

AI ACT

Co oznaczać, czego nie oznaczać i gdzie najłatwiej się wyłożyć

13 sierpia 2026

tomasz.turba@securitum.pl



konsultacja prawna:

Mikołaj Prochownik - Radca prawny w **Konieczny Wierzbicki Kancelaria Radców Prawnych**

> 14 666 uczestników

Sekurak.Academy

> 1 337 uczestników

NIS2 Academy



sekurak.pl



SOS.SEKURAK.PL

szkolenia.sekurak.pl

securitum.pl

hackingparty.pl

ksiazka.sekurak.pl

securITum



Tomasz Turba

certified ethical hacker, phdc in AI

20+ lat w hackowaniu świata

10+ lat w AI



185 000 osób przeszkolonych z AI



Przedstawione informacje służą tylko celom edukacyjnym

Dlaczego robimy szkolenie?

AI jest dzisiaj **ogromne** i jest **wszędzie**

Strach przed nową technologią

Przystępny zakres wiedzy bardzo podstawowej **za darmo**

Jeżeli to świat dla Ciebie to zapraszamy na pełne szkolenie

Narzędziownik AI 3.0 Revolutions [NAI.sekurak.pl]

[**20** sesji szkoleniowych w 5 aktach; ćwiczenia; playbooki; dokumenty; nagrania; certyfikaty; dedykowane QA]

Ten sam **trener** co tutaj :-) (podobno bardzo **przyjazny**)

Logistyka szkolenia

~1,5 godziny i sesja Q&A

Przerwa - 2x 5 min

Pytania - w dowolnym momencie z Q:

nagranie, prezentacja, certyfikaty, checklista decyzyjna - w mailingu

Agenda

01 Co zmieniło się 2 i 11 sierpnia 2026

02 Role, klasyfikacja i drzewo decyzji

03 Teksty i kontrola redakcyjna

04 Grafika, audio, wideo i deepfake

05 Marketing i social media: przypadki

06 Jak, gdzie i czym oznaczać

07 Proces, nadzór w Polsce, dowody

08 Q&A



ZACZNIJMY OD DWÓCH ZŁYCH SKRAJNOŚCI

OZNACZAĆ WSZYSTKO?
NIE.

NIE OZNACZAĆ NICZEGO?
TEŻ NIE.

Decydują: rola + rodzaj treści + kontekst + realna kontrola człowieka

Nazwa narzędzia sama nie daje odpowiedzi.

01

Co zmieniło się 2 i 11 sierpnia 2026

Art. 50 zaczął być stosowany 2 sierpnia. Polska ustawa o systemach AI weszła w życie 11 sierpnia.

ART. 50

ROLE

TERMINY

AI Act w jednym kadrze

Rozporządzenie (UE) 2024/1689 tworzy warstwowy system obowiązków, a nie jeden znaczek "AI".



02.02.2025

ZAKAZANE PRAKTYKI

oraz obowiązek
kompetencji AI z art. 4.
Działa od ponad roku,
także u Ciebie.

02.08.2025

GPAI I GOVERNANCE

modele ogólnego
przeznaczenia, organy,
przepisy o karach.
Dotyczy głównie
dostawców modeli.

02.08.2026

PRZEJRZYSTOŚĆ ART. 50

chatboty, deepfake, tekst
interesu publicznego.
Bez ogólnego odroczenia.

JESTEŚMY TUTAJ

2027 / 2028

SYSTEMY WYSOKIEGO RYZYKA

nowe daty po Omnibusie:
2 grudnia 2027 i 2 sierpnia
2028.

Obowiązek widocznego oznaczania jest wyjątkiem uruchamianym przez konkretny scenariusz. Nie obejmuje automatycznie każdej treści wspieranej przez AI.

Podstawa terminów: art. 113 rozporządzenia (UE) 2024/1689 w brzmieniu nadanym rozporządzeniem (UE) 2026/1744 (Digital Omnibus on AI).

Oś czasu po AI Omnibusie

Najwięcej błędów bierze się z wrzucania wszystkich terminów do jednego worka.

02.02.2025

ZAKAZANE PRAKTYKI

oraz kompetencje AI (art. 4)

02.08.2025

GPAI I GOVERNANCE

modele ogólnego przeznaczenia,
organy, kary

02.08.2026

ART. 50 I WIĘKSZOŚĆ ZASAD

przejrzystość, chatboty, deepfake,
tekst

JESTEŚMY TUTAJ

02.12.2026

KONIEC OKRESU 50 UST. 2

techniczne znakowanie u dostawców
starszych systemów

02.12.2027

HIGH-RISK, ZAŁĄCZNIK III

systemy samodzielne (art. 6 ust. 2)

02.08.2028

HIGH-RISK, ZAŁĄCZNIK I

AI w produktach regulowanych (art. 6
ust. 1)

Okres do 2 grudnia 2026 r. dotyczy wyłącznie technicznego znakowania z art. 50 ust. 2 dla części systemów obecnych na rynku przed 2 sierpnia. To nie są wakacje od oznaczania deepfake ani tekstu interesu publicznego.

Kto ma jaki obowiązek?

Pracownik zwykle działa w ramach organizacji. Nie staje się osobnym podmiotem stosującym.

DOSTAWCA

tworzy system albo zleca jego budowę i udostępnia go pod własną marką

np. producent generatora, firma z własnym asystentem

SYSTEM AI

narzędzie, model, agent, chatbot

punkt styku obowiązków

PODMIOT STOSUJĄCY

używa systemu pod własną kontrolą w działalności zawodowej

najczęściej Twoja firma

ODBIORCA

widzi, słyszy lub wchodzi w interakcję z treścią

ma dostać informację

PRACOWNIK

korzysta z ChatGPT w obowiązkach służbowych

→ podmiotem stosującym jest zasadniczo firma

AGENCJA

sama wybiera narzędzie i sposób jego użycia

→ klient nie musi być dostawcą tego systemu

Rola nie jest etykietą raz na zawsze. Zmienia się razem z tym, kto wybiera narzędzie, kto kontroluje sposób użycia i pod czyją marką materiał trafia do odbiorcy.

Cztery zdania, które porządkują 2026

01

Art. 50 stosuje się od 2 sierpnia 2026

Dla chatbotów, deepfake i tekstów interesu publicznego nie ma ogólnego odroczenia.

02

Okres przejściowy do 2 grudnia jest wąski

Dotyczy technicznego znakowania przez dostawców części starszych systemów.

03

Nie oznaczamy wstecz treści sprzed 2 sierpnia

Ponowna publikacja lub nowa dystrybucja po tej dacie wymaga świeżej oceny kontekstu.

04

Polska ustawa nie zatrzymuje rozporządzenia UE

Dz.U. 2026 poz. 1003: organ i piaskownice od 11 sierpnia, kontrole, postępowania i kary od 28 października.

Stan prawny na 12 sierpnia 2026 r. Podstawy: rozporządzenie (UE) 2024/1689, rozporządzenie (UE) 2026/1744 (Digital Omnibus on AI), ustawa z 3 lipca 2026 r. o systemach sztucznej inteligencji (Dz.U. 2026 poz. 1003).

Ustawa o systemach AI: co weszło 11 sierpnia

Rozporządzenie UE działa bezpośrednio. Ustawa krajowa dokłada organ, procedury i sankcje.

27.07.2026 · OGŁOSZENIE

Ustawa z 3 lipca 2026 r. o systemach sztucznej inteligencji, Dz.U. 2026 poz. 1003. Zmienia przy okazji dziesięć innych ustaw.

11.08.2026 · WEJŚCIE W ŻYCIE

Powstaje KRIBSI jako organ nadzoru rynku i pojedynczy punkt kontaktowy (art. 5). Ruszają piaskownica i środki wspierające innowacyjność.

28.10.2026 · EGZEKWOWANIE

Rozdziały 3, 4, 5, 8 i 9 oraz art. 8-18: kontrole, postępowania, kary i opinie indywidualne (art. 127).

CZEGO USTAWA NIE ZMIENIA

Art. 50 obowiązuje od 2 sierpnia 2026 r. niezależnie od krajowego kalendarza. Brak powołanego organu to nie okres przejściowy. Materiał opublikowany dziś zwykle jest dostępny także po 28 października.

KOGO USTAWA NIE OBEJMUJE

Osoby fizycznej używającej AI wyłącznie prywatnie, poza działalnością zawodową, gospodarczą i rolniczą (art. 3 ust. 1 pkt 1). Obrony narodowej, służb specjalnych i badań naukowych bez testów w warunkach rzeczywistych (art. 2).

Rozporządzenie mówi, co masz zrobić. Ustawa krajowa mówi, kto Cię z tego rozliczy i w jakim trybie.

Kalendarz powołania organu: Przewodniczącego powołuje Sejm za zgodą Senatu do 11 października 2026 r., pierwsze posiedzenie Komisji do 11 listopada 2026 r. (art. 125 ust. 2 i 3).

02

Co AI zrobiła z treścią

Robocza klasyfikacja pomaga zacząć analizę. O obowiązku nadal decyduje przepis i kontekst.



ASSISTED

MANIPULATED

GENERATED

Assisted → manipulated → generated

ASSISTED

AI pomaga

research • literówki • format
kadr • kolory • kompresja

Zwykle bez widocznej etykiety

MANIPULATED

AI zmienia

argument • głos • scenę
wygląd lub funkcję produktu

Ocena skutku i autentyczności

GENERATED

AI tworzy

nowy tekst • obraz • audio
video • osobę • wydarzenie

Kontekst nadal przesądza

Pytanie kontrolne: czy AI zmieniła znaczenie, dowód albo pozorną autentyczność treści?

Standardowa edycja czy istotna zmiana?

STANDARDOWA EDYCJA

literówki i interpunkcja
format i układ
kadrowanie i rozdzielczość
kolor, kompresja, redukcja szumu
techniczna poprawa jakości

SENS I RZECZYWISTOŚĆ POZOSTAJĄ

VS

ISTOTNA ZMIANA

nowe twierdzenia i argumenty
spreparowana wypowiedź lub głos
zdarzenie, które nie miało miejsca
nieistniejąca cecha produktu
realistyczna syntetyczna osoba

ZMIENIA SIĘ PRZEKAZ LUB POZÓR AUTENTYCZNOŚCI

Jeżeli nie umiesz obronić tezy "to tylko techniczna korekta", traktuj zmianę jako istotną i przejdź pełne drzewo decyzji.

Pięć wejść do art. 50

Najpierw ustal rolę, potem scenariusz. Dopiero na końcu wybierasz komunikat.

PRZEPIS I ADRESAT	PYTANIE KONTROLNE	CO MUSISZ ZROBIĆ
ART. 50 UST. 1 DOSTAWCA	System ma bezpośrednio wchodzić w interakcję z człowiekiem?	ZAPROJEKTUJ SYSTEM TAK, BY ODBIORCA WIEDZIAŁ, ŻE ROZMAWIA Z AI
ART. 50 UST. 2 DOSTAWCA	System generuje syntetyczny obraz, audio, video lub tekst?	ZNAKUJ WYJŚCIA MASZYNOWO CZYTELNE I W SPOSÓB WYKRYWALNY
ART. 50 UST. 3 PODMIOT STOSUJĄCY	Rozpoznawanie emocji albo kategoryzacja biometryczna?	POINFORMUJ OSOBY PODDANE DZIAŁANIU SYSTEMU I PILNUJ PODSTAWY W RODO
ART. 50 UST. 4 PODMIOT STOSUJĄCY	Obraz, audio lub video spełnia test deepfake?	UJAWNIJ WIDOCZNIE LUB SŁYSZALNIE
ART. 50 UST. 4 AK. 2 PODMIOT STOSUJĄCY	Tekst publikowany, by informować opinię publiczną o sprawie interesu publicznego?	UJAWNIJ, CHYBA ŻE DZIAŁA WYJĄTEK REDAKCYJNY

Żaden z tych scenariuszy: art. 50 zwykle nie wymaga widocznej etykiety. Formę i moment określa art. 50 ust. 5: jasno, rozróżnialnie, najpóźniej przy pierwszej interakcji lub ekspozycji, zgodnie z wymogami dostępności.

Dostawca i podmiot stosujący: inny zakres

Ta sama treść, inny przepis i inny obowiązek. Najpierw ustal, w jakiej roli występujesz.

DOSTAWCA · ART. 3 PKT 3

Tworzy system albo zleca jego zbudowanie i wprowadza go do obrotu lub oddaje do użytku **pod własną nazwą lub znakiem towarowym**.

art. 50 ust. 1 informacja o interakcji, wbudowana w projekt systemu

art. 50 ust. 2 maszynowo czytelne znakowanie wyjść

Typowo: producent generatora, firma z własnym asystentem.

PODMIOT STOSUJĄCY · ART. 3 PKT 4

Używa systemu **pod własną kontrolą** w działalności zawodowej, na własną odpowiedzialność.

art. 50 ust. 3 informacja przy rozpoznawaniu emocji i biometrii

art. 50 ust. 4 ujawnienie deepfake i tekstu interesu publicznego

Typowo: agencja, redakcja, marketing, Twoja firma.

KIEDY PODMIOT STOSUJĄCY STAJE SIĘ DOSTAWCĄ

WŁASNA MARKA

Oddajesz do użytku cudzy system pod swoją nazwą lub znakiem towarowym (art. 3 pkt 3, dla wysokiego ryzyka wprost art. 25 ust. 1 lit. a).

ISTOTNA MODYFIKACJA

Zmieniasz system wysokiego ryzyka tak głęboko, że nadal jest wysokiego ryzyka (art. 25 ust. 1 lit. b).

ZMIANA PRZEZNACZENIA

Używasz systemu w sposób, który czyni z niego system wysokiego ryzyka (art. 25 ust. 1 lit. c).

Sam prompt, persona czy podłączenie API zwykle nie czynią Cię dostawcą. Decyduje wprowadzenie do obrotu lub oddanie do użytku pod własną marką. Skutek zmiany roli: przejmujesz pełny pakiet obowiązków dostawcy.

03

Teksty i kontrola redakcyjna

Nie każdy tekst z AI trzeba oznaczyć. Dla spraw publicznych liczy się cel publikacji i realna odpowiedzialność człowieka.

INTERES PUBLICZNY

REVIEW

ODPOWIEDZIALNOŚĆ

Trzy bramki interesu publicznego

Dopiero komplet odpowiedzi TAK uruchamia obowiązek, z zastrzeżeniem wyjątku redakcyjnego.

01**TEKST**

AI wygenerowała go lub istotnie zmieniła?

TAK

02**CEL PUBLIKACJI**

ma informować opinię publiczną?

TAK

03**TEMAT**

dotyczy sprawy interesu publicznego?

TAK

**3×
TAK**

dopiero komplet uruchamia
obowiązek ujawnienia

WYNIK PRZY 3× TAK

Oznacz tekst jako wygenerowany lub istotnie zmodyfikowany przez AI, jasno i najpóźniej przy pierwszej ekspozycji (art. 50 ust. 4 akapit 2 oraz ust. 5).

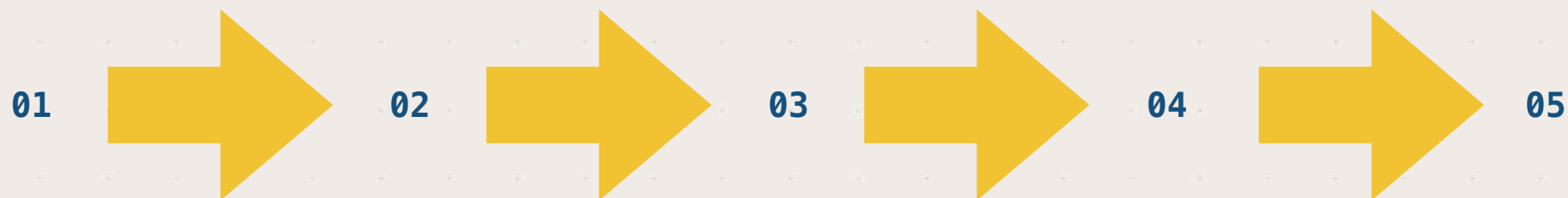
WYJĄTEK REDAKCYJNY

Nie oznaczasz, jeżeli tekst przeszedł merytoryczną kontrolę człowieka, ktoś ponosi odpowiedzialność redakcyjną i to człowiek zdecydował o publikacji.

Przykładowe tematy interesu publicznego: zdrowie • bezpieczeństwo konsumentów • środowisko • regulacje • cyberbezpieczeństwo • ważne zdarzenia gospodarcze.

"Wygląda dobrze" to nie kontrola

Kontrola jest merytoryczna, udokumentowana i daje człowiekowi realną władzę nad publikacją.



OTWÓRZ
ŹRÓDŁA

ZWERYFIKUJ
TWIERDZENIA

SPRAWDŹ DATY,
LICZBY, NAZWISKA

POPRAW LUB
ODRZUĆ

ZATWIERDŹ I WEŹ
ODPOWIEDZIALNOŚĆ

NIE WYSTARCZY

drugi model • kilka przecinków • szybki rzut oka

MUSI BYĆ

konkretna osoba • data • możliwość odrzucenia

PO ZMIANIE AI

istotna ponowna edycja = ponowny review

Odpowiedzialność redakcyjna nie oznacza automatycznie działu prawnego. Oznacza nazwanego właściciela decyzji.

Teksty: sześć szybkich werdyktów



AI robi research, człowiek sprawdza źródła i pisze

NIE OZNACZAĆ

AI poprawia literówki, format i przecinki

NIE OZNACZAĆ

AI tworzy zwykły opis szkolenia lub produktu

ZWYKLE NIE

AI pisze artykuł o podatności bez realnego review

OZNACZAĆ

Ten sam artykuł po udokumentowanej kontroli redakcyjnej

NIE, WYJĄTEK

Reklama zawiera twierdzenia o zdrowiu, bezpieczeństwie lub ekologii

TO ZALEŻY

Zwykła reklama nie staje się sprawą interesu publicznego tylko dlatego, że użyto AI.

04

Grafika, audio, wideo i deepfake

Deepfake jest szerszy niż podmiana twarzy. Liczy się podobieństwo do istniejącej rzeczywistości i pozór autentyczności.

3 TESTY

KONTEKST

PIERWSZY KONTAKT

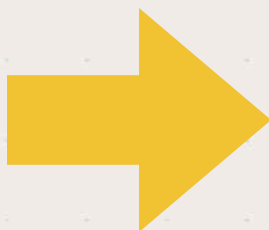
Deepfake: trzy testy łącznie

Jeżeli którykolwiek warunek odpada, materiał nie spełnia pełnej definicji deepfake z AI Act.

01

FORMAT + AI

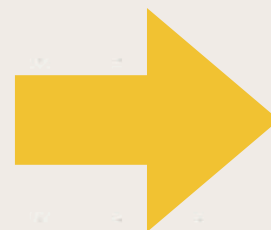
obraz, audio lub video
wygenerowane albo zmienione przez
AI



02

PODOBIENSTWO

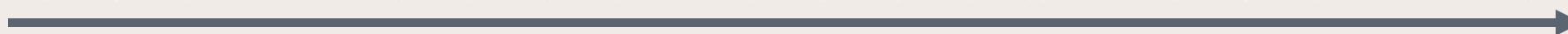
do istniejącej osoby, obiektu,
miejsca, podmiotu lub wydarzenia



03

POZÓR AUTENTYCZNOŚCI

w kontekście może fałszywie
wyglądać na autentyczne



**DEEPPFAKE
OZNACZAĆ**

Test wykonuje się oczami przeciętnego odbiorcy i w realnym kontekście publikacji. Zgoda osoby na użycie wizerunku nie usuwa obowiązku transparentności, jeśli materiał nadal jest deepfakiem.

Od jawnej fikcji do pozoru dokumentu

CYBERPUNKOWY TOMEK

wojownik z mieczem, ewidentna fantazja

ZWYKLE NIE DEEFAKE

JAWNA FIKCJA

SYNTETYCZNY INFLUENCER

realistycznie testuje prawdziwy produkt

OZNACZAĆ

KONTEKST ZMIENIA WYNIK

AWATAR PREZESA

mówi słowa, których prezes nie nagrał

OZNACZAĆ

POZÓR AUTENTYCZNOŚCI

Klucz: nie pytaj tylko "czy wygląda realistycznie?". Pytaj też: kogo lub co przypomina, co sugeruje i czego odbiorca spodziewa się w tym kanale.

Sztuka, satyra i ewidentna fikcja mogą korzystać z łagodniejszej formy ujawnienia, która nie psuje odbioru dzieła. To nadal ocena kontekstowa, nie automatyczne zwolnienie.

Przykład 1

CYBERPUNKOWY TOMEK

wojownik z mieczem, ewidentna
fantazja

ZWYKLE NIE DEEPPFAKE



Przykład 2

SYNTETYCZNY INFLUENCER

realistycznie testuje prawdziwy
produkt

OZNACZAĆ

KONTEKST ZMIENIA WYNIK

Grok Segments



AWATAR PREZESA

mówi słowa, których prezes nie
nagrał

OZNACZAĆ

POZÓR AUTENTYCZNOŚCI

AI MODIFIED



Głos, awatar, produkt, zdarzenie

Sklonowany głos prawdziwego prowadzącego

OZNACZAĆ

Awatar CEO przekazuje wypowiedź, której CEO nie nagrał

OZNACZAĆ

Prawdziwy produkt na wygenerowanym tle bez zmiany cech

ZWYKLE NIE

AI dodaje produktowi funkcję albo efekt, którego nie ma

OZNACZAĆ + RYZYKO REKLAMOWE

Wygenerowany pożar, protest lub włamanie wyglądające jak news

OZNACZAĆ

AI dubbing: samo tłumaczenie kontra sklonowany głos konkretnej osoby

TO ZALEŻY, DOMYŚLNIE OSTROŻNIE

Samo tłumaczenie, które nie imituje konkretnej osoby, zwykle nie uruchamia art. 50 ust. 4. Sklonowany głos, twarz albo ruch ust realnej osoby to już materiał do testu deepfake. Wyjątek dla treści artystycznych nie jest tu oczywisty, więc domyślnie stosuj podejście ostrożnościowe.

Etykieta nie legalizuje braku zgody, naruszenia praw autorskich ani reklamy wprowadzającej w błąd.

05



Marketing i social: przypadki

Przećwiczmy decyzję na sytuacjach, które naprawdę trafiają do publikacji, a nie na abstrakcyjnych definicjach.

WERDYKT

UZASADNIENIE

RYZYKO

Cztery materiały przed publikacją

POST NAPISANY PRZEZ AI

Pracownik tylko kliknął "approve".

TO ZALEŻY

Czy spełnia definicję deepfake? Czy temat jest publiczny? Czy review było realne?

PRODUKT + NOWE TŁO

Produkt i jego cechy są niezmienione.

ZWYKLE NIE

Tło nie może sugerować nieistniejących faktów.

"ULEPSZONY" PRODUKT

AI pokazuje funkcję, której produkt nie ma.

OZNACZAĆ

Do tego dochodzi ryzyko reklamy wprowadzającej w błąd.

SYNTETYCZNY INFLUENCER

Realistycznie testuje prawdziwy produkt.

OZNACZAĆ

Przypomina autentyczną osobę i sytuację.

Werdykt opisuje obowiązek z art. 50. Przy systemach wysokiego ryzyka dochodzą odrębne obowiązki przejrzystości i informowania z art. 13, 16 i 26 rozporządzenia, czego art. 50 ust. 6 nie uchyla. Inne przepisy mogą dać dodatkowy zakaz lub obowiązek.

Cztery materiały przed publikacją

POST NAPISANY PRZEZ AI

Pracownik tylko kliknął "approve".

TO ZALEŻY

Czy spełnia definicję deepfake? Czy temat jest publiczny? Czy review było realne?

*Napisz mi tekst promujący nowe super lekarstwo - **Sekurakomarin**, który poprawia koncentrację, ułatwia nabywanie wiedzy i podnosi kompetencje*

SEKURAKOMARIN™ — na przewlekły niedobór kompetencji

Masz problemy z koncentracją? Nowa wiedza wylatuje z głowy szybciej niż niezatana podatność trafia do exploit-db? Sięgnij po **Sekurakomarin™** — skoncentrowaną dawkę praktycznej wiedzy od Sekuraka.

Regularne stosowanie:

- ✓ poprawia koncentrację,
- ✓ ułatwia przyswajanie wiedzy,
- ✓ podnosi kompetencje,
- ✓ zmniejsza podatność na cyberbzdury.

Dawkowanie: szkolenia, artykuły i materiały Sekuraka — najlepiej regularnie.

Możliwe działania niepożądane: nagła potrzeba aktualizowania systemów, poprawiania hasel oraz tłumaczenia współpracownikom, dlaczego „u mnie działa” nie kończy analizy incydentu.

Sekurakomarin™. Wiedza, która zaczyna działać od pierwszej dawki.



AI MODIFIED

Cztery materiały przed publikacją

PRODUKT + NOWE TŁO

Produkt i jego cechy są niezmienione.

ZWYKLE NIE

Tło nie może sugerować nieistniejących faktów.



Cztery materiały przed publikacją

"ULEPSZONY" PRODUKT

AI pokazuje funkcję, której produkt nie ma.

OZNACZAĆ

Do tego dochodzi ryzyko reklamy wprowadzającej w błąd.

AI MODIFIED



Cztery materiały przed publikacją

SYNTECYZNY INFLUENCER

Realistycznie testuje prawdziwy produkt.

OZNACZAĆ

Przypomina autentyczną osobę i sytuację.



Kiedy zgoda nie wystarcza

AWATAR CEO

CEO zgadza się na publikację, ale nie nagrał tej wypowiedzi.

OZNACZAĆ

Zgoda rozwiązuje część ryzyk, nie usuwa deepfake.

KLON GŁOSU

Syntetyczny lektor brzmi jak realny prowadzący.

OZNACZAĆ

Audio może spełnić wszystkie trzy testy.

CLAIM: ZDROWIE / EKO

AI tworzy reklamowe twierdzenie o wpływie produktu.

TO ZALEŻY

Może być tekstem informującym o interesie publicznym.

AGENCJA NIE MÓWI O AI

Klient publikuje materiał, nie wiedząc, że powstał w AI.

NIE DA SIĘ SPEŁNIĆ ART. 50 UST. 5

Bez historii powstania nie ujawnisz AI przy pierwszej ekspozycji.
Ujawnienie wpisz do umowy.

Transparentność odpowiada na pytanie "co widzi odbiorca". Zgoda odpowiada na inne pytanie.

Najwięcej ginie na przekazaniu materiału

Platforma, format i eksport potrafią usunąć kontekst, oznaczenie albo metadane.



Minimum w zleceniu: narzędzia • typ użycia AI • odpowiedzialność za ocenę • obowiązek zachowania oznaczeń • przekazanie dowodów.

przerwa NAI.sekurak.pl



-75% rabatu tylko dziś 13.08, do godz. 23:59

później rabat spada...

startujemy 24 września 2026

06

Jak i gdzie oznaczać

Właściwy komunikat w złym miejscu nie spełnia celu. Odbiorca ma go zauważyć przy pierwszym kontakcie.

WIDOCZNE

SŁYSZALNE

WYKRYWALNE

AI ACT / PRAKTYKA / 2026



Maszyna wykrywa. Człowiek rozumie.

DOSTAWCA / ART. 50(2)

TECHNICZNE ZNAKOWANIE

metadane

znak wodny

Content Credentials / C2PA

inne mechanizmy maszynowo wykrywalne

ma być skuteczne, interoperacyjne, odporne i wiarygodne



ART. 50(1) DOSTAWCA • ART. 50(3), (4) PODMIOT STOSUJĄCY

INFORMACJA DLA ODBIORCY

etykieta na obrazie lub poście

plansza / overlay w wideo

komunikat audio

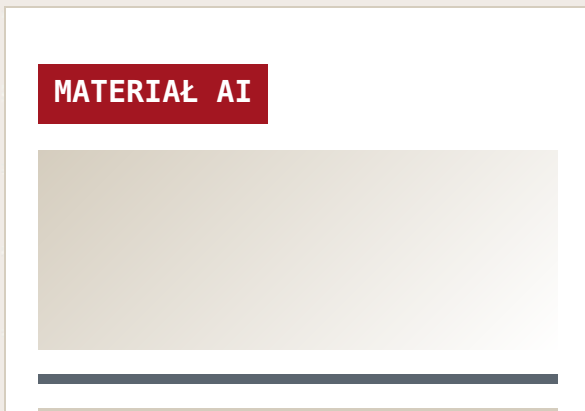
informacja przed pierwszą interakcją

ma być jasna, rozróżnialna i dostępna

Metadane nie wystarczą do oznaczenia deepfake, jeśli odbiorca potrzebowałby specjalnego narzędzia, aby je odczytać. Formę i moment ujawnienia narzuca art. 50 ust. 5.

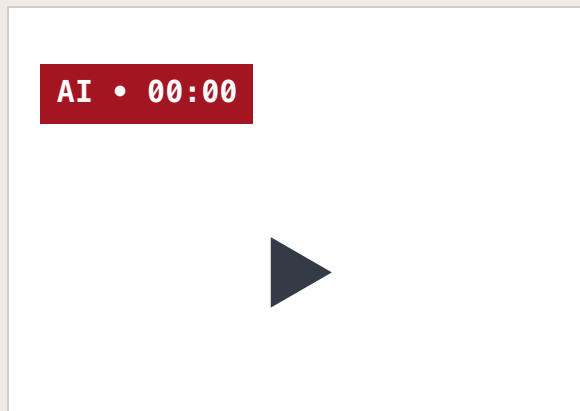
Oznaczenie musi przeżyć kanał

FEED / POST



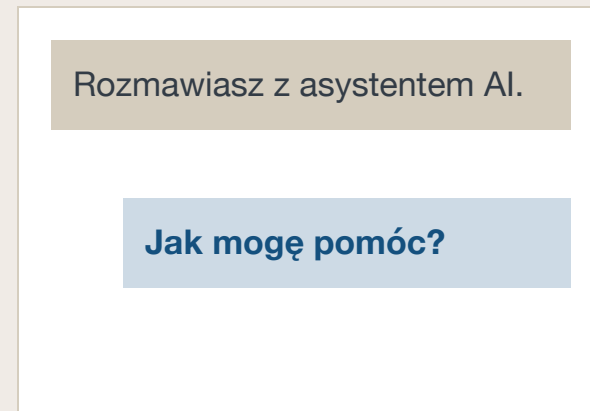
widoczne przy materiale, nie pod trzema kliknięciami

WIDEO / AUDIO



plansza lub komunikat na początku, ewentualnie także stale

CHATBOT / AGENT



najpóźniej przy pierwszej interakcji

Po publikacji: otwórz materiał jak zwykły użytkownik • sprawdź mobile i desktop • zrób screenshot • ponów ocenę po przeniesieniu na inny kanał.



Gotowe komunikaty bez prawniczego dymu

CHATBOT

Rozmawiasz z asystentem wykorzystującym sztuczną inteligencję.

OBRAZ / WIDEO / GŁOS

Materiał został wygenerowany lub istotnie zmodyfikowany przy użyciu AI.

TEKST

Tekst został wygenerowany lub istotnie zmodyfikowany przy użyciu AI.

DOBRZE

krótko • konkretnie • przy pierwszym kontakcie • dostępne

UNIKAJ

"AI mogło zostać użyte"

Ikonki

Komisja Europejska udostępniła zestaw ikon do oznaczania treści AI. Ikony są opcjonalne. Obowiązek z art. 50 nie jest.

BASIC

OGÓLNY ZNACZNIK AI

gdy trzeba zasygnalizować udział AI w deepfake albo w tekście objętym obowiązkiem

FULLY

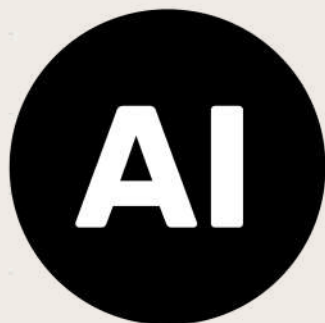
AI-GENERATED

całość powstała w AI, bez elementu stworzonego przez człowieka

PARTIALLY

AI-MODIFIED

autentyczny materiał częściowo zmieniony przez AI



Ikona to warstwa wizualna, nie dowód zgodności. Jeżeli platforma przytnie kadr albo usunie warstwę, obowiązek nadal jest po Twojej stronie. Pliki SVG i PNG w czterech wariantach kolorystycznych pobierzesz ze strony Komisji, bez wymogu atrybucji.

07

Wdrożenie, nadzór i dowody

Compliance nie kończy się na etykiecie. Potrzebujesz właścicieli, ścieżki akceptacji, śladu decyzji i wiedzy, kto Cię z tego rozliczy.

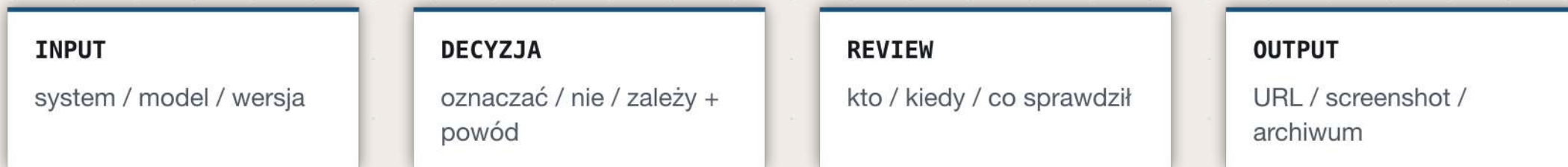
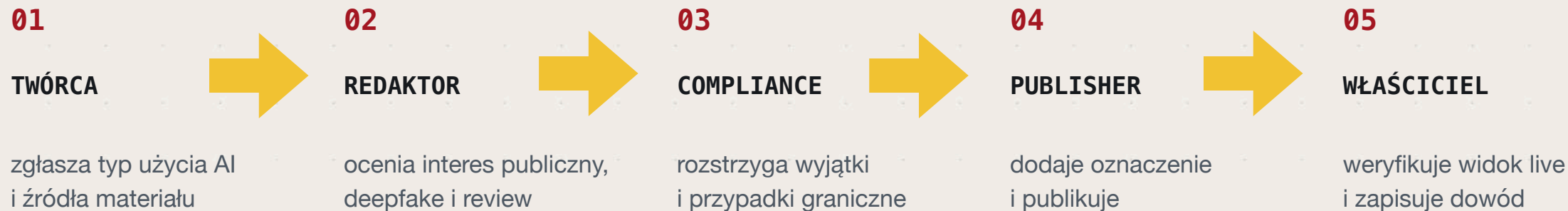
WORKFLOW

EVIDENCE

KRiBSI

Ścieżka od promptu do publikacji

Compliance wchodzi tylko tam, gdzie przypadek jest graniczny. Reszta ma działać operacyjnie.



Zasada: decyzja ma mieć właściciela. "Marketing wrzucił" nie jest właścicielem.

Dowód recenzji, sprawdzenia i historii

AIA-2026-0813-07		DECYZJA PUBLIKACYJNA
Materiał / URL	kampania / avatar-ceo-v3.mp4	
System i wersja	generator X / model Y / 2026-08	
Użycie AI	syntetyczny obraz + głos realnej osoby	
Test deepfake	TAK / TAK / TAK	
Decyzja	OZNACZAĆ przy pierwszym kontakcie	
Review / owner	A. Kowalska / 13.08.2026	
Dowód	screenshot + plik źródłowy + zgoda	

MINIMUM PÓL

ID materiału
narzędzie / wersja
typ użycia AI
temat i cel publikacji
test deepfake / public interest
decyzja + uzasadnienie
osoba zatwierdzająca
data i dowód live

Rejestr może być prostą listą w systemie, który już macie.

Nie zapisuj promptów z danymi poufnymi tylko po to, żeby "mieć compliance". Dowód ma być proporcjonalny.

Pięć wymagań dla agencji i freelancerów

- | | | |
|----|-----------------|--|
| 01 | UJAWNIENIE | jakie systemy i do czego wykorzystano |
| 02 | PRAWA | zgody na wizerunek i głos, licencje, dane wejściowe |
| 03 | OZNACZENIA | kto decyduje, kto umieszcza, kto sprawdza live |
| 04 | METADANE | nie usuwać bez zgody, raportować utratę przy eksporcie |
| 05 | DOWODY I ZMIANY | przekazać pliki, screenshoty i informować o istotnych zmianach |

Dodaj też prawo do wstrzymania publikacji. Termin kampanii nie jest wyjątkiem w AI Act.

Kompetencje do konkretnej roli

Obowiązek z art. 4 działa od 2 lutego 2025 r. Omnibus przeformułował go na obowiązek starannego działania: wspierasz rozwój kompetencji, nie gwarantujesz poziomu wiedzy konkretnej osoby.

01

TWÓRCA

halucynacje • źródła • dane
prawa • oznaczenia

02

REDAKTOR

public interest • deepfake
review • prawo do odrzucenia

03

AKCEPTUJĄCY

właściciel decyzji • dowody
eskalacja • incydenty

04

TECHNICZNY

metadane • C2PA • eksport
integracja chatbota

Program proporcjonalny: krótkie szkolenie + przykłady z własnej pracy + test scenariuszowy + aktualizacja przy zmianie narzędzi lub procesu. W Polsce KRIBSI sprawdza poziom wiedzy i kompetencji podmiotów kontrolowanych w toku kontroli (art. 25 pkt 3 ustawy).

DOWÓD

data • zakres • uczestnicy • wynik ćwiczenia • wersja instrukcji

NIE MA WYMOGU

jednego państwowego certyfikatu • AI Oficera • gwarantowania
poziomu wiedzy konkretnej osoby

Kary są górnym pułapem, nie cennikiem ikon



15 mln € LUB **3% obrotu**

naruszenie obowiązków przejrzystości, m.in. art. 50 (art. 99 ust. 4)

35 mln € LUB **7% obrotu**

zakazane praktyki AI, odrębna kategoria naruszeń (art. 99 ust. 3)

Procent może liczyć się od **całkowitego rocznego światowego obrotu przedsiębiorstwa** z poprzedniego roku obrotowego. Dla przedsiębiorstwa stosuje się wyższy z limitów, dla MŚP i startupów niższy.

POLSKA: KTO I OD KIEDY

KRiBSI nakłada kary decyzją (art. 104)

11.08.2026: wejście w życie, powstaje organ

28.10.2026: kontrole, postępowania i kary

Kara płatna w 30 dni od uprawomocnienia

Odwołanie: SOKiK w Warszawie (art. 109)

CO WPŁYWA NA KARĘ

waga, czas i skutki naruszenia

liczba odbiorców i rozmiar szkody

wielkość podmiotu i udział w rynku

współpraca i działania naprawcze

wcześniejsze naruszenia tego samego rodzaju

AI Act jest rozporządzeniem stosowanym bezpośrednio. Krajowy harmonogram organów nie zawiesza art. 50. Podanie organowi nieprawdziwych informacji to odrębna kara do 7,5 mln € lub 1% obrotu (art. 99 ust. 5).

KRiBSI: kto naprawdę kontroluje

Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji jest organem nadzoru rynku i pojedynczym punktem kontaktowym (art. 5 ustawy).

SKŁAD KOMISJI • ART. 19

Przewodniczący powoływany przez Sejm za zgodą Senatu na 5 lat (art. 28).

Dwóch Zastępców Przewodniczącego wyłanianych w naborze.
Czterech członków wskazanych przez Prezesa UOKiK, KNF, KRRiT i Prezesa UKE.

Obsługa: komórka w urzędzie ministra do spraw informatyzacji.

CO ROBI • ART. 6

Kontrola przestrzegania rozporządzenia i ustawy.

Postępowania, decyzje i administracyjne kary pieniężne.

Rejestr skarg oraz wiążące opinie indywidualne.

Piaskownica regulacyjna i wsparcie innowacyjności.

NIE TYLKO KRiBSI

Organem notyfikującym jest minister do spraw informatyzacji (art. 86). Komisja współpracuje m.in. z PUODO, UOKiK, KNF, KRRiT, UKE, koordynatorem DSA i Prokuratorem Generalnym (art. 20).

KALENDARZ POWOŁANIA

Przewodniczący do 11 października 2026 r., pierwsze posiedzenie Komisji do 11 listopada 2026 r. (art. 125). Do tego czasu obowiązki z art. 50 i tak obowiązują.

Nadzór to nie jedyna ścieżka. Za brak oznaczenia można odpowiadać już dziś: przed UOKiK za nieuczciwe praktyki rynkowe, przed KRRiT w usługach medialnych, a także cywilnie za wizerunek i prawa autorskie.

Kontrola i skarga: jak zaczyna się sprawa

Rozdziały o kontroli, postępowaniu i karach działają od 28 października 2026 r.

01

WEJŚCIE

Plan kontroli, ustalenia własne Komisji albo skarga z zewnątrz (art. 48, 49, 58).

02

ZAWIADOMIENIE

Kontrola nie wcześniej niż 7 dni po zawiadomieniu, co do zasady zdalna (art. 49).

03

OSTRZEŻENIE

Działania naprawcze wskazane przez Komisję. 21 dni na odpowiedź (art. 61).

04

DECYZJA

Usunięcie skutków w 14 dni. Przy realnym ryzyku nakaz wycofania systemu (art. 62, 63).

05

KARA

Kara płatna w 30 dni od uprawomocnienia. Odwołanie do SOKiK (art. 104, 109).

SKARGĘ MOŻE ZŁOŻYĆ KAŻDY • ART. 59

Osoba fizyczna, prawna lub jednostka organizacyjna, elektronicznie. To realne źródło spraw: konkurencja, odbiorcy, organizacje branżowe.

CZEGO NIE ROBIĆ

Utrudnianie kontroli to wykroczenie zagrożone karą ograniczenia wolności albo grzywny (art. 112). Niewykonanie decyzji o wycofaniu systemu tak samo (art. 113).

CO OBNIŻA KARĘ

Wykonanie ostrzeżenia w 3 miesiące: obniżka o 10-50% (art. 107). Układ: 20-70%, przy zgłoszeniu z własnej inicjatywy 30-90% (art. 70 i 84).

CO BOLI POZA KARĄ

Komisja publikuje decyzje w BIP oraz jawny wykaz systemów, wobec których nałożono karę (art. 66).

Zanim przyjdzie kontrola

Ustawa daje trzy mechanizmy, z których korzysta się z własnej inicjatywy.

OPINIA INDYWIDUALNA • ART. 8–16

Ocena konkretnego stanu faktycznego lub planu.

Opłata 150 zł.

Termin 30 dni, w sprawach skomplikowanych 60.

Brak odpowiedzi w terminie = opinia po Twojej myśli.

Wiąże Komisję.

Dostępna od 28 października 2026 r.

UKŁAD I SAMOZGŁOSZENIE • ROZDZ. 5

Zaprzestanie naruszenia i ujawnienie okoliczności pozwala zawrzeć układ.

Obniżka kary o 20-70%.

Przy zgłoszeniu z własnej inicjatywy o 30-90% (art. 84).

Przy nadzwyczajnych okolicznościach możliwe odstępstwo od sankcji.

PIASKOWNICA • ROZDZ. 7

Komisja ogłasza konkurs na uczestnictwo.

Dla mikro, małych i średnich firm nieodpłatnie (art. 93).

Dla JST do dwukrotności minimalnego wynagrodzenia, dla reszty do czterokrotności.

Możliwe odstępstwa i wsparcie w dochodzeniu do zgodności.

OBNIŻKA ZA REAKCJĘ • ART. 107

Wykonanie działań z ostrzeżenia w 3 miesiące od doręczenia decyzji obniża karę o 10-50%, o ile naruszenie nie doprowadziło do śmierci ani poważnego uszczerbku na zdrowiu.

KOSZT REPUTACYJNY • ART. 66

Komisja publikuje treść decyzji w Biuletynie Informacji Publicznej i prowadzi jawny wykaz ukaranych systemów wraz z opisem ich działania.

Rejestr decyzji publikacyjnych, który budujecie dzisiaj, jest dokładnie tym materiałem, o który poprosi kontrola i który uzasadnia obniżkę kary.

Minimum compliance w 7 dni

D1

D2

D3

D4

D5

D6

D7

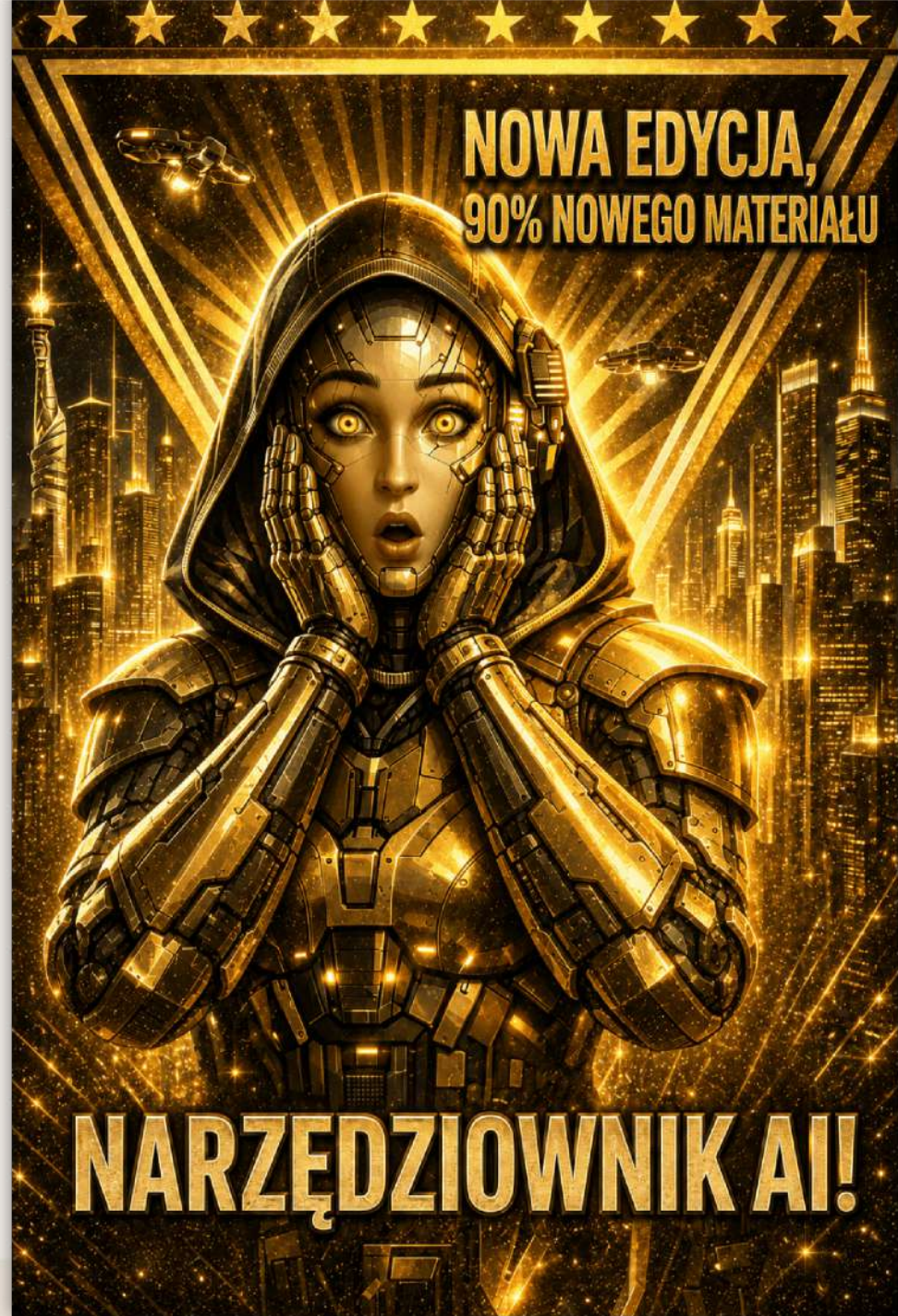
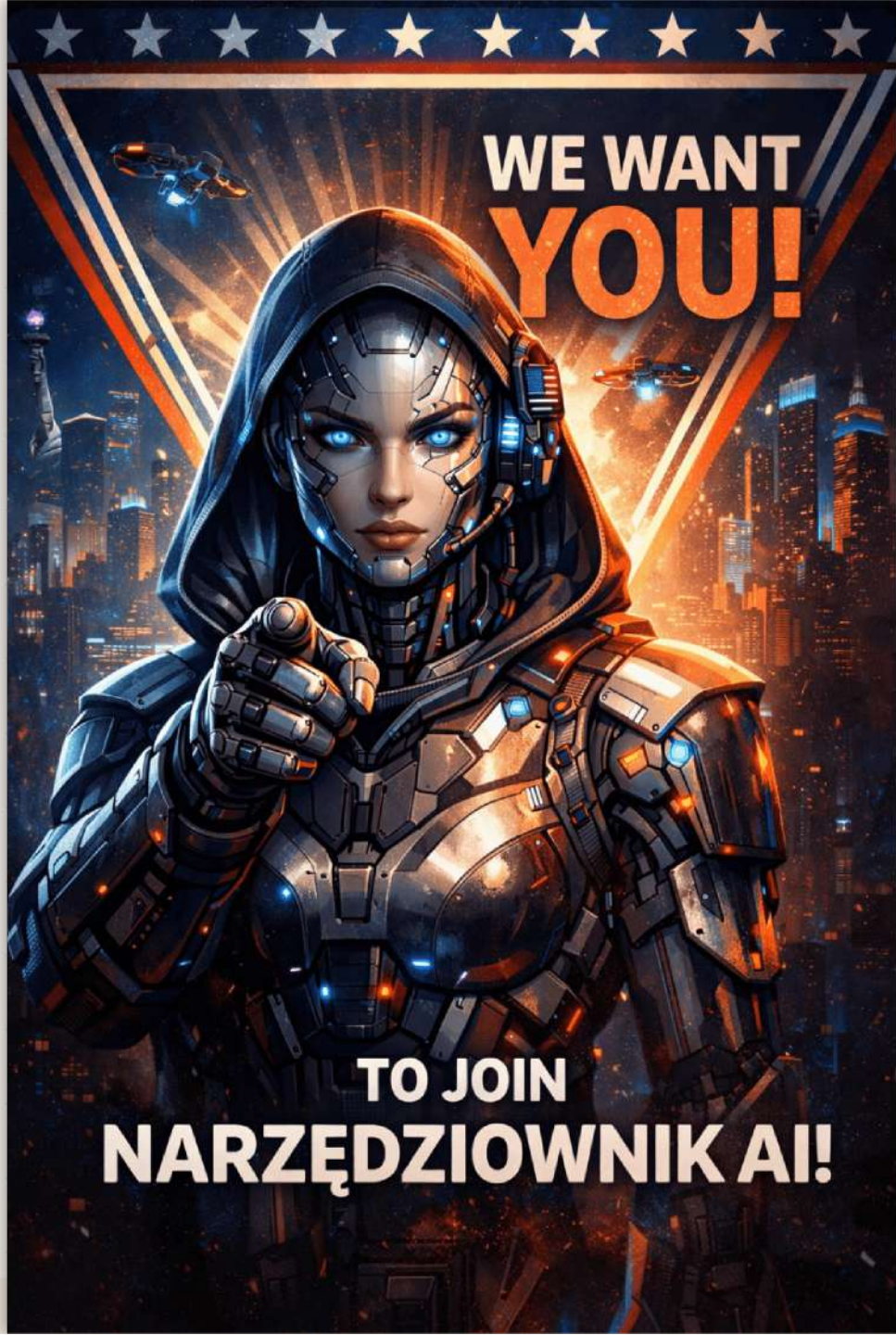
INWENTARYZACJA**ROLE****TAKSONOMIA****KOMUNIKATY****REVIEW + DOWÓD****UMOWY****ĆWICZENIE**systemy • kanały •
agencjeprovider • deployer •
ownerassisted • deepfake
• public interestcopy • miejsce •
dostępnośćchecklista • rejestr •
screenshotagencje • metadane
• odpowiedzialnośćszkolenie • dry run •
poprawki

Cel po tygodniu: każda publikacja z AI ma właściciela, ścieżkę decyzji, właściwe oznaczenie i dowód tego, co zobaczył odbiorca.

PODSUMOWANIE

NARZĘDZIE NIE PRZESĄDZA. KONTEKST PRZESĄDZA.

- 01 Chatbot informuje o AI najpóźniej przy pierwszej interakcji.
- 02 Deepfake oznaczamy widocznie lub słyszalnie przy pierwszym kontakcie.
- 03 Tekst interesu publicznego: oznaczenie albo realny wyjątek redakcyjny.
- 04 Metadane, ikona UE i platformowy label nie zwalniają z weryfikacji widoku odbiorcy.
- 05 Zapisz decyzję, właściciela i dowód. Przeszkol role, które publikują.



Narzędziownik AI - nowe szkolenie!

3.0 Revolutions

9 edycja!

5 modułów po **4** szkolenia każdy

20 spotkań na żywo po **2-3** godz.

Nagrania na zawsze

Certyfikat PL i EN

Ćwiczenia

Checklisty

Dokumenty

Minibook PDF

Test sprawdzający wiedzę

Discord społeczności AI

Narzędziownik AI 3.0

Moduł I: Jak się odnaleźć w świecie AI?

SESJA 1: AI 2026 BEZ LUKRU: CO DZIAŁA, A CO JEST HYPE'EM – O AI OGÓLNIC

SESJA 2: PROMPT ENGINEERING 3.0 I CONTEXT ENGINEERING

SESJA 3: OD POMYSŁU DO BUSINESS CASE'U AI

SESJA 4: ODPOWIEDZIALNE WDRAŻANIE: PRAWO, ETYKA I ZMIANA

Narzędziownik AI 3.0

Moduł II: Tworzenie treści AI

SESJA 5: GRAFIKA AI I PROFESJONALNA EDYCJA OBRAZU

SESJA 6: VIDEO, GŁOS, MUZYKA I AWATARY

SESJA 7: BRANDING I KOMPLETNY CONTENT PIPELINE

SESJA 8: VIBE-CODING I BUILDERY DLA OSÓB NIETECHNICZNYCH

Narzędziownik AI 3.0

Moduł III: AI w codziennej pracy

SESJA 9: DOKUMENTY, PDF-Y, ARKUSZE I DANE

SESJA 10: SPOTKANIA, KOMUNIKACJA I ZARZĄDZANIE PRACĄ

SESJA 11: MICROSOFT 365 COPILOT NA MAKSA

SESJA 12: ASYSTENCI STANOWISKOWI I PROFESJONALNY RESEARCH

Narzędziownik AI 3.0

Moduł IV: Budowanie rozwiązań AI

SESJA 13: SAAS, API CZY MODEL LOKALNY?

SESJA 14: PROGRAMOWANIE Z AI I AI-ASSISTED DEVELOPMENT

SESJA 15: RAG I FIRMOWE SYSTEMY WIEDZY

SESJA 16: AGENCI, MCP I AUTOMATYZACJA

Narzędziownik AI 3.0

Moduł V: Bezpieczeństwo AI

SESJA 17: AI AWARENESS: JAK AI ATAKUJE CZŁOWIEKA

SESJA 18: ATAKI NA APLIKACJE LLM

SESJA 19: BEZPIECZEŃSTWO AGENTÓW I MCP

SESJA 20: OBRONA, MONITORING I BEZPIECZNE WDROŻENIE



Rozwiązanie konkursu

Zasady konkursowe

Będą 3 pytania - każdy to osobny konkurs

Odpowiedzi na każdy konkurs wysyłamy pod adres ca@securitum.pl

W tytule wpisz temat: **konkurs AI #1** lub **konkurs AI #2** lub **konkurs AI #3**



x9 kubek sekuraka!

Ile było wszystkich
czarodziejów w
prezentacji?

Jeden czarodziej miał
inny **kolor** - jaki to kolor?

Jakiego przedmiotu czarodziej
NIE MIAŁ na jednym zdjęciu?

Q & A

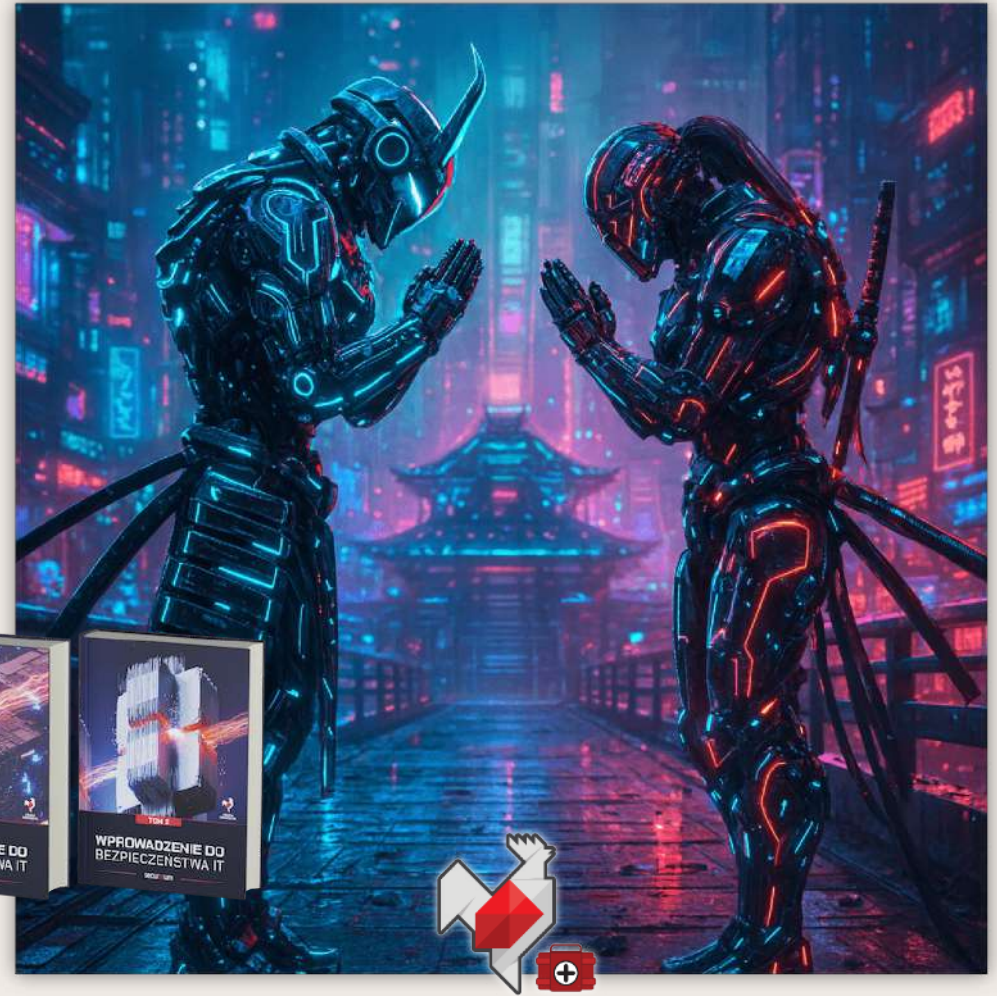
Dziękuję za uwagę

NAI.sekurak.pl

tomasz.turba@securitum.pl



Securitum 2026 (c) Wszelkie prawa zastrzeżone



SOS.SEKURAK.PL