Disaster recovery, bedrijfscontinuïteit en incidentrespons van ProcessMind

Ingangsdatum: 14 september 2026

Dit document bevat een samenvatting op hoofdlijnen van de procedures van ProcessMind B.V. voor disaster recovery ("DR"), bedrijfscontinuïteit ("BCP") en beveiligingsincidentrespons voor zijn clouddienst. Het vormt een aanvulling op de Beveiligingsmaatregelen, het SaaS-hostingbeleid, de Service Level Agreement en het Addendum gegevensverwerking.

Het legt onze huidige aanpak uit en creëert geen afzonderlijke contractuele doelstellingen voor hersteltijd, herstelpuntdoelstellingen, garanties inzake gegevensduurzaamheid, meldingstermijnen, serviceniveaus of aansprakelijkheidsnormen bovenop wat uitdrukkelijk is bepaald in de toepasselijke overeenkomst, DPA of SLA.

---

1. Doelstellingen en reikwijdte

ProcessMind handhaaft deze procedures om:

- de vertrouwelijkheid, integriteit en beschikbaarheid van Klantgegevens tijdens een verstorende gebeurtenis te beschermen
- kritieke productieonderdelen van de dienst te herstellen na storingen in door ProcessMind beheerde systemen
- incidentbeheer, klantcommunicatie en operationele besluitvorming tijdens dienstverstoringen voort te zetten
- te herstellen van storingen in infrastructuur, implementatie, applicatie of gegevenslaag met behulp van gedocumenteerde procedures en infrastructuurdefinities die onder bronbeheer staan
- Beveiligingsincidenten te identificeren en te beoordelen, bedreigingen in te dammen, onderliggende oorzaken weg te nemen, getroffen systemen te herstellen, waar vereist te communiceren en geleerde lessen vast te leggen

Deze procedures zijn van toepassing op de productieclouddienst van ProcessMind en op beveiligingsgebeurtenissen waarbij subverwerkers of clouddiensten betrokken zijn, voor zover deze de Service beïnvloeden en binnen het redelijke vermogen van ProcessMind vallen om te onderzoeken en te beheren. Ontwikkel- en testomgevingen zijn gescheiden en worden niet beschouwd als hersteldoelen voor klantgerichte productieverbintenissen.

---

2. Veerkrachtstrategie

2.1 Regionaal ontwerp. Productiediensten worden gehost in AWS EU (Frankfurt, Duitsland, `eu-central-1`). De architectuur steunt op door AWS beheerde diensten binnen die 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 herstel naar een bepaald tijdstip, in plaats van een standby binnen de regio. ProcessMind exploiteert momenteel geen tweede actieve regio voor klantgegevens.

2.2 Beheerde en serverloze diensten. ProcessMind steunt op AWS Lambda, Amazon API Gateway, Amazon CloudFront, Amazon Aurora PostgreSQL, Amazon S3, Amazon SQS, Amazon SNS en Amazon CloudWatch. Dit vermindert de afhankelijkheid van langdurig draaiende servers die door klanten worden beheerd en ondersteunt herstel vanaf broncode voor applicatie- en statische componenten.

2.3 Scheiding van omgevingen. Productie- en ontwikkelomgevingen werken in afzonderlijke AWS-accounts met afzonderlijke databases en infrastructuurstacks. Dit vermindert het risico dat ontwikkelactiviteiten gevolgen hebben voor productieherstelactiviteiten.

2.4 Monitoring en detectie. CloudWatch-alarmen, dashboards, meldingen van dead-letter queues, gecentraliseerde logging en synthetische servicemonitoring ondersteunen incidentdetectie, triage en escalatie. Mogelijke incidenten kunnen ook worden geïdentificeerd via

supportmeldingen, rapportages van medewerkers, meldingen van leveranciers of andere aanleidingen voor onderzoek.

---

3. Herstelprioriteiten

Tijdens een groot incident zijn de herstelprioriteiten van ProcessMind doorgaans:

1. De integriteit van klantgegevens beschermen en verdere schade voorkomen.
2. Het incident indammen en getroffen systemen stabiliseren.
3. De centrale productietoegangspaden en kritieke workflows herstellen.
4. De werking van de dienst, de gegevensintegriteit en de monitoring valideren voordat het herstel als voltooid wordt verklaard.
5. Statusupdates, gevolgen voor klanten en vervolgacties communiceren.

De exacte volgorde kan variëren afhankelijk van de aard van het incident, waaronder de vraag of het de gegevensintegriteit, klanttoegang, asynchrone verwerking of ondersteunende infrastructuur beïnvloedt.

---

4. Disaster-recoveryprocedures

4.1 Incidentverklaring en coördinatie. Wezenlijke dienstverstoringen en beveiligingsincidenten worden getrieerd via incidentresponsprocedures. ProcessMind wijst een incidentleider aan, beperkt deelname aan de respons tot geautoriseerd personeel, beoordeelt ernst en reikwijdte, coördineert technische responders en volgt herstelacties totdat het incident is opgelost of afgeschaald.

4.2 Indamming. ProcessMind spant zich commercieel redelijkerwijs in om de voortdurende impact te stoppen of te beperken voordat breder herstel begint. Afhankelijk van de storingsmodus kunnen indammingsmaatregelen bestaan uit het terugdraaien van recente wijzigingen, het uitschakelen van

getroffen paden, het isoleren van defecte componenten, het pauzeren van achtergrondverwerking terwijl integriteitscontroles worden uitgevoerd, het intrekken of roteren van credentials of het blokkeren van misbruik.

4.3 Wegnemen van de oorzaak. Nadat de onmiddellijke impact is gestabiliseerd, werkt ProcessMind eraan de onderliggende oorzaak of bijdragende omstandigheid weg te nemen. Dit kan bestaan uit het toepassen van code- of configuratieoplossingen, het verwijderen van kwaadaardige artefacten, het roteren van secrets, het herstellen van een vertrouwde configuratie of het sluiten van blootgestelde toegangspaden.

4.4 Databaseherstel. Aurora PostgreSQL voert continu geautomatiseerde back-ups uit met een bewaartermijn van zeven (7) dagen en ondersteunt herstel naar een bepaald tijdstip. Als voor herstel een databasefout, corruptiegebeurtenis of onbedoelde destructieve wijziging op databaseniveau moet worden teruggedraaid, kan ProcessMind herstellen vanaf de meest geschikte recente back-up of naar een geselecteerd tijdstip, de herstelde omgeving valideren en het applicatieverkeer terugleiden naar het herstelde databasepad.

4.5 Herstel van objecten en artefacten. Uploads van klantbestanden en operationele artefacten worden opgeslagen in Amazon S3. Versioning is ingeschakeld voor de uploadbucket en resourcebuckets ter ondersteuning van herstel na onbedoelde verwijdering of overschrijving. Website- en frontend-deploymentbuckets worden beschouwd als reproduceerbare artefacten en kunnen opnieuw worden opgebouwd vanuit de broncode in plaats van als back-up te worden hersteld.

4.6 Herstel van asynchrone workloads. Asynchrone verwerkingspaden gebruiken dead-letter queues om mislukte gebeurtenissen voor onderzoek te bewaren. Herstel kan bestaan uit het opnieuw proberen van mislukte berichten, het opnieuw uitvoeren van verwerkingslogica of het opnieuw afspelen van werk wanneer de onderliggende workflow veilige herverwerking ondersteunt.

4.7 Herbouw van applicatie en infrastructuur. Infrastructuur wordt beheerd via infrastructuur-as-code-definities die onder bronbeheer staan. Als applicatie-infrastructuur of statische assets opnieuw moet worden gecreëerd, kan ProcessMind getroffen componenten opnieuw opbouwen en implementeren vanuit versiebeheerde definities en buildartefacten.

4.8 Validatie vóór hervatting van de dienst. Voordat een incident wordt gesloten, valideert ProcessMind de gezondheid van de dienst met beschikbare monitoring, logboeken, synthetische controles en gerichte functionele verificatie, en herstelt het getroffen functionaliteit met behulp van gevalideerde implementatie-, herstel- en infrastructuurprocedures. Aanvullende beoordeling kan worden uitgevoerd wanneer het incident betrekking had op gegevensherstel of risico's voor de gegevensintegriteit.

---

5. Maatregelen voor bedrijfscontinuïteit

5.1 Operationele continuïteit. ProcessMind onderhoudt gedocumenteerde operationele procedures zodat incidentafhandeling, intake van klantondersteuning, engineeringrespons en besluitvorming tijdens verstorende gebeurtenissen kunnen doorgaan.

5.2 Communicatie. Voor wezenlijke productie-incidenten spant ProcessMind zich commercieel redelijkerwijs in om updates te verstrekken via klantenondersteuningskanalen en, waar passend, de openbare statuspagina op processmind.com/status.

5.3 Gecontroleerd wijzigingsbeheer. Een softwareontwikkelingslevenscyclus met defense-in-depth, meerdere onafhankelijke geautomatiseerde validatielagen, gecontroleerde implementaties, gecentraliseerde monitoring en evaluatie na incidenten wordt gebruikt om vermijdbare uitval te beperken en de continuïteit in de loop der tijd te verbeteren.

5.4 Beveiliging tijdens herstel. Herstelacties worden uitgevoerd met inachtneming van dezelfde algemene beveiligingsbeginselen die tijdens

normale bedrijfsvoering gelden, waaronder toegang volgens het beginsel van minimale bevoegdheden, waar beschikbaar gelogde operationele activiteiten en gecontroleerde toegang tot productiesystemen en gegevens.

---

6. Samenvatting van back-ups en gegevensbescherming

6.1 Databaseback-ups. Geautomatiseerde Aurora-back-ups zijn versleuteld en worden zeven (7) dagen bewaard; herstel naar een bepaald tijdstip is binnen die bewaartermijn beschikbaar.

6.2 S3-bescherming. Amazon S3 biedt een hoge duurzaamheid voor opgeslagen objecten. Wijzigbare buckets met klantgegevens zijn afhankelijk van duurzaamheid en versiebeheer binnen de primaire regio. ProcessMind maakt momenteel geen S3-replicatie tussen regio's voor deze buckets mogelijk.

6.3 Logboeken en diagnostiek. Gecentraliseerde logboeken, alarmen en telemetrie ondersteunen onderzoek naar storingen en validatie van herstel. Deze mechanismen ondersteunen de bedrijfscontinuïteit, maar worden niet zelf gepresenteerd als een afzonderlijk back-upproduct.

---

7. Identificatie en triage van incidenten

7.1 Eerste beoordeling. Gemelde gebeurtenissen worden getrieerd om vast te stellen of ze voldoen aan de definitie van een Security Incident, welke systemen of gegevens mogelijk zijn getroffen, wat de waarschijnlijke omvang en ernst zijn en of onmiddellijke inperking vereist is. Het bewaren van bewijsmateriaal gebeurt op een wijze die passend is bij de aard van het incident en de betrokken systemen.

7.2 Piketdienst en escalatie. ProcessMind handhaaft een piketdienst voor productie-incidenten, waaronder 24x7-dekking voor Critical incidents (zoals gedefinieerd in de Service Level Agreement), zodat incidenten op elk moment kunnen worden erkend en getrieerd.

7.3 Documentatie. ProcessMind documenteert materiële onderzoeksbevindingen, responsmaatregelen en herstelbeslissingen, zodat de tijdlijn van het incident en de daaruit voortvloeiende corrigerende maatregelen na de gebeurtenis kunnen worden beoordeeld.

---

8. Communicatie en kennisgeving

8.1 Interne communicatie. ProcessMind coördineert degenen die reageren, besluitvormers en ondersteuningskanalen, zodat de technische respons en communicatie met klanten gedurende de gehele levenscyclus van het incident op elkaar afgestemd blijven.

8.2 Kennisgeving aan klanten. In geval van een Security Incident waarvoor op grond van de DPA of toepasselijke wetgeving kennisgeving vereist is, stelt ProcessMind getroffen klanten zonder onnodige vertraging op de hoogte en, waar haalbaar, binnen tweeënzeventig (72) uur nadat ProcessMind zich bewust is geworden van het incident. Kennisgevingen bevatten doorgaans de aard en omvang van het incident, de getroffen gegevenscategorieën indien bekend, de maatregelen die zijn genomen om het incident in te perken en te verhelpen, en aanbevolen maatregelen voor klanten waar relevant.

8.3 Doorlopende updates. Wanneer het incident actief blijft of materiële feiten veranderen, verstrekt ProcessMind vervolgupdates zodra aanvullende geverifieerde informatie beschikbaar komt. Voor bredere verstoringen van productiediensten kan ProcessMind ook klantenondersteuningskanalen gebruiken en, waar passend, de openbare statuspagina op processmind.com/status.

---

9. Testen, beoordeling en onderhoud

ProcessMind beoordeelt deze procedures ten minste jaarlijks en na materiële incidenten of belangrijke architectuurwijzigingen, oefent periodiek relevante onderdelen van de respons- en herstelbenadering

(zoals herstel van back-ups, opnieuw opbouwen van implementaties, monitoring, waarschuwingen en incidentcommunicatie) en verwerkt geleerde lessen in zijn procedures voor beveiliging, betrouwbaarheid en bedrijfscontinuïteit.

---

10. Beperkingen en contractuele grenzen

Dit document is een samenvatting op hoofdlijnen en beschrijft niet elk intern runbook, escalatiepad, elke onderzoeksmethode of elke stap voor het omgaan met bewijsmateriaal in operationeel detail. Het verplicht ProcessMind niet tot een afzonderlijk failoverontwerp tussen regio's, onveranderlijke opslagbewaring voor alle wijzigbare buckets of onafhankelijke RTO/RPO-garanties, behalve voor zover uitdrukkelijk bepaald in de toepasselijke overeenkomst of bestelling.

In geval van strijdigheid tussen dit document en de toepasselijke Customer Agreement, Data Processing Addendum, Service Level Agreement of dwingende wetgeving, prevaleren die bronnen.