

PRZEWODNIK WDROŻENIOWY · DLA IT, IOD I ZARZĄDU

Jak bezpiecznie podłączyć AI do ERP

Sposób połączenia, droga danych, uprawnienia, zatwierdzanie zapisów, audyt i checklista wdrożenia. Bez zakładania jednego modelu technicznego dla każdego systemu ERP.

Połączenie dopasowane do ERP

Zakres danych i uprawnienia

RODO: pytania do IOD

Warunki usługi AI do weryfikacji

Checklista dla IT i IOD

Plan pilotażu od jednego procesu

PO CO TEN DOKUMENT

Decyduje sposób wdrożenia, nie sam fakt użycia AI

Pytanie „czy AI jest bezpieczne dla naszych danych?” nie ma jednej odpowiedzi. Ryzyko zależy od tego, **jak** rozwiązanie łączy się z konkretnym ERP, jaką ma ścieżkę danych i jakie operacje wolno mu wykonać.

Ten przewodnik pomaga przygotować wdrożenie do rozmowy z IT, IOD i właścicielem procesu. Zamiast obiecywać jeden model dla wszystkich systemów, wskazuje elementy, które należy potwierdzić dla ERP, jego wersji i modelu hostingu.

1. O jakim „AI nad ERP” tu mówimy

Chodzi o **warstwę rozmowy z ERP**: rozwiązanie, które przekłada język naturalny na dozwolone odczyty i działania w systemie. Pozwala zadać pytanie, którego nie ma w gotowym raporcie, a przygotowaną zmianę przekazać człowiekowi do zatwierdzenia.

Po co taka warstwa

Ułatwia pracę z danymi i procesami bez przechodzenia przez kolejne widoki oraz eksporty. Pytanie po polsku może prowadzić do kontrolowanej odpowiedzi lub propozycji działania.

Dlaczego wymaga oceny

Każdy ERP ma inne interfejsy, rozszerzenia i środowisko działania. Zanim podłączysz AI do danych produkcyjnych, ustal mechanizm połączenia, zakres dostępu i zasady zapisu.

NAJWAŻNIEJSZE W JEDNYM ZDANIU

Bezpieczne wdrożenie zaczyna się od minimalnego zakresu danych, kontrolowanych uprawnień, potwierdzania zapisów przez człowieka i audytu — a nie od założenia, że każdy ERP można podłączyć w ten sam sposób.

Dla kogo jest ten przewodnik

- **Dział IT / administrator ERP**, by ocenić dostępne interfejsy, środowisko i uprawnienia.
- **IOD / dział prawny**, by zmapować przepływ danych oraz obowiązki z RODO.
- **Zarząd / właściciel procesu**, by zrozumieć ryzyko, zakres i kryteria pilotażu.

NIE MA JEDNEGO MODELU DLA WSZYSTKICH ERP

2. Architektura dopasowana do systemu

Połączenie z ERP może wykorzystywać API, dedykowany konektor, integrację z bazą lub inny udokumentowany interfejs. Właściwy wybór zależy od systemu, wersji, rozszerzeń, dostępnych uprawnień i modelu hostingu.

Model językowy nie powinien samodzielnie dostawać szerokiego dostępu do danych. Warstwa integracyjna egzekwuje dozwolone narzędzia, zakresy oraz zasady zatwierdzania. Przed pilotażem potwierdź te mechanizmy z właścicielem ERP.

Droga zapytania krok po kroku



Sposób połączenia, środowisko działania i zakres zwracanych danych potwierdź dla konkretnego ERP przed uruchomieniem.

Co trzeba ustalić

- Dostępny i wspierany mechanizm integracji
- Miejsce działania komponentów
- Role, konta techniczne i uprawnienia
- Zakres odczytu, zapisu i audytu

Co powinna egzekwować integracja

- Tylko dozwolone operacje
- Tylko dane niezbędne do zadania
- Potwierdzenie przed zapisem
- Ślad audytowy operacji

Nie pytaj tylko „gdzie to działa?”. Zapytaj „jak dokładnie działa to połączenie w naszym ERP, wersji i hostingu — oraz kto kontroluje dostęp?”.

KONKRETNY PRZYKŁAD

3. Gdzie trafiają Twoje dane

Weźmy pytanie: „pokaż faktury wymagające reakcji”. To, co wydarzy się dalej, zależy od skonfigurowanego połączenia i warunków wybranej usługi AI.

Źle zaprojektowane wdrożenie

Ktoś kopiuje pełne zestawienia danych do okna czatu. Zakres jest niekontrolowany, warunki dostawcy nie są zweryfikowane, a operacji nie da się później odtworzyć.

Dobrze zaprojektowana integracja

Narzędzie zwraca tylko pola i rekordy niezbędne do konkretnego pytania. Zakres jest ograniczony rolą użytkownika, a planowana zmiana trafia do człowieka do potwierdzenia.

Udokumentuj pełną drogę: pytanie użytkownika, dane przekazane do usługi AI, odpowiedź narzędzia, operację w ERP i audyt. Nie zakładaj z góry, że dane pozostają w jednym miejscu albo że każdy dostawca ma identyczne warunki.

CO NALEŻY ZWERYFIKOWAĆ

Przed pilotażem potwierdź, jakie informacje opuszczają ERP, dokąd trafiają, jak długo są przechowywane oraz jakie warunki obowiązują u dostawców. Ustal też, które dane są potrzebne do odpowiedzi, a które trzeba wykluczyć.

Trzy granice, które ustawiasz

- **Granica narzędzi.** Lista dozwolonych odczytów i działań zamiast ogólnego dostępu do całego systemu.
- **Granica zakresu.** Minimalny zestaw pól i rekordów, odpowiedni do danego pytania i roli użytkownika.
- **Granica zapisu.** Człowiek zatwierdza planowaną zmianę, a system rejestruje jej przebieg.

CZTERY FILARY

4. Zgodność z RODO

RODO nie zakazuje używania AI. Wymaga, by organizacja знаła przepływ danych, podstawę przetwarzania, role stron i zastosowane zabezpieczenia. Szczegóły zależą od wdrożenia.

1 Minimalizacja danych

Zdefiniuj pola i rekordy niezbędne do danego zadania. Nie udostępniaj całych zbiorów, gdy odpowiedź wymaga tylko ich fragmentu.

2 Role i umowy

Ustal role organizacji, dostawcy integracji i dostawcy AI. Z IOD sprawdź, czy konieczne są umowy powierzenia oraz aktualizacja dokumentacji.

3 Rozliczalność

Ślad audytowy powinien pozwolić ustalić, kto uruchomił operację, jakie dane i uprawnienia zastosowano oraz jaki był jej wynik.

4 Kontrola dostępu

Zakres dostępu wynika z roli użytkownika i procesu. Regularnie przeglądaj uprawnienia oraz listę dozwolonych narzędzi.

To nie jest porada prawna. Ostateczną ocenę zgodności, podstawę prawną i wymagane zabezpieczenia określa Twój IOD lub kancelaria.

WARUNKI DO SPRAWDZENIA PRZED PILOTAŻEM

5. Wybór usługi i planu AI

Nie wybieraj usługi wyłącznie po nazwie planu. Funkcje, warunki i dostępność integracji zmieniają się. Przed użyciem danych produkcyjnych zweryfikuj aktualną dokumentację oraz ustalenia umowne.

OBSZAR	PYTANIE KONTROLNE	CO POTWIERDZIĆ PRZED STARTEM
Dane	Jakie dane są przekazywane do usługi AI?	Zakres, retencję, lokalizację przetwarzania i zasady wykorzystania danych.
Integracja	Czy wybrany plan obsługuje potrzebny sposób połączenia?	Dostępność funkcji, ograniczenia techniczne i wymagania administracyjne.
Administracja	Kto zarządza użytkownikami i uprawnieniami?	Role, kontrolę dostępu, logi oraz procedurę odebrania dostępu.
Umowy	Jakie warunki obowiązują strony?	Aktualne dokumenty, role w przetwarzaniu i ewentualne umowy powierzenia.
Rekomendacja	Wybierz wariant, który pozwala spełnić wymagania procesu i organizacji. Stan funkcji oraz warunków sprawdź w aktualnej dokumentacji dostawcy przed uruchomieniem pilotażu.	

ZASADA DOBORU

Zacznij od jednego procesu o ograniczonym zakresie. Najpierw potwierdź przepływ danych, uprawnienia i sposób integracji, a dopiero potem rozszerzaj rozwiązanie na kolejne zespoły lub operacje.

Warunki dostawców i dostępność funkcji mogą się zmieniać. Materiał nie zastępuje ich aktualnej dokumentacji ani uzgodnień z działem prawnym.

DO PRZEKAZANIA DZIAŁOWI IT I IOD

6. Checklista wdrożenia AI w ERP

Zanim uruchomisz pilotaż, sprawdź te punkty. Edytowalną wersję do wklejenia do własnej dokumentacji dołączamy osobno.

☐ **Czy potwierdziliśmy sposób połączenia właściwy dla ERP, wersji i hostingu?**

API, konektor, integracja z bazą lub inny udokumentowany mechanizm — wraz z jego ograniczeniami.

☐ **Czy znamy drogę danych od pytania do odpowiedzi?**

Zakres danych, odbiorcy, retencja i lokalizacja przetwarzania są opisane i zatwierdzone.

☐ **Czy narzędzia mają minimalny zakres odczytu i zapisu?**

Tylko pytania, pola i operacje niezbędne w pilotażu, bez ogólnego dostępu do systemu.

☐ **Czy każdy zapis wymaga potwierdzenia człowieka?**

AI może przygotować propozycję, ale zmiana nie jest wykonywana automatycznie.

☐ **Czy istnieje audyt każdej operacji?**

Można odtworzyć użytkownika, czas, zakres działania, wynik i ewentualne potwierdzenie.

☐ **Czy możemy ograniczyć dostęp według roli i zakresu danych?**

Uprawnienia użytkowników i kont technicznych są nadane zgodnie z zasadą najmniejszych uprawnień.

☐ **Czy sprawdziliśmy aktualne warunki wybranej usługi AI?**

Zasady wykorzystania danych, retencja, funkcje administracyjne oraz wymagane umowy.

☐ **Czy IOD ocenił wdrożenie i role stron?**

Dokumentacja RODO, umowy i ewentualna ocena ryzyka są dopasowane do rzeczywistego przepływu danych.

☐ **Od którego jednego procesu zaczynamy pilotaż?**

Wąski, mierzalny proces z jasno wskazanym właścicielem i kryteriami sukcesu.

OD CZEGO ZACZĄĆ

7. Plan pilotażu od jednego procesu

Najszybsza droga do oceny wartości i ryzyka to wąski, mierzalny pilotaż. Zamiast podłączać AI do całego ERP naraz, wybierz jeden proces, w którym co tydzień powtarza się ten sam koszt pracy.

Przykład: uzgadnianie wpływów

Osoba odpowiedzialna za rozliczenia sprawdza niedopasowane wpłaty. Pytanie po polsku może wskazać przypadki wymagające decyzji, a zatwierdzona operacja trafia do ERP z audytem.

Przykład: działania wobec należności

Proces wskazuje kontrahentów wymagających reakcji według ustalonych reguł. AI może przygotować propozycję działania, którą człowiek weryfikuje przed zapisem.

Cztery kroki pilotażu

- **Wybór procesu.** Jeden, mierzalny i powtarzalny — z realnym kosztem czasu.
- **Definicja narzędzi i zakresu.** Ustal pytania, dane, działania oraz role użytkowników.
- **Konfiguracja i weryfikacja połączenia.** Dopasuj ją do ERP, wersji i hostingu; uruchom audyt oraz potwierdzanie zapisów.
- **Pomiar.** Porównaj wynik z punktem wyjścia: czas, liczbę obsłużonych przypadków lub jakość decyzji.

O NOVAINSIGHT

Most między ChatGPT a Twoim ERP

NovaiInsight pomaga zespołom pytać o dane po polsku, przygotowywać działania oraz zapisywać zatwierdzone decyzje z audytem. Zakres i sposób połączenia potwierdzamy przed pilotażem dla konkretnego środowiska ERP.

Chcesz omówić to na swoim procesie? Napisz: kontakt@novainsight.pl lub wejdź na novainsight.pl