

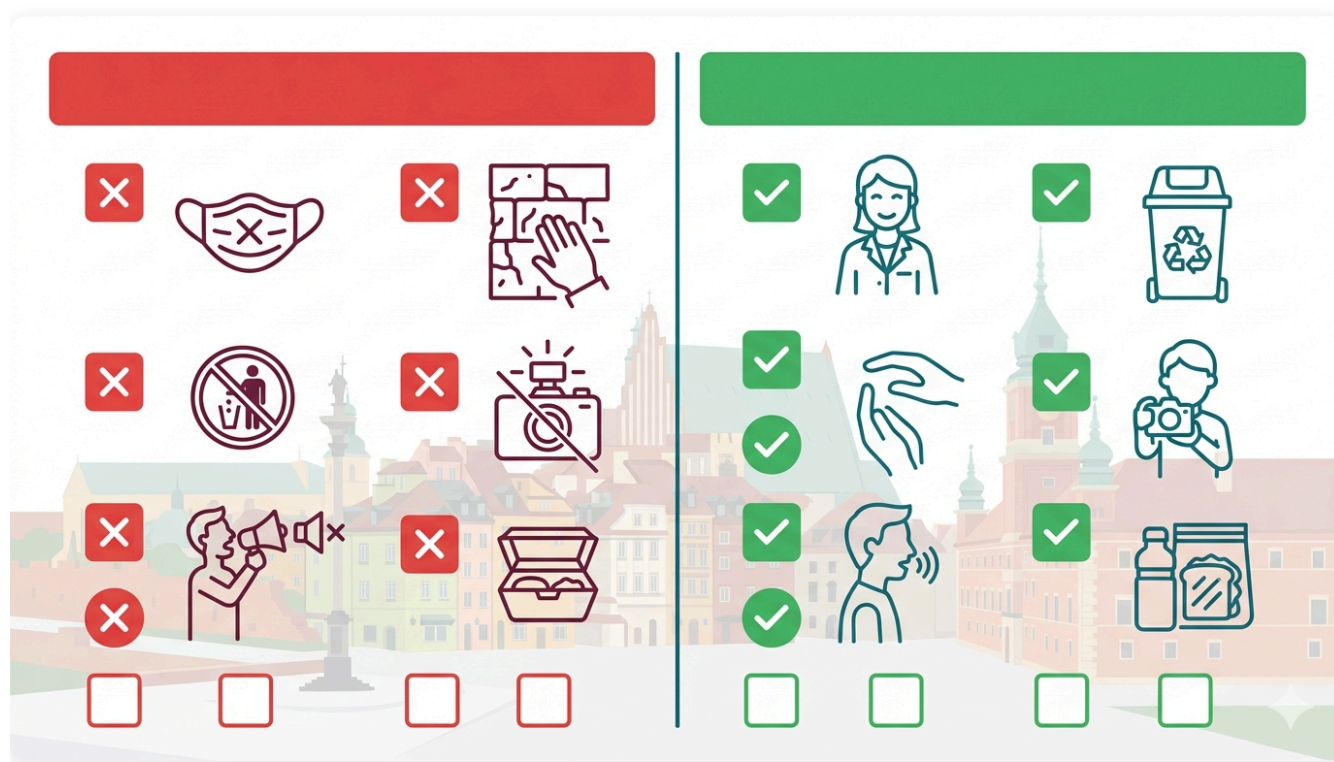
Bezpieczeństwo, prywatność i etyka AI – checklista i polityka

Lekcja: 1.4 (Moduł 1 – Fundamenty) · Czas czytania: ~6 min · Dostęp:  darmowy

⚠ **To nie jest porada prawna.** To praktyczne zasady i zdrowy rozsądek. Przy większej skali przetwarzania danych osobowych skonsultuj się ze specjalistą (np. prawnik, inspektor ochrony danych).

W skrócie

AI jest bezpieczna, jeśli trzymasz się kilku nawyków – tak jak samochód jest bezpieczny, gdy zapinasz pasy. Trzy filary: **chronić dane, sprawdzać fakty, bądź uczciwy i odpowiedzialny.**



Złota zasada danych

Zanim cokolwiek wpiszesz do AI, zapytaj: „**Czy chciałbym, żeby to trafiło na zewnątrz?**” Wiele narzędzi może wykorzystywać wpisywane treści do dalszego uczenia. Traktuj okno czatu jak rozmowę przez otwarte okno, nie jak zamknięty sejf.

Czego nie wpisywać do AI

☐ Nie wpisuj	☒ Bezpiecznie
Dane osobowe klientów (nazwisko + adres, PESEL, telefon)	Treści ogólne i przykładowe
Umowy, faktury, dane finansowe	Szkice bez prawdziwych danych
Dane medyczne, wrażliwe	Pytania o ogólną wiedzę
Hasła, numery kart	Teksty już publiczne
Tajemnice firmy (nieopublikowana oferta, lista kontrahentów)	—

Nawyk: pracuj na przykładach, a prawdziwe dane wstawiaj na końcu, ręcznie, u siebie.

RODO po ludzku (praktyczne wnioski)

1. Dane klientów masz **pod opieką**, nie na własność – wpisanie ich do zewnętrznego narzędzia to przekazanie dalej.
2. Jeśli używasz AI w obsłudze klienta – **informuj** o tym, nie udawaj, że zawsze odpowiada człowiek.
3. Przy większej skali danych osobowych – **konsultacja** ze specjalistą RODO.

Weryfikacja: uwaga na halucynacje

AI potrafi podać nieprawdę z pełnym przekonaniem (np. nieistniejący przepis, zmyśloną liczbę). **Co można sprawdzić – sprawdzaj u źródła:** liczby, daty, przepisy, nazwy własne, cytaty. Im wyższa stawka, tym dokładniejsza kontrola.

Etyka w trzech punktach

- **Przejrzystość** – nie udawaj tam, gdzie dla odbiorcy liczy się autentyczność.
- **Cudze prawa** – inspiracja tak; podrabianie stylu, znaków i tekstów chronionych – nie.
- **Odpowiedzialność** – co publikujesz, jest Twoje, niezależnie od tego, kto to napisał.

Checklista bezpieczeństwa (przed każdym użyciem)

- ☐ Czy w tym, co wpisuję, są dane poufne? Jeśli tak – podmieniam na przykładowe.
- ☐ Czy są fakty do sprawdzenia? Sprawdzam u źródła.
- ☐ Czy przeczytałem całość i poprawiłem pod swój głos?
- ☐ Czy biorę odpowiedzialność za tę treść wobec odbiorcy?

Szablon: mini-polityka AI w firmie (1 strona)

Skopiuj i uzupełnij. Działa nawet jeśli pracujesz sam – a jest niezbędny, gdy masz zespół.

1. Jakich danych NIE wpisujemy do AI: ... (np. dane osobowe klientów, umowy, dane finansowe, hasła)

2. Co ZAWSZE sprawdzamy przed wystaniem: ... (np. liczby, daty, przepisy, nazwiska, ton)

3. Kto decyduje w razie wątpliwości: ... (imię / rola)

4. Z jakich narzędzi korzystamy (sprawdzone): ... (lista 2–4 narzędzi i do czego)

Data ustalenia: ... **Przegląd co:** ... (np. co pół roku)

Dalej

- Poprzednia lekcja: **Jak rozmawiać z AI** (1.3)
- To koniec **Modułu 1 – Fundamenty**. Następny: Moduł 2 – Zastosowania.
- Strona: intelligentnatransformacja.org.pl