BOREK DOLIŃSKI
RADCOWIE PRAWNI

Modele AI a wymogi AI ACT

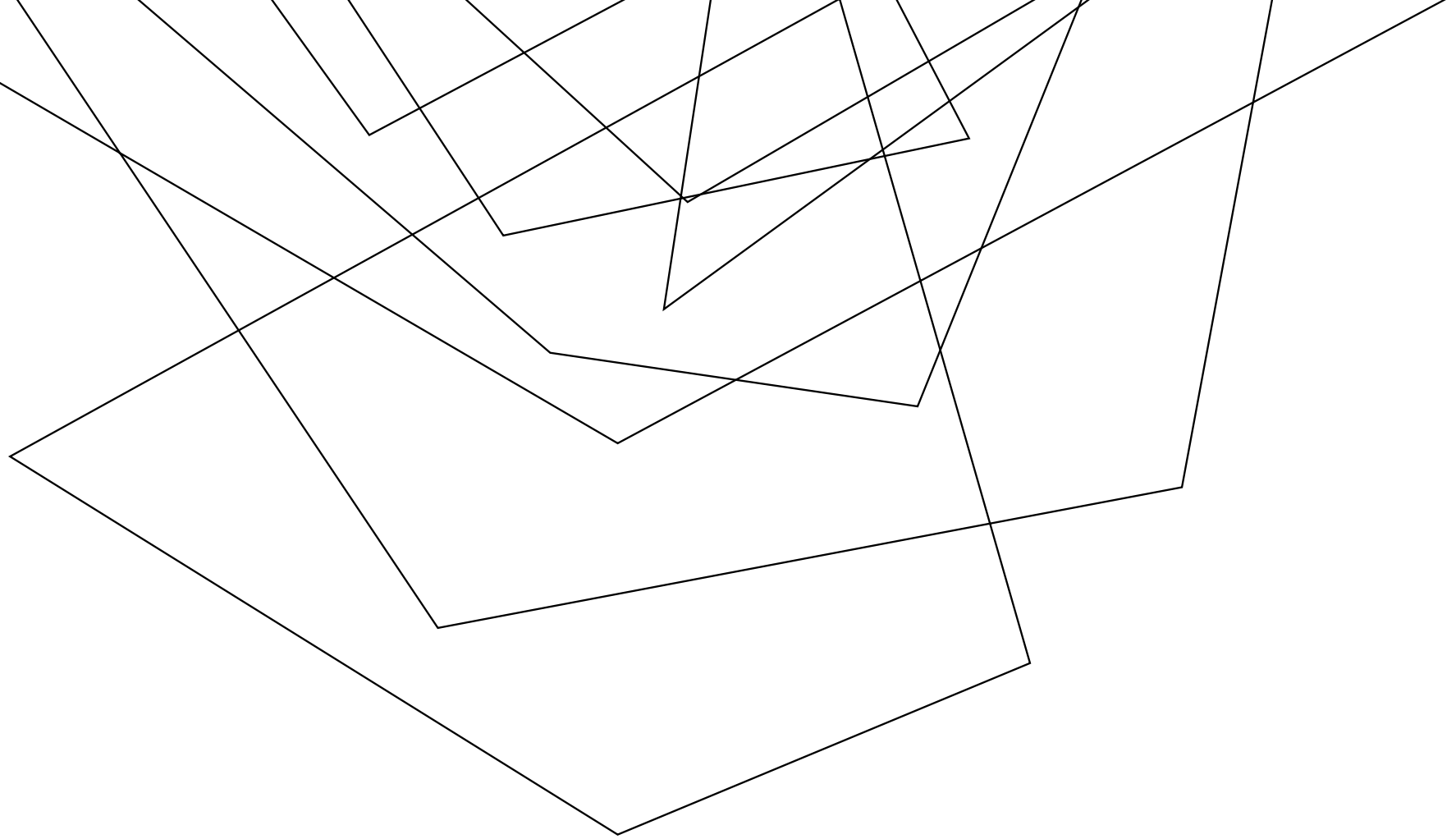
- informacje dla innowatorów

https://bdrp.pl/ai

08/05/2025

SPIS TREŚCI

https://bdrp.pl/ai



CZYM JEST MODEL AI?

https://bdrp.pl/ai

Sztuczna inteligencja jest zjawiskiem, które przeobraża naszą rzeczywistość. Jako technologia przetwarzania danych, generująca wnioski na wzór ludzkiej inteligencji, niesie ze sobą całą gamę korzyści, jak również wyzwań i zagrożeń dla człowieka.

Zagrożeniom tym wychodzi naprzeciw **rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji** (akt w sprawie sztucznej inteligencji), potocznie zwany **„AI ACT”**.

AI ACT nie reguluje wszystkich aspektów związanych ze sztuczną inteligencją. Twórcy rozporządzenia skoncentrowali się bowiem na aspekcie tworzenia narzędzi AI, adresując szereg obowiązków dla dostawców systemów AI oraz modeli AI ogólnego przeznaczenia.

W tym kontekście kluczowe jest rozróżnienie modelu AI oraz systemu AI:

Model AI to algorytm (lub ich zbiór), który umożliwia proces generowania danych wyjściowych (output) na podstawie otrzymanych danych wejściowych (input). Jest to swoisty mózg lub silnik przy wykorzystywaniu sztucznej inteligencji.

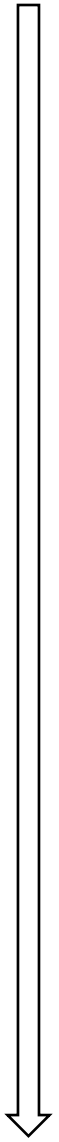
System AI to model AI obudowany interfejsem użytkownika. O ile więc model AI jest mózgiem przy stosowaniu sztucznej inteligencji, system AI będzie całym organizmem umożliwiającym pełne zastosowanie tej technologii i jej społeczne oddziaływanie.

model AI = algorytm lub zbiór algorytmów **(mózg)**

np. GPT-4 od OpenAI

system AI =algorytm(y) + interfejs użytkownika **(organizm)**

np. ChatGPT od OpenAI



https://bdrp.pl/ai

JAKIE MODELE AI REGULUJE AI ACT?

https://bdrp.pl/ai

Z lektury AI ACT wynika, że nie każdy model AI będzie podlegał pod rozporządzenie, a tym samym nie każdy dostawca modelu AI będzie zobligowany do implementacji szeregu obowiązków, które nakłada ten unijny akt.

Przepisy AI ACT wyróżniają pojęcie **modeli AI ogólnego przeznaczenia**, przez które należy rozumieć modele trenowane dużą ilością danych, na dużą skalę, wykazujące znaczną ogólność i będące w stanie kompetentnie wykonywać szeroki zakres różnych zadań, które można zintegrować z różnymi systemami lub aplikacjami niższego szczebla.

Algorytmy lub ich zbiory mające wąski zakres zadań lub ściśle określone zastosowanie nie będą podpadać pod powyższą definicję, a tym samym dostawcy tych modeli nie będą podlegać stosownym przepisom AI ACT, regulującym zasady tworzenia i obrotu modelami AI.

To samo dotyczy dostawców modeli AI o ogólnym zastosowaniu, które są wykorzystywane jedynie na potrzeby działań w zakresie badań, rozwoju i tworzenia prototypów przed wprowadzeniem ich do obrotu.

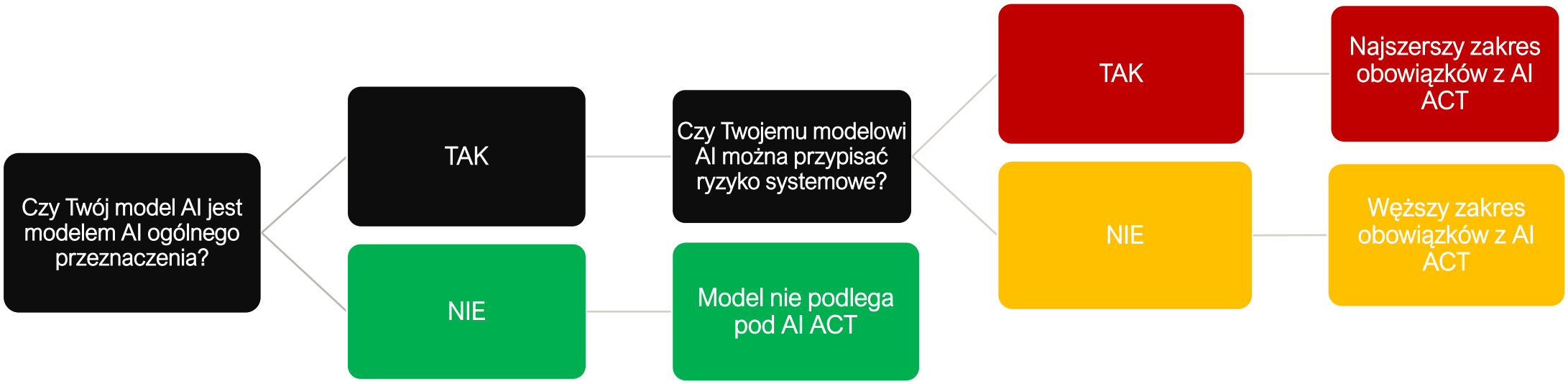
AI ACT dodatkowo wyróżnia pojęcie **modeli AI ogólnego przeznaczenia z ryzykiem systemowym**. Jest to kwalifikowana postać modeli AI, do której przypisane zostały dodatkowe obowiązki.

Ryzyko systemowe zawiera w sobie 3 elementy. Występuje gdy model AI:

- posiada **zdolności dużego oddziaływania** (najbardziej zaawansowane modele AI);
- ma znaczący wpływ na rynek UE ze względu na zasięg tych modeli lub rzeczywiste, bądź dające się racjonalnie przewidzieć **negatywne skutki** dla zdrowia publicznego, porządku publicznego, bezpieczeństwa publicznego, praw podstawowych lub całego społeczeństwa,
- może rozprzestrzenić się na dużą skalę w całym łańcuchu wartości.

Na dostawcach modeli AI ogólnego przeznaczenia z ryzykiem systemowym ciążyć będzie jeszcze szerszy zakres obowiązków określonych w AI ACT. Podyktowane jest to większą skalą zagrożeń, jakie niesie ze sobą ryzyko o charakterze systemowym.

Ustalanie zakresu obowiązków ciążących na dostawcy modelu sztucznej inteligencji



https://bdrp.pl/ai

JAKIE OBOWIĄZKI NAKŁADA AI ACT?

https://bdrp.pl/ai

Jeśli analiza zagadnień wskazanych we wcześniejszym rozdziale doprowadzi dostawcę modelu AI do wniosku, że podlega on przepisom AI ACT, ustalić należy zakres ciążących na nim obowiązków.

Podstawowe obowiązki dostawców modeli AI ogólnego przeznaczenia (art. 53 AI ACT) to:

- sporządzenie i aktualizacja dokumentacji technicznej modelu AI;
- przekazywanie odpowiednich informacji dostawcom systemów AI niższego szczebla;
- przestrzeganie europejskich zasad ochrony własności intelektualnej oraz sporządzenie polityki służącej zapewnieniu zgodności z tymi zasadami;
- dbałość o dobór odpowiednich danych treningowych oraz ich dokumentacja.

Więcej informacji dotyczących podstawowych obowiązków dostawców modeli AI znaleźć można pod adresem: https://bdrp.pl/prawo/ai/obowiazki-dostawcow-modeli-ai.

Obowiązki dostawców modeli AI ogólnego przeznaczenia z ryzykiem systemowym (art. 55 AI ACT):

- odpowiednia ocena modelu i testy mające na celu identyfikację i ograniczenie ryzyka systemowego;
- ocena i ograniczanie ryzyka systemowego;
- rejestracja, dokumentacja i zgłaszanie Urzędowi ds. AI informacji dot. poważnych incydentów;
- zapewnienie odpowiedniego poziomu cyberochrony modelu AI oraz jego infrastruktury fizycznej.

Kalendarium obowiązywania wymogów AI ACT dla dostawców modeli AI

02.08.2025

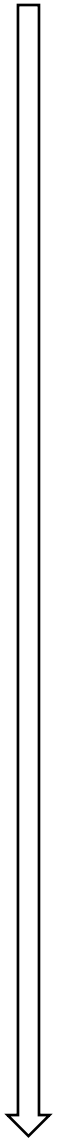
- przepisy AI ACT dla dostawców modeli AI ogólnego przeznaczenia

02.08.2026

- przepisy o karach (m.in. dla dostawców modeli AI) za naruszenie AI ACT

02.08.2027

- data końcowa na wdrożenie wymogów AI ACT dla tych dostawców modeli AI ogólnego przeznaczenia, którzy zdążyli wprowadzić swój model AI do obrotu przed 2.08.2025 r.



https://bdrp.pl/ai

O CZYM NALEŻY PAMIĘTAĆ WDRAŻAJĄC AI ACT?

https://bdrp.pl/ai

Rozpoczynając proces wdrażania AI ACT kieruj się następującymi zasadami:

- ✓ zmapuj swoje modele AI i przeanalizuj odrębnie każdy z nich;
- ✓ ustal czy Twój model AI jest modelem ogólnego przeznaczenia w rozumieniu AI ACT;
- ✓ ustal czy Twojemu modelowi AI można przypisać ryzyko systemowe;
- ✓ ustal zakres obowiązków spoczywających na dostawcy modelu AI;
- ✓ ustal czy planowane przez Ciebie wykorzystanie modelu AI nie jest zabronione przez art. 5 AI ACT lub inne przepisy prawa (np. RODO);
- ✓ sprawdź czy możesz testować swój model AI w ramach tzw. piaskownic regulacyjnych;
- ✓ pamiętaj o zasadzie rozliczalności (accountability) – udokumentuj przeprowadzone analizy oraz wdrożenie wymogów prawnych.

https://bdrp.pl/ai

Przy tworzeniu modeli AI należy też pamiętać o zasadach dotyczących zbiorów danych, które służą do jego trenowania.

Zbiory danych treningowych, walidacyjnych i testowych muszą być bowiem:

- adekwatne,
- wystarczająco reprezentatywne,
- w jak największym stopniu wolne od błędów i kompletne z punktu widzenia przeznaczenia,
- cechować się odpowiednimi właściwościami statystycznymi,
- pozyskane zgodnie z poszanowaniem przepisów prawa (RODO, zasady poufności).

https://bdrp.pl/ai

Na pewno warto rozpocząć od przeanalizowania, które modele AI spośród opracowywanych, oferowanych lub wykorzystywanych przez Ciebie podlegają w ogóle obowiązkom wynikającym z AI ACT.

Najprawdopodobniej większość Twoich modeli nie będzie podlegać obowiązkom rozporządzenia – upewnij się jednak, że tak właśnie jest i odpowiednio to udokumentuj.

Pamiętaj, że obowiązków wynikających z AI ACT może być naprawdę wiele, zwłaszcza jeśli jesteś dostawcą modelu AI z ryzykiem systemowym.

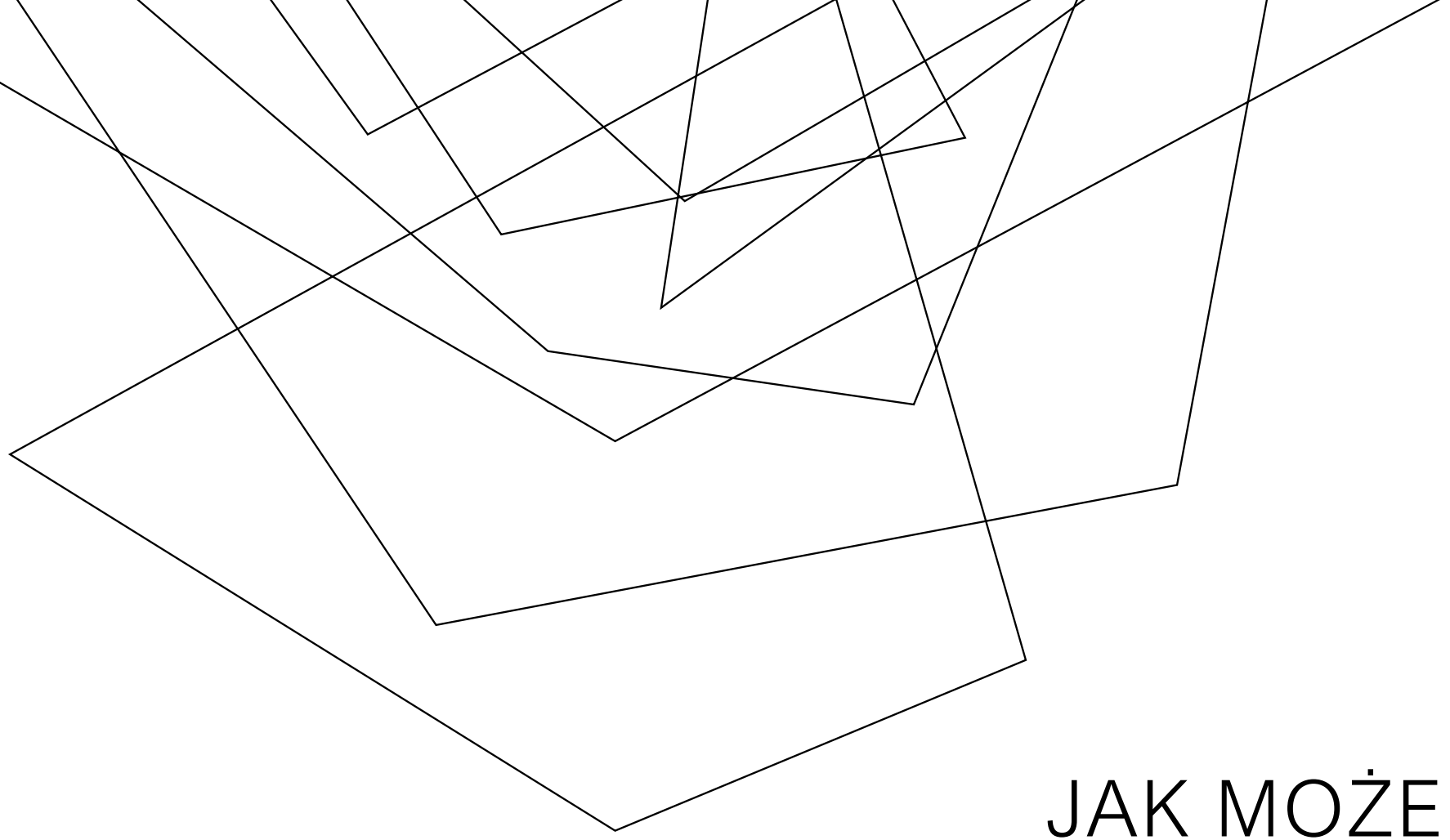
Nie zwlekaj więc na ostatnią chwilę z rozpoczęciem procesu wdrożenia.

Twórcy algorytmów powinni także wiedzieć, że AI ACT przewiduje dla innowatorów ciekawą regulację w postaci **piaskownic regulacyjnych** (ang. sandbox). Piaskownice są swoistym poligonem doświadczalnym, na którym można testować nowoczesne technologie (produkty lub usługi) w rzeczywistym środowisku z pominięciem pewnych przepisów, aby ocenić czy planowane rozwiązania zdadzą egzamin.

Piaskownice mają też służyć zapoznaniu się przez przedsiębiorców z oczekiwaniami regulacyjnymi oraz ze sposobami spełnienia wymogów wynikających z AI ACT, a organy państwowe mają udzielać w tym zakresie wskazówek.

Podkreślić jednak należy, że dostawcy modeli AI mogą z tej opcji skorzystać jeśli swój model sprzęgną z systemem AI, bowiem sandboxy nie są dedykowane samym modelom AI.

Więcej na ten temat piszemy na naszej stronie internetowej pod adresem: https://bdrp.pl/prawo/ai/piaskownice-regulacyjne-ai.



JAK MOŻEMY POMÓC TWOJEJ ORGANIZACJI?

https://bdrp.pl/ai

AI ASSESSMENT

- prowadzimy audyty mające na celu ustalenie zakresu podlegania obowiązkom wynikającym z AI ACT.

AI GOVERNANCE

- pomagamy w przygotowaniu i wdrożeniu polityk korzystania z AI.

AI COMPLIANCE

- pomagamy w przygotowaniu dokumentacji wymaganej dla modeli AI ogólnego przeznaczenia.

AI CONSULTANCY

- doradzamy, odpowiadamy na pytania dotyczące obowiązków wynikających z AI ACT.

AI LITERACY

- prowadzimy szkolenia podnoszące świadomość prawną personelu w zakresie korzystania z narzędzi AI oraz pozwalające zadośćuczynić obowiązkowi nakładanemu przez art. 4 AI ACT.

https://bdrp.pl/ai

PODSUMOWANIE

Od AI nie ma odwrotu i rozsądnie wykorzystywana przyczynić może się do wzrostu produktywności Twojej organizacji i uzyskania przewagi konkurencyjnej. Nierozważne korzystanie z niej może jednak zatopić nawet największą organizację.

https://bdrp.pl/ai

BOREK DOLIŃSKI
RADCOWIE PRAWNI

DZIĘKUJEMY

Borek Doliński Radcowie Prawni sp. j.
ul. Grunwaldzka 224b/9
60-166 Poznań
KRS: 852234 | NIP: 7831821915

https://bdrp.pl/ai
office@bdrp.pl
530 001 500 | 510 551 991