PRZYKŁAD SYNTETYCZNY — TO NIE JEST OCENA KLIENTA

Europe Cyber-Safe

Paszport stosowania AI — oświadczenie z samooceny

Organizacja	Przykładowa Agencja Kreatywna sp. z o.o. (15 osób)	**Numer referencyjny**	SAMPLE-0002
Data wypełnienia	2026-10-30	**Osoba wypełniająca**	director@example.com
Zestaw pytań	v1.1-EU-pl (EU, pl) · `3ccebb07e6df1053`		

> **Samoocena wypełniona przez organizację. Odpowiedzi nie zostały zbadane przez Europe Cyber-Safe ani przez nikogo innego. Niniejszy raport nie stanowi porady prawnej.**

Raport opisuje stan wyłącznie na dzień wypełnienia.

Oceny obszarów

Każdy obszar otrzymuje ocenę na podstawie udzielonych odpowiedzi: czerwony, jeśli którakolwiek odpowiedź wyzwala poziom czerwony; w przeciwnym razie żółty, jeśli którakolwiek odpowiedź ma poziom żółty lub pozostała bez odpowiedzi; w pozostałych przypadkach zielony. Ocena ogólna nie jest wyznaczana.

Obszar	Ocena
D1 Wykaz narzędzi AI	CZERWONY
D2 Ochrona danych	CZERWONY
D3 Zarządzanie i polityka	CZERWONY
D4 Nadzór człowieka	ŻÓŁTY
D5 Nadzór nad dostawcami	ŻÓŁTY
D6 Reagowanie na incydenty AI	ŻÓŁTY

Działania

Najpierw obszary czerwone, następnie działania najszybsze do wykonania.

#	Obszar	Działanie	Nakład pracy
1	D1	Wyznaczyć właściciela wykazu i wpisać go do polityki korzystania z AI.	godzina
2	D1	Wpisać kwartalną kontrolę wykazu do kalendarza wyznaczonego właściciela.	godzina
3	D2	Dodać do klauzuli informacyjnej część o korzystaniu z AI, wskazując cele i kategorie dostawców; opublikować ją i poinformować pracowników.	godzina
4	D2	Przekazać wszystkim pracownikom listę zakazanych danych i umieścić ją w widocznym miejscu tam, gdzie używa się narzędzi.	godzina

PRZYKŁAD SYNTETYCZNY — TO NIE JEST OCENA KLIENTA

5	D2	Zapisać dla każdego narzędzia lokalizację danych i mechanizm przekazywania na podstawie dokumentacji dostawcy; jeśli dane opuszczają EOG, potwierdzić mechanizm (decyzja stwierdzająca odpowiedni stopień ochrony albo standardowe klauzule umowne UE wraz z oceną skutków przekazania).	godzina
6	D2	Dla każdego narzędzia znaleźć funkcję usuwania danych lub umowne zobowiązanie do ich usunięcia; wycofać narzędzia, w których nie ma ani jednego, ani drugiego, jeśli przetwarzane są w nich dane osobowe.	godzina
7	D3	Wyznaczyć osobę podejmującą decyzje w sprawach AI i spisać trzy pytania, które zadaje ona przed dopuszczeniem narzędzia do użytku (jakie dane, na jakich warunkach, kto sprawdza wyniki).	godzina
8	D1	Uzupełnić wykaz narzędzi AI przy użyciu szablonu; zapytać każdego kierownika zespołu, z jakich narzędzi korzysta on i jego zespół, w tym z rozszerzeń przeglądarki i aplikacji na telefon.	dzień
9	D1	Natychmiast przestać wprowadzać dane osobowe do narzędzi na warunkach konsumenckich lub nieznanych. Przenieść to użycie do planu biznesowego z umową powierzenia przetwarzania danych albo z niego zrezygnować.	dzień
10	D1	Sprawdzić ustawienia AI w każdym ważnym produkcie (transkrypcja spotkań, streszczanie, autouzupełnianie) i dodać je do wykazu; zdecydować, które z nich wyłączyć.	dzień
11	D2	Wypełnić szablon analizy wstępnej DPIA dla każdego narzędzia, które ma styczność z danymi osobowymi; przeprowadzić pełną DPIA, jeśli wynika to z analizy.	dzień
12	D3	Przyjąć szablon polityki korzystania z AI (dwie strony), uzyskać podpis właściciela, przekazać ją wszystkim pracownikom i odnotować, kto się z nią zapoznał.	dzień
13	D3	Przeprowadzić dla wszystkich pracowników godzinną sesję uświadamiającą na temat AI (szablon prezentacji) i zachować listę obecności.	dzień
14	D3	Sprawdzić pięć najważniejszych umów z klientami oraz wytyczne Państwa samorządu lub organizacji zawodowej dotyczące AI pod kątem klauzul poufności i klauzul dotyczących AI; zapisać wynik.	dzień
15	D4	Poinformować pracowników o typowych błędach AI przy użyciu jednostronicowej notatki; dodać rzeczywisty przykład z Państwa branży.	godzina
16	D4	Uzgodnić prostą konwencję (stopka, pole, folder) oznaczania istotnych wyników powstałych z pomocą AI.	godzina
17	D5	Sprawdzić oświadczenie każdego dostawcy o wykorzystaniu danych; włączyć rezygnację (opt-out) lub przejść na plan wykluczający trenowanie; zapisać wynik w wykazie.	godzina
18	D5	Zebrać dla każdego dostawcy informacje ze strony o bezpieczeństwie lub z centrum zaufania (trust center) i przechowywać je razem z wykazem.	godzina
19	D5	Wyznaczyć osobę odbierającą powiadomienia od dostawców; dla każdego kluczowego narzędzia napisać jednoakapitową notatkę o wyjściu (jak wyeksportować dane, jak zakończyć korzystanie).	godzina

20	D6	Dodać incydenty AI do istniejącej procedury obsługi incydentów lub skarg, z trzema przykładami i wskazaną osobą kontaktową.	godzina
21	D6	Wyznaczyć osobę podejmującą decyzje w sprawie naruszeń i mieć pod ręką formularz zgłoszenia naruszenia Państwa organu ochrony danych oraz szablon rejestru naruszeń (art. 33 RODO wymaga dokumentowania każdego naruszenia).	godzina
22	D6	Włączyć rejestrowanie aktywności w narzędziach na planach biznesowych; jeśli nie jest dostępne, prowadzić prosty wspólny rejestr zastosowań obejmujących dane osobowe lub poufne.	godzina
23	D4	Wprowadzić imiennie przypisany etap sprawdzania wszystkich wyników AI kierowanych do klientów lub wpływających na dokumentację; włączyć go do zwykłej procedury akceptacji.	dzień
24	D5	Uzyskać od każdego dostawcy warunki planu biznesowego lub umowę powierzenia przetwarzania danych; jeśli ich brak, przestać przekazywać temu dostawcy dane osobowe.	dzień
25	D5	Przenieść narzędzia AI na konta zarządzane przez firmę z MFA; dodać je do listy kontrolnej dla odchodzących pracowników.	dzień
26	D6	Dla każdego kluczowego narzędzia raz przetestować eksport i zapisać, jak wyłączyć dostęp; przechowywać niezbędne dokumenty poza narzędziem.	dzień
27	D4	Udokumentować etap kontroli przez człowieka, podstawę prawną i przeprowadzone kontrole stronniczości; ustalić, czy zastosowanie mieści się w załączniku III aktu w sprawie sztucznej inteligencji (rozporządzenie (UE) 2024/1689, AI Act), i zaplanować spełnienie obowiązków podmiotów stosujących, które mają zastosowanie od 2 grudnia 2027 r.	tydzień

Udzielone odpowiedzi

D1 Wykaz narzędzi AI — CZERWONY

ID	Pytanie	Odpowiedź	Poziom
D1-1	Czy sporządzili Państwo wykaz wszystkich narzędzi AI używanych w firmie, w tym bezpłatnych kont, z których pracownicy korzystają na własnych urządzeniach lub z użyciem własnych danych logowania?	Brak wykazu	czerwony
D1-2	Czy którekolwiek narzędzie z wykazu otrzymuje dane osobowe klientów, pacjentów, zleceniodawców lub pracowników?	Tak - w co najmniej jednym narzędziu na warunkach konsumenckich lub na nieznanych warunkach	czerwony
D1-3	Czy wyznaczono osobę odpowiedzialną za aktualizowanie wykazu i dopuszczanie nowych narzędzi do użytku?	Nie	żółty

D1-4	Czy funkcje AI wbudowane w produkty, z których Państwo już korzystają (poczta e-mail, CRM, księgowość, przeglądarki, narzędzia do spotkań, telefony), są ujęte w wykazie?	Nie wiem	żółty
D1-5	Kiedy ostatnio porównano wykaz z tym, z czego pracownicy faktycznie korzystają?	Nigdy lub brak wykazu	czerwony

D2 Ochrona danych — CZERWONY

ID	Pytanie	Odpowiedź	Poziom
D2-1	Czy Państwa klauzula informacyjna (polityka prywatności) informuje klientów i pracowników, że używane są narzędzia AI, w jakim celu i u jakich dostawców?	Nie	czerwony
D2-2	Czy w przypadku narzędzi przetwarzających dane osobowe przeprowadzili Państwo ocenę skutków dla ochrony danych (DPIA) lub udokumentowaną analizę wstępną, z której wynika, że nie jest ona potrzebna?	Nie	czerwony
D2-3	Czy pracownicy mają pisemną listę informacji, których nigdy nie wolno wprowadzać do narzędzia AI (np. danych pacjentów, numerów kart płatniczych, identyfikatorów klientów, haseł)?	Przekazana ustnie, nic na piśmie	żółty
D2-4	Czy wiedzą Państwo, gdzie każdy dostawca przechowuje i przetwarza Państwa dane oraz czy opuszczają one Europejski Obszar Gospodarczy (EOG)?	W przypadku niektórych narzędzi	żółty
D2-5	Czy mogą Państwo usunąć dane przechowywane w każdym narzędziu AI lub zlecić ich usunięcie dostawcy, gdy przestaną Państwo z niego korzystać lub gdy zażąda tego dana osoba?	Nie wiem	żółty

D3 Zarządzanie i polityka — CZERWONY

ID	Pytanie	Odpowiedź	Poziom
D3-1	Czy istnieje pisemna polityka korzystania z AI, z którą zapoznali się pracownicy i która określa, co jest dozwolone, a co nie?	Opracowana, ale nieprzekazana	żółty
D3-2	Kto decyduje, czy nowe narzędzie AI lub nowa funkcja AI mogą być używane do celów służbowych?	Kierownictwo, nieformalnie	żółty

D3-3	Czy polityka wymienia zakazane zastosowania - np. podejmowanie decyzji dotyczących ludzi bez kontroli człowieka lub generowanie treści przedstawianych jako napisane przez człowieka, jeżeli wprowadzałoby to w błąd?	Tak	zielony
D3-4	Czy wszyscy pracownicy korzystający z narzędzi AI przeszli w ciągu ostatnich 12 miesięcy szkolenie uświadamiające obejmujące ograniczenia dotyczące wprowadzania danych, typowe błędy narzędzi i politykę?	Część pracowników	żółty
D3-5	Czy umowy z klientami, zasady zawodowe lub organ regulacyjny ograniczają sposób, w jaki mogą Państwo wykorzystywać AI w odniesieniu do informacji klientów, i czy Państwo tych ograniczeń przestrzegają?	Ograniczenia istnieją i nie mamy pewności, czy ich przestrzegamy	czerwony

D4 Nadzór człowieka — ŻÓŁTY

ID	Pytanie	Odpowiedź	Poziom
D4-1	Czy wyniki AI są sprawdzane przez kompetentną osobę, zanim trafią do klienta, do dokumentacji lub do decyzji dotyczącej konkretnej osoby?	Zazwyczaj	żółty
D4-2	Czy pracownicy korzystający z narzędzi AI znają rodzaje błędów popełnianych przez te narzędzia - zmyślone fakty i źródła, nieaktualne informacje, błędy podawane z pełnym przekonaniem, stronniczość?	Część pracowników	żółty
D4-3	Czy mogą Państwo ustalić po fakcie, które dokumenty, wiadomości e-mail lub zapisy powstały z pomocą AI?	Czasami	żółty
D4-4	Czy wyznaczona osoba odpowiada za decyzję podjętą z pomocą AI dokładnie tak samo jak za decyzję podjętą przez człowieka?	Tak	zielony
D4-5	Czy wykorzystują Państwo AI przy rekrutacji, ocenie zdolności kredytowej, ustalaniu cen, ocenie uprawnień, ocenie wyników pracy lub innych decyzjach dotyczących konkretnych osób?	Tak, z rzeczywistą kontrolą człowieka i udokumentowaną podstawą	żółty

D5 Nadzór nad dostawcami — ŻÓŁTY

ID	Pytanie	Odpowiedź	Poziom

PRZYKŁAD SYNTETYCZNY — TO NIE JEST OCENA KLIENTA

D5-1	Czy w przypadku każdego dostawcy AI, który przetwarza Państwa dane, mają Państwo umowę lub warunki obejmujące umowę powierzenia przetwarzania danych?	Dla niektórych	żółty
D5-2	Czy wiedzą Państwo, czy każdy dostawca wykorzystuje wprowadzane przez Państwa dane do trenowania lub ulepszania swoich modeli, i czy tam, gdzie to możliwe, zrezygnowali Państwo z tego (opt-out)?	Nie wiadomo	żółty
D5-3	Czy otrzymali Państwo od każdego dostawcy niezależne dowody bezpieczeństwa (np. certyfikat ISO/IEC 27001, raport SOC 2, krajowy program bazowego poziomu bezpieczeństwa, podsumowanie testu penetracyjnego)?	Nie	żółty
D5-4	Czy dostęp do każdego narzędzia AI jest kontrolowany za pomocą kont firmowych, uwierzytelniania wieloskładnikowego i usuwania dostępu po odejściu pracownika?	Częściowo	żółty
D5-5	Gdyby dostawca zmienił warunki, doznał naruszenia bezpieczeństwa lub zakończył działalność, czy dowiedzieliby się Państwo o tym i czy mają Państwo sposób, by szybko przestać z niego korzystać?	Nie	żółty

D6 Reagowanie na incydenty AI — ŻÓŁTY

ID	Pytanie	Odpowiedź	Poziom
D6-1	Czy pracownicy wiedzą, co jest incydentem AI (np. dane osobowe wklejone do narzędzia, szkodliwy lub błędny wynik, na podstawie którego podjęto działania, powiadomienie dostawcy o naruszeniu) i jak go zgłosić?	Nieformalnie	żółty
D6-2	Czy byliby Państwo w stanie dotrzymać wynikającego z RODO 72-godzinnego terminu zgłoszenia do organu ochrony danych, gdyby dane osobowe zostały ujawnione za pośrednictwem narzędzia AI?	Nie wiem	żółty
D6-3	Czy w ciągu ostatnich 12 miesięcy wystąpił u Państwa incydent AI lub czy przeprowadzili Państwo ćwiczenie sztabowe (tabletop) dotyczące takiego incydentu?	Tak	zielony
D6-4	Czy prowadzą Państwo wystarczające zapisy (kto użył jakiego narzędzia, kiedy i w jakim celu), aby po fakcie zbadać incydent AI?	Częściowo	żółty

PRZYKŁAD SYNTETYCZNY — TO NIE JEST OCENA KLIENTA

PRZYKŁAD SYNTETYCZNY — TO NIE JEST OCENA KLIENTA

D6-5	Czy mogliby Państwo w ciągu jednego dnia roboczego przestać korzystać z konkretnego narzędzia AI, gdyby zostało ono skompromitowane, bez utraty niezbędnych dokumentów firmy?	Częściowo	żółty

Przywołane wytyczne

- Akt w sprawie sztucznej inteligencji (rozporządzenie (UE) 2024/1689, AI Act), art. 26 (obowiązki podmiotów stosujących systemy AI wysokiego ryzyka) i załącznik III; w przypadku zastosowań z załącznika III obowiązki te mają zastosowanie od 2 grudnia 2027 r. na mocy rozporządzenia (UE) 2026/1744
- Akt w sprawie sztucznej inteligencji (rozporządzenie (UE) 2024/1689, AI Act), art. 4 (kompetencje w zakresie AI), stosowany od 2 lutego 2025 r. i zmieniony rozporządzeniem (UE) 2026/1744: dostawcy i podmioty stosujące muszą podejmować środki wspierające kompetencje w zakresie AI swojego personelu i innych osób korzystających z systemów AI w ich imieniu
- Akt w sprawie sztucznej inteligencji (rozporządzenie (UE) 2024/1689, AI Act), art. 50 (przejrzystość: informowanie osób, że wchodzą w interakcję z systemem AI; ujawnianie treści wygenerowanych lub zmanipulowanych przez AI), stosowany od 2 sierpnia 2026 r.
- ISO/IEC 27001:2022; krajowe programy bazowego poziomu bezpieczeństwa (np. rekomendacje CERT Polska / NASK, BSI IT-Grundschutz, CyberFundamentals); uwierzytelnianie wieloskładnikowe oraz kontrola przyjęć i odejść pracowników
- Komisja Europejska, AI literacy - Questions and Answers (2025) (kompetencje w zakresie AI - pytania i odpowiedzi)
- Opinia EROD 28/2024 w sprawie aspektów ochrony danych przy przetwarzaniu danych osobowych w kontekście modeli AI (grudzień 2024 r.); wytyczne dotyczące AI wydane przez krajowy organ ochrony danych (np. Prezes Urzędu Ochrony Danych Osobowych (UODO))
- Krajowe prawo pracy i przepisy dotyczące przedstawicielstwa pracowników (rad pracowników) w zakresie monitorowania oraz AI w rekrutacji i zarządzaniu; akt w sprawie sztucznej inteligencji (rozporządzenie (UE) 2024/1689, AI Act), załącznik III pkt 4 (zastosowania w obszarze zatrudnienia należą do wysokiego ryzyka)
- ENISA, Multilayer Framework for Good Cybersecurity Practices for AI (2023); NCSC/CISA i agencje partnerskie, Guidelines for secure AI system development (listopad 2023 r.)
- Unijne dyrektywy w sprawie równego traktowania (2000/43/WE, 2000/78/WE, 2006/54/WE) oraz krajowe przepisy antydyskryminacyjne (dyskryminacja bezpośrednia i pośrednia)
- Ogólne rozporządzenie o ochronie danych (RODO), art. 22 (zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach); wytyczne Grupy Roboczej Art. 29 w sprawie zautomatyzowanego podejmowania decyzji i profilowania (WP251 rev.01)
- Ogólne rozporządzenie o ochronie danych (RODO), art. 33-34 (zgłoszenie organowi nadzorczemu w ciągu 72 godzin, jeżeli istnieje ryzyko dla osób fizycznych; dokumentowanie każdego naruszenia); wytyczne EROD 9/2022 w sprawie zgłaszania naruszeń ochrony danych osobowych
- Ogólne rozporządzenie o ochronie danych (RODO), art. 35 (ocena skutków dla ochrony danych); wytyczne Grupy Roboczej Art. 29 dotyczące DPIA (WP248 rev.01, poparte przez EROD); wykaz rodzajów operacji przetwarzania wymagających DPIA ogłoszony przez krajowy organ ochrony danych
- Ogólne rozporządzenie o ochronie danych (RODO), rozdział V (art. 44-49): decyzje stwierdzające odpowiedni stopień ochrony; standardowe klauzule umowne (decyzja Komisji 2021/914); zalecenia EROD 01/2020 dotyczące środków uzupełniających
- Ogólne rozporządzenie o ochronie danych (RODO), art. 12-14 (informacje przekazywane osobom, których dane dotyczą)
- Wytyczne ENISA dotyczące obsługi incydentów; wytyczne krajowego zespołu CSIRT dotyczące zgłaszania incydentów; zgłaszanie na podstawie art. 23 dyrektywy NIS2 (dla podmiotów objętych jej zakresem)
- ISO/IEC 42001:2023, systemy zarządzania sztuczną inteligencją (role, ocena skutków, cykl życia, dostawcy)
- ISO/IEC 27001:2022, załącznik A 8.15 (rejestrowanie zdarzeń) i 8.16 (monitorowanie działań)
- NIST AI Risk Management Framework 1.0 (Govern, Map, Measure, Manage) oraz jego profil dla generatywnej AI (NIST AI 600-1)

PRZYKŁAD SYNTETYCZNY — TO NIE JEST OCENA KLIENTA

- OWASP Top 10 for LLM Applications 2025 (wstrzykiwanie poleceń (prompt injection), ujawnianie informacji wrażliwych, łańcuch dostaw)
- Wytyczne ENISA dotyczące bezpieczeństwa łańcucha dostaw ICT; dyrektywa NIS2, art. 21(2)(d) - bezpieczeństwo łańcucha dostaw (dla podmiotów objętych jej zakresem)

Wytyczne to publicznie dostępne źródła wymienione dla wygody; przed oparciem się na nich należy sprawdzić ich aktualną wersję. Niniejsze oświadczenie nie stanowi porady prawnej ani certyfikatu.