

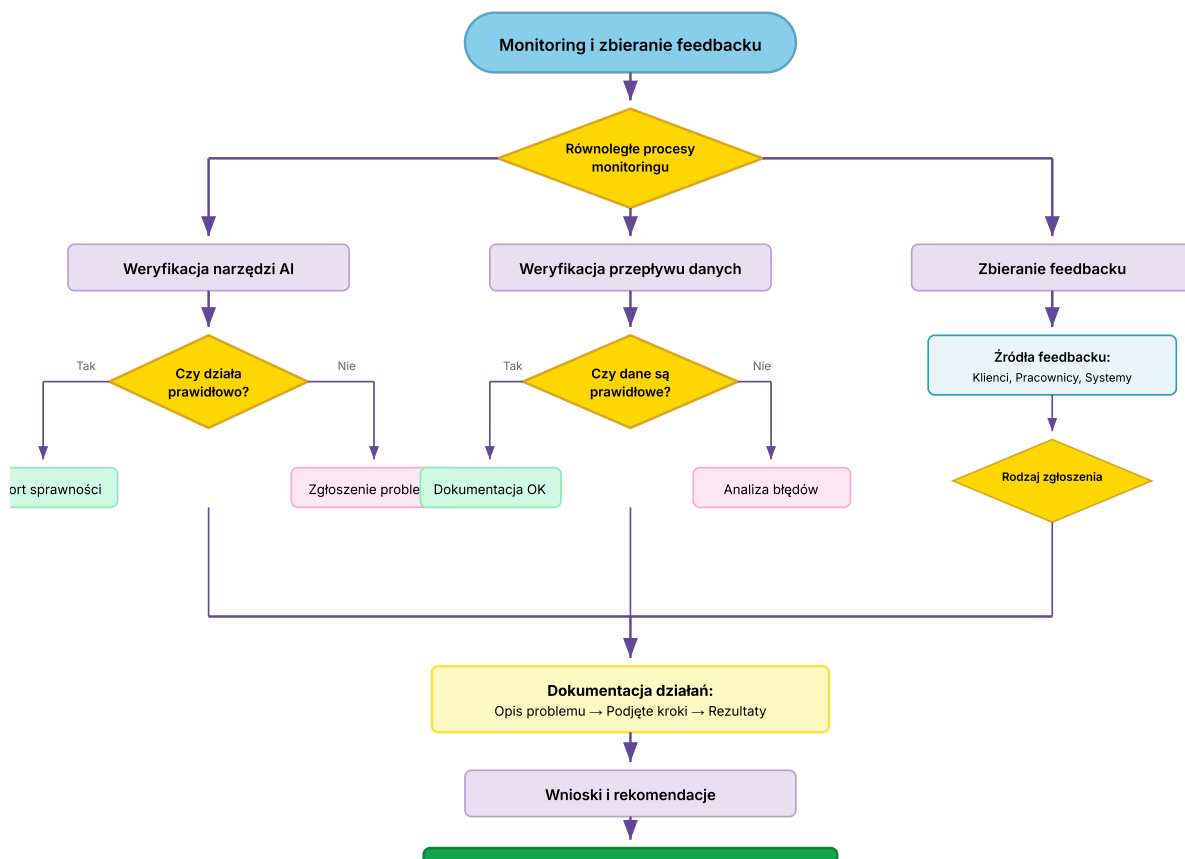
Monitoring systemów AI

Procedury monitorowania, audytu i kontroli jakości systemów sztucznej inteligencji stosowanych w Viking Potatoes sp. z o.o.

1. Cel monitoringu

Monitoring systemów AI ma na celu zapewnienie, że wykorzystywane narzędzia działają zgodnie z przyjętymi standardami etycznymi, prawnymi i jakościowymi. Regularna kontrola pozwala na wczesne wykrywanie i eliminację potencjalnych problemów.

2. Schemat procesu monitoringu



3. Zakres monitoringu

OBSZAR	CO MONITORUJEMY	CZĘSTOTLIWOŚĆ
Jakość wyników	Dokładność, spójność i adekwatność treści generowanych przez AI	Każdorazowo (przy każdym użyciu)

OBSZAR	CO MONITORUJEMY	CZĘSTOTLIWOŚĆ
Bezpieczeństwo danych	Czy dane wprowadzane do AI nie zawierają informacji wrażliwych	Każdorazowo
Zgodność z polityką	Czy korzystanie z AI odbywa się zgodnie z wewnętrznymi procedurami	Miesięcznie
Aktualność narzędzi	Czy stosowane narzędzia AI są aktualne i bezpieczne	Kwartalnie
Regulacje prawne	Czy firma jest zgodna z obowiązującymi przepisami (AI Act, RODO)	Kwartalnie
Satysfakcja klientów	Feedback klientów dotyczący materiałów tworzonych z AI	Na bieżąco

3. Procedury kontrolne

3.1 Kontrola bieżąca (każde użycie AI)

- Weryfikacja merytoryczna wygenerowanego materiału
- Sprawdzenie, czy materiał nie zawiera halucynacji (fałszywych informacji)
- Ocena, czy wynik jest adekwatny do potrzeb projektu
- Upewnienie się, że nie wprowadzono danych wrażliwych

3.2 Przegląd miesięczny

- Analiza liczby i rodzajów zastosowań AI w projektach
- Identyfikacja powtarzających się problemów
- Ocena efektywności — czy AI faktycznie przyspiesza pracę
- Weryfikacja zgodności z procedurą z Załącznika 1

3.3 Audyt kwartalny

- Przegląd listy dopuszczonych narzędzi AI
- Aktualizacja oceny ryzyka dla każdego narzędzia
- Przegląd zmian w przepisach (AI Act, RODO, wytyczne UODO)
- Aktualizacja dokumentacji wewnętrznej
- Szkolenie zespołu z nowych wytycznych (jeśli dotyczy)

4. Matryca ryzyka

RYZYO	PRAWDOPODOBIENSTWO	WPŁYW	MITYGACJA
Halucynacje AI (fałszywe informacje)	Średnie	Wysoki	Obowiązkowa weryfikacja przez człowieka
Wyciek danych wrażliwych	Niskie	Wysoki	Procedura sprawdzania danych przed wprowadzeniem
Naruszenie praw autorskich	Średnie	Średni	Weryfikacja unikalności treści, unikanie kopii
Niezgodność z AI Act	Niskie	Średni	Kwartalne przeglądy regulacyjne
Upředzenia (bias) w wynikach	Średnie	Średni	Zróznicowane narzędzia, ludzka weryfikacja

5. Procedura eskalacji

W przypadku wykrycia istotnego problemu z systemem AI:

1. **Natychmiastowe wstrzymanie** — zaprzestanie korzystania z problematycznego narzędzia
2. **Dokumentacja incydentu** — szczegółowy opis problemu, okoliczności, potencjalnych skutków
3. **Powiadomienie przełożonego** — eskalacja do osoby odpowiedzialnej za AI w firmie
4. **Ocena szkód** — analiza wpływu na projekty klientów i dane
5. **Działania naprawcze** — wdrożenie poprawek, powiadomienie klientów (jeśli dotyczy)
6. **Aktualizacja procedur** — wyciągnięcie wniosków i aktualizacja dokumentacji

6. Raportowanie

Raporty z monitoringu są przechowywane przez okres 3 lat i udostępniane na żądanie klientów lub organów nadzorczych. Raporty zawierają: okres objęty analizą, liczbę zastosowań AI, wykryte incydenty, podjęte działania naprawcze.

7. Postanowienia końcowe

Monitoring jest integralną częścią zarządzania AI w firmie. Każdy pracownik i współpracownik ma obowiązek zgłaszania nieprawidłowości związanych z działaniem systemów AI. Dokument podlega przeglądowi co 6 miesięcy.

