenorientierten Produktion nicht als Wiederherstellungsziele behandelt.

---

2. Resilienzstrategie

2.1 Regionale Architektur. Produktionsdienste werden in AWS EU (Frankfurt, Deutschland, `eu-central-1`) gehostet. Die Architektur stützt sich auf verwaltete AWS-Dienste innerhalb dieser Region, die AWS über mehrere Availability Zones hinweg betreibt. Der Aurora-Cluster läuft derzeit mit einer einzelnen Writer-Instanz; daher stützt sich die Datenbankwiederherstellung auf automatisierte Backups und Point-in-Time-Recovery statt auf einen Standby innerhalb der Region. ProcessMind betreibt derzeit keine zweite aktive Region für Kundendaten.

2.2 Verwaltete und serverlose Dienste. ProcessMind stützt sich auf AWS Lambda, Amazon API Gateway, Amazon CloudFront, Amazon Aurora PostgreSQL, Amazon S3, Amazon SQS, Amazon SNS und Amazon CloudWatch. Dies verringert die Abhängigkeit von kundenseitig verwalteten, langfristig laufenden Servern und unterstützt die Wiederherstellung aus dem Quellcode für Anwendungs- und statische Komponenten.

2.3 Trennung der Umgebungen. Produktions- und Entwicklungsumgebungen werden in getrennten AWS-Konten mit getrennten Datenbanken und Infrastruktur-Stacks betrieben. Dies verringert das Risiko, dass Entwicklungsaktivitäten die Wiederherstellungsmaßnahmen der Produktion beeinträchtigen.

2.4 Überwachung und Erkennung. CloudWatch-Alarme, Dashboards, Warnungen für Dead-Letter-Queues, zentralisierte Protokollierung und synthetisches Service-Monitoring unterstützen die Erkennung, Triage und Eskalation von Vorfällen. Potenzielle Vorfälle können außerdem durch Support-Anfragen, Meldungen von Mitarbeitern, Benachrichtigungen von Anbietern oder andere Untersuchungsanlässe erkannt werden.

---

3. Wiederherstellungsprioritäten

Während eines schwerwiegenden Vorfalls gelten für ProcessMind im Allgemeinen folgende Wiederherstellungsprioritäten:

1. Die Integrität der Kundendaten schützen und weiteren Schaden verhindern.
2. Den Vorfall eindämmen und betroffene Systeme stabilisieren.
3. Zentrale Produktionszugänge und kritische Workflows wiederherstellen.
4. Das Verhalten des Dienstes, die Datenintegrität und die Überwachung überprüfen, bevor die Wiederherstellung als abgeschlossen erklärt wird.
5. Statusaktualisierungen, Auswirkungen auf Kunden und Folgemaßnahmen kommunizieren.

Die genaue Reihenfolge kann je nach Art des Vorfalls variieren, insbesondere danach, ob er die Datenintegrität, den Kundenzugang, die asynchrone Verarbeitung oder die unterstützende Infrastruktur betrifft.

---

4. Verfahren zur Notfallwiederherstellung

4.1 Erklärung und Koordinierung von Vorfällen. Wesentliche Dienstunterbrechungen und Sicherheitsvorfälle werden über Verfahren zur Reaktion auf Vorfälle einer Triage unterzogen. ProcessMind bestimmt einen Vorfallleiter, beschränkt die Teilnahme an der Reaktion auf autorisiertes Personal, bewertet Schweregrad und Umfang, koordiniert die technischen

Einsatzkräfte und verfolgt die Wiederherstellungsmaßnahmen, bis der Vorfall behoben oder herabgestuft wurde.

4.2 Eindämmung. ProcessMind unternimmt wirtschaftlich angemessene Anstrengungen, um laufende Auswirkungen zu stoppen oder zu verringern, bevor eine umfassendere Wiederherstellung beginnt. Je nach Fehlerart können Eindämmungsmaßnahmen das Zurücksetzen kürzlich vorgenommener Änderungen, die Deaktivierung betroffener Pfade, die Isolierung fehlerhafter Komponenten, das Anhalten der Hintergrundverarbeitung während der Durchführung von Integritätsprüfungen, den Widerruf oder die Rotation von Zugangsdaten oder die Blockierung missbräuchlicher Aktivitäten umfassen.

4.3 Beseitigung. Nachdem die unmittelbaren Auswirkungen stabilisiert wurden, arbeitet ProcessMind daran, die Grundursache oder den beitragenden Umstand zu beseitigen. Dies kann das Anwenden von Code- oder Konfigurationskorrekturen, das Entfernen schädlicher Artefakte, die Rotation von Secrets, die Wiederherstellung einer vertrauenswürdigen Konfiguration oder das Schließen offengelegter Zugangspfade umfassen.

4.4 Datenbankwiederherstellung. Aurora PostgreSQL führt kontinuierliche automatisierte Backups mit einer Aufbewahrungsfrist von sieben (7) Tagen durch und unterstützt Point-in-Time-Recovery. Wenn ein Fehler auf Datenbankebene, ein Korruptionsereignis oder eine versehentlich destruktive Änderung eine Wiederherstellung erfordert, kann ProcessMind aus dem letzten geeigneten Backup oder auf einen ausgewählten Zeitpunkt wiederherstellen, die wiederhergestellte Umgebung validieren und den Anwendungsverkehr wieder auf den wiederhergestellten Datenbankpfad leiten.

4.5 Wiederherstellung von Objekten und Artefakten. Von Kunden hochgeladene Dateien und betriebliche Artefakte werden in Amazon S3 gespeichert. Für den Upload-Bucket und Ressourcen-Buckets ist die Versionierung aktiviert, um die Wiederherstellung nach versehentlichem Löschen oder Überschreiben zu unterstützen. Website- und Frontend-Bereitstellungs-Buckets werden als reproduzierbare Artefakte behandelt

und können aus dem Quellcode neu erstellt werden, anstatt aus Backups wiederhergestellt zu werden.

4.6 Wiederherstellung asynchroner Workloads. Asynchrone Verarbeitungspfade verwenden Dead-Letter-Queues, um fehlgeschlagene Ereignisse zur Untersuchung aufzubewahren. Die Wiederherstellung kann das erneute Versenden fehlgeschlagener Nachrichten, die erneute Ausführung der Verarbeitungslogik oder die Wiederholung von Arbeiten umfassen, sofern der zugrunde liegende Workflow eine sichere erneute Verarbeitung unterstützt.

4.7 Neuaufbau von Anwendung und Infrastruktur. Die Infrastruktur wird mithilfe quellcodeverwalteter Infrastructure-as-Code-Definitionen verwaltet. Wenn Anwendungsinfrastruktur oder statische Assets neu erstellt werden müssen, kann ProcessMind betroffene Komponenten anhand versionskontrollierter Definitionen und Build-Artefakte neu erstellen und bereitstellen.

4.8 Validierung vor der Wiederaufnahme des Dienstes. Vor dem Abschluss eines Vorfalls validiert ProcessMind den Zustand des Dienstes mithilfe verfügbarer Überwachung, Protokolle, synthetischer Prüfungen und gezielter funktionaler Verifizierung und stellt betroffene Funktionen mithilfe validierter Bereitstellungs-, Wiederherstellungs- und Infrastrukturverfahren wieder her. Eine zusätzliche Prüfung kann durchgeführt werden, wenn der Vorfall eine Datenwiederherstellung oder ein Risiko für die Datenintegrität betraf.

---

5. Maßnahmen zur Geschäftskontinuität

5.1 Betriebliche Kontinuität. ProcessMind unterhält dokumentierte betriebliche Verfahren, damit die Bearbeitung von Vorfällen, die Aufnahme von Kundenanfragen beim Support, die Reaktion des Engineering-Teams und die Entscheidungsfindung während störender Ereignisse fortgesetzt werden können.

5.2 Kommunikation. Bei wesentlichen Produktionsvorfällen unternimmt ProcessMind wirtschaftlich angemessene Anstrengungen, Aktualisierungen über Kundensupportkanäle und gegebenenfalls über die öffentliche Statusseite unter processmind.com/status bereitzustellen.

5.3 Kontrolliertes Änderungsmanagement. Ein Softwareentwicklungslebenszyklus mit Defense-in-Depth, mehreren unabhängigen automatisierten Validierungsebenen, kontrollierten Bereitstellungen, zentralisierter Überwachung und einer Überprüfung nach Vorfällen wird eingesetzt, um vermeidbare Ausfälle zu reduzieren und die Kontinuität im Laufe der Zeit zu verbessern.

5.4 Sicherheit während der Wiederherstellung. Wiederherstellungsmaßnahmen werden unter Beachtung derselben allgemeinen Sicherheitsprinzipien durchgeführt, die auch im normalen Betrieb gelten, einschließlich Zugriff nach dem Prinzip der geringsten Privilegien, protokollierter betrieblicher Aktivitäten, soweit verfügbar, und kontrollierten Zugriffs auf Produktionssysteme und -daten.

---

6. Zusammenfassung von Backups und Datenschutz

6.1 Datenbank-Backups. Automatisierte Aurora-Backups werden verschlüsselt und sieben (7) Tage aufbewahrt; innerhalb dieses Aufbewahrungszeitraums ist Point-in-Time-Recovery verfügbar.

6.2 S3-Schutzmaßnahmen. Amazon S3 bietet eine hohe Dauerhaftigkeit für gespeicherte Objekte. Änderbare Buckets mit Kundendaten stützen sich innerhalb der primären Region auf Dauerhaftigkeit und Versionierung. ProcessMind aktiviert derzeit keine regionsübergreifende S3-Replikation für diese Buckets.

6.3 Protokolle und Diagnosen. Zentralisierte Protokolle, Alarme und Telemetriedaten unterstützen die Untersuchung von Ausfällen und die Validierung der Wiederherstellung. Diese Mechanismen unterstützen den

Betrieb zur Aufrechterhaltung der Kontinuität, werden jedoch nicht selbst als separates Backup-Produkt dargestellt.

---

7. Identifizierung und Triage von Vorfällen

7.1 Ersteinschätzung. Gemeldete Ereignisse werden einer Triage unterzogen, um festzustellen, ob sie der Definition eines Sicherheitsvorfalls entsprechen, welche Systeme oder Daten betroffen sein könnten, welcher Umfang und Schweregrad wahrscheinlich sind und ob eine sofortige Eindämmung erforderlich ist. Die Beweissicherung erfolgt in einer Weise, die der Art des Vorfalls und den betroffenen Systemen angemessen ist.

7.2 Bereitschaftsdienst und Eskalation. ProcessMind unterhält eine Bereitschaftsabdeckung für Vorfälle in Produktionsumgebungen, einschließlich einer 24/7-Abdeckung für Kritische Vorfälle (wie im Service Level Agreement definiert), damit Vorfälle jederzeit bestätigt und einer Triage unterzogen werden können.

7.3 Dokumentation. ProcessMind dokumentiert wesentliche Untersuchungsergebnisse, Reaktionsmaßnahmen und Wiederherstellungsentscheidungen, damit die Zeitleiste des Vorfalls und die daraus resultierenden Korrekturmaßnahmen nach dem Ereignis überprüft werden können.

---

8. Kommunikation und Benachrichtigung

8.1 Interne Kommunikation. ProcessMind koordiniert die an der Reaktion Beteiligten, Entscheidungsträger und Supportkanäle, damit die technische Reaktion und die Kundenkommunikation während des gesamten Lebenszyklus des Vorfalls aufeinander abgestimmt bleiben.

8.2 Benachrichtigung der Kunden. Im Falle eines Sicherheitsvorfalls, der nach dem DPA oder dem anwendbaren Recht eine Benachrichtigung erfordert, benachrichtigt ProcessMind betroffene Kunden unverzüglich und, soweit möglich, innerhalb von zweiundsiebzig (72) Stunden, nachdem

ProcessMind von dem Vorfall Kenntnis erlangt hat. Benachrichtigungen enthalten im Allgemeinen die Art und den Umfang des Vorfalls, sofern bekannt die betroffenen Datenkategorien, die zur Eindämmung und Behebung des Vorfalls ergriffenen Maßnahmen sowie gegebenenfalls empfohlene Maßnahmen für Kunden.

8.3 Laufende Aktualisierungen. Wenn der Vorfall weiterhin aktiv ist oder sich wesentliche Tatsachen ändern, stellt ProcessMind Folgeaktualisierungen bereit, sobald zusätzliche verifizierte Informationen verfügbar werden. Bei umfassenderen Störungen des Produktionsdienstes kann ProcessMind außerdem Kunden-Supportkanäle und, soweit angemessen, die öffentliche Statusseite unter processmind.com/status nutzen.

---

9. Tests, Überprüfung und Wartung

ProcessMind überprüft diese Verfahren mindestens jährlich sowie nach wesentlichen Vorfällen oder erheblichen architektonischen Änderungen, führt regelmäßig Übungen zu relevanten Elementen des Reaktions- und Wiederherstellungsansatzes durch (wie der Wiederherstellung von Backups, dem Neuaufbau von Deployments, der Überwachung, der Alarmierung und der Kommunikation bei Vorfällen) und integriert gewonnene Erkenntnisse in seine Sicherheits-, Zuverlässigkeits- und Kontinuitätsverfahren.

---

10. Einschränkungen und vertragliche Grenzen

Dieses Dokument ist eine Zusammenfassung auf hoher Ebene und beschreibt nicht jedes interne Runbook, jeden Eskalationsweg, jede Untersuchungsmethode oder jeden Schritt der Beweishandhabung im operativen Detail. Es verpflichtet ProcessMind weder zu einem separaten regionsübergreifenden Failover-Design noch zu einer Aufbewahrung in unveränderlichem Speicher für alle veränderbaren Buckets oder zu

unabhängigen RTO/RPO-Garantien, die über das hinausgehen, was in der anwendbaren Vereinbarung oder Bestellung ausdrücklich festgelegt ist.

Im Falle eines Widerspruchs zwischen diesem Dokument und der anwendbaren Kundenvereinbarung, dem Data Processing Addendum, dem Service Level Agreement oder zwingendem Recht sind diese Quellen maßgeblich.