

Hosting SaaS ProcessMind

Data wejścia w życie: 14 września 2026 r.

1. Wprowadzenie

ProcessMind B.V. („my”, „nas”, „nasz”) świadczy rozwiązania w modelu Software as a Service (SaaS), hostowane w infrastrukturze Amazon Web Services (AWS) zlokalizowanej we **Frankfurcie w Niemczech**. Niniejsza Polityka hostingowa określa nasze zobowiązania wobec klientów oraz standardy, zgodnie z którymi prowadzimy działalność, aby zapewnić niezawodność, bezpieczeństwo i zgodność naszego środowiska hostingowego.

2. Infrastruktura hostingowa

Nasze rozwiązania SaaS są hostowane w AWS, z wykorzystaniem solidnej, skalowalnej i bezpiecznej infrastruktury udostępnianej przez Amazon Web Services. Główne centrum danych obsługujące nasze usługi znajduje się we Frankfurcie w Niemczech, co zapewnia przechowywanie Państwa danych na terenie Unii Europejskiej (UE).

3. Bezpieczeństwo danych

Zobowiązujemy się do utrzymywania bezpieczeństwa i integralności danych naszych klientów. AWS zapewnia wysoce bezpieczne środowisko z kompleksowym zestawem usług bezpieczeństwa, obejmującym między innymi:

- **Bezpieczeństwo fizyczne:** Centra danych AWS są chronione za pomocą rozbudowanych środków bezpieczeństwa fizycznego, które zapobiegają nieuprawnionemu dostępowi.
- **Bezpieczeństwo sieci:** Zapory sieciowe, monitorowanie sieci i szyfrowana komunikacja chronią dane podczas przesyłania i przechowywania.
- **Kontrola dostępu:** Wdrożono rygorystyczne mechanizmy kontroli dostępu i uwierzytelniania, aby zapewnić, że dostęp do danych

klientów mają wyłącznie upoważnione osoby.

4. Prywatność danych

Prywatność Państwa danych jest dla nas ważna. Przestrzegamy wszystkich właściwych przepisów o ochronie danych, w tym ogólnego rozporządzenia o ochronie danych (RODO). Więcej informacji o tym, jak przetwarzamy Państwa dane osobowe, można znaleźć w naszej [Polityce prywatności](#).

5. Dostępność usługi

Projektujemy środowisko produkcyjne z myślą o wysokiej dostępności, wykorzystując redundancję, monitorowanie, kontrolowane wdrożenia i procedury reagowania operacyjnego. Niniejsza Polityka hostingu ma charakter informacyjny i sama w sobie nie ustanawia umownych zobowiązań dotyczących czasu dostępności.

ProcessMind publikuje aktualny status, wartości procentowe czasu dostępności oraz historię czasów reakcji pod adresem processmind.com/status. Strona statusu jest hostowana oddzielnie od frontendu aplikacji; jej dane o statusie na żywo są udostępniane przez nasze API, dlatego w przypadku awarii API sama strona pozostaje dostępna, ale może wyświetlać ograniczone informacje o statusie. Informacje o sposobie pomiaru czasu dostępności zawiera [Umowa o poziomie usług](#).

Umowne zobowiązania dotyczące dostępności, cele w zakresie reagowania na incydenty, rekompensaty za przerwy w świadczeniu usług oraz warunki wsparcia opisano w [Umowie o poziomie usług](#).

6. Kopie zapasowe i odzyskiwanie po awarii

- **Kopie zapasowe:** Automatyczne kopie zapasowe produkcyjnych danych klientów są wykonywane co najmniej raz dziennie i trwale przechowywane w regionie AWS; obecnie kopie zapasowe nie są replikowane do drugiego regionu.
- **Odzyskiwanie po awarii:** Środki i priorytety dotyczące odzyskiwania opisano w dokumencie podsumowującym dotyczącym

odzyskiwania po awarii, ciągłości działania i reagowania na incydenty.

7. Zgodność

ProcessMind jest hostowany w infrastrukturze AWS, która posiada następujące certyfikaty:

- **ISO 27001**: zarządzanie bezpieczeństwem informacji
- **ISO 27017**: zabezpieczenia właściwe dla chmury
- **ISO 27018**: ochrona danych osobowych w chmurze
- **SOC 1, SOC 2, SOC 3**: kontrole organizacji usługowych

Certyfikaty te dotyczą infrastruktury AWS, na której działa ProcessMind. ProcessMind korzysta z tych zabezpieczeń za pośrednictwem zarządzanych usług AWS. ProcessMind wybrał ścieżkę certyfikacji w zakresie własnego certyfikatu ISO 27001 i atestacji SOC 2 Type II; formalny proces jeszcze się nie rozpoczął.

ProcessMind przestrzega ogólnego rozporządzenia o ochronie danych (RODO) w zakresie ochrony danych i prywatności. Szczegółowe informacje o własnych technicznych i organizacyjnych środkach bezpieczeństwa ProcessMind zawiera dokument [Środki bezpieczeństwa](#).

8. Obowiązki klienta

Klienci odpowiadają za zabezpieczenie danych uwierzytelniających do swoich kont oraz za wszelkie działania podejmowane z użyciem tych kont.

Klienci powinni:

- Używać silnych, unikalnych haseł do swoich kont.
- Korzystać z uwierzytelniania wieloskładnikowego (MFA), jeśli jest dostępne.
- Regularnie aktualizować i weryfikować uprawnienia dostępu.
- Niezwłocznie zgłaszać naszemu zespołowi wsparcia wszelkie podejrzane działania lub naruszenia bezpieczeństwa.

9. Zmiany Polityki hostingu

Możemy od czasu do czasu aktualizować niniejszą Politykę hostingu, aby uwzględnić zmiany naszych praktyk lub wymogów prawnych. O wszelkich istotnych zmianach powiadomimy klientów za pośrednictwem naszej strony internetowej lub bezpośredniej komunikacji.

Powiązane polityki

Informacje o przyjmowaniu zgłoszeń do wsparcia, ustalaniu priorytetów żądań i zobowiązaniach umownych zawiera Umowa o poziomie usług.

Dane kontaktowe

W razie pytań lub wątpliwości dotyczących niniejszej Polityki hostingu prosimy o kontakt:

ProcessMind B.V.

Willem Sandbergstraat 33,
7425RC, Deventer,
Holandia

Telefon: +31 85 060 68 09

E-mail: support@processmind.com

Korzystając z naszych usług, potwierdzają Państwo, że zapoznali się z niniejszą Polityką hostingu. Ma ona charakter informacyjny i nie ustanawia zobowiązań umownych wykraczających poza zobowiązania określone w Umowie z klientem, Dodatku dotyczącym przetwarzania danych, Umowie o poziomie usług i Środkach bezpieczeństwa.