AI Act – odpowiedzi na kluczowe pytania

(red.: Marcin Ręgorowicz; współautorzy: Aleksandra Kołodziejczyk, Marcin Ręgorowicz, Kamila Dymek, Dominik Gabor, Piotr Konieczny)

Eksperci IAB Polska z Grupy Zadaniowej Prawo AI IAB Polska przygotowali odpowiedzi na kluczowe pytania, które mogą pojawić się w odniesieniu do tzw. ***AI Act***, czyli **Aktu w sprawie sztucznej inteligencj**i.

Niektóre zagadnienia zostały opracowane w uproszczony sposób, aby ułatwić odbiór tekstu. Pamiętaj, że poszczególne przepisy *AI Act* mogą regulować część tematów w sposób bardziej precyzyjny. **Zatem jeśli chcesz zastosować Rozporządzenie w praktyce, zawsze konieczna będzie analiza konkretnych przepisów**.

1. Czym jest *AI Act* i jakie są jego cele?

***Akt w sprawie sztucznej inteligencji* to pierwszy akt prawny zarówno w Unii Europejskiej, jak i na świecie, który kompleksowo reguluje i określa ramy prawne w zakresie sztucznej inteligencji.**

Regulacje te dotyczą rozwoju, wprowadzania do obrotu, oddawania do użytku i wykorzystywania systemów sztucznej inteligencji (AI).

AI Act powstał po to, by **upowszechniać godną zaufania i ukierunkowaną na człowieka AI.** Wszystko to przy zapewnieniu wysokiego poziomu ochrony zdrowia, bezpieczeństwa i praw zapisanych w Karcie praw podstawowych UE.

AI Act ma także **wspierać innowacje i zapewniać swobodny transgraniczny przepływ towarów i usług opartych na AI**. Oznacza to, że państwa członkowskie nie mogą ograniczać rozwoju, wprowadzania do obrotu i wykorzystywania systemów AI.

Pełna nazwa dokumentu to: *„Rozporządzenie Parlamentu Europejskiego i Rady (UE) ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji i zmieniające rozporządzenia (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektywy 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji)*”.

2. Czego dotyczy AI Act?

***AI Act* reguluje podstawowe zasady korzystania z systemów opartych na sztucznej inteligencji. Ponadto klasyfikuje systemy AI w zależności od ryzyka, jakie za sobą pociągają i wpływu, jaki mogą wywierać na użytkowników.**

- Przy poziomie ryzyka, który zostanie zidentyfikowany jako **niedopuszczalny**, użycie systemu AI jest zakazane (np. systemy scoringu społecznego i systemy stosujące celowe techniki manipulacyjne).
- Systemy AI **wysokiego** i **ograniczonego** ryzyka podlegać będą dodatkowym wymogom i ograniczeniom. Te pierwsze bardziej rygorystycznym i to ich dotyczy przeważająca część przepisów *AI Act*.

Większość wymogów Rozporządzenia adresowana jest do dostawców i podmiotów stosujących systemy AI. Co więcej, ma do nich zastosowanie niezależnie od tego, czy mają siedzibę w Unii Europejskiej czy poza nią – ważny jest sam fakt, że wyniki działania systemów AI są wykorzystywane w UE.

3. Od kiedy obowiązuje AI Act?

***AI Act* zacznie w pełni obowiązywać po 24 miesiącach od daty jego wejścia w życie** (datą wejścia w życie AI Act jest dwudziesty dzień po opublikowaniu Rozporządzenia w Dzienniku Urzędowym Unii Europejskiej).

Niektóre przepisy *AI Act* będą stosowane już wcześniej, np. dotyczące zakazanych praktyk w zakresie AI (po 6 miesiącach od daty wejścia Rozporządzenia w życie), nakładające obowiązki dostawców modeli AI ogólnego przeznaczenia czy większość przepisów dotyczących kar (po 12 miesiącach od daty wejścia Rozporządzenia w życie).

Dłuższy termin (36 miesięcy od dnia wejścia w życie) przewidziany został w przypadku przepisów dotyczących systemów AI, które są elementami produktu związanymi z bezpieczeństwem lub same są takimi produktami, a także szczególne systemy z określonych obszarów, o których mowa w załączniku III.

4. Kogo dotyczy AI Act?

***AI Act* ma zastosowanie do szeregu podmiotów, zarówno przedsiębiorstw, jak i osób fizycznych, które wykorzystują AI.** Rozporządzenie dzieli te podmioty na następujące kategorie:

- dostawcy
- podmioty stosujące AI,
- importerzy,
- dystrybutorzy,
- upoważnieni przedstawiciele dostawców,
- producenci (którzy wraz ze swoim produktem wprowadzają do obrotu lub oddają do użytku system AI opatrzony ich nazwą handlową lub znakiem towarowym),
- operatorzy (zbiorcze określenie na wszystkie powyższe kategorie).

***AI Act* znajdzie jednak najszersze i najbardziej praktyczne zastosowanie przede wszystkim w stosunku do dwóch pierwszych grup, czyli dostawców systemów AI (ang. *providers*) oraz do podmiotów stosujących AI (ang. *deployers*), czyli np. do organizacji, które wdrażają systemy AI na potrzeby swojej działalności**.

Pozostałe kategorie podmiotów będą podlegać tylko niektórym z obowiązków przewidzianych w Rozporządzeniu.

AI Act obejmie również takie systemy AI, które zostaną wprowadzone na rynek UE lub których użycie będzie miało wpływ na osoby znajdujące się w UE. **Oznacza to, że nowe przepisy dotyczą także tych podmiotów, które nie mają siedziby na terenie UE**.

Większość szczegółowych wymogów wprowadzonych przez *AI Act* będzie dotyczyła głównie systemów AI wysokiego ryzyka, czyli wykorzystywanych w krytycznych obszarach, np. w sektorze finansowym, opiece zdrowotnej czy edukacji. Zatem, mimo że *AI Act* obejmuje wiele podmiotów, to tylko niektóre z nich będą objęte najbardziej dotkliwymi obowiązkami.

5. Kogo nie dotyczy *AI Act*?

Mimo że regulacje *AI Act* obejmują wiele podmiotów, przewidują również pewne istotne wyjątki, które wyłączają z ich zakresu niektóre aktywności i systemy, np. w przypadku zastosowań osobistych czy militarnych.

Obowiązki wynikające z *AI Act* nie dotyczą:

- osób korzystających z systemów AI w ramach osobistej działalności pozazawodowej;
- konkretnych systemów AI, np. tych przeznaczonych wyłącznie do celów wojskowych, obronnych lub do celów bezpieczeństwa narodowego;
- działań badawczych i rozwojowych poprzedzających wprowadzenie systemów na rynek.

6. Jak AI Act wpływa na podmioty działające na rynku reklamy internetowej?

AI Act istotnie wpływa na działalność wszystkich firm na rynku reklamy internetowej wykorzystujących AI (niezależnie o rodzaju działalności), ale stopień tego wpływu może być różny.

Przede wszystkim nowe przepisy nakładają na firmy obowiązek weryfikacji tego, czy korzystanie z danego systemu AI w ogóle jest dopuszczalne oraz jakie czynności się z tym wiążą.

Dodatkowo na wszystkie firmy wykorzystujące narzędzia AI zostaną nałożone także pewne generalne obowiązki, np. w zakresie transparentności i wewnętrznych zasad korzystania z systemów, a także ograniczenia, np. praktyki zakazane. Do tej pory takich szczególnych regulacji czy ograniczeń dotyczących rozwiązań opartych na AI nie było.

Stopień wpływu regulacji *AI Act* na podmioty działające na rynku reklamy internetowej zależy przede wszystkim od:

a) kwalifikacji danego systemu AI (praktyki zakazane, systemy wysokiego ryzyka czy systemy o ograniczonym lub minimalnym ryzyku),
b) roli, w jakiej występuje dany podmiot wykorzystujący AI - czy jest podmiotem stosującym („*deployer*") czy dostawcą („*provider*") lub ewentualnie kwalifikuje się do innej kategorii, np. jest importerem.

Z jednej strony zatem wszystkie firmy wykorzystujące AI będą musiały spełnić pewne ogólne obowiązki, ale konkretny wpływ na dany podmiot będzie zależał od powyższej kwalifikacji.

- W przypadku części firm konieczna może być całkowita przebudowa procesów biznesowych i zaprzestanie stosowania narzędzi AI w ramach określonej działalności. Będzie to miało miejsce np. w przypadku, gdy dane zastosowanie AI będzie stanowiło praktykę zakazaną m.in. w przypadku niedostosowanych do rynku unijnego systemów AI pozwalających na targetowanie reklam lub profilowanie użytkowników, zwłaszcza opartych na technikach manipulacyjnych czy podprogowych.

- W innych przypadkach wpływ może być minimalny (np. konieczność wprowadzenia wewnętrznej polityki czy spełnienia obowiązków informacyjnych, np. przez umieszczenie odpowiednich informacji w danym narzędziu).

Większość podmiotów z branży reklamy internetowej (np. agencje, wydawcy) najczęściej będzie działała jako podmioty stosujące („*deployers*") systemy AI, ponieważ będą co do zasady korzystać z gotowych, dostępnych na rynku narzędzi do generowania lub obróbki treści.

Jeśli Twoja firma wykorzystuje gotowe systemy AI, powinieneś:

- zapoznać się z obowiązkami przewidzianymi dla takich podmiotów w zakresie systemów AI wysokiego ryzyka (zob. art. 26 *AI Act*) oraz innych systemów AI (zob. art. 50 *AI Act);*
- zwrócić uwagę na możliwość przypisania im roli dostawcy systemu AI wysokiego ryzyka, co zdecydowanie poszerzy zakres obowiązków do spełnienia (zob. art. 25 i art. 16 *AI Act*);
- przeanalizować oraz uregulować także:
    - korzystanie z systemów AI przez pracowników lub współpracowników (np. content creatorów, specjalistów od digital marketingu),
    - zasady realizowania umów zawieranych między reklamodawcami a agencjami na prowadzenie kampanii reklamowych (np. możliwość lub zakaz korzystania z systemów AI dla potrzeb realizacji kampanii).

7. Na jakie inne przepisy wpływa *AI Act*?

W pełnym brzmieniu tytułu *AI Act* zostały wymienione rozporządzenia i dyrektywy unijne, które ulegną zmianie na mocy nowych przepisów. Zakres zmian wskazano w *Rozdziale XIII* dokumentu.

Jako rozporządzenie harmonizujące *AI Act* wpływa również na liczne regulacje sektorowe. Wykaz unijnego prawodawstwa harmonizacyjnego jest zamieszczony w *Załączniku I do AI Act*.

8. Czym jest system AI?

Zgodnie z definicją zawartą w Rozporządzeniu **„system AI" to system maszynowy, który został zaprojektowany do działania z różnym poziomem autonomii po jego wdrożeniu oraz który może wykazywać zdolność adaptacji po jego wdrożeniu, a także który – na potrzeby wyraźnych lub dorozumianych celów – wnioskuje, jak generować na podstawie otrzymanych danych wejściowych wyniki, takie jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne.**

Taki system ma następujące cechy:

- (po dokonaniu wdrożenia) może wykazywać zdolność samouczenia ;
- (po dokonaniu wdrożenia) może wnioskować – generować na podstawie danych wejściowych ("*input"*) wyniki ("*output"*): predykcje, treści, zalecenia, decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne;
- może uzyskiwać modele lub algorytmy. Wyniki wnioskowania mogą wpływać na środowisko fizyczne lub wirtualne;
- nie jest ograniczony tylko do podstawnego przetwarzania danych, gdyż umożliwia uczenie się, rozumowanie lub modelowanie.

***AI Act* nie definiuje natomiast pojęcia samej „sztucznej inteligencji".** Co więcej, definicja i jej sformułowania budzą wątpliwości w praktyce. Problem stanowi np. rozdzielenie zwykłych programów komputerowych od algorytmów AI, czy rzeczywista istotność kryterium wykorzystania maszyn jako elementu odróżniającego systemy AI od innych systemów komputerowych.

9. Czym jest system AI ogólnego przeznaczenia?

Zgodnie z definicją zawartą w Rozporządzeniu **„system AI ogólnego przeznaczenia" to system AI służący różnym celom oparty na modelu AI ogólnego przeznaczenia**. Może być wykorzystywany samodzielnie lub po integracji z innymi systemami.

„Model AI ogólnego przeznaczenia", zawarty w tej definicji, **oznacza model AI, w tym model AI trenowany dużą ilością danych z wykorzystaniem nadzoru własnego na dużą skalę, który wykazuje znaczną ogólność i jest w stanie kompetentnie wykonywać szeroki zakres różnych zadań, niezależnie od sposobu, w jaki model ten jest wprowadzany do obrotu, i który można zintegrować z różnymi systemami lub aplikacjami niższego szczebla – z wyłączeniem modeli AI, które są wykorzystywane na potrzeby działań w zakresie badań, rozwoju i tworzenia prototypów przed wprowadzeniem ich do obrotu.**

Przykładem są duże generatywne modele AI (np. GPT-4). Model może być integrowany z różnymi systemami lub aplikacjami niższego szczebla. Wyjątek stanowią modele AI wykorzystywane do badań, rozwoju i tworzenia prototypów przed wprowadzeniem ich do obrotu. **Model nie jest systemem AI**, chyba że zostanie poszerzony np. o interfejs użytkownika lub zostanie dodany do systemu.

Model jest silnikiem, który napędza system, jest jego kluczowym elementem, ale nie jedynym. System zawiera w sobie więcej części, np. graficzny interfejs użytkownika. **Przykładowo: Chat GPT jest systemem AI, który korzysta z modelu AI w postaci GPT-4o, dzięki któremu może wykonywać różne działania.**

10. Czym jest *deepfake* i jakie obowiązki są związane z jego stosowaniem?

Zgodnie z definicją zawartą w *AI Act* **„*deepfake*" to wygenerowany lub zmanipulowany obraz, dźwięk lub wideo.** Taka treść różni się od innych generowanych przez systemy AI treści tym, że **przypomina istniejące osoby, przedmioty, miejsca lub inne podmioty lub zdarzenia, które odbiorca *deepfake'a* mógłby niesłusznie uznać za autentyczne lub prawdziwe.**

Jeśli stosujesz system AI do tworzenia *deepfake'ów* albo wygenerowanych lub zmanipulowanych tekstów dotyczących interesu publicznego i publikowanych w celu informacyjnym, **musisz ujawnić, że treść została sztucznie wygenerowana lub zmanipulowana, chyba że jest ona legalnym elementem wykrywania lub zwalczania przestępstw.**

Powyższy obowiązek musisz realizować w sposób jasny, wyraźny, dostępny i najpóźniej w momencie pierwszego zetknięcia się z treścią. Oznaczanie *deepfake'ów* nie może utrudniać wyświetlania lub korzystania z utworów. Obowiązek nie dotyczy tekstu, jeżeli ten został zweryfikowany przez człowieka lub poddany kontroli redakcyjnej, a odpowiedzialność redakcyjną za jego publikację ponosi osoba fizyczna lub prawna.

11. Jakie rodzaje systemów AI są zakazane?

Zakazane jest stosowanie praktyk w zakresie sztucznej inteligencji, które z uwagi na swoje szczególnie szkodliwe cechy stwarzają istotne zagrożenie dla zdrowia, bezpieczeństwa i praw człowieka (m.in. prawa do prywatności, praw pracowniczych czy praw dziecka).

Oznacza to, że zakazane są praktyki polegające na wprowadzaniu do obrotu, oddawaniu do użytku lub wykorzystywaniu systemów AI:

- stosujących techniki podprogowe, celowe techniki manipulacyjne lub wprowadzające w błąd;
- wykorzystujących dowolne słabości osób fizycznych ze względu na ich wiek, niepełnosprawność lub szczególną sytuację społeczną lub ekonomiczną;
- oceniających lub klasyfikujących osoby fizyczne na podstawie ich cech lub zachowania społecznego (systemy "*social scoringu*");

- przewidujących prawdopodobieństwo popełnienia przestępstwa przez osobę fizyczną wyłącznie na podstawie profilowania tej osoby;
- tworzących bazy danych do celów rozpoznawaniu twarzy, które pozyskują wizerunki twarzy z internetu lub nagrań CCTV ("*scraping"*);
- wyciągających wnioski na temat emocji osoby fizycznej w miejscu pracy lub instytucjach edukacyjnych;
- wykorzystujących kategoryzacje biometryczne, które wnioskują na temat: rasy, poglądów politycznych, przynależności do związków zawodowych, przekonań religijnych lub filozoficznych, życia seksualnego lub orientacji seksualnej;
- stosujących zdalną identyfikację biometryczną w czasie rzeczywistym w przestrzeni publicznej do celów ścigania przestępstw (z pewnymi wyjątkami).

Pamiętaj, że zakazane są jedynie określone praktyki odnoszące się do wskazanych powyżej systemów AI, a nie jakiekolwiek praktyki odnoszące się do takich systemów.

Zakaz dotyczący powyższych systemów będzie obowiązywał **już po sześciu miesiącach od wejścia *AI Act* w życie**.

12. Czym jest system AI wysokiego ryzyka?

Systemy AI wysokiego ryzyka to takie systemy, które - choć stwarzają ryzyko dla zdrowia, bezpieczeństwa i praw człowieka - mogą również wiązać się ze znaczącymi korzyściami dla jednostek. Dlatego też *AI Act* dopuszcza je do obrotu, ale dopiero po spełnieniu dodatkowych wymogów.

System AI jest uznawany za system AI wysokiego ryzyka w dwóch grupach przypadków:

1. Jeżeli system AI jest elementem związanym z bezpieczeństwem produktu objętego unijnym prawodawstwem harmonizacyjnym (wymienionym w Załączniku I do *AI Act)* lub sam będzie takim produktem, a dodatkowo będzie podlegał – na podstawie prawa UE – obowiązkowej ocenie zgodności dokonanej przez stronę trzecią.

   Unijne akty prawne wymienione w załączniku I odnoszą się do m.in.:
   - bezpieczeństwa zabawek,
   - urządzeń radiowych,
   - środków ochrony indywidulanej,
   - wyrobów medycznych,
   - homologacji pojazdów.

2. Jeżeli taki system AI jest wprost oznaczony w załączniku III do AI Act. Są to systemy, które zostały przyporządkowane do następujących sektorów:

   - biometria,
   - infrastruktura krytyczna,

- kształcenie i szkolenie zawodowe,
- zatrudnienie, zarządzanie pracownikami i dostęp do samozatrudnienia,
- dostęp do podstawowych usług prywatnych oraz podstawowych usług i świadczeń publicznych, a także korzystanie z nich,
- ściganie przestępstw,
- zarządzanie migracją, azylem i kontrolą graniczną,
- sprawowanie wymiaru sprawiedliwości i procesy demokratyczne.

Nie wszystkie systemy AI wykorzystywane w ramach powyższych sektorów są systemami AI wysokiego ryzyka. Zaliczają się do nich jedynie te z nich, które wprost zostały wskazane w załączniku III.

Ponadto w przepisach Rozporządzenia znajduje się wyłączenie, na podstawie którego nie wszystkie system AI wskazane w załączniku III należy uznać za system AI wysokiego ryzyka. Warunki związane z tym wyłączeniem zostały wskazane w kolejnym pytaniu.

13. Kiedy system AI wskazany w załączniku III nie będzie systemem AI wysokiego ryzyka?

System AI wskazany w załączniku III może nie zostać uznany za system AI wysokiego ryzyka, jeżeli nie stwarza znaczącego ryzyka spowodowania szkody dla zdrowia, bezpieczeństwa lub praw podstawowych.

Ma to miejsce, gdy system AI jest przeznaczony do:

- wykonywania wąskiego zadania proceduralnego;
- poprawienia wyniku zakończonej uprzednio czynności wykonywanej przez człowieka;
- wykrywania wzorców podejmowania decyzji lub odstępstw od wzorców podjętych uprzednio decyzji i nie ma na celu zastąpienia ani wywarcia wpływu na ukończoną uprzednio ocenę dokonaną przez człowieka;
- wykonywania zadań przygotowawczych w kontekście oceny istotnej z punktu widzenia przypadków jego użycia wymienionych w załączniku III *AI Act*.

Aby system AI nie został uznany za system wysokiego ryzyka, wystarczy spełnienie co najmniej jednego z powyższych warunków. Jednocześnie Komisja Europejska została upoważniona do przyjmowania dodatkowych aktów prawnych, które mogą modyfikować powyższe warunki.

14. Jakie obowiązki nakłada *AI Act* na wszystkie systemy AI (niezależnie od stopnia ryzyka)?

Dostawcy wszystkich systemów AI powinni zapewnić:

- aby osoby fizyczne, które wchodzą w bezpośrednią interakcję z systemem AI, były informowane o tym, że prowadzą interakcję z takim systemem;

- aby systemy AI generujące treści w postaci syntetycznych dźwięków, obrazów, wideo lub tekstu wprowadzały do nich oznakowanie w formacie nadającym się do odczytu maszynowego, że wynik ich działania został sztucznie wygenerowany lub zmanipulowany.

Jeśli stosujesz systemy AI (jesteś "deployerem"), które generują lub modyfikują obrazy, treści audio lub wideo stanowiące *deepfake,* powinieneś **ujawnić, że te treści zostały sztucznie wygenerowane lub zmanipulowane**.

Powinieneś również zapewnić, aby systemy AI generujące lub modyfikujące teksty informujące społeczeństwo o sprawach leżących w interesie publicznym **jasno wskazywały, że taki tekst został sztucznie wygenerowany lub zmanipulowany.**

15. Jakie obowiązki są nakładane na systemy AI wysokiego ryzyka?

Użycie systemów AI wysokiego ryzyka wiąże się z koniecznością spełnienia szeregu różnych obowiązków, w zależności od wielu czynników, np.:

- wdrożenia systemu zarządzania ryzykiem przez cały cykl życia systemu AI;
- właściwego zarządzania danymi;
- przygotowania odpowiedniej dokumentacji technicznej;
- bieżącego rejestrowania zdarzeń przez cały cykl życia systemu AI;
- zapewnienia przejrzystości i informowania (w tym umożliwienia interpretacji wyników działania systemu AI i przygotowania odpowiednich instrukcji obsługi);
- możliwości zapewnienia nadzoru nad systemem AI ze strony człowieka;
- dokładności, solidności i cyberbezpieczeństwa systemu AI (w tym odporności na błędy, usterki lub „stronniczość" systemu, a także podejmowania działań naprawczych);
- przeprowadzenia procedury oceny zgodności;
- monitorowania systemu AI po wprowadzeniu go do obrotu i zgłaszania poważnych incydentów.

Przed zastosowaniem systemu AI wysokiego ryzyka zidentyfikowanego na podstawie załącznika III do *AI Act* niektóre podmioty stosujące AI (głównie związane z sektorem publicznym) będą zobowiązane przeprowadzić ocenę wpływu wykorzystania systemu AI na prawa podstawowe.

16. Na kogo nakładane są obowiązki dotyczące systemów AI wysokiego ryzyka?

Obowiązki wynikające z *AI Act* nakładane są praktycznie na wszystkie podmioty, które pojawią się w cyklu życia określonego systemu AI wysokiego ryzyka.

Największa pula obowiązków będzie jednak nakładana na dostawców systemów AI, czyli podmioty, które opracowują lub zlecają opracowanie systemu AI (lub modelu AI ogólnego przeznaczenia) i które wprowadzają go do obrotu lub oddają do użytku pod własną nazwą (zarówno odpłatnie, jak i Aby ograniczyć potencjalne szkody związane z systemami AI wysokiego ryzyka, *AI Act* nakłada na nie dodatkowe obowiązki. Wymogi te

będą obowiązywały w całym cyklu życia systemu AI – zarówno w fazie jego opracowywania, jak i w momencie, gdy będzie on już wykorzystywany przez użytkowników.

W mniejszym zakresie indywidualne obowiązki będą również nakładane na importerów, dystrybutorów oraz podmioty stosujące systemy AI.

Co więcej, wskazane powyżej podmioty przejmą rolę dostawców systemów AI (będą traktowane jak dostawcy), jeżeli:

- umieszczą swoją nazwę lub znak towarowy w systemie AI wysokiego ryzyka, który został już wprowadzony do obrotu lub oddany do użytku;
- dokonają istotnej zmiany we wprowadzonym już do obrotu lub oddanym do użytku systemie AI wysokiego ryzyka;
- zmienią przeznaczenie „zwykłego" systemu AI w taki sposób, że stanie się on systemem AI wysokiego ryzyka.

17. Jakie organy będą właściwe do rozstrzygania w sprawach *AI Act*?

Podstawowym organem zajmującym się AI na obszarze UE będzie **Europejski Urząd ds. Sztucznej Inteligencji.** Urząd będzie zajmował się wdrażaniem, monitorowaniem i nadzorowaniem systemów AI oraz zarządzaniem AI.

Wyróżnione są także dwa organy krajowe właściwe w sprawach stosowania rozporządzenia:

- organ notyfikujący, który odpowiada za: opracowanie i stosowanie procedur koniecznych do oceny, wyznaczania i notyfikowania jednostek oceniających zgodność oraz za ich monitorowanie;
- organ nadzoru rynku wyznaczony w celu sprawowania nadzoru rynku państwa członkowskiego (rozporządzenie 2019/1020).

Aktualnie w Polsce toczy się debata, czy powinny zostać powołane nowe organy czy też role organów w zakresie AI powinny zostać przyznane już istniejącym (np. jedną z propozycji jest przyznawanie takich uprawnień organom właściwym ws. ochrony danych osobowych).

18. Jakie są obowiązki dostawców modeli AI ogólnego przeznaczenia?

***AI Act* nakłada szczególne obowiązki na dostawców modeli AI ogólnego przeznaczenia.** Wynika to z faktu, że specyfika tych modeli obejmuje możliwość zintegrowania ich z systemami niższego szczebla.

AI Act ma więc zapewnić, że **dostawcy tych modeli ujawnią wszystkie niezbędne informacje dostawcom systemów niższego szczebla, tak aby te systemy były bezpieczne i zgodne z przepisami.**

Obowiązki te będą obejmować między innymi: sporządzenie dokumentacji technicznej, wdrożenie polityki zapewniającej zgodność z prawem autorskim oraz przygotowanie streszczenia treści użytych do trenowania modelu.

19. Jak uregulowane są modele ogólnego przeznaczenia mogące stwarzać ryzyko systemowe, takie jak GPT-4o?

AI Act wyodrębnia spośród modeli AI ogólnego przeznaczenia szczególną kategorię takich modeli, które mogą stwarzać ryzyko systemowe, w szczególności ze względu na **zdolność dużego oddziaływania**.

To, czy model ma zdolność dużego oddziaływania, zależy od liczby obliczeń wykorzystywanych do jego trenowania. Obecnie warunek ten spełniają jedynie niektóre modele (np. GPT-4o od OpenAI). Próg dla spełnienia tego warunku może być aktualizowany w miarę postępu technologicznego.

Dostawcy takich modeli podlegają dodatkowym wymogom, związanym z rygorystyczną oceną i testowaniem modeli, oceną i ograniczaniem ryzyka, szerokimi obowiązkami sprawozdawczymi czy też zapewnieniem cyberbezpieczeństwa.

20. Na jakie systemy nakładane są szczególne wymogi w zakresie przejrzystości?

W przypadku niektórych systemów AI nakładane są szczególne wymogi w zakresie przejrzystości, zwłaszcza wtedy gdy istnieje **wyraźne ryzyko manipulacji**. *AI Act* zakłada, że w takich sytuacjach **użytkownicy powinni być świadomi, że mają do czynienia z maszyną.**

- W przypadku **systemów przeznaczonych do wchodzenia w bezpośrednią interakcję z osobami fizycznymi (np. chatbotów)** dostawcy mają zapewnić, że użytkownicy będą informowani o interakcji z AI, chyba że jest ona oczywista z punktu widzenia użytkownika – osoby fizycznej.
- W przypadku **systemów AI generujących syntetyczne treści (dźwięk, obrazy, wideo, tekst)** dostawcy muszą oznaczać wyniki ich działania jako sztucznie wygenerowane. Oznaczenia mają być zapewnione w formacie nadającym się do odczytu maszynowego (np. w postaci metadanych), tak aby treści powstałe przy użyciu systemów AI mogły zostać wykryte.
- Podmioty stosujące **systemy rozpoznawania emocji lub biometrycznej kategoryzacji** muszą informować o ich stosowaniu osoby, wobec których systemy te są stosowane, a także przestrzegać odpowiednich przepisów o ochronie danych.

21. Czego nie znajdziemy w AI Act?

W *AI Act* nie znajdziemy:

- **uregulowań dotyczących pozaumownej odpowiedzialności cywilnej za AI -** to ma zostać określone odrębną dyrektywą, nad którą toczą się prace;
- **regulacji kwestii własności intelektualnej i „rewolucji" w sprawie prawnoautorskich aspektów AI**.

AI Act nie legitymizuje bezwarunkowo wykorzystywania chronionych utworów w celu trenowania modeli AI i wymaga od dostawców, aby wykorzystanie materiałów objętych prawami autorskimi odbywało się w zgodzie z obowiązującymi w Unii przepisami.

Rozporządzenie uznaje przy tym wcześniej przyjęte wyjątki, takie jak dozwolony użytek w zakresie eksploracji tekstów i danych, wynikający z przepisów DSM (tj. Dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE).

AI Act nie wypowiada się także o charakterze prawnym wytworów generatywnej AI i nie przyznaje sztucznej inteligencji przymiotu twórcy.

22. W jaki sposób AI Act ma służyć wspieraniu innowacyjności?

Jednym z zadań *AI Act* jest wspieranie innowacyjnej działalności przedsiębiorstw, w szczególności MŚP i start-upów.

W tym celu *AI Act* umożliwia między innymi tworzenie tzw. **piaskownic regulacyjnych („*regulatory sandbox*")** i **testowanie systemów w świecie rzeczywistym**, a w określonych przypadkach również poza piaskownicami.

- **Piaskownica to specjalne warunki stworzone przez władze krajowe, które pozwalają firmom pracującym nad AI na: rozwijanie, trenowanie, sprawdzanie i testowanie innowacyjnych systemów przed ich wprowadzeniem do obrotu**. Odbywa się to na podstawie wcześniej ustalonego planu, przez ograniczony czas i pod nadzorem regulacyjnym. W praktyce pozwala to na testowanie nowych technologii w realnych warunkach.

- **Właściwy krajowy organ ma stworzyć przynajmniej jedną piaskownicę regulacyjną, która zostanie uruchomiona w ciągu 24 miesięcy od daty wejścia rozporządzenia w życie**. Pierwszeństwo w dostępie do piaskownic ma być przyznane MŚP, które mają siedzibę statutową lub oddział w Unii Europejskiej.

- **Ponadto państwa członkowskie mają organizować specjalne wydarzenia informacyjne i szkoleniowe** poświęcone stosowaniu przepisów rozporządzenia oraz wykorzystywać istniejące kanały, aby pomagać i odpowiadać na pytania dotyczące wdrożenia nowych przepisów.

23. Jakie są zasady testów systemów AI wysokiego ryzyka w warunkach rzeczywistych?

Testy działania systemów AI wysokiego ryzyka w warunkach rzeczywistych mogą trwać tylko tak długo, jak jest to konieczne dla osiągnięcia ich celów, maksymalnie przez 6 miesięcy, z opcją przedłużenia o dodatkowe 6 miesięcy.

- **Aby rozpocząć testy, konieczne jest przygotowanie i zgłoszenie planu testowego** do organu nadzorującego rynek, który musi wyrazić zgodę na plan oraz ustalone warunki testów.

- **Testowanie w warunkach rzeczywistych wymaga spełnienia określonych warunków zabezpieczających**, takich jak m.in.: uzyskanie świadomej zgody od uczestników, możliwość odwrócenia lub zignorowania wyników testów, zapewnienie braku negatywnych skutków testów dla uczestników, obowiązek usunięcia danych po zakończeniu testowania oraz zapewnienie możliwości wycofania zgody przez uczestników.

24. Na czym polega obowiązek monitorowania systemu AI wysokiego ryzyka po wprowadzeniu go do obrotu?

Dostawcy systemów AI wysokiego ryzyka muszą utworzyć i dokumentować system monitorowania po wprowadzeniu produktu na rynek.

- System ten ma polegać na aktywnym i systematycznym zbieraniu, dokumentowaniu i analizowaniu danych o działaniu systemów AI przez cały ich cykl życia, zarówno od użytkowników AI, jak i z innych źródeł.
  Dzięki temu dostawcy mogą regularnie oceniać, czy systemy AI spełniają wymagania określone w przepisach. W niektórych przypadkach monitorowanie obejmuje także analizę interakcji z innymi systemami AI.
- System monitorowania powinien być dostosowany do charakteru technologii i związanego z nią ryzyka. Opiera się on na planie, który jest częścią dokumentacji technicznej wymaganej przez *AI Act*. Ponadto Komisja ma przyjąć akt wykonawczy zawierający szczegółowe przepisy określające wzór planu monitorowania oraz wykaz elementów, które należy w nim zawrzeć.

Dostawcy systemów AI wysokiego ryzyka wprowadzonych do obrotu na rynku UE mają też obowiązek zgłaszania wszelkich poważnych incydentów organom nadzoru rynku w państwie członkowskim, w którym miał miejsce incydent.

25. Czym są dobrowolne kodeksy postępowania i wytyczne Komisji dotyczące stosowania systemów AI?

Zgodnie z *AI Act* dostawcy systemów AI nieobarczonych wysokim ryzykiem mogą poświadczać ich bezpieczeństwo dzięki własnym, dobrowolnym kodeksom postępowania lub poprzez stosowanie kodeksów opracowanych przez reprezentujące ich organizacje. Takie kodeksy w całości lub w części mogą odzwierciedlać wymogi, które AI Act przewiduje względem systemów wysokiego ryzyka.

Dobrowolne kodeksy postępowania mogą być tworzone również przez podmioty stosujące AI, które nie są ich dostawcami. Takie kodeksy powinny zawierać w szczególności: wytyczne etyczne UE dla godnej zaufania AI, ocenę i minimalizację wpływu AI na środowisko, promocję kompetencji AI, wspieranie inkluzywności i różnorodności w projektowaniu AI oraz ocenę i zapobieganie negatywnemu oddziaływaniu na osoby lub grupy szczególnie wrażliwe.

Właściwe organy mają wspierać tworzenie kodeksów i zachęcać do ich przyjmowania, szczególnie przez organizacje reprezentujące dostawców systemów AI i podmioty je stosujące.

Pomoc przy wdrożeniu *AI Act* mają również stanowić wytyczne dotyczące praktycznego wdrażania nowych przepisów opracowane przez Komisję. Wytyczne te będą wyjaśniać sposób realizacji poszczególnych obowiązków i wymogów, np. obowiązków w zakresie przejrzystości (patrz: pytanie 13).

26. Jakie kary przewiduje AI Act?

Rozporządzenia przewiduje szereg administracyjnych kar pieniężnych za niedostosowanie się do nowych przepisów:

- **Naruszenie zakazu praktyk w zakresie AI** – do 35 000 000 EUR lub (w przypadku przedsiębiorstwa) 7% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (karą jest wyższa wartość spośród tych dwóch kwot; w przypadku MŚP i start-upów – karą jest wartość niższa).
- **Niezgodność systemu AI z obowiązkami dostawców, upoważnionych przedstawicieli, importerów, dystrybutorów, podmiotów stosujących AI** (np. brak nadzoru wykwalifikowanego człowieka, brak kontroli nad inputem, wymogami i obowiązkami jednostek notyfikowanych, obowiązkami dostawców i użytkowników w zakresie przejrzystości – do 15 000 000 EUR lub (w przypadku przedsiębiorstwa) 3% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (karą jest wyższa wartość spośród tych dwóch kwot; w przypadku MŚP i start-upów – karą jest wartość niższa).
- **Przekazywanie nieprawidłowych, niekompletnych lub wprowadzających w błąd informacji jednostkom notyfikowanym lub właściwym organom krajowym w odpowiedzi na ich wezwanie** – do 7 500 000 EUR lub (w przypadku przedsiębiorstwa) 1% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (karą jest wyższa wartość spośród tych dwóch kwot; w przypadku MŚP i start-upów – karą jest wartość niższa).
- **Celowe lub w wyniku zaniedbania naruszenie AI Act przez dostawcę modelu AI ogólnego przeznaczenia** – do 15 000 000 EUR lub 3% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (karą jest zawsze wyższa wartość spośród tych dwóch kwot - niezależnie od tego, czy podmiot jest MŚP lub start-upem).

***AI Act* przewiduje także administracyjne kary pieniężne nakładane przez EIOD (Europejski Inspektor Danych Osobowych) na instytucje, organy i jednostki organizacyjne UE.**

Kary to nie jedyny sposób na zapewnienie egzekwowania *AI Act*. Rozporządzenie przewiduje, że odpowiednie organy będą posiadały także innego rodzaju uprawnienia (np. uzyskanie dostępu do kodu źródłowego systemu AI wysokiego ryzyka), w tym te o charakterze sankcji (np. wycofanie z rynku systemu AI wysokiego ryzyka).

27. Czy AI Act wymaga implementacji do prawa polskiego?
Nie. Jako unijne rozporządzenie *AI Act* jest wiążące w całości i bezpośrednio stosowane w państwach członkowskich bez potrzeby odrębnej implementacji.