

Środki bezpieczeństwa ProcessMind

Data wejścia w życie: 14 września 2026 r.

Niniejszy dokument opisuje techniczne i organizacyjne środki („TOM”), które ProcessMind B.V. stosuje w celu ochrony poufności, integralności i dostępności Danych klienta. ProcessMind stosuje podejście oparte na wielowarstwowej ochronie, w ramach którego wiele niezależnych warstw zabezpieczeń chroni Dane klienta na każdym poziomie — od sieci i infrastruktury, przez tożsamość, autoryzację, izolację danych, szyfrowanie i monitorowanie, po tworzenie oprogramowania. Środki te uzupełniają [Dodatek dotyczący przetwarzania danych](#), [Politykę prywatności](#) oraz [Politykę hostingu SaaS](#). ProcessMind dokonuje przeglądu tych środków i aktualizuje je co najmniej raz w roku.

Dane klienta nigdy nie są sprzedawane, udostępniane ani wykorzystywane przez osoby trzecie do ich własnych celów.

1. Bezpieczeństwo infrastruktury

1.1 Platforma chmurowa. ProcessMind jest hostowany wyłącznie w Amazon Web Services (AWS) w UE (Frankfurt, Niemcy, eu-central-1). AWS posiada certyfikaty ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3 i PCI DSS. Pełna lista znajduje się w [programach zgodności AWS](#).

1.2 Architektura bezserwerowa. Logika aplikacji ProcessMind działa w AWS Lambda i usługach zarządzanych przez AWS. ProcessMind nie obsługuje długotrwale działających serwerów aplikacji zarządzanych przez klienta, co eliminuje znaczną część prac związanych z instalowaniem poprawek systemu operacyjnego i wzmacnianiem zabezpieczeń serwerów.

1.3 Granice sieci. ProcessMind utrzymuje AWS VPC na potrzeby kontroli bazy danych i sieci. Aurora PostgreSQL działa w podsieciach prywatnych, bez dostępu do internetu na zewnątrz, nie jest publicznie dostępna, a dzienniki przepływu VPC są włączone. Domyślnie ProcessMind nie

umieszcza funkcji Lambda aplikacji w VPC. Funkcje Lambda łączą się z Aurora za pośrednictwem AWS RDS Data API przez TLS, z użyciem uwierzytelniania IAM i Secrets Manager.

1.4 Dostarczanie treści i zabezpieczenia brzegowe. Strona internetowa przeznaczona dla klientów, frontend SPA i ruch dotyczący zasobów publicznych są obsługiwane przez Amazon CloudFront. Wszystkie dystrybucje CloudFront wymuszają minimalną politykę TLS 1.2 (2021). Dystrybucje strony internetowej i frontendu SPA dodają również nagłówki zabezpieczeń odpowiedzi, w tym HTTP Strict Transport Security (HSTS), Content Security Policy (CSP), `frame-ancestors 'none'`, `X-Frame-Options: DENY`, `X-Content-Type-Options`, politykę referrer oraz politykę uprawnień. Dystrybucja zasobów publicznych korzysta z CloudFront Origin Access Control, aby zachować prywatność zasobnika źródłowego. Ruch API przeznaczony dla klientów jest obsługiwany oddzielnie przez Amazon API Gateway: ruch żądań i odpowiedzi HTTPS jest obsługiwany przez HTTP API w dedykowanej subdomenie API, a połączenia klientów w czasie rzeczywistym są obsługiwane przez oddzielne API WebSocket API Gateway w dedykowanej subdomenie WebSocket.

1.5 Rozdzielenie środowisk. Środowiska produkcyjne i programistyczne korzystają z oddzielnych kont AWS, oddzielnych baz danych i oddzielnych stosów infrastruktury. Dane uwierzytelniające programistów nie zapewniają dostępu do produkcyjnych Danych klienta.

2. Szyfrowanie danych

2.1 Szyfrowanie podczas przesyłania. Wszystkie dane przesyłane między klientami a usługami ProcessMind są szyfrowane przy użyciu TLS 1.2 lub nowszego. Punkty końcowe przeznaczone dla klientów są udostępniane przez HTTPS. Zasobniki S3, tematy SNS i kolejki SQS utworzone bezpośrednio przez ProcessMind wymuszają dostęp wyłącznie przez SSL. Dostęp do bazy danych za pośrednictwem RDS Data API oraz inne wywołania usług AWS korzystają z HTTPS/TLS.

2.2 Szyfrowanie przechowywanych danych. Aurora PostgreSQL jest szyfrowana w stanie spoczynku przy użyciu kluczy AWS KMS zarządzanych przez klienta, z automatyczną rotacją kluczy. Zasobniki S3 zawierające dane klientów i dane operacyjne, utworzone bezpośrednio przez ProcessMind, w tym zasobniki przesyłanych plików, zasobów i dzienników dostępu, korzystają z kluczy KMS zarządzanych przez klienta. Grupy dzienników CloudWatch, tematy SNS i kolejki SQS utworzone bezpośrednio przez ProcessMind również korzystają z kluczy KMS zarządzanych przez klienta. Zasobniki źródłowe strony internetowej i frontendu zarządzane przez SST korzystają z szyfrowania po stronie serwera S3 zarządzanego przez AWS (SSE-S3 / AES-256), a nie z kluczy KMS zarządzanych przez klienta.

2.3 Zarządzanie kluczami i danymi poufnymi. Klucze szyfrujące bazę danych są zarządzane centralnie za pośrednictwem AWS KMS, a dostęp do kluczy podlega politykom IAM opartym na zasadzie najmniejszych uprawnień. Dane uwierzytelniające do bazy danych są przechowywane w AWS Secrets Manager. Główny sekret Aurora oraz sekret ograniczonego użytkownika aplikacji są automatycznie rotowane co trzydzieści (30) dni. Klucze i sekrety produkcyjne nigdy nie są przechowywane w kodzie źródłowym; dane uwierzytelniające używane wyłącznie w środowisku programistycznym są odizolowane od środowiska produkcyjnego. Niektóre zasoby pomocnicze zarządzane przez AWS/CDK/SST nadal korzystają z szyfrowania zarządzanego przez AWS, gdy usługa lub platforma nie udostępnia konfiguracji kluczy zarządzanych przez klienta.

3. Izolacja i lokalizacja danych

3.1 Izolacja dzierżawców. Każdy dzierżawca będący klientem otrzymuje dedykowaną, odizolowaną instancję bazy danych. Dane klienta nigdy nie są łączone z danymi innych klientów na poziomie bazy danych. Wspólne metadane (np. rekordy kont, rozliczenia, mapowania użytkowników na dzierżawców) są przechowywane w oddzielnej bazie danych obsługującej wielu dzierżawców, z rygorystyczną kontrolą dostępu. Współdzielone tabele o zakresie ograniczonym do dzierżawcy lub organizacji są dodatkowo

chronione przez polityki zabezpieczeń na poziomie wierszy PostgreSQL (RLS), egzekwowane za pośrednictwem kontekstu bazy danych określonego dla danego żądania.

3.2 Lokalizacja danych. Wszystkie Dane klienta, w tym bazy danych, przesłane pliki, kopie zapasowe i wyniki zapytań, są przechowywane wyłącznie w UE (Frankfurt, Niemcy). Jeżeli do określonej czynności przetwarzania zaangażowany zostanie podmiot przetwarzający zlokalizowany poza EOG (na przykład w celu przetwarzania przez model AI lub obsługi płatności), przekazanie danych jest objęte odpowiednim mechanizmem przekazywania opisanym w Dodatku dotyczącym przetwarzania danych, a podmiot przetwarzający i miejsce przetwarzania są wymienione na Liście podmiotów przetwarzających.

3.3 Przechowywanie i usuwanie danych. Terminy przechowywania i usuwania określono w sekcji 6 [Dodatku dotyczącego przetwarzania danych](#). Klienci mogą w dowolnym momencie usunąć swoje dane za pośrednictwem aplikacji lub kontaktując się z ProcessMind. Kopie zapasowe są usuwane po upływie właściwych okresów ich przechowywania (sekcja 7.1).

4. Zarządzanie tożsamością i dostępem

4.1 Uwierzytelnianie. ProcessMind obsługuje jednokrotne logowanie (SSO) za pośrednictwem Microsoft Entra ID (Azure AD), Google OAuth 2.0/OIDC i LinkedIn OAuth 2.0/OIDC. ProcessMind działa jako strona ufająca i nie przechowuje haseł użytkowników. Uwierzytelnianie wieloskładnikowe jest wymuszane przez dostawcę tożsamości – na przykład gdy organizacja łączy się z Microsoft Entra ID (Azure AD), zastosowanie mają własne zasady MFA i dostępu tej organizacji.

4.2 Zarządzanie sesjami. Sesje przeglądarki korzystają z podpisanych tokenów JSON Web Token (JWT), przesyłanych za pośrednictwem bezpiecznych plików cookie HttpOnly z flagami SameSite i Secure. Podpisy tokenów są weryfikowane przy każdym uwierzytelnionym żądaniu.

4.3 Model autoryzacji. ProcessMind nie opiera się na natywnych mechanizmach autoryzacji API Gateway w przypadku podstawowych interfejsów API aplikacji. Autoryzacja jest egzekwowana we wspólnych opakowaniach procedur obsługi Lambda, które weryfikują stan sesji i zakres dzierżawcy przed uruchomieniem logiki biznesowej. Trasy publiczne są jawnie umieszczone na liście dozwolonych dla przepływów nieuwierzytelnionych, webhooków, przyjmowania zdarzeń i wstępnych żądań CORS. Zewnętrzne punkty końcowe API korzystają z dedykowanych procedur obsługi uwierzytelniania. Dostęp do Danych klienta jest ograniczony do kontekstu uwierzytelnionego dzierżawcy lub organizacji.

4.4 Zasada najmniejszych uprawnień. Systemy wewnętrzne działają zgodnie z zasadą najmniejszych uprawnień. Zakres ról IAM jest ograniczany do minimalnego zestawu wymaganych zasobów, o ile platforma umożliwia precyzyjne określenie zakresu. Niektóre role generowane przez SST/CDK korzystają z szerszych zarządzanych lub wbudowanych polityk na potrzeby powiązań i działania w środowisku wykonawczym; przypadki te są weryfikowane, w miarę możliwości ograniczane do konkretnych zasobów i rejestrowane jako jawne wyjątki.

4.5 Kontrola dostępu pracowników. Dostęp pracowników do systemów wewnętrznych jest zarządzany za pośrednictwem Active Directory z SSO i obowiązkowym MFA. Kontrola dostępu oparta na rolach (RBAC) zapewnia, że dostęp do Danych klienta mają wyłącznie upoważnione osoby, którym jest on niezbędny do wykonywania obowiązków. Uprawnienia dostępu są okresowo weryfikowane.

5. Rejestrowanie, monitorowanie i audyt

5.1 Scentralizowane rejestrowanie. Rejestrowanie dostępu do HTTP API i WebSocket jest włączone; dzienniki zawierają ustrukturyzowane pola JSON i są zapisywane w Amazon CloudWatch Logs z okresem przechowywania wynoszącym jeden (1) rok. Te grupy dzienników dostępu są szyfrowane kluczem AWS KMS zarządzanym przez klienta. Dzienniki aplikacji są

centralizowane w grupach dzienników Amazon CloudWatch szyfrowanych kluczem AWS KMS zarządzanym przez klienta i przechowywane przez dziesięć (10) lat. Oddzielne grupy dzienników audytowych i telemetrycznych są również szyfrowane kluczem AWS KMS zarządzanym przez klienta i przechowywane przez dziesięć (10) lat. Grupa eksportu dzienników silnika Aurora PostgreSQL jest przechowywana przez jeden (1) tydzień.

5.2 Zakres rejestrowanych i nierejestrowanych informacji. ProcessMind rejestruje zdarzenia dostępu do HTTP API i WebSocket – czas żądania, identyfikatory żądań, trasę lub ścieżkę, status odpowiedzi i opóźnienie. Dzienniki dostępu nie zawierają źródłowego adresu IP ani agenta użytkownika osoby wywołującej. ProcessMind rejestruje również zdarzenia uwierzytelniania, ścieżki błędów przetwarzania asynchronicznego oraz pomocniczą aktywność aplikacji Lambda w scentralizowanych grupach dzienników CloudWatch. Dzienniki przepływu VPC są włączone. Obecnie ProcessMind nie włącza standardowego rejestrowania dostępu CloudFront dla dystrybucji strony internetowej, frontendu SPA ani zasobów publicznych.

5.3 Monitorowanie i alerty. Alarmy i dashboardy CloudWatch monitorują stan systemu, kolejki komunikatów niedostarczonych oraz awarie istotne z punktu widzenia bezpieczeństwa. Błędy przetwarzania asynchronicznego są kierowane do szyfrowanych kolejek komunikatów niedostarczonych (okres przechowywania wynosi czternaście (14) dni; w przypadku kolejek miniatur i indeksu wyszukiwania – dwa (2) dni), a alarmy DLQ uruchamiają powiadomienia SNS w celu przeprowadzenia analizy. Ponadto ProcessMind korzysta z Sentry do śledzenia błędów frontendu w czasie rzeczywistym, monitorowania wydajności i odtwarzania sesji. Odtwarzanie sesji jest rejestrowane wyłącznie w przypadku sesji, w których wystąpi błąd, a tekst, dane wprowadzane do formularzy i multimedia są maskowane lub blokowane w nagraniach. Dane Sentry są przyjmowane w UE (Frankfurt) i ograniczają się do Danych o korzystaniu z ProcessMind (błędy przeglądarki, ślady wydajności, metadane urządzenia i zamaskowane nagrania odtwarzania). Sentry jest wymienione na [liście podmiotów przetwarzających](#).

5.4 Ochrona dzienników. Dzienniki są przechowywane w dedykowanych grupach dzienników CloudWatch z kontrolą dostępu i szyfrowaniem danych w stanie spoczynku. Dzienniki produkcyjne i programistyczne są rozdzielone według środowiska i granic kont.

6. Zautomatyzowana walidacja zabezpieczeń i zarządzanie podatnościami

6.1 Działania ProcessMind. ProcessMind uruchamia cdk-nag w ramach syntezy infrastruktury i workflow wdrożeniowego, korzystając z wielu zestawów reguł branżowych (w tym AWS Solutions, NIST 800-53 i PCI DSS). Raporty dla poszczególnych stosów są generowane i weryfikowane w ramach zarządzania zmianami infrastruktury. Ustalenia są klasyfikowane jako naprawione, zaakceptowane ryzyko lub planowane usprawnienie.

6.2 Zarządzanie wyjątkami. Wyłączenia są rejestrowane w centralnym rejestrze, jeśli pozwala na to platforma, ograniczane do stosów, których dotyczą, i wymagają pisemnego uzasadnienia; jeśli stos zawiera wyłączenie wbudowane, jest ono dokumentowane wraz z tym stosem. Po usunięciu przyczyny ustalenia odpowiednie wyłączenie jest aktualizowane lub usuwane. ProcessMind nie traktuje wyłączenia jako ogólnego zwolnienia z weryfikacji.

6.3 Działania, których ProcessMind obecnie nie podejmuje. ProcessMind śledzi i weryfikuje istotne wyjątki dotyczące zabezpieczeń infrastruktury. Najważniejsze z nich to:

- funkcje Lambda aplikacji nie są domyślnie umieszczane w VPC; łączą się z Aurora za pośrednictwem RDS Data API przez TLS, z użyciem uwierzytelniania IAM i Secrets Manager
- żadna część usługi nie jest chroniona przez AWS WAF: AWS WAF nie obsługuje HTTP API API Gateway, a pozostałe punkty wejścia również nie są chronione przez WAF (połączenia WebSocket korzystają z krótkotrwałych tokenów HMAC; ograniczenia geograficzne dotyczące płatności są egzekwowane w systemie płatniczym);

statyczne dystrybucje również nie korzystają ze standardowego rejestrowania dostępu CloudFront

- odzyskiwanie bazy danych opiera się na automatycznych kopiach zapasowych Aurora i odzyskiwaniu do określonego punktu w czasie, a nie na oddzielnym planie AWS Backup ani Aurora Enhanced Monitoring
- nie ma replikacji S3 między regionami ani S3 Object Lock dla modyfikowalnych zasobników
- niektóre zasoby pomocnicze zarządzane przez AWS/CDK/SST korzystają z szyfrowania zarządzanego przez AWS lub szerszych, generowanych polityk IAM, gdy usługa nie udostępnia alternatywy kontrolowanej przez klienta

Pełny rejestr wyłączeń jest przechowywany wraz z kodem infrastruktury i udostępniany na żądanie. Korzystanie z zestawów reguł cdk-nag stanowi walidację zabezpieczeń w ramach prac inżynierskich, a nie zewnętrzną certyfikację, opinię z audytu ani poświadczenie prawne zgodności z HIPAA, NIST lub PCI DSS.

6.4 Zarządzanie zależnościami. Zależności oprogramowania są stale monitorowane pod kątem znanych podatności. Podatności krytyczne i o wysokim poziomie istotności są usuwane w docelowym terminie siedmiu (7) dni. Zależności są aktualizowane zgodnie z regularnym harmonogramem.

6.5 Bezpieczny cykl życia oprogramowania (SDLC). ProcessMind stosuje podejście oparte na wielowarstwowej ochronie w procesie tworzenia oprogramowania. Każda zmiana w środowisku produkcyjnym musi przejść przez wiele niezależnych, zautomatyzowanych warstw walidacji przed wdrożeniem:

- **Analiza statyczna i bezpieczeństwo typów:** Tryb ścisły TypeScript i ESLint wymuszają poprawność typów, bezpieczeństwo wartości null oraz wzorce kodowania istotne z punktu widzenia bezpieczeństwa na etapie kompilacji.

- **Przegląd kodu wspomagany przez AI:** Analiza wspomagana przez AI zapewnia dodatkową perspektywę podczas przeglądu pull requestów, pomagając wykrywać zagrożenia bezpieczeństwa, błędy logiczne i odstępstwa od przyjętych konwencji, a także uzupełniając testy automatyczne.
- **Testy jednostkowe i integracyjne:** kompleksowy zestaw testów Vitest weryfikuje logikę biznesową, wzorce dostępu do danych, działanie API i obsługę błędów w odniesieniu do aktywnych zasobów AWS w środowisku programistycznym.
- **Testy kompleksowe:** Testy przeglądarkowe oparte na Playwright weryfikują krytyczne workflow użytkowników, w tym uwierzytelnianie, przesyłanie danych, modelowanie procesów, symulację i izolację wielu dzierżawców.
- **Skanowanie infrastruktury pod kątem zgodności:** cdk-nag weryfikuje kod infrastruktury jako kodu pod kątem wielu ram zgodności przy każdej zmianie.
- **Skanowanie zależności pod kątem podatności:** automatyczne audyty zależności blokują wdrożenie w środowisku produkcyjnym oprogramowania z rozpoznanymi podatnościami krytycznymi i o wysokim poziomie istotności.

Przegląd prowadzony przez człowieka koncentruje się na architekturze, granicach bezpieczeństwa i decyzjach projektowych, a nie na kontroli poszczególnych wierszy kodu. W przypadku zmian strukturalnych, wrażliwych z punktu widzenia bezpieczeństwa lub dotyczących infrastruktury, oprócz walidacji automatycznej wymagane jest wyraźne zatwierdzenie przez człowieka.

Wszystkie warstwy walidacji są egzekwowane za pośrednictwem CI jako wymagane bramki scalania zmian aplikacji i infrastruktury z gałęzią główną. Treści strony internetowej i wydania zasobów statycznych podlegają odrębnemu, udokumentowanemu procesowi wydawniczemu z kontrolami w czasie wdrożenia — w tym automatyczną kontrolą aktualności dokumentów prawnych — zamiast bramki CI stosowanej dla

aplikacji. Awaryjne poprawki produkcyjne mogą ominąć bramkę CI, ale w ciągu dwudziestu czterech (24) godzin należy następnie uruchomić pełny potok i przeprowadzić przegląd po incydencie.

7. Kopie zapasowe i odzyskiwanie po awarii

7.1 Automatyczne kopie zapasowe. Amazon Aurora wykonuje ciągłe, automatyczne kopie zapasowe, które są przechowywane przez siedem (7) dni. Kopie zapasowe są szyfrowane przy użyciu tych samych kluczy KMS zarządzanych przez klienta co źródłowe bazy danych.

7.2 Odzyskiwanie do określonego punktu w czasie. Aurora obsługuje odzyskiwanie do dowolnej sekundy w okresie przechowywania kopii zapasowych, umożliwiając szybkie przywrócenie danych w przypadku ich uszkodzenia lub przypadkowego usunięcia.

7.3 Trwałość i wersjonowanie S3. Przesłane pliki i artefakty operacyjne są przechowywane w Amazon S3, który zapewnia trwałość na poziomie 99,999999999% (11 dziewiątek). Wersjonowanie jest włączone w zasobniku przesłanych plików i zasobników zasobów, aby umożliwić odzyskiwanie i przywracanie poprzednich wersji. Zasobniki wdrożeniowe strony internetowej i frontendu zawierają odtwarzalne artefakty kompilacji i nie są traktowane jako system kopii zapasowych. Obecnie ProcessMind nie włącza replikacji S3 między regionami.

7.4 Ciągłość działania. Procedury odzyskiwania po awarii są udokumentowane i okresowo testowane. Podsumowanie jest dostępne w dokumencie [Odzyskiwanie po awarii, ciągłość działania i reagowanie na incydenty](#). Architektura opiera się na usługach zarządzanych przez AWS w regionie eu-central-1, który AWS obsługuje w wielu strefach dostępności; klaster Aurora działa obecnie z pojedynczą instancją zapisującą, dlatego odzyskiwanie bazy danych opiera się na automatycznych kopiach zapasowych i odzyskiwaniu do określonego punktu w czasie, a nie na instancji zapasowej w tym samym regionie. Kopie zapasowe Aurora,

trwałość S3, kolejki komunikatów niedostarczonych i statyczne zasoby odtwarzane z kodu źródłowego stanowią elementy strategii odzyskiwania.

8. Reagowanie na incydenty

8.1 Powiadamianie o incydentach. W przypadku Incydentu bezpieczeństwa (zgodnie z definicją w DPA) ProcessMind powiadomi klientów, których dotyczy incydent, bez zbędnej zwłoki, a jeśli będzie to możliwe – w ciągu siedemdziesięciu dwóch (72) godzin od uzyskania informacji o incydencie.

8.2 Obsługa incydentów. ProcessMind utrzymuje udokumentowane procedury reagowania na incydenty, obejmujące ich identyfikację, powstrzymanie, usunięcie, odzyskiwanie i przegląd po incydencie. Podsumowanie jest dostępne w dokumencie [Odzyskiwanie po awarii, ciągłość działania i reagowanie na incydenty](#). Wnioski wyciągnięte z incydentów są uwzględniane w zabezpieczeniach i procesach.

8.3 Komunikacja. Powiadomienia o incydentach zawierają informacje o charakterze i zakresie incydentu, kategoriach danych, których dotyczy, środkach podjętych w celu jego powstrzymania oraz zalecanych działaniach klienta.

9. Środki organizacyjne

9.1 Zarządzanie bezpieczeństwem informacji. ProcessMind utrzymuje system zarządzania bezpieczeństwem informacji zgodny z zasadami ISO 27001. ProcessMind wybrał ścieżkę certyfikacji w zakresie certyfikatu ISO 27001 i atestacji SOC 2 Type II; formalny proces certyfikacji jeszcze się nie rozpoczął.

9.2 Świadomość bezpieczeństwa. Cały personel mający dostęp do Danych klienta przechodzi szkolenia z zakresu świadomości bezpieczeństwa. Najlepsze praktyki bezpieczeństwa są uwzględniane w

procesie wdrażania nowych pracowników, workflow programistycznych i procedurach operacyjnych.

9.3 Zarządzanie dostawcami i podmiotami przetwarzającymi. Podmioty przetwarzające są zobowiązane umownie do przestrzegania standardów ochrony danych równoważnych standardom opisanym w niniejszym dokumencie. ProcessMind prowadzi publiczną [listę podmiotów przetwarzających](#) i powiadamia o zamiarze zaangażowania nowego podmiotu przetwarzającego z co najmniej trzydziestodniowym (30) wyprzedzeniem. Podmioty przetwarzające są corocznie weryfikowane pod kątem zgodności.

9.4 Poufność. Cały personel upoważniony do przetwarzania Danych klienta jest związany pisemnymi zobowiązaniami do zachowania poufności.

10. Zgodność i certyfikaty

Ramy / norma	Status
RODO (ogólne rozporządzenie UE o ochronie danych)	Zgodność zapewniona
Lokalizacja danych w UE (Frankfurt, Niemcy)	Wymuszona
Certyfikaty infrastruktury AWS (ISO 27001, SOC 2, PCI DSS)	Obowiązują za pośrednictwem AWS
ISO 27001 (ProcessMind)	Planowane – wybrano ścieżkę certyfikacji; formalny proces jeszcze się nie rozpoczął

Ramy / norma	Status
SOC 2 Type II (ProcessMind)	Planowane — wybrano ścieżkę certyfikacji; formalny proces jeszcze się nie rozpoczął
Zautomatyzowana walidacja zabezpieczeń infrastruktury (cdk-nag w zakresie AWS Solutions, HIPAA Security, NIST 800-53 R4/R5, PCI DSS 3.2.1, Serverless)	Wdrożona jako walidacja zabezpieczeń w ramach prac inżynierskich, a nie certyfikacja
Standardowe klauzule umowne (SCC) dotyczące przekazywania danych za granicę	Wdrożone (zob. DPA)
Dodatek dotyczący przetwarzania danych (DPA)	Publicznie dostępny

Korzystanie z zestawów reguł cdk-nag nie oznacza, że ProcessMind posiada formalny certyfikat ani że został poddany niezależnemu audytowi w zakresie HIPAA, NIST lub PCI DSS. Zestawy reguł są wykorzystywane jako zabezpieczenia inżynierskie do walidacji projektu infrastruktury i jawnego śledzenia luk.

W razie pytań dotyczących bezpieczeństwa lub zgodności albo w celu uzyskania dokumentacji, takiej jak raporty z audytu lub wypełnione kwestionariusze bezpieczeństwa, prosimy o kontakt pod adresem support@processmind.com.