

A ProcessMind katasztrófa utáni helyreállítási, üzletmenet-folytonossági és incidenskezelési eljárásai

Hatálybalépés napja: 2026. szeptember 14.

Ez a dokumentum magas szintű összefoglalót nyújt a ProcessMind B.V. felhőszolgáltatására vonatkozó katasztrófa utáni helyreállítási („DR”), üzletmenet-folytonossági („BCP”) és biztonsági incidenskezelési eljárásairól. Kiegészíti a [Biztonsági intézkedéseket](#), a [SaaS-tárhelyszolgáltatási szabályzatot](#), a [Szolgáltatási szintre vonatkozó megállapodást](#) és az [Adatfeldolgozási kiegészítést](#).

Ismerteti jelenlegi megközelítésünket, és nem keletkeztet külön szerződéses helyreállítási időcélokat, helyreállítási pontcélokat, az adatok tartósságára vonatkozó szavatosságot, értesítési határidőket, szolgáltatási szinteket vagy felelősségi szabályokat azon túl, amit az alkalmazandó megállapodás, DPA vagy SLA kifejezetten előír.

1. Célok és hatály

A ProcessMind az alábbi célokból tartja fenn ezeket az eljárásokat:

- az Ügyféladatok bizalmasságának, sértetlenségének és rendelkezésre állásának védelme zavaró esemény esetén
- a kritikus éles szolgáltatási összetevők helyreállítása a ProcessMind által ellenőrzött rendszerek meghibásodását követően
- az incidenskezelés, az ügyfelekkel folytatott kommunikáció és a működési döntéshozatal folytatása a szolgáltatás megszakadása alatt
- az infrastruktúra, a telepítés, az alkalmazás vagy az adatréteg meghibásodása utáni helyreállítás dokumentált eljárások és forráskód-kezelés alatt álló infrastruktúra-definíciók alkalmazásával
- a biztonsági incidensek azonosítása és értékelése, a fenyegetések megfékezése, a kiváltó okok megszüntetése, az érintett rendszerek

helyreállítása, az előírt kommunikáció és a levont tanulságok rögzítése

Ezek az eljárások a ProcessMind éles felhőszolgáltatására, valamint az alfeldolgozókat vagy felhőszolgáltatásokat érintő biztonsági eseményekre vonatkoznak, amennyiben azok hatással vannak a Szolgáltatásra, és kivizsgálásuk, illetve kezelésük a ProcessMind észszerű lehetőségein belül van. A fejlesztési és tesztkörnyezetek elkülönülnek, és nem minősülnek az ügyfelek számára vállalt éles szolgáltatási kötelezettségek helyreállítási célpontjainak.

2. Rezilienciastratégia

2.1 Regionális kialakítás. Az éles szolgáltatásokat az AWS EU-régiójában (Frankfurt, Németország, eu-central-1) üzemeltetjük. Az architektúra az adott régióon belül az AWS által felügyelt szolgáltatásokra támaszkodik, amelyeket az AWS több rendelkezésre állási zónán keresztül működtet. Az Aurora-fürt jelenleg egyetlen írópéldányt futtat, ezért az adatbázis helyreállítása automatikus biztonsági mentéseken és egy adott időpontra történő visszaállításon alapul, nem pedig egy régióon belüli készenléti példányon. A ProcessMind jelenleg nem üzemeltet második, ügyféladatokat tartalmazó aktív régiót.

2.2 Felügyelt és szerver nélküli szolgáltatások. A ProcessMind az AWS Lambda, az Amazon API Gateway, az Amazon CloudFront, az Amazon Aurora PostgreSQL, az Amazon S3, az Amazon SQS, az Amazon SNS és az Amazon CloudWatch szolgáltatásokra támaszkodik. Ez csökkenti az ügyfél által felügyelt, hosszú élettartamú szerverektől való függőséget, és támogatja az alkalmazás- és statikus összetevők forrásból történő újraépítésével megvalósuló helyreállítást.

2.3 A környezetek elkülönítése. Az éles és a fejlesztési környezetek külön AWS-fiókokban, külön adatbázisokkal és infrastruktúra-veremekkel működnek. Ez csökkenti annak kockázatát, hogy a fejlesztési tevékenység hatással legyen az éles környezet helyreállítási műveleteire.

2.4 Felügyelet és észlelés. A CloudWatch-riasztások, dashboardok, a holtbetűsor-üzenetsorokra vonatkozó riasztások, a központosított naplózás és a szintetikus szolgáltatásfelügyelet támogatják az incidensek észlelését, kezdeti értékelését és eskalációját. A lehetséges incidensek az ügyfélszolgálati bejelentések, a munkavállalói jelentések, a beszállítói értesítések vagy más vizsgálatot kiváltó körülmények révén is azonosíthatók.

3. Helyreállítási prioritások

Jelentős incidens esetén a ProcessMind helyreállítási prioritásai általában a következők:

1. Az ügyfeladatok sértetlenségének védelme és a további károk megelőzése.
2. Az incidens megfékezése és az érintett rendszerek stabilizálása.
3. Az alapvető éles hozzáférési útvonalak és kritikus munkafolyamatok helyreállítása.
4. A szolgáltatás működésének, az adatok sértetlenségének és a felügyeletnek az ellenőrzése a helyreállítás befejezettnek nyilvánítása előtt.
5. Állapotfrissítések, az ügyfelekre gyakorolt hatás és a további intézkedések közlése.

A pontos sorrend az incidens jellegétől függően változhat, többek között attól függően, hogy az az adatok sértetlenségét, az ügyfelek hozzáférését, az aszinkron feldolgozást vagy a támogató infrastruktúrát érinti-e.

4. Katasztrófa utáni helyreállítási eljárások

4.1 Az incidens bejelentése és koordinációja. A jelentős szolgáltatáskieséseket és biztonsági incidenseket az incidenskezelési eljárások szerint értékeljük. A ProcessMind kijelöl egy incidensvezetőt, a válaszadásban való részvételt az arra felhatalmazott személyekre

korlátozza, felméri a súlyosságot és a hatókört, koordinálja a műszaki reagálókat, valamint nyomon követi a helyreállítási intézkedéseket az incidens megoldásáig vagy alacsonyabb súlyossági szintre sorolásáig.

4.2 Megfékezés. A ProcessMind kereskedelmileg észszerű erőfeszítéseket tesz a folyamatban lévő hatás megszüntetésére vagy csökkentésére, mielőtt megkezdene a szélesebb körű helyreállítást. A hiba jellegétől függően a megfékezésre irányuló intézkedések közé tartozhat a közelmúltbeli módosítások visszaállítása, az érintett útvonalak letiltása, a hibásan működő összetevők elkülönítése, a háttérfeldolgozás szüneteltetése az adatok sértetlenségének ellenőrzése alatt, a hitelesítő adatok visszavonása vagy cseréje, illetve a visszaélészerű tevékenység blokkolása.

4.3 Felszámolás. A közvetlen hatás stabilizálását követően a ProcessMind azon dolgozik, hogy megszüntesse a kiváltó okot vagy a közreható körülményt. Ez magában foglalhatja kód- vagy konfigurációs javítások alkalmazását, rosszindulatú elemek eltávolítását, titkos kulcsok cseréjét, a megbízható konfiguráció visszaállítását vagy a nyitott hozzáférési útvonalak lezárását.

4.4 Adatbázis-helyreállítás. Az Aurora PostgreSQL folyamatos automatikus biztonsági mentéseket végez, amelyek megőrzési időtartama hét (7) nap, és támogatja az adott időpontra történő visszaállítást. Ha adatbázisszintű hiba, adatsérülés vagy véletlen, romboló módosítás miatt visszaállításra van szükség, a ProcessMind visszaállíthatja az adatbázist a legutóbbi megfelelő biztonsági mentésből vagy egy kiválasztott időpontra, ellenőrizheti a visszaállított környezetet, majd az alkalmazás forgalmát a helyreállított adatbázis útvonalára irányíthatja.

4.5 Objektumok és műtermékek helyreállítása. Az ügyfelek fájlfeltöltéseit és a működési műtermékeket az Amazon S3 tárolja. A feltöltési tárolóban és az erőforrás-tárolókban engedélyezve van a verziókezelés, amely támogatja a véletlen törlés vagy felülírás utáni helyreállítást. A weboldal és a frontend telepítési tárolóit újra előállítható műtermékeknek tekintjük, ezért biztonsági mentésből történő visszaállítás helyett forrásból is újraépíthetők.

4.6 Az aszinkron munkaterhelés helyreállítása. Az aszinkron feldolgozási útvonalak holtbetűsor-üzenetsorokat használnak a sikertelen események vizsgálat céljából történő megőrzésére. A helyreállítás magában foglalhatja a sikertelen üzenetek újrapróbálását, a feldolgozási logika újbóli futtatását vagy a munka ismételt lejátszását, amennyiben az alapul szolgáló munkafolyamat támogatja a biztonságos újbóli feldolgozást.

4.7 Az alkalmazás és az infrastruktúra újraépítése. Az infrastruktúrát forráskód-kezelés alatt álló infrastruktúra-kódként kezelt definíciók segítségével kezeljük. Ha az alkalmazás infrastruktúráját vagy statikus eszközeit újra kell létrehozni, a ProcessMind a verziókezelés alatt álló definíciókból és buildműtermékekből újraépítheti és telepítheti az érintett összetevőket.

4.8 Ellenőrzés a szolgáltatás újbóli elindítása előtt. Az incidens lezárása előtt a ProcessMind a rendelkezésre álló felügyeleti eszközök, naplók, szintetikus ellenőrzések és célzott funkcionális vizsgálatok segítségével ellenőrzi a szolgáltatás állapotát, továbbá érvényesített telepítési, helyreállítási és infrastruktúra-eljárások alkalmazásával állítja helyre az érintett funkciókat. További felülvizsgálatra kerülhet sor, ha az incidens adat-visszaállítással vagy az adatok sértetlenségét érintő kockázattal járt.

5. Üzletmenet-folytonossági intézkedések

5.1 Működési folytonosság. A ProcessMind dokumentált működési eljárásokat tart fenn annak érdekében, hogy az incidenskezelés, az ügyfélszolgálati bejelentések fogadása, a mérnöki reagálás és a döntéshozatal zavaró események idején is folytatódhasson.

5.2 Kommunikáció. Jelentős éles üzemi incidensek esetén a ProcessMind kereskedelmileg észszerű erőfeszítéseket tesz arra, hogy az ügyfélszolgálati csatornákon, valamint adott esetben a nyilvános állapotoldalon, a processmind.com/status címen tájékoztatást nyújtson.

5.3 Ellenőrzött változáskezelés. A megelőzhető szolgáltatáskiesések csökkentése és a folytonosság idővel történő javítása érdekében mélységi védelmet biztosító szoftverfejlesztési életciklust alkalmazunk, amely több, egymástól független automatizált érvényesítési réteget, ellenőrzött telepítéseket, központosított felügyeletet és incidens utáni felülvizsgálatot foglal magában.

5.4 Biztonság a helyreállítás során. A helyreállítási intézkedésekre ugyanazok az általános biztonsági elvek vonatkoznak, mint a rendes működésre, ideértve a legkisebb jogosultság elvét, a műveleti tevékenységek rendelkezésre álló naplózását, valamint az éles rendszerekhez és adatokhoz való hozzáférés ellenőrzését.

6. A biztonsági mentések és az adatvédelem összefoglalása

6.1 Adatbázis-biztonsági mentések. Az Aurora automatikus biztonsági mentései titkosítottak, és hét (7) napig kerülnek megőrzésre; ezen megőrzési időtartamon belül adott időpontra történő visszaállítás is rendelkezésre áll.

6.2 S3-védelmi intézkedések. Az Amazon S3 magas szintű tartósságot biztosít a tárolt objektumok számára. A módosítható ügyféladat-tárolók az elsődleges régión belüli tartósságra és verziókezelésre támaszkodnak. A ProcessMind jelenleg nem engedélyez régiók közötti S3-replikációt ezekhez a tárolókhoz.

6.3 Naplók és diagnosztika. A központosított naplók, riasztások és telemetria támogatják a hibák kivizsgálását és a helyreállítás ellenőrzését. Ezek a mechanizmusok támogatják az üzletmenet-folytonossági műveleteket, de önmagukban nem minősülnek külön biztonsági mentési terméknek.

7. Az incidensek azonosítása és kezdeti értékelése

7.1 Kezdeti értékelés. A bejelentett eseményeket kezdeti értékelésnek vetjük alá annak megállapítására, hogy megfelelnek-e a Biztonsági incidens fogalmának, mely rendszerek vagy adatok lehetnek érintettek, mi a valószínű hatókör és súlyosság, valamint szükséges-e azonnali megfékezés. A bizonyítékok megőrzése az incidens jellegének és az érintett rendszereknek megfelelő módon történik.

7.2 Ügyeleti szolgálat és eskaláció. A ProcessMind ügyeleti lefedettséget biztosít az éles üzemi incidensek esetére, beleértve a Kritikus incidensek (a Szolgáltatási szintre vonatkozó megállapodásban meghatározott) 24x7 lefedettségét, hogy az incidenseket bármikor vissza lehessen igazolni és kezdeti értékelésnek lehessen alávetni.

7.3 Dokumentálás. A ProcessMind dokumentálja a vizsgálat lényeges megállapításait, a válaszingázkedéseket és a helyreállítással kapcsolatos döntéseket, hogy az eseményt követően felül lehessen vizsgálni az incidens idővonalát és az abból következő korrekciós intézkedéseket.

8. Kommunikáció és értesítés

8.1 Belső kommunikáció. A ProcessMind koordinálja a reagálókat, a döntéshozókat és az ügyfélszolgálati csatornákat annak érdekében, hogy a műszaki válaszingázkedések és az ügyfelekkel folytatott kommunikáció az incidens teljes életciklusa során összehangoltak maradjanak.

8.2 Ügyfelek értesítése. Ha olyan Biztonsági incidens történik, amelyről a DPA vagy az alkalmazandó jogszabályok alapján értesítést kell küldeni, a ProcessMind indokolatlan késedelem nélkül, és amennyiben megvalósítható, az incidensről való tudomásszerzéstől számított hetvenkét (72) órán belül értesíti az érintett ügyfeleket. Az értesítések általában tartalmazzák az incidens jellegét és hatókörét, az érintett adatkategóriákat, ha azok ismertek, az incidens megfékezése és orvoslása érdekében tett

intézkedéseket, valamint adott esetben az ügyfelek számára javasolt intézkedéseket.

8.3 Folyamatos tájékoztatás. Ha az incidens továbbra is fennáll, vagy lényeges tények változnak, a ProcessMind további, ellenőrzött információk rendelkezésre állásakor újabb tájékoztatást nyújt. Az éles szolgáltatás szélesebb körű kiesése esetén a ProcessMind az ügyfélszolgálati csatornákat, valamint adott esetben a nyilvános állapotoldalt is használhatja, amely a processmind.com/status címen érhető el.

9. Tesztelés, felülvizsgálat és karbantartás

A ProcessMind legalább évente, továbbá jelentős incidenseket vagy lényeges architektúrális változásokat követően felülvizsgálja ezeket az eljárásokat, időszakosan gyakorolja a válaszadási és helyreállítási megközelítés releváns elemeit (például a biztonsági mentés visszaállítását, a telepítés újraépítését, a felügyeletet, a riasztást és az incidensekkel kapcsolatos kommunikációt), valamint a levont tanulságokat beépíti biztonsági, megbízhatósági és folytonossági eljárásaiba.

10. Korlátozások és szerződéses keretek

Ez a dokumentum magas szintű összefoglaló, és nem ismerteti részletesen az összes belső üzemeltetési útmutatót, eskalációs útvonalat, vizsgálati módszert vagy bizonyítékekezelési lépést. Nem kötelezi a ProcessMindot külön régiók közötti átállási kialakításra, valamennyi módosítható tároló megváltoztathatatlan megőrzésére, illetve az alkalmazandó megállapodásban vagy megrendelésben kifejezetten rögzítetteken túl önálló RTO/RPO-garanciák nyújtására.

Ha e dokumentum és az alkalmazandó Ügyfélmegállapodás, Adatfeldolgozási kiegészítés, Szolgáltatási szintre vonatkozó megállapodás vagy kötelező jogszabály között ellentmondás áll fenn, az utóbbiak az irányadók.