RYMARZ · ZDORT · MARUTA

AI Act – co zmienia i jak się do niego przygotować?

13 marca 2024 r. Parlament Europejski przyjął AI Act. To ważna data i dobry moment na krótkie podsumowanie, gdzie jesteśmy i co nas czeka w tym obszarze.

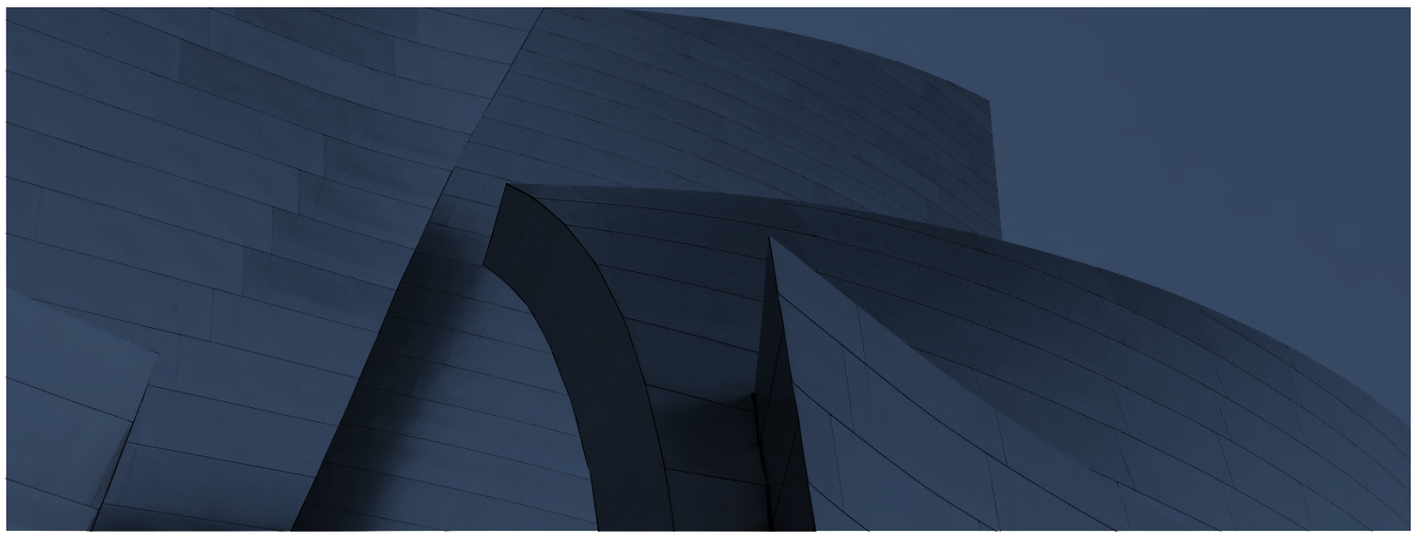
Zapraszamy do zapoznania się z krótkim opracowaniem, które podsumowuje kluczowe zagadnienia wprowadzone przez AI Act. Na pogłębione analizy na pewno jeszcze przyjdzie czas. Jesteśmy natomiast przekonani, że myśleć o właściwym podejściu do zarządzania AI w organizacji należy już teraz. Z jednej strony nie możemy bowiem zapominać, że stosowanie rozwiązań z zakresu AI dotyka bezpośrednio również innych, w pełni obowiązujących regulacji, chociażby z obszarów ochrony prywatności, własności intelektualnej czy cyberbezpieczeństwa. Z drugiej strony prawidłowe wdrożenie zasad AI Governance (odwołujące się do istniejących norm i standardów) to pierwszy krok do zapewnienia zgodności z przepisami przyszłego rozporządzenia.

Czym jest AI Act i co reguluje?

AI Act to rozporządzenie unijne, a zatem akt prawny, który nie wymaga transpozycji do krajowych porządków prawnych. Na jego podstawie kwestie systemów AI uregulowane zostaną, co do zasady, jednakowo we wszystkich krajach UE. Ma to zapewnić jednolite podejście i zagwarantować jeden standard ochrony we wszystkich państwach członkowskich.

AI Act reguluje zasady w zakresie przejrzystości, wykorzystywania i monitorowania oraz nadzoru nad AI. Chodzi zatem zarówno o wymogi związane z wprowadzeniem systemu czy modelu AI do obrotu, jak i dalszego ich wykorzystania. W tym sensie można powiedzieć, że rozporządzenie dotyka całego cyklu życia AI i na każdego uczestnika tego cyklu (dostawców, importerów, dystrybutorów czy użytkowników) nakłada określone obowiązki. Wymogi i zasady będą różne w zależności od roli, ale przede wszystkim od kategorii rozwiązania AI oraz ryzyka, które zostanie przypisane do tej kategorii.

AI Act określa również listę zakazanych praktyk w zakresie stosowania AI. To szczególnie ryzykowne sposoby wykorzystania AI (co obejmuje zarówno wprowadzenie do obrotu, oddawanie do użytku, jak i wykorzystanie danego systemu). Przykładowo AI Act zakazuje takich systemów AI, które (i) wykorzystują techniki podprogowe lub celowe techniki manipulacyjne, czego celem lub skutkiem jest zniekształcenie zachowania danej osoby, (ii) są wykorzystywane, by ocenić lub przewidzieć prawdopodobieństwo popełnienia przestępstwa przez osobę fizyczną wyłącznie na podstawie profilowania, (iii) są wykorzystywane do rozpoznawania twarzy poprzez scrapping internetu oraz CCTV w celu rozbudowy baz twarzy osób fizycznych, (iv) są wykorzystywane do wnioskowania o emocjach w miejscach pracy oraz instytucjach naukowych.

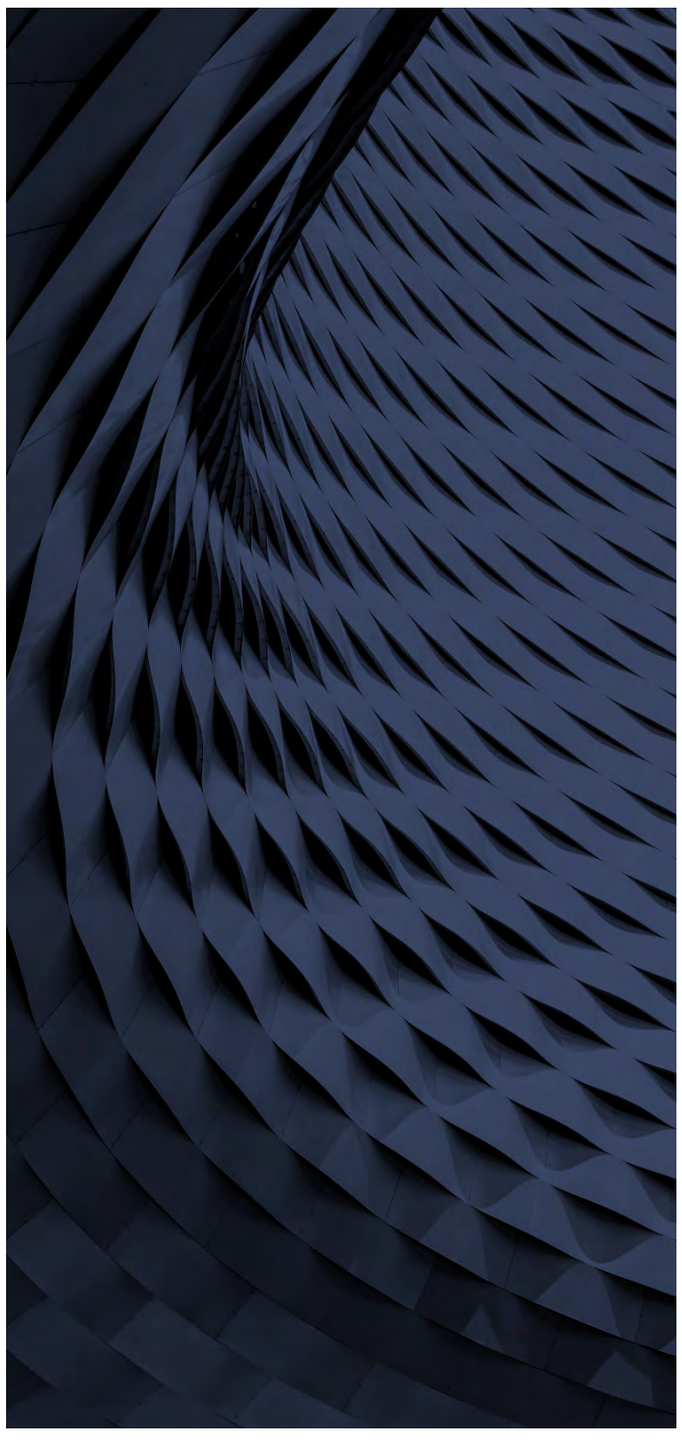


System AI i system GPAI – trochę definicji

Zgodnie z projektem rozporządzenia System AI to system oparty na koncepcji maszyny, zaprojektowany do działania na wielu poziomach autonomii, który po wdrożeniu wykazuje zdolność adaptacji oraz dokonuje, na podstawie otrzymywanych danych wejściowych, wnioskowania, w jaki sposób generować dane wyjściowe. Sama już tylko ta – jak się wydaje, absolutnie podstawowa – definicja wielokrotnie była zmieniana, co chyba dobrze oddaje poziom skomplikowania prac legislacyjnych. Ostatecznie mamy bardzo szeroką definicję, która obejmie obszerny zakres systemów i narzędzi opartych na rozwiązaniach AI.

Jedną z podkategorii systemów AI, która pojawiła się w ostatniej wersji projektu rozporządzenia, jest „system AI ogólnego przeznaczenia" (general purpose artificial ineligence, GPAI).

AI Act wprowadza również definicję „modelu AI ogólnego przeznaczenia". To model AI trenowany dużą ilością danych, wykazujący znaczną ogólność i będący w stanie wykonywać szeroki zakres zadań, a także, co istotne – model, który można zintegrować z różnymi systemami lub aplikacjami niższego rzędu. AI Act przewiduje dla nich dodatkowe wymogi, w szczególności w zakresie oceny takich modeli, szacowania ryzyka systemowego, jak również obowiązków notyfikacyjnych. Dostawcy takich modeli AI będą mieli obowiązek m.in. sporządzania i regularnej aktualizacji ich dokumentacji technicznej. Dokumentacja będzie musiała zawierać opis procesu trenowania i testowania określonego systemu. AI Act przewiduje również obowiązek udostępniania dokumentacji modeli GPAI innym dostawcom, którzy chcieliby je wykorzystać w ramach swojego systemu AI. Szczególnego podkreślenia wymaga, że dostawcy takich modeli zobowiązani będą także posiadać politykę w zakresie przestrzegania unijnych przepisów dot. ochrony praw autorskich.



Systemy wysokiego ryzyka – kluczowe wymogi

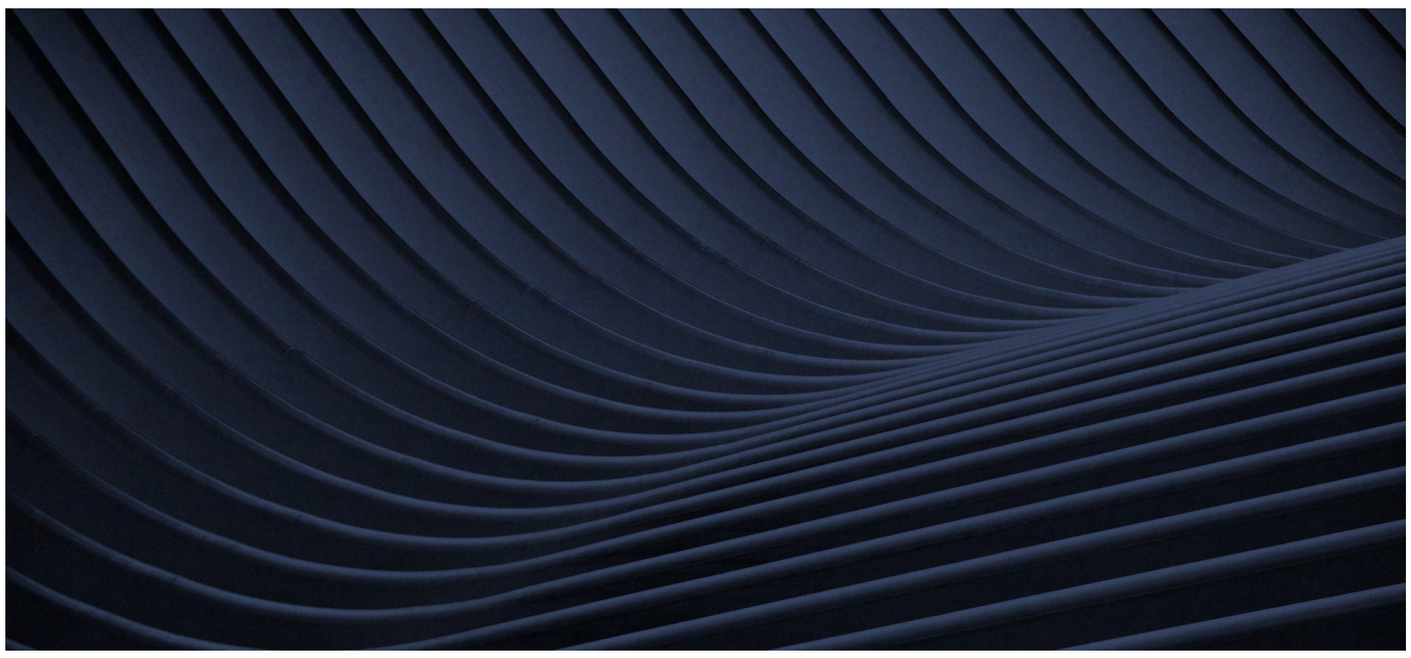
Systemy AI mogą być zakwalifikowane jako tzw. systemy wysokiego ryzyka. Ich właśnie dotyczy najwięcej wymogów i obowiązków. O jakie systemy chodzi? Będą to m.in. systemy identyfikacji biometrycznej, systemy wykorzystywane w ramach infrastruktury krytycznej czy przeznaczone do celów rekrutacji, w tym filtrowania podań o pracę czy oceny kandydatów (systemy wymienione w Załączniku III do AI Act).

Konsekwencją przyjęcia, że mamy do czynienia z systemem wysokiego ryzyka, będzie konieczność spełnienia wielu dodatkowych wymogów i obowiązków. W szczególności chodzi tutaj o obowiązek posiadania systemu zarządzania ryzykiem w odniesieniu do takich systemów AI. Również dane wykorzystywane do trenowania systemów AI wysokiego ryzyka będą musiały spełnić określone kryteria jakości, a zarządzanie nimi będzie musiało odbywać się wedle kryteriów określonych w AI Act. Rozporządzenie określa też szczególne wymogi dotyczące rejestrowania zdarzeń, przejrzystości działania systemów AI wysokiego ryzyka oraz nadzoru nad ich działaniem ze strony człowieka.

Warto również zwrócić uwagę, że wprowadzenie do obrotu systemu AI wysokiego ryzyka wiązać się będzie z koniecznością przeprowadzenia oceny wpływu na prawa podstawowe (tzw. FRIA – fundamental rights impact assesment). Tego rodzaju ocena będzie musiała objąć m.in. (i) opis procesów podmiotu stosującego AI, w których dany system będzie wykorzystany, (ii) opis okresu i częstotliwości wykorzystania danego systemu AI, (iii) opis kategorii osób fizycznych i grup, na które może mieć wpływ wykorzystanie systemu. To rozwiązanie podobne do znanej już z RODO oceny skutków dla ochrony danych (DPIA – art. 35 RODO). Zresztą przepisy AI Act wprost odwołują się do DPIA, pozwalając w określonych przypadkach traktować FRIA jako jego uzupełnienie.

Kary administracyjne

Podobieństw do RODO jest więcej. Dotyczą one m.in. konstrukcji i wysokości kar administracyjnych nakładanych przez właściwe organy nadzoru. W tym zakresie AI Act przewiduje np. kary w wysokości 35 mln EUR lub 7% całkowitego rocznego światowego obrotu przedsiębiorstwa za naruszenie przepisów dotyczących zakazanych systemów AI (w zależności od tego, która kwota jest wyższa), a także 7,5 mln EUR lub 1% całkowitego rocznego światowego obrotu za podanie nieprawidłowych informacji właściwym organom.



Ważne terminy – kiedy AI Act wejdzie w życie?

AI Act wejdzie w życie 20 dni po jego ogłoszeniu w dzienniku urzędowym UE, ale większość przepisów będzie obowiązywała dopiero po upływie kolejnych 24 miesięcy. W praktyce oznacza to zatem dwuletni okres, aby dostosować się do wymogów regulacji. Jednak niektóre przepisy zaczną obowiązywać już wcześniej, tj. po 6 lub 12 miesiącach od wejścia w życie AI Act. Dotyczy to w szczególności zakazanych sposobów wykorzystania AI czy wybranych kar administracyjnych.

RYMARZ · ZDORT · MARUTA

Osoby do kontaktu:

Paweł Tobiczyk

Partner
pawel.tobiczyk@rzmlaw.com

Marcin Serafin

Partner
marcin.serafin@rzmlaw.com

Piotr Kalina

Partner
piotr.kalina@rzmlaw.com

Wojciech Piszewski

Counsel
wojciech.piszewski@rzmlaw.com