

Informacja Ministerstwa Cyfryzacji zamieszczona w dniu 3 sierpnia 2026 r.

AI Act - co się zmieniło 2 sierpnia 2026 roku?

Przepisy unijnego rozporządzenia AI Act zaczynają obowiązywać etapami. Od 2 sierpnia 2026 r. podmioty stosujące systemy generujące treści mają obowiązek poinformowania odbiorców o tym, że dany materiał został wygenerowany lub zmodyfikowany przy użyciu AI. Natomiast przesunął się termin stosowania przepisów dotyczących systemów AI wysokiego ryzyka. Powodem jest czas potrzebny na dostosowanie tych systemów do nowych wymogów.

Obowiązek poinformowania o treści wygenerowanej przez AI

Od 2 sierpnia 2026 r. podmioty udostępniające tzw. deepfake w rozumieniu art. 3 pkt 60 AI Act (realistyczne obrazy oraz treści audio lub wideo przedstawiające osoby, przedmioty, miejsca lub wydarzenia, które zostały sztucznie wygenerowane albo zmienione i mogą zostać błędnie uznane za autentyczne) mają obowiązek poinformować odbiorcę, że materiał został wygenerowany lub zmodyfikowany przy użyciu AI. Jeżeli treści stanowią część utworu lub programu o wyrażnie artystycznym, twórczym, satyrycznym, fikcyjnym lub analogicznym charakterze, obowiązek ogranicza się do odpowiedniego ujawnienia korzystania z systemu AI w produkcji w sposób, który nie utrudnia wyświetlania lub korzystania z utworu.

Obowiązek informacyjny dotyczy również tekstów publikowanych w celu informowania społeczeństwa o sprawach leżących w interesie publicznym, jeżeli zostały one wygenerowane lub zmodyfikowane przez sztuczną inteligencję. Obowiązek nie ma zastosowania, jeśli treści wygenerowane przez AI zostały poddane przeglądowi przez człowieka lub kontroli redakcyjnej, a odpowiedzialność redakcyjną za publikację tekstu ponosi osoba fizyczna lub prawna.

Dostawcy systemów generujących treści od 2 sierpnia muszą zapewnić, aby materiały dźwiękowe, wizualne, audiowizualne lub tekstowe mogły zostać rozpoznane jako wygenerowane albo zmodyfikowane przez sztuczną inteligencję. W tym celu treści powinny być oznaczane w formacie nadającym się do odczytu maszynowego. Zastosowane rozwiązania powinny być skuteczne, interoperacyjne, niezawodne i technicznie możliwe do wdrożenia, z uwzględnieniem rodzaju treści, kosztów wdrożenia oraz aktualnego stanu wiedzy technicznej.

Zmiany terminów przyjęte w ramach unijnego pakietu upraszczającego, określanego jako AI Omnibus, przewidują okres przejściowy dla niektórych systemów generatywnych wprowadzonych do obrotu lub oddanych do użytku przed 2 sierpnia 2026 r. Dostawcy takich systemów otrzymali czas do 2 grudnia 2026 r. na dostosowanie ich do technicznych obowiązków dotyczących oznaczania treści. Materiały wygenerowane i udostępnione przed 2 sierpnia 2026 r. nie muszą być oznaczane wstecznie.

Obowiązek poinformowania o rozmowie z maszyną

Jedną z najważniejszych zmian obowiązujących od 2 sierpnia 2026 r. są wymagania dotyczące przejrzystości. Osoba korzystająca z systemu AI powinna zostać w sposób jasny poinformowana, że prowadzi interakcję z maszyną, jeżeli nie jest to oczywiste. Dotyczy to m.in. chatbotów, wirtualnych asystentów i automatycznych systemów obsługi

użytkowników. Informacja powinna zostać przekazana najpóźniej przy pierwszym kontakcie oraz w sposób jasny, zrozumiały i dostępny, również dla osób ze szczególnymi potrzebami. Obowiązek poinformowania osób, których dotyczy działanie systemu, obejmie także wykorzystywanie systemów rozpoznawania emocji oraz systemów kategoryzacji biometrycznej. Organizacje korzystające z takich rozwiązań powinny zadbać nie tylko o przekazanie odpowiedniej informacji, lecz także o zgodność przetwarzania danych osobowych z przepisami o ochronie danych. AI Act nie zastępuje ogólnego rozporządzenia o ochronie danych ani innych regulacji chroniących prywatność. Przepisy te należy stosować równolegle.

Obowiązki wobec systemów AI wysokiego ryzyka - zmiany w harmonogramie.

Istotna zmiana dotyczy systemów AI wysokiego ryzyka. Pierwotny harmonogram przewidywał rozpoczęcie stosowania części przepisów dotyczących tych systemów 2 sierpnia 2026 r., a w przypadku systemów związanych z produktami regulowanymi 2 sierpnia 2027 r. Terminy te zostały przesunięte przez pakiet nowelizujący rozporządzenie - AI Omnibus. Przepisy dotyczące systemów wysokiego ryzyka wymienionych w załączniku III do AI Act będą stosowane od 2 grudnia 2027 r. Chodzi m.in. o określone zastosowania AI w edukacji, zatrudnieniu, dostępie do podstawowych usług, wymiarze sprawiedliwości, migracji oraz niektórych działaniach organów publicznych.

W odniesieniu do systemów AI wysokiego ryzyka, które są elementami produktów objętych unijnymi przepisami dotyczącymi bezpieczeństwa, termin rozpoczęcia stosowania odpowiednich wymagań został przesunięty na 2 sierpnia 2028 r. Przesunięcie terminów ma umożliwić przygotowanie norm, narzędzi i procedur potrzebnych do jednolitego stosowania wymagań w całej Unii. Nie oznacza jednak, że organizacje powinny wstrzymać przygotowania. Dostosowanie systemów wysokiego ryzyka może wymagać zmian technicznych, organizacyjnych i umownych, których wdrożenie będzie czasochłonne.

Obowiązki stosowane przed 2 sierpnia 2026 r.

Od 2 lutego 2025 roku stosowane są m.in. zakazy dotyczące niedopuszczalnych praktyk AI oraz wymagania związane z rozwijaniem kompetencji w zakresie sztucznej inteligencji.

Sposób egzekwowania przepisów

Od 2 sierpnia 2026 r. Komisja Europejska może korzystać z pełnych uprawnień w zakresie egzekwowania obowiązków dotyczących modeli AI ogólnego przeznaczenia. Komisja będzie mogła żądać informacji i dokumentacji, przeprowadzać oceny modeli, wymagać działań ograniczających ryzyko oraz nakładać sankcje.