KL&M LAW

Kobylańska · Lewoszewski · Mednis

Projekt unijnego rozporządzenia w sprawie sztucznej inteligencji

Dr hab. Arwid Mednis

21 kwietnia 2021

Kobylańska Lewoszewski Mednis sp. j.
ul. Śniadeckich 10, 00-656 Warszawa
T: +48 22 25 34567, E: kancelaria@klmlaw.pl

KRS 699343, SR dla m.st. Warszawy
NIP 701-073-97-04
REGON 368541558

www.klmlaw.pl

KL&M LAW
Kobylanska · Lewoszewski · Mednis

Publikacja projektu

Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii – projekt Komisji z 21 kwietnia 2021 r. (COM(2021) 206 final)

Prace nad projektem trwają, zgłoszono liczne uwagi i opinie.

KL&M LAW
Kobylanska · Lewoszewski · Mednis

Kontekst projektu

Wraz z publikacją projektu dokonano przeglądu Skoordynowanego Planu na rzecz AI z 2018 r.:

- Celem jest osiągnięcie przez UE globalnego przywództwa w dziedzinie AI;
- Proponuje się zwiększenie inwestycji w AI, m. in. poprzez finansowanie w postaci różnych unijnych programów;
- W latach 2021-2027 UE ma zainwestować w AI rocznie 1 mld EUR;
- Inwestycje prywatne i publiczne w AI mają stopniowo wzrastać aby osiągnąć pod koniec dekady poziom 20 mld EUR rocznie;
- Niezbędna jest koordynacja działań, m. in. poprzez huby technologiczne, itp.;
- Odpowiedź na globalne wyzwania i ujednolicenie działań (w szczególności w dziedzinach ochrony zdrowia i ochrony środowiska);
- Sztuczna inteligencja ma być zorientowana na człowieka, godna zaufania, bezpieczna, zrównoważona i inkluzywna, z pełnym poszanowaniem podstawowych wartości europejskich.

Akt ws. AI

- Wniosek Komisji służy nie tyle promowaniu AI, ile osiągnięciu celu jakim jest przeciwdziałanie zagrożeniom wynikającym z niektórych zastosowań AI. Chodzi o budowę ekosystemu zaufania poprzez zaproponowanie ram prawnych dotyczących godnej zaufania sztucznej inteligencji.

- Projekt został poprzedzony analizą ryzyka, jest wyrazem zastosowania zasady proporcjonalności w działaniach legislacyjnych organów UE.

KL&M LAW
Kobylanska · Lewoszewski · Mednis

Definicja AI

Definicję systemu sztucznej inteligencji sformułowano w taki sposób, aby „w możliwie największym stopniu była neutralna pod względem technologicznym i nie ulegała dezaktualizacji, biorąc pod uwagę szybki rozwój technologiczny i rozwój sytuacji rynkowej w dziedzinie AI”.

„System sztucznej inteligencji” oznacza oprogramowanie opracowane przy użyciu co najmniej jednej spośród technik i podejść wymienionych w załączniku I, które może – dla danego zestawu celów określonych przez człowieka – generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję.

Uzupełnieniem jest załącznik I zawierający szczegółowy wykaz podejść i technik na potrzeby rozwoju AI, które mają być dostosowywane przez Komisję w świetle postępu technologicznego..

KL&M LAW
Kobylanska · Lewoszewski · Mednis

Definicja AI – załącznik I

Techniki i podejścia z zakresu sztucznej inteligencji:

a) mechanizmy uczenia maszynowego, w tym uczenie nadzorowane, uczenie się maszyn bez nadzoru i uczenie przez wzmacnianie, z wykorzystaniem szerokiej gamy metod, w tym uczenia głębokiego;
b) metody oparte na logice i wiedzy, w tym reprezentacja wiedzy, indukcyjne programowanie (logiczne), bazy wiedzy, silniki inferencyjne i dedukcyjne, rozumowanie (symboliczne) i systemy ekspertowe;
c) podejścia statystyczne, estymacja bayesowska, metody wyszukiwania i optymalizacji.

Komisja jest uprawniona do przyjmowania aktów delegowanych w celu zmiany wykazu technik i podejść wymienionych w załączniku I, aby uaktualnić ten wykaz z uwzględnieniem rozwoju sytuacji rynkowej i rozwoju technologicznego na podstawie cech, które są podobne do technik i podejść w nim wymienionych.

Poziomy ryzyka w zastosowaniach AI/ ryzyko niedopuszczalne

3 poziomy ryzyka: niedopuszczalne, wysokie ryzyko oraz niskie/minimalne ryzyko.

Poziom niedopuszczalny – zakaz wprowadzania do obrotu, wykorzystywania, itp.:

a) Systemu AI, który stosuje **techniki podprogowe będące poza świadomością danej osoby** w celu istotnego **zniekształcenia zachowania** tej osoby w sposób, który powoduje lub może powodować u niej lub u innej osoby **szkodę fizyczną lub psychiczną**;

b) Systemu AI, który **wykorzystuje dowolne słabości** określonej grupy osób ze względu na ich wiek, niepełnosprawność ruchową lub zaburzenie psychiczne w celu istotnego zniekształcenia zachowania osoby należącej do tej grupy w sposób, który powoduje lub może powodować u tej osoby lub u innej osoby szkodę fizyczną lub psychiczną;

c) Systemów AI przez organy publiczne lub w ich imieniu na potrzeby oceny lub klasyfikacji wiarygodności osób fizycznych prowadzonej przez określony czas na podstawie ich **zachowania społecznego** lub znanych bądź przewidywanych cech osobistych lub cech osobowości, kiedy to **punktowa ocena społeczna** prowadzi do jednego lub obu z następujących skutków:

(i) krzywdzącego lub niekorzystnego traktowania niektórych osób fizycznych lub całych ich grup w kontekstach społecznych, które nie są związane z kontekstami, w których pierwotnie wygenerowano lub zgromadzono dane;

(ii) krzywdzącego lub niekorzystnego traktowania niektórych osób fizycznych lub całych ich grup, które jest nieuzasadnione lub nieproporcjonalne do ich zachowania społecznego lub jego wagi;

Ryzyko niedopuszczalne

d) systemów zdalnej **identyfikacji biometrycznej** „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa, chyba że i w zakresie, w jakim takie wykorzystanie jest absolutnie niezbędne do jednego z następujących celów:

(i) ukierunkowanego poszukiwania konkretnych potencjalnych ofiar przestępstw, w tym zaginionych dzieci;
(ii) zapobiegnięcia konkretnemu, poważnemu i bezpośredniemu zagrożeniu życia lub bezpieczeństwa fizycznego osób fizycznych lub atakowi terrorystycznemu;
(iii) wykrywania, lokalizowania, identyfikowania lub ścigania sprawcy przestępstwa lub podejrzanego o popełnienie przestępstwa, o którym mowa w art. 2 ust. 2 decyzji ramowej Rady 2002/584/WSiSW62 i które w danym państwie członkowskim podlega karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności przez okres, którego górna granica wynosi co najmniej trzy lata, zgodnie z prawem danego państwa członkowskiego.

KL&M LAW
Kobylanska · Lewoszewski · Mednis

Wysokie ryzyko

System AI uznaje się za system wysokiego ryzyka, jeżeli spełnione są oba poniższe warunki:

a) system AI jest przeznaczony do wykorzystywania jako związany z bezpieczeństwem element produktu objętego unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku II lub sam jest takim produktem;

b) produkt, którego związanym z bezpieczeństwem elementem jest system AI, lub sam system AI jako produkt podlegają – na podstawie unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku II – ocenie zgodności przeprowadzanej przez osobę trzecią w celu wprowadzenia tego produktu do obrotu lub oddania go do użytku;

Za systemy wysokiego ryzyka uważa się także systemy wymienione w załączniku III.

Systemy AI wysokiego ryzyka – załącznik III

Systemy AI wysokiego ryzyka to określone systemy z poniższych obszarów:

1. identyfikacja i kategoryzacja biometryczna osób fizycznych;
2. zarządzanie infrastrukturą krytyczną i jej eksploatacja;
3. kształcenie i szkolenie zawodowe;
4. zatrudnienie, zarządzanie pracownikami i dostęp do samozatrudnienia;
5. dostęp do podstawowych usług prywatnych (m. in. ocena zdolności kredytowej) oraz usług i świadczeń publicznych, a także korzystanie z nich;
6. ściganie przestępstw;
7. zarządzanie migracją, azylem i kontrolą graniczną;
8. sprawowanie wymiaru sprawiedliwości i procesy demokratyczne.

KL&M LAW
Kobylanska · Lewoszewski · Mednis

Systemy AI wysokiego ryzyka

Komisja jest uprawniona do przyjmowania aktów delegowanych w celu aktualizacji wykazu zawartego w załączniku III poprzez dodanie systemów AI wysokiego ryzyka, jeżeli spełnione są oba poniższe warunki:

a) systemy AI są przeznaczone do wykorzystywania w którymkolwiek z obszarów wymienionych w załączniku III pkt 1–8;

b) systemy AI stwarzają ryzyko szkody dla zdrowia i bezpieczeństwa lub ryzyko niekorzystnego wpływu na prawa podstawowe, które pod względem dotkliwości i prawdopodobieństwa wystąpienia jest równoważne ryzyku szkody lub niekorzystnego wpływu, które stwarzają systemy AI wysokiego ryzyka wymienione już w załączniku III, lub jest od niego większe.

KL&M LAW
Kobylanska · Lewoszewski · Mednis

Systemy AI wysokiego ryzyka - wymogi

- System zarządzania ryzykiem (identyfikacja, ocena, zarządzanie ryzykiem);
- Systemy AI wysokiego ryzyka, które wykorzystują techniki obejmujące trenowanie modeli z wykorzystaniem danych, opracowuje się na podstawie zbiorów danych treningowych, walidacyjnych i testowych spełniających określone w Akcie kryteria jakości;
- Dokumentacja techniczna;
- Rejestrowanie zdarzeń, zapewniający poziom identyfikowalności jego funkcjonowania odpowiedni do przeznaczenia, w tym zdarzeń mających wpływ na ryzyko;
- Przejrzystość działania systemu;
- Nadzór ze strony człowieka;
- Dokładność, solidność i cyberbezpieczeństwo.

Odrębnie uregulowane obowiązki dostawców i użytkowników systemów AI (powyższe oraz dodatkowe).

KL&M LAW
Kobylanska · Lewoszewski · Mednis

Pozostałe postanowienia

- Organy notyfikujące i jednostki notyfikowane, procedura notyfikacyjna;
- Normy, ocena zgodności, certyfikaty, rejestracja – systemy wysokiego ryzyka
- Dostawcy zapewniają, aby systemy AI przeznaczone do wchodzenia w interakcję z osobami fizycznymi projektowano i opracowywano w taki sposób, aby osoby fizyczne były informowane o tym, że prowadzą interakcję z systemem AI, chyba że okoliczności i kontekst korzystania z systemu jednoznacznie na to wskazują (są tu wyjątki).
- Podobnie – w odniesieniu do systemów rozpoznawania emocji lub systemów kategoryzacji biometrycznej;
- Użytkownicy AI, który generuje obrazy, treści dźwiękowe lub treści wideo, które łudząco przypominają istniejące osoby, obiekty, miejsca lub inne podmioty lub zdarzenia, lub który tymi obrazami i treściami manipuluje, przez co osoba będąca ich odbiorcą mogłaby niesłusznie uznać je za autentyczne lub prawdziwe („deepfake”), ujawniają, że dane treści zostały wygenerowane lub zmanipulowane przez system AI.

KL&M LAW
Kobylanska · Lewoszewski · Mednis

Pozostałe postanowienia

- Środki wspierające innowacyjność (piaskownice regulacyjne)
- Nowe organy: Europejska Rada ds. AI, organy krajowe
- Unijna baza danych dla samodzielnych systemów sztucznej inteligencji wysokiego ryzyka
- Monitorowanie po wprowadzeniu do obrotu, wymiana informacji, nadzór rynku
- Kodeksy postępowania
- Poufność i kary

KL&M LAW
Kobylanska · Lewoszewski · Mednis

Główne uwagi do projektu Aktu ws. AI

- Prywatny „social scoring” – czy powinien być zakazany? (EDPB/EDPS)
- Całkowity zakaz systemów biometrycznego rozpoznawania osób w miejscach publicznych (EDPB/EDPS)
- Wyróżnianie i nagradzanie dobrych praktyk
- Ocena ryzyka powinna brać pod uwagę korzyści z korzystania z danego systemu AI
- Problem definicji AI
- Akt powinien skupiać się na poszczególnych technologiach AI a nie na wpływie AI na osoby
- Rolą Aktu powinno być wspieranie AI a nie zakazy

KL&M LAW

Kobylanska · Lewoszewski · Mednis

Kontakt

Dr hab. Arwid Mednis

Radca prawny

E: arwid.mednis@klmlaw.pl
M: +48 (0) 510.087.786

KL&MLAW

Kobylanska · Lewoszewski · Mednis