Oświadczenie ProcessMind dotyczące dziennika audytowego i SIEM

Data wejścia w życie: 12 listopada 2026 r.

Niniejsze oświadczenie opisuje, w jaki sposób ProcessMind B.V. rejestruje działania związane z bezpieczeństwem i działania administracyjne wykonywane w odniesieniu do Danych Klienta ("dziennik audytowy"). Uzupełnia ono Środki bezpieczeństwa, Dodatek dotyczący przetwarzania danych, Umowę z Klientem oraz Listę podmiotów przetwarzających.

---

1. Zakres

1.1 Jeden dziennik audytowy. ProcessMind prowadzi jeden dziennik audytowy dotyczący działań związanych z bezpieczeństwem i działań administracyjnych wykonywanych w odniesieniu do Danych Klienta i Usługi ProcessMind. Dziennik audytowy jest odrębny od rejestrowania operacyjnego (aplikacyjnego), rejestrowania dostępu HTTP oraz kanału aktywności produktu; strumienie te służą różnym celom i nie są przedstawiane jako ścieżka audytowa.

1.2 Czym dziennik nie jest. Dziennik audytowy nie stanowi zapisu każdego odczytu Danych Klienta ani historii zmian produktu dotyczącej modeli procesów, diagramów, dokumentacji lub symulacji. Są one rejestrowane w historii zmian procesu dostępnej w produkcie.

---

2. Zawartość każdego zapisu audytowego

2.1 Pola. Każdy zapis zawiera wymienione poniżej pola. Ich zestaw jest określony w schemacie zapisu: zapis nie może zawierać pola spoza tej listy, a działanie nie może dodać pola, którego nie zadeklarowano w rejestrze.

- *schemaVersion* (liczba): wersja schematu zapisu, obecnie 1.
- *eventId* (ciąg znaków): unikalny identyfikator zapisu. Nowe zapisy używają ULID; wiersze przeniesione z wcześniejszego magazynu

zachowują UUID.

- *occurredAt*, *ingestedAt* (znaczniki czasu): kiedy nastąpiło działanie oraz kiedy zapis został zapisany przez mechanizm rejestrujący audyt. Oba czasy podane w UTC.
- *eventClass* (wyliczenie): security, auth, admin, data, api, ai lub platform.
- *action* (wyliczenie): jeden kod z zamkniętego, podlegającego przeglądowi rejestru działań, na przykład auth.login.blocked lub api.key.revoked.
- *outcome* (wyliczenie): success, failure, denied lub error.
- *severity* (wyliczenie): info, notice, warning lub critical, określane na podstawie wyniku. Dla działania zakończonego powodzeniem stosowana jest wartość domyślna z rejestru (info, chyba że dla danego działania określono inaczej), niepowodzenie jest rejestrowane jako notice, a odmowa lub błąd jako warning.
- *actor* (obiekt): podmiot, który wykonał działanie. type (user, apiKey, service, system lub anonymous), id, email, displayName oraz onBehalfOf i onBehalfOfEmail, jeśli działanie wykonano w imieniu innego konta.
- *actorContext* (obiekt): sesja, w ramach której wykonano działanie. sessionId, authMethod (oidc, password, loginToken, apiKey lub none) oraz flaga sesji pomocy technicznej.
- *organizationId*, *tenantId* (identyfikatory, dopuszczające wartość null): organizacja i środowisko, których dotyczy działanie. Wartość null w przypadku zapisów niedotyczących żadnego klienta lub znajdujących się powyżej poziomu środowiska.
- *resource* (obiekt, dopuszczający wartość null): obiekt, którego dotyczy działanie. type, id i name, gdzie type przyjmuje jedną z wartości: apiKey, artifact, connection, database, datatable, export, lead, model, organization, process, role, session, setting, storage, tenant lub user.
- *source* (obiekt): miejsce utworzenia zapisu. service (api, externalApi, superadminApi, worker, cron lub webSocket), function i version.

- *stage*, *region* (ciągi znaków): etap wdrożenia, w którym utworzono zapis (na przykład prod), oraz region AWS (eu-central-1 w przypadku zapisów dotyczących klientów).
- *correlation* (obiekt): requestId, traceId i parentEventId, które wiążą zapis z żądaniem, które go spowodowało, oraz z wcześniejszymi zapisami w tym samym przepływie.
- *network* (obiekt, dopuszczający wartość null): sourceIp i userAgent. Rejestrowane wyłącznie w przypadku działań, dla których wpis w rejestrze przewiduje takie dane: logowanie, decyzje dotyczące dostępu, zmiany administracyjne i zmiany ustawień, przesyłanie, pobieranie i eksport danych, zmiany kluczy API oraz zmiany zasad dotyczących AI.
- *detail* (obiekt): własny ładunek danych działania, zweryfikowany względem schematu tego działania. Wartości mogą być wyłącznie typami prostymi (ciąg znaków, liczba, wartość logiczna, null), dzięki czemu zapis pozostaje możliwy do przeszukiwania i redagowania.

2.2 Zamknięty słownik. Działania pochodzą ze stałej, podlegającej przeglądowi listy kodów działań; zapis audytowy nie zawiera dowolnego tekstu. Każde działanie określa również, jakie dodatkowe pola może zawierać, dzięki czemu zapis nie może po cichu zyskać nowego rodzaju treści.

---

3. Rejestrowane działania

3.1 Obecnie rejestrowane. ProcessMind rejestruje między innymi:

- **Uwierzytelnianie:** pomyślne i nieudane logowania, zablokowane logowania (zablokowane konto, niedozwolona domena, niezweryfikowany adres e-mail dostawcy tożsamości), wylogowania, wydanie tokenu logowania i przekazanie go.
- **Autoryzacja:** odmowy dostępu, w tym każde odrzucenie danych uwierzytelniających zewnętrznego API, zakresu uprawnień i stanu dzierżawcy, a także odrzucenia pochodzenia (CORS).

- **Dostęp pomocy technicznej:** rozpoczęcie sesji pomocy technicznej ProcessMind na koncie klienta, ze wskazaniem zarówno operatora, jak i konta, którego dotyczy działanie.
- **Dane uwierzytelniające API:** utworzenie, zmiana zakresu uprawnień i unieważnienie kluczy API, w tym przyznane zakresy uprawnień.
- **Administracja kontami i rolami:** tworzenie użytkowników, wysyłanie zaproszeń, edycja profili administratorów, usuwanie, przyznawanie i odbieranie ról oraz zmiany członkostwa w dzierżawcy lub organizacji.
- **Cykl życia organizacji:** tworzenie, usuwanie, przywracanie, planowanie usunięcia i jego anulowanie oraz zakończone usunięcie danych.
- **Przesyłanie, pobieranie i eksport danych:** przesyłanie, pobieranie i usuwanie artefaktów, przesyłanie i aktualizowanie danych tabelarycznych, pobieranie eksportów, usuwanie tabel danych oraz tworzenie, zmienianie i usuwanie webhooków (połączeń).
- **Stan rozliczeń:** zmiany planu, zawieszenie i przywrócenie usługi z powodu płatności oraz anulowanie subskrypcji.
- **Konsola dostawcy ProcessMind:** wykonywanie uprzywilejowanych zapytań, administracja użytkownikami i organizacjami, zmiany ustawień i funkcji, żądania synchronizacji rozliczeń oraz migracje.
- **Działania administracyjne i destrukcyjne wykonywane przez zaplanowane zadania ProcessMind:** usuwanie dzierżawców, organizacji, użytkowników i potencjalnych klientów, przeglądy retencji oraz błędy potoków przetwarzania.
- **Integralność dziennika audytowego:** niepowodzenia własnej ścieżki zapisu dziennika audytowego.

3.2 Edycje w obszarze roboczym. Edycje w obszarze roboczym (modele procesów, dokumentacja, symulacje, dashboardy, komentarze i zakładki) są rejestrowane w historii zmian procesu w produkcie, a nie w dzienniku audytowym. Dziennik audytowy rejestruje, kto przesłał, pobrał, wyeksportował lub usunął dane; historia zmian rejestruje, co zmieniono w modelu. Aktualna lista rejestrowanych kodów działań jest dostępna na żądanie w ProcessMind.

4. Informacje, które nigdy nie są rejestrowane

Hasła, tokeny uwierzytelniające, wartości kluczy API, pliki cookie, nagłówki autoryzacyjne, treść żądań lub odpowiedzi, zawartość plików, wstępnie podpisane adresy URL oraz prompty lub odpowiedzi AI nigdy nie są zapisywane w dzienniku audytowym. Zapisy audytowe mogą zawierać dane osobowe niezbędne do przypisania działania do podmiotu: adres e-mail podmiotu wykonującego działanie oraz źródłowy adres IP i user agent w przypadku działań, dla których wpis w rejestrze przewiduje takie dane (logowanie, decyzje dotyczące dostępu, zmiany administracyjne i zmiany ustawień, przenoszenie danych, zmiany kluczy API i zasad dotyczących AI). Dozwolone pola są określane dla każdego działania i podlegają przeglądowi przy dodawaniu działania.

---

5. Integralność

5.1 Tylko dopisywanie. Dziennik audytowy jest przeznaczony wyłącznie do dopisywania. Żadna rola aplikacji nie ma uprawnień do jego aktualizowania ani usuwania, a ograniczenie bazy danych odrzuca obie te operacje.

5.2 Jeden mechanizm zapisujący. Zapisy są tworzone przez jeden komponent, który przed zapisem weryfikuje kod działania i jego ładunek danych. Zapis, który nie przejdzie weryfikacji, jest odrzucany i zgłaszany, zamiast być zapisany częściowo.

5.3 Obsługa błędów. Nieudany zapis audytowy nigdy nie powoduje niepowodzenia opisywanego działania biznesowego. Jest rejestrowany w monitorowanej i alarmowanej ścieżce operacyjnej, a sam zapis jest zachowywany w kopii zapasowej, aby można go było odzyskać.

---

6. Okres przechowywania i lokalizacja

6.1 Okres przechowywania. Zapisy audytowe są przechowywane przez co najmniej dziesięć (10) lat od daty zdarzenia.

6.2 Lokalizacja i szyfrowanie. Zapisy audytowe są przechowywane w Unii Europejskiej (Frankfurt, Niemcy, `eu-central-1`) i szyfrowane w stanie spoczynku przy użyciu klucza AWS KMS zarządzanego przez klienta. Kopia bieżąca jest dodatkowo zapisywana w grupie dzienników Amazon CloudWatch z kontrolą dostępu, aby umożliwić badanie incydentu w trakcie jego trwania.

6.3 Brak replikacji między regionami. Zapisy audytowe nie są replikowane poza Unię Europejską.

---

7. Dostęp do zapisów audytowych

7.1 Uprawnienia. Dziennik audytowy dostępny w aplikacji jest objęty planem Process Architecture i planami wyższymi. Administrator organizacji może odczytywać dane całej organizacji; administrator z zakresem ograniczonym do dzierżawcy może odczytywać dane własnego dzierżawcy. Zakres jest ustalany na podstawie uwierzytelnionej sesji i sprawdzany przed wykonaniem zapytania, dlatego żądanie nie może rozszerzyć go na innego dzierżawcę ani inną organizację.

7.2 Personel ProcessMind. Personel ProcessMind uzyskuje dostęp do zapisów audytowych wyłącznie w celu świadczenia pomocy technicznej, reagowania na incydenty lub wypełnienia obowiązku prawnego, w zakresie niezbędnym do realizacji tych celów. Dostęp do danych wielu klientów jest ograniczony do dedykowanej roli pomocy technicznej, a taki dostęp sam w sobie stanowi działanie administracyjne.

7.3 Sposób uzyskania zapisów. Administratorzy organizacji i dzierżawcy mogą odczytywać swoje zapisy audytowe w dzienniku audytowym dostępnym w aplikacji oraz pobierać je lub eksportować za pośrednictwem zewnętrznego API. W przypadku większego żądania lub żądania

wymagającego pomocy ProcessMind udostępnia zapisy w formacie CSV lub JSON dla wskazanej organizacji, dzierżawcy i zakresu czasu; standardowe żądanie jest realizowane w ciągu pięciu (5) dni roboczych.

---

8. Usuwanie zapisów audytowych

8.1 Na żądanie. Po otrzymaniu zweryfikowanego pisemnego żądania ProcessMind usuwa z magazynu audytowego zapisy audytowe dotyczące organizacji klienta i potwierdza usunięcie na piśmie. Kopii operacyjnej w CloudWatch nie można edytować zapis po zapisie; wygasa ona zgodnie z własnym okresem przechowywania.

8.2 Informacje przechowywane. Zapis potwierdzający dokonanie usunięcia (identyfikator organizacji, data, wnioskodawca, powód i liczba usuniętych zapisów) jest przechowywany jako zapis audytowy na poziomie platformy i nie zawiera Danych Klienta. Żądanie usunięcia danych klienta nie wpływa na zapisy niedotyczące żadnego klienta (zdarzenia platformy ProcessMind).

8.3 Żądania usunięcia dotyczące osób fizycznych. Jeżeli żądanie dotyczy osoby fizycznej będącej częścią klienta, który nadal jest aktywny, zapis dotyczący bezpieczeństwa jest przechowywany w celu ustalenia, dochodzenia lub obrony roszczeń prawnych, zgodnie z art. 17 ust. 3 lit. b) i e) RODO; podstawa ta jest odnotowywana w rejestrze czynności przetwarzania oraz w Polityce prywatności.

---

9. Integracja z SIEM i eksport

9.1 Dostępność. Niezmienialne archiwum audytowe jest opcją Enterprise, włączaną dla organizacji klienta na żądanie. Zapisuje codziennie skompresowane obiekty NDJSON pod prefiksem przypisanym do danej organizacji w zasobniku S3 z blokadą obiektów (WORM), wraz z manifestem i nocnym uzgadnianiem.

9.2 Obecny sposób dostarczania. ProcessMind nie oferuje obecnie natywnego łącznika SIEM ani strumienia danych typu push. Dane są pobierane z trzech źródeł: API odczytu (`GET /v1/tenant/{tenantId}/audit`), ograniczonego zadania eksportu (utwórz je za pomocą `POST /v1/tenant/{tenantId}/audit/exports` i pobierz wynik za pośrednictwem wywołania statusu, które zwraca krótkotrwały adres URL pobierania) oraz, w przypadku archiwum Enterprise, codziennych obiektów pod własnym prefiksem organizacji w zasobniku z blokadą obiektów, odczytywanych przez SIEM klienta na podstawie uzgodnionego dostępu. ProcessMind nie dostarcza zapisów do wybranej przez klienta lokalizacji według własnego harmonogramu.

9.3 Własne monitorowanie ProcessMind. Monitorowanie bezpieczeństwa ProcessMind korzysta z tych samych zapisów: nieudane zapisy audytowe, serie nieudanych uwierzytelnień, zmiany uprawnień i destrukcyjne działania administracyjne wywołują wewnętrzne alarmy.

---

10. Dowody dostępne dla klientów

Na żądanie i, w stosownych przypadkach, z zachowaniem poufności ProcessMind udostępnia niniejsze oświadczenie, Środki bezpieczeństwa, Dodatek dotyczący przetwarzania danych, Listę podmiotów przetwarzających, zredagowany przykładowy zestaw zapisów audytowych oraz procedurę stosowaną w przypadku żądań dostępu i usunięcia.

---

11. Ograniczenia

Dla uniknięcia wątpliwości ProcessMind deklaruje, że dla każdej organizacji prowadzi magazyn audytowy przeznaczony wyłącznie do dopisywania, a w przypadku włączenia uprawnienia do archiwum audytowego — kopię z blokadą obiektów (WORM) i nocnym uzgadnianiem manifestu.
ProcessMind nie deklaruje obecnie stosowania łańcucha skrótów, natywnego łącznika SIEM typu push działającego w czasie rzeczywistym,

redagowania zapisów audytowych dla poszczególnych użytkowników, poświadczenia zgodności z ISO 27001 lub SOC 2 obejmującego tę kontrolę ani rejestrowania każdego odczytu Danych Klienta. Klienci mogą samodzielnie odczytywać i eksportować dane za pośrednictwem dziennika audytowego dostępnego w aplikacji oraz zewnętrznego API.