

Polityka korzystania z narzędzi sztucznej inteligencji

[Nazwa firmy] | Wersja 1.0 | Obowiązuje od: [data] | Właściciel dokumentu: [imię i nazwisko, stanowisko]

Szablon ma charakter pomocniczy i nie stanowi porady prawnej. Elementy w nawiasach kwadratowych uzupełnij lub usuń. Przed wdrożeniem skonsultuj dokument z prawnikiem, zwłaszcza jeśli przetwarzasz dane osobowe lub działasz w sektorze regulowanym.

1. Cel i zakres

Polityka określa, jak pracownicy i współpracownicy [Nazwa firmy] mogą korzystać z narzędzi sztucznej inteligencji (AI) w pracy, aby wykorzystać ich użyteczność bez narażania firmy na wyciek danych, błędne decyzje i naruszenie przepisów.

Dotyczy wszystkich osób pracujących dla firmy (etat, umowy cywilnoprawne, praktykanci) oraz wszystkich narzędzi AI, w tym generatorów tekstu i obrazu, asystentów wbudowanych w pakiety biurowe, tłumaczy, narzędzi do transkrypcji i agentów automatyzujących zadania. Obejmuje także narzędzia darmowe i prywatne konta używane do zadań służbowych.

2. Definicje

Narzędzie AI	Każde oprogramowanie lub usługa, która generuje treści, odpowiedzi, klasyfikacje lub decyzje z użyciem modeli uczenia maszynowego.
Narzędzie zatwierdzone	Narzędzie wpisane na Listę zatwierdzonych narzędzi AI, używane wyłącznie na koncie firmowym.
Shadow AI	Używanie narzędzi AI do zadań służbowych bez wiedzy i zgody firmy, w tym na kontach prywatnych.
Właściciel tematu AI	[Imię i nazwisko, stanowisko]. Osoba odpowiedzialna za wdrożenie i egzekwowanie polityki.

3. Właściciel tematu AI

Właściciel tematu AI prowadzi rejestr narzędzi AI, zatwierdza i wycofuje narzędzia, odpowiada na pytania pracowników („czy mogę tego użyć do...”), przyjmuje zgłoszenia incydentów i raz na [6] miesięcy przedstawia zarządowi krótki raport. Ma prawo wstrzymać użycie narzędzia do czasu wyjaśnienia ryzyka.

4. Narzędzia zatwierdzone

- Do zadań służbowych wolno używać wyłącznie narzędzi z Listy zatwierdzonych narzędzi AI, prowadzonej przez właściciela tematu AI.
- Narzędzia używa się wyłącznie na kontach firmowych. Konta prywatne i darmowe wersje nie mogą służyć do przetwarzania danych firmy.
- Chcesz użyć nowego narzędzia? Zgłoś to właścicielowi tematu AI. Odpowiedź w ciągu [5] dni roboczych. Do czasu decyzji narzędzia nie używasz do danych żółtych i czerwonych.
- Zatwierdzenie poprzedza ocena dostawcy według Checklisty oceny dostawcy narzędzia AI oraz wpis do rejestru.

5. Klasy danych

Przed wklejeniem czegokolwiek do narzędzia AI określ, do jakiej klasy należą dane.

Klasa	Przykłady	Zasada
ZIELONE	Treści publiczne: strona WWW, publikowane materiały, oferta w wersji publicznej, ogólne pytania o wiedzę.	Dowolne narzędzie zatwierdzone.
ŻÓŁTE	Dokumenty wewnętrzne bez danych osobowych: procedury, notatki ze spotkań bez danych klientów, szkice ofert bez nazw i cen indywidualnych.	Tylko narzędzia zatwierdzone, konto firmowe, wyniki sprawdzasz przed użyciem.
CZERWONE	Dane osobowe klientów i pracowników, dane finansowe, tajemnice handlowe, kod źródłowy, umowy z klientami, hasła i klucze dostępu, informacje poufne objęte umową.	Zakaz, chyba że właściciel tematu AI pisemnie zatwierdził konkretne zastosowanie po ocenie ryzyka.

Wątpliwości rozstrzygasz na korzyść wyższej klasy danych.

6. Zasady korzystania

Należy

- sprawdzać wynik pracy narzędzia przed użyciem: fakty, liczby, nazwy, cytaty, linki;
- zanonimizować dane, jeśli zadanie tego wymaga i anonimizacja nie zmienia sensu zadania;
- zgłaszać właścicielowi tematu AI nowe zastosowania, które wpływają na klientów lub pracowników.

Nie wolno

- wprowadzać do narzędzi AI danych czerwonych bez zatwierdzenia;
- używać AI do podejmowania lub przygotowywania decyzji o osobach (rekrutacja, ocena pracowników, zwolnienia, scoring klientów) bez zgody zarządu i konsultacji prawnej;
- wysyłać klientom odpowiedzi wygenerowanych przez AI bez weryfikacji przez człowieka;
- podłączać narzędzi AI do skrzynek pocztowych, dysków, systemów finansowych lub CRM bez zatwierdzenia zakresu uprawnień;
- omijać zabezpieczeń narzędzi ani korzystać z narzędzi zakazanych.

7. Odpowiedzialność za wynik

Osoba, która wysyła, publikuje lub wykorzystuje treść przygotowaną z udziałem AI, odpowiada za jej treść tak, jakby napisała ją samodzielnie. Powołanie się na to, że „tak odpowiedziało narzędzie”, nie zmienia odpowiedzialności.

8. Treści publikowane na zewnątrz

Obrazy, nagrania i teksty generowane przez AI, które publikujemy na zewnątrz, są oznaczane tam, gdzie wymagają tego przepisy (w szczególności art. 50 rozporządzenia o sztucznej inteligencji) lub gdzie brak oznaczenia mógłby wprowadzać odbiorców w błąd. Wątpliwości zgłaszasz właścicielowi tematu AI przed publikacją.

9. Zgłaszanie incydentów

Za incydent uważamy w szczególności wklejenie danych czerwonych do niezatwierdzonego narzędzia, wysłanie klientowi błędnej treści wygenerowanej przez AI, nieautoryzowany dostęp do konta narzędzia oraz utratę urządzenia z zalogowanym kontem. Zgłoś incydent niezwłocznie, nie później niż w ciągu [24] godzin od jego zauważenia, na adres [e-mail / telefon]. Zgłoszenie w dobrej wierze nie jest podstawą do wyciągania konsekwencji wobec zgłaszającego. Właściciel tematu AI ocenia, czy incydent wymaga zgłoszenia do inspektora ochrony danych, UODO lub klienta.

10. Szkolenie

Każda osoba używająca narzędzi AI przechodzi szkolenie wstępne ([60] minut) obejmujące niniejszą politykę, klasy danych i przykłady z naszej pracy. Szkolenie powtarzamy raz na [12] miesięcy i przy istotnej zmianie polityki. Lista uczestników jest przechowywana przez [właściciela tematu AI].

11. Przegląd i sankcje

Politykę przeglądamy co [6] miesięcy oraz przy zmianie przepisów lub wdrożeniu nowego rodzaju narzędzi. Naruszenie polityki może skutkować cofnięciem dostępu do narzędzi oraz konsekwencjami przewidzianymi w regulaminie pracy lub umowie.

Zatwierdził (zarząd):	Właściciel tematu AI:
[imię, nazwisko, data, podpis]	[imię, nazwisko, data, podpis]