Wdrażanie i stosowanie systemów sztucznej inteligencji (AI). Prawa i obowiązki podmiotów. Komentarz praktyczny

Wstęp

Wstęp

Rozporządzenie w sprawie sztucznej inteligencji (AI Act) to pierwszy kompleksowy akt prawny dotyczący AI wydany na świecie.

Akt ten odwołuje się do koncepcji tzw. Nowych Ram Legislacyjnych (szerzej zob. https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en?prefLang=pl, dostęp: 15.1.2026 r.), przenosząc ciężar odpowiedzialności na podmioty wprowadzające technologie na rynek. Ustanawia zestaw wymogów zasadniczych, w szczególności dotyczących jakości danych, nadzoru człowieka, bezpieczeństwa, odporności, cyberbezpieczeństwa i dokumentacji, oraz przewiduje procedury oceny zgodności i oznakowanie CE dla systemów wysokiego ryzyka. Konstrukcja ta łączy logikę prawa dotyczącego bezpieczeństwa produktów z ochroną praw podstawowych, ponieważ wymogi projektowe i organizacyjne służą nie tylko zapewnieniu bezpieczeństwa technicznego, lecz także, a może przede wszystkim, realizacji zasad proporcjonalności, niedyskryminacji i rozliczalności.

AI Act ma znaczenie również ze względu na swoją architekturę regulacyjną. Ustanawia model różnicowania obowiązków w zależności od poziomu ryzyka: od praktyk zakazanych (art. 5), poprzez systemy wysokiego ryzyka (art. 6–49), po obowiązki przejrzystości w przypadku systemów ograniczonego ryzyka (art. 52) oraz ramy dla modeli i systemów ogólnego przeznaczenia (GPAI) (art. 51–56). W ten sposób powstaje spójny system gradacji ciężaru regulacyjnego, uzasadniony potencjalnym wpływem poszczególnych kategorii systemów na prawa i sytuację jednostki.

Regulacja ta wpisuje się również w szersze zjawisko określane jako „efekt brukselski" (szerzej o efekcie Brukseli zob. w szczególności *A. Bradford*, The Brussels Effect). Ze względu na wielkość rynku wewnętrznego oraz pionierski charakter unijnych wymogów dostawcy globalni będą najpewniej harmonizować swoje produkty z poziomem unijnym na wszystkich obsługiwanych rynkach w celu ograniczenia kosztów zapewnienia zgodności wielowariantowej. Włączenie AI Act w proces normalizacji technicznej (normy CEN/CENELEC i specyfikacje wspólne) dodatkowo

wzmacnia tendencję do ujednolicania metod oceny ryzyka, testowania, dokumentowania czy praktyk MLOps (skrót od *Machine Learning Operations*, czyli Operacje Uczenia Maszynowego – to zestaw praktyk, procesów i narzędzi, które mają na celu usprawnienie i zautomatyzowanie całego cyklu życia modeli uczenia maszynowego) w skali globalnej.

AI Act precyzyjnie określa role i obowiązki w cyklu życia systemów AI.

Po pierwsze, dostawca odpowiada za ocenę zgodności, dokumentację techniczną, system zarządzania jakością, nadzór po wprowadzeniu do obrotu, działania korygujące oraz oznakowanie CE i, w odpowiednich przypadkach, wpis do rejestru unijnego.

Po drugie, importerzy i dystrybutorzy pełnią funkcję kontrolną, weryfikując deklaracje zgodności, instrukcje oraz oznakowanie, a w razie rebrandingu lub modyfikacji stają się dostawcami.

Po trzecie, podmiot stosujący odpowiada za zgodne z przeznaczeniem stosowanie systemu, nadzór ludzki, monitorowanie działania, rejestrowanie zdarzeń oraz szkolenie personelu. Osobny reżim dotyczy modeli ogólnego przeznaczenia, które podlegają obowiązkom dokumentacyjnym, informacyjnym i, w przypadku modeli o znaczących oddziaływaniach, dodatkowym wymogom dotyczącym zarządzania ryzykiem systemowym i bezpieczeństwem łańcucha dostaw.

Centralnym elementem konstrukcji AI Act są praktyki zakazane (art. 5). Ustawodawca unijny zdecydował się na zastosowanie tego środka wyłącznie w tych sytuacjach, w których ryzyka naruszenia praw i godności jednostki nie da się zneutralizować środkami proporcjonalnymi. Katalog obejmuje m.in. techniki istotnie zniekształcające zachowanie osoby, wykorzystywanie szczególnej podatności oraz systemy oceny społecznej stosowane przez władze publiczne.

Na drugim krańcu znajdują się systemy minimalnego ryzyka, obejmujące zastosowania o marginalnych skutkach dla zdrowia, bezpieczeństwa i praw podstawowych (np. filtry antyspamowe, proste rekomendacje, podstawowe narzędzia tekstowe). Ustawodawca nie nakłada tu obowiązków formalnych ani oceny zgodności; zachęca natomiast do tworzenia kodeksów postępowania i dobrowolnych standardów. Ich celem jest uporządkowanie procesów dotyczących jakości danych, walidacji modeli, minimalnych zasad nadzoru człowieka czy obsługi skarg, a także ograniczenie ryzyka niezamierzonego podnoszenia kategorii ryzyka wraz ze zmianą funkcji systemu.

Między tymi biegunami znajdują się systemy wysokiego ryzyka i systemy ograniczonego ryzyka. Systemy wysokiego ryzyka, wskazane w załączniku III AI Act (m.in. biometria, infrastruktura krytyczna, edu-

kacja, zatrudnienie, udzielanie kredytów, egzekwowanie prawa, migracja, administracja wymiarem sprawiedliwości i procesy demokratyczne), podlegają rygorystycznym wymogom *ex ante*. Dostawca musi m.in. ustanowić system zarządzania ryzykiem, zapewnić jakość danych treningowych, walidacyjnych i testowych, prowadzić dokumentację techniczną, logowanie, nadzór ludzki i zapewnić odpowiednią dokładność oraz bezpieczeństwo. Wymogi te są weryfikowane w ramach procedury oceny zgodności prowadzącej do sporządzenia deklaracji zgodności UE i oznakowania CE. Po wprowadzeniu do obrotu dostawca utrzymuje monitoring post-market i raportuje poważne incydenty.

Systemy ograniczonego ryzyka podlegają wymogom przejrzystości, w tym obowiązkowi informowania o interakcji z AI, użyciu rozpoznawania emocji lub kategoryzacji biometrycznej, a także oznaczaniu treści generowanych lub modyfikowanych syntetycznie. Celem jest ochrona użytkowników przed ryzykiem poznawczym i zapewnienie świadomego odbioru treści.

Model czterech poziomów ryzyka (praktyki zakazane – wysokie ryzyko – ograniczone ryzyko – minimalne ryzyko) tworzy spójną drabinę regulacyjną. Każdy poziom odpowiada innemu ciężarowi dowodowemu i innemu zakresowi obowiązków, co pozwala uniknąć zarówno nadmiernej regulacji prostych zastosowań, jak i niedostatecznego nadzoru nad systemami o poważnych konsekwencjach społecznych.

AI Act funkcjonuje w powiązaniu z innymi aktami prawa UE, w szczególności z:

1) RODO;
2) DSA;
3) DMA;
4) MDR;
5) przepisami dotyczącymi maszyn (tj. rozporządzenie 2023/1230);
6) przepisami dotyczącymi cyberbezpieczeństwa (CRA – które wchodzi w życie 11.9.2026 r., a stosuje się od 11.12.2027 r., i NIS2)

– i innymi regulacjami sektorowymi.

Konstrukcja *lex generalis / lex specialis* oraz wspólne moduły oceny zgodności wymagają spojrzenia systemowego na zgodność obejmującego cały cykl życia systemu, łańcuch dostaw, proces aktualizacji oraz walidację działania w praktyce.

Warto zaznaczyć, że już teraz trwają prace nad nowelizacją AI Act. Komisja Europejska przedstawiła tzw. *Digital Omnibus on AI* [Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the sim-

plification of the implementation of harmonised rules on artificial intelligence, SWD(2025) 836 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025PC0836, dostęp: 15.1.2026 r.], którego celem jest uproszczenie wdrażania rozporządzenia. Konsultacje pokazały bowiem, że istnieją realne zagrożenia dla skutecznego wejścia w życie kluczowych przepisów – w szczególności opóźnienia w wyznaczaniu organów nadzoru, brak jednostek oceniających zgodność oraz brak zharmonizowanych norm technicznych. Te czynniki mogą znacząco podwyższyć koszty zgodności i spowolnić innowacje.

Proponowane zmiany obejmują m.in.:

1) powiązanie stosowania przepisów o wysokim ryzyku z dostępnością norm i narzędzi wsparcia;
2) rozszerzenie ułatwień dla MŚP na tzw. *small mid-caps*, w tym uproszczone wymogi dokumentacyjne i łagodniejsze podejście sankcyjne;
3) przeniesienie obowiązku rozwijania *AI literacy* na Komisję i państwa członkowskie zamiast nakładania go w sposób ogólny na dostawców i podmioty stosujące (przy utrzymaniu obowiązków szkoleniowych dla sektorów wysokiego ryzyka);
4) większą elastyczność w monitorowaniu działania systemów po ich wprowadzeniu na rynek;
5) zmniejszenie obciążeń związanych z rejestracją systemów, które są stosowane w obszarach wysokiego ryzyka, lecz same nie mają charakteru wysokiego ryzyka;
6) centralizację nadzoru nad dużą liczbą systemów opartych na modelach GPAI w *AI Office*;
7) ułatwienia w zakresie przetwarzania danych wrażliwych dla celów wykrywania i korygowania biasu;
8) szersze wykorzystanie piaskownic regulacyjnych oraz *real-world testing*, w tym utworzenie od 2028 r. piaskownicy na poziomie UE;
9) doprecyzowanie relacji między AI Act a innymi aktami prawa UE oraz usprawnienie procedur operacyjnych rozporządzenia.

Niniejsza publikacja uwzględnia te projektowane zmiany.

Celem tego komentarza jest połączenie analizy dogmatycznej i systemowej z funkcją przewodnika wdrożeniowego. Tekst prowadzi czytelnika przez najważniejsze elementy konstrukcyjne AI Act, obejmujące w szczególności klasyfikację ryzyka, wymogi projektowe, dokumentację, obowiązki poszczególnych ról, system GPAI, nadzór i egzekwowanie oraz reżim sankcyjny.