

ProcessMind: odzyskiwanie po awarii, ciągłość działania i reagowanie na incydenty

Data wejścia w życie: 14 września 2026 r.

Niniejszy dokument zawiera ogólne podsumowanie procedur ProcessMind B.V. dotyczących odzyskiwania po awarii („DR”), ciągłości działania („BCP”) i reagowania na incydenty bezpieczeństwa w odniesieniu do jej usługi chmurowej. Uzupełnia on dokumenty [Środki bezpieczeństwa](#), [Polityka hostingu SaaS](#), [Umowa o gwarantowanym poziomie świadczenia usług](#) oraz [Aneks dotyczący przetwarzania danych](#).

Dokument opisuje nasze obecne podejście i nie ustanawia odrębnych, umownych celów dotyczących czasu odzyskiwania, punktu odzyskiwania, gwarancji trwałości danych, terminów powiadomień, poziomów świadczenia usług ani standardów odpowiedzialności wykraczających poza te wyrażnie określone w mającej zastosowanie umowie, DPA lub SLA.

1. Cele i zakres

ProcessMind utrzymuje niniejsze procedury w celu:

- ochrony poufności, integralności i dostępności Danych Klienta podczas zdarzenia zakłócającego działanie
- przywracania krytycznych komponentów usługi produkcyjnej po awariach systemów kontrolowanych przez ProcessMind
- zapewnienia ciągłości zarządzania incydentami, komunikacji z klientami i podejmowania decyzji operacyjnych podczas zakłóceń w świadczeniu usług
- przywracania działania po awariach infrastruktury, wdrożeń, aplikacji lub warstwy danych z wykorzystaniem udokumentowanych procedur i definicji infrastruktury kontrolowanych za pomocą systemu kontroli wersji
- identyfikowania i oceny Incydentów bezpieczeństwa, powstrzymywania zagrożeń, usuwania ich przyczyn źródłowych,

przywracania działania systemów, których dotyczyły, przekazywania wymaganych informacji oraz wyciągania wniosków

Niniejsze procedury mają zastosowanie do produkcyjnej usługi chmurowej ProcessMind oraz zdarzeń związanych z bezpieczeństwem, w które zaangażowani są podwykonawcy przetwarzania lub usługi chmurowe, w zakresie, w jakim wpływają one na Usługę i mieszczą się w granicach uzasadnionych możliwości ProcessMind w zakresie ich zbadania i zarządzania nimi. Środowiska programistyczne i testowe są odseparowane i nie są traktowane jako cele odtwarzania w ramach zobowiązań dotyczących produkcji udostępnianej klientom.

2. Strategia odporności

2.1 Projekt regionalny. Usługi produkcyjne są hostowane w AWS EU (Frankfurt, Niemcy, eu-central-1). Architektura opiera się na zarządzanych przez AWS usługach w tym regionie, które AWS obsługuje w wielu strefach dostępności. Klaster Aurora działa obecnie z pojedynczą instancją zapisującą, dlatego odtwarzanie bazy danych opiera się na automatycznych kopiach zapasowych i odtwarzaniu do określonego punktu w czasie, a nie na instancji zapasowej w tym samym regionie. ProcessMind nie obsługuje obecnie drugiego aktywnego regionu danych klientów.

2.2 Usługi zarządzane i bezserwerowe. ProcessMind korzysta z AWS Lambda, Amazon API Gateway, Amazon CloudFront, Amazon Aurora PostgreSQL, Amazon S3, Amazon SQS, Amazon SNS i Amazon CloudWatch. Ogranicza to zależność od serwerów zarządzanych przez klienta i działających przez długi czas oraz umożliwia odtwarzanie komponentów aplikacji i statycznych na podstawie kodu źródłowego.

2.3 Rozdzielenie środowisk. Środowiska produkcyjne i programistyczne działają na oddzielnych kontach AWS, z oddzielnymi bazami danych i stosami infrastruktury. Ogranicza to ryzyko, że działania programistyczne wpłyną na operacje odtwarzania środowiska produkcyjnego.

2.4 Monitorowanie i wykrywanie. Alarmy CloudWatch, dashboardy, alerty dotyczące kolejek wiadomości niedostarczonych, scentralizowane rejestrowanie oraz syntetyczne monitorowanie usług wspierają wykrywanie incydentów, ich wstępną ocenę i eskalację. Potencjalne incydenty mogą być również identyfikowane na podstawie zgłoszeń do pomocy technicznej, raportów pracowników, powiadomień od dostawców lub innych przesłanek do wszczęcia dochodzenia.

3. Priorytety odtwarzania

W przypadku poważnego incydentu priorytety ProcessMind w zakresie odtwarzania są zasadniczo następujące:

1. Ochrona integralności danych klientów i zapobieganie dalszym szkodom.
2. Ograniczenie incydentu i ustabilizowanie systemów, których dotyczy.
3. Przywrócenie podstawowych ścieżek dostępu do środowiska produkcyjnego i krytycznych workflow.
4. Weryfikacja działania usługi, integralności danych i monitorowania przed uznaniem odtwarzania za zakończone.
5. Przekazywanie aktualizacji statusu, informacji o wpływie na klientów i działaniach następnych.

Dokładna kolejność może się różnić w zależności od charakteru incydentu, w tym od tego, czy wpływa on na integralność danych, dostęp klientów, przetwarzanie asynchroniczne czy infrastrukturę pomocniczą.

4. Procedury odtwarzania po awarii

4.1 Zgłoszenie incydentu i koordynacja. Poważne zakłócenia w świadczeniu usług i incydenty związane z bezpieczeństwem są wstępnie oceniane zgodnie z procedurami reagowania na incydenty. ProcessMind wyznacza osobę kierującą incydem, ogranicza udział w reagowaniu do upoważnionego personelu, ocenia wagę i zakres incydentu, koordynuje

działania osób reagujących technicznie oraz śledzi działania naprawcze do czasu rozwiązania incydentu lub obniżenia jego kategorii.

4.2 Ograniczanie skutków. ProcessMind dokłada uzasadnionych komercyjnie starań, aby zatrzymać lub ograniczyć trwające skutki, zanim rozpocznie się szersze przywracanie działania. W zależności od rodzaju awarii działania ograniczające skutki mogą obejmować wycofanie ostatnich zmian, wyłączenie dotkniętych ścieżek, odizolowanie wadliwie działających komponentów, wstrzymanie przetwarzania w tle na czas przeprowadzania kontroli integralności, unieważnienie lub rotację danych uwierzytelniających albo blokowanie nadużyć.

4.3 Usunięcie przyczyny. Po ustabilizowaniu bezpośrednich skutków ProcessMind podejmuje działania w celu usunięcia przyczyny źródłowej lub czynnika, który się do nich przyczynił. Może to obejmować zastosowanie poprawek kodu lub konfiguracji, usunięcie złośliwych artefaktów, rotację kluczy tajnych, przywrócenie zaufanej konfiguracji lub zamknięcie ujawnionych ścieżek dostępu.

4.4 Odtwarzanie bazy danych. Aurora PostgreSQL wykonuje ciągłe automatyczne kopie zapasowe z siedmiodniowym (7) okresem przechowywania i obsługuje odtwarzanie do określonego punktu w czasie. Jeżeli awaria na poziomie bazy danych, zdarzenie związane z uszkodzeniem danych lub przypadkowa destrukcyjna zmiana wymaga odtworzenia, ProcessMind może odtworzyć bazę z najnowszej odpowiedniej kopii zapasowej lub do wybranego punktu w czasie, zweryfikować odtworzone środowisko i skierować ruch aplikacji z powrotem do odtworzonej bazy danych.

4.5 Odtwarzanie obiektów i artefaktów. Pliki przesyłane przez klientów i artefakty operacyjne są przechowywane w Amazon S3. Włączono wersjonowanie w zasobniku przesyłanych plików i zasobnikach zasobów, aby umożliwić odtwarzanie po przypadkowym usunięciu lub nadpisaniu. Zasobniki wdrożeniowe witryny internetowej i interfejsu frontendowego są traktowane jako odtwarzalne artefakty i mogą być ponownie tworzone na podstawie kodu źródłowego, zamiast odtwarzania z kopii zapasowych.

4.6 Odtwarzanie przetwarzania asynchronicznego. W asynchronicznych ścieżkach przetwarzania wykorzystywane są kolejki wiadomości niedostarczonych, w których przechowywane są nieudane zdarzenia na potrzeby dochodzenia. Odtwarzanie może obejmować ponawianie nieudanych wiadomości, ponowne uruchamianie logiki przetwarzania lub ponowne odtwarzanie zadań, jeżeli dany workflow umożliwia ich bezpieczne ponowne przetworzenie.

4.7 Odtwarzanie aplikacji i infrastruktury. Infrastruktura jest zarządzana za pomocą definicji infrastruktury jako kodu kontrolowanych w systemie kontroli wersji. Jeżeli konieczne jest ponowne utworzenie infrastruktury aplikacji lub zasobów statycznych, ProcessMind może ponownie utworzyć i wdrożyć dotknięte komponenty na podstawie definicji kontrolowanych w systemie kontroli wersji i artefaktów kompilacji.

4.8 Weryfikacja przed przywróceniem usługi. Przed zamknięciem incydentu ProcessMind weryfikuje stan usługi za pomocą dostępnych narzędzi monitorowania, dzienników, testów syntetycznych i ukierunkowanej weryfikacji funkcjonalnej oraz przywraca działanie dotkniętych funkcji, stosując zweryfikowane procedury wdrażania, odtwarzania i obsługi infrastruktury. W przypadku incydentu obejmującego odtwarzanie danych lub ryzyko naruszenia ich integralności może zostać przeprowadzona dodatkowa kontrola.

5. Środki zapewnienia ciągłości działania

5.1 Ciągłość operacyjna. ProcessMind utrzymuje udokumentowane procedury operacyjne, aby obsługa incydentów, przyjmowanie zgłoszeń do pomocy technicznej, reagowanie zespołu inżynieryjnego i podejmowanie decyzji mogły być kontynuowane podczas zdarzeń zakłócających działanie.

5.2 Komunikacja. W przypadku poważnych incydentów produkcyjnych ProcessMind dokłada uzasadnionych komercyjnie starań, aby przekazywać aktualizacje za pośrednictwem kanałów pomocy technicznej dla klientów

oraz, w stosownych przypadkach, publicznej strony statusu pod adresem processmind.com/status.

5.3 Kontrolowane zarządzanie zmianami. W celu ograniczenia możliwych do uniknięcia przerw w działaniu i stopniowego poprawiania ciągłości stosuje się wielowarstwowy cykl życia oprogramowania, obejmujący wiele niezależnych, zautomatyzowanych warstw walidacji, kontrolowane wdrożenia, scentralizowane monitorowanie i przegląd po incydencie.

5.4 Bezpieczeństwo podczas odtwarzania. Działania związane z odtwarzaniem są prowadzone zgodnie z tymi samymi ogólnymi zasadami bezpieczeństwa, które mają zastosowanie podczas normalnych operacji, w tym z zasadą minimalnych uprawnień, rejestrowaniem działań operacyjnych, gdy jest to możliwe, oraz kontrolowanym dostępem do systemów i danych produkcyjnych.

6. Podsumowanie dotyczące kopii zapasowych i ochrony danych

6.1 Kopie zapasowe baz danych. Automatyczne kopie zapasowe Aurora są szyfrowane i przechowywane przez siedem (7) dni; w tym okresie dostępne jest odtwarzanie do określonego punktu w czasie.

6.2 Zabezpieczenia S3. Amazon S3 zapewnia wysoką trwałość przechowywanych obiektów. Zmienne zasobniki danych klientów opierają się na trwałości i wersjonowaniu w regionie podstawowym. ProcessMind nie włączył obecnie replikacji między regionami S3 dla tych zasobników.

6.3 Dzienniki i diagnostyka. Scentralizowane dzienniki, alarmy i dane telemetryczne wspierają badanie awarii i weryfikację odtwarzania. Mechanizmy te wspierają działania na rzecz ciągłości, ale same w sobie nie są przedstawiane jako odrębny produkt do tworzenia kopii zapasowych.

7. Identyfikacja incydentów i ich wstępna ocena

7.1 Wstępna ocena. Zgłoszone zdarzenia są wstępnie oceniane w celu ustalenia, czy spełniają definicję Incydentu bezpieczeństwa, jakich systemów lub danych mogą dotyczyć, jaki jest prawdopodobny zakres i waga zdarzenia oraz czy konieczne jest natychmiastowe ograniczenie jego skutków. Dowody są zabezpieczane w sposób odpowiedni do charakteru incydentu i zaangażowanych systemów.

7.2 Dyżury i eskalacja. ProcessMind zapewnia dyżury na potrzeby incydentów produkcyjnych, w tym całodobową obsługę krytycznych incydentów (zgodnie z definicją w Umowie o poziomie usług), tak aby incydenty mogły być przyjmowane i wstępnie oceniane o każdej porze.

7.3 Dokumentacja. ProcessMind dokumentuje istotne ustalenia z dochodzenia, działania podjęte w ramach reagowania oraz decyzje dotyczące odtwarzania, aby po zdarzeniu można było przeanalizować chronologię incydentu i wynikające z niego działania naprawcze.

8. Komunikacja i powiadomienia

8.1 Komunikacja wewnętrzna. ProcessMind koordynuje działania osób reagujących, decydentów i kanałów pomocy technicznej, tak aby reagowanie techniczne i komunikacja z klientami pozostawały spójne przez cały cykl życia incydentu.

8.2 Powiadamianie klientów. W przypadku Incydentu bezpieczeństwa wymagającego powiadomienia na podstawie DPA lub obowiązującego prawa ProcessMind powiadamia klientów, których dotyczy incydent, bez zbędnej zwłoki, a jeśli jest to wykonalne – w ciągu siedemdziesięciu dwóch (72) godzin od uzyskania wiedzy o incydencie. Powiadomienia zasadniczo zawierają informacje o charakterze i zakresie incydentu, kategoriach danych, których dotyczy, jeśli są znane, środkach podjętych w celu ograniczenia skutków i usunięcia incydentu oraz zalecanych działaniach klientów, jeśli są istotne.

8.3 Bieżące aktualizacje. Jeżeli incydent nadal trwa lub istotne fakty ulegną zmianie, ProcessMind przekazuje dalsze aktualizacje w miarę uzyskiwania dodatkowych, zweryfikowanych informacji. W przypadku szerszych zakłóceń w świadczeniu usług produkcyjnych ProcessMind może również korzystać z kanałów pomocy technicznej dla klientów oraz, w stosownych przypadkach, publicznej strony statusu pod adresem processmind.com/status.

9. Testowanie, przegląd i utrzymanie

ProcessMind dokonuje przeglądu niniejszych procedur co najmniej raz w roku oraz po poważnych incydentach lub istotnych zmianach architektury, okresowo testuje odpowiednie elementy podejścia do reagowania i odtwarzania (takie jak przywracanie kopii zapasowych, ponowne tworzenie wdrożeń, monitorowanie, alertowanie i komunikacja dotycząca incydentów) oraz uwzględnia wyciągnięte wnioski w procedurach dotyczących bezpieczeństwa, niezawodności i ciągłości działania.

10. Ograniczenia i granice umowne

Niniejszy dokument stanowi ogólne podsumowanie i nie opisuje szczegółowo wszystkich wewnętrznych instrukcji operacyjnych, ścieżek eskalacji, metod dochodzeniowych ani czynności związanych z postępowaniem z dowodami. Nie zobowiązuje on ProcessMind do wdrożenia odrębnego projektu przełączania awaryjnego między regionami, niezmiennego przechowywania wszystkich zmiennych zasobników ani niezależnych gwarancji RTO/RPO wykraczających poza to, co wyraźnie określono w odpowiedniej umowie lub zamówieniu.

W przypadku jakiegokolwiek sprzeczności między niniejszym dokumentem a odpowiednią Umową z Klientem, Dodatkiem dotyczącym przetwarzania danych, Umową o poziomie usług lub bezwzględnie obowiązującymi przepisami prawa, pierwszeństwo mają te dokumenty lub przepisy.