Warszawa, 6 sierpnia 2021 r.

STANOWISKO

KOALICJI AI W ZDROWIU

ORAZ GRUPY ROBOCZEJ DS. SZTUCZNEJ INTELIGENCJI (SEKCJA ZDROWIE)

W SPRAWIE

PROJEKTU ROZPORZĄDZENIA WS. SZTUCZNEJ INTELIGENCJI

Działając w imieniu Koalicji AI w Zdrowiu oraz Grupy Roboczej ds. Sztucznej Inteligencji (sekcja zdrowie), mając na uwadze potrzebę odpowiedzialnego wykorzystania potencjału systemów AI w sektorze ochrony zdrowia, niniejszym składam uwagi do projektu Rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie Sztucznej Inteligencji) i zmieniającego niektóre akty ustawodawcze Unii, dalej zwanego „**Projektem**”[1].

Stanowisko zostało przygotowane przez prawników kancelarii prawnej Domański Zakrzewski Palinka: Jana Pachockiego, Rafała Lorenta, Pawła Kaźmierczyka, Monikę Kupis, Aleksandrę Auleytner oraz Pawła Gruszeczkiego.

1. KOALICJA AI W ZDROWIU

W skład Koalicji AI w Zdrowiu, dalej zwanej „**Koalicją**”, wchodzą firmy technologiczne, farmaceutyczne oraz z zakresu opieki medycznej o zasięgu lokalnym i globalnym. Łączy nas zainteresowanie rozwojem potencjału systemów AI. Wykorzystujemy oraz prowadzimy prace badawczo-rozwojowe nad technologiami umożliwiającymi zastosowanie systemów AI w zakresie m.in.: opieki medycznej, w tym telemedycyny oraz zaawansowanej diagnostyki, zarządzania w ochronie zdrowia, badaniach klinicznych, dystrybucji produktów leczniczych. Tworzymy produkty lecznicze i wyroby medyczne korzystające z tych technologii.

2. GRUPA ROBOCZA DS. SZTUCZNEJ INTELIGENCJI (SEKCJA ZDROWIE)

Grupa Robocza ds. Sztucznej Inteligencji (sekcja zdrowie), dalej zwana „**Grupą**”, to grupa ekspercka, która została utworzona w ramach Kancelarii Prezesa Rady Ministrów. Grupa zrzesza kilkudziesięciu ekspertów z sektora prywatnego i publicznego, którzy zajmują się zagadnieniami dot. sztucznej inteligencji w ochronie zdrowia. Celem Grupy jest wypracowanie rozwiązań legislacyjnych umożliwiających

[1] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM/2021/206 final).

skuteczny i bezpieczny rozwój oraz wdrażanie systemów AI w zdrowiu, a także edukacja i popularyzacja rozwiązań opartych o systemy AI.

3. PODSUMOWANIE

Koalicja oraz Grupa zwracają uwagę przede wszystkim na następujące kluczowe zagadnienia o charakterze systemowym:

ZAGADNIENIE	STANOWISKO
Brak uwzględnienia kwestii dot. systemów AI w sektorze ochrony zdrowia	Projekt nie zawiera w zasadzie żadnych regulacji dotyczących wykorzystania systemów AI w sektorze ochrony zdrowia, pomimo deklaracji zawartej w pierwszym motywie rozporządzenia. Tymczasem wykorzystanie systemów AI to wielka szansa i jedno z głównych wyzwań dla systemów ochrony zdrowia w państwach członkowskich.
Wadliwa definicja systemu AI	Definicja systemu AI zastosowana w Projekcie jest bardzo szeroka. Obejmuje nie tylko oprogramowanie oparte na mechanizmach uczenia maszynowego, lecz także np. bazy wiedzy oraz metody wyszukiwania. Tymczasem konieczne jest ponowne przeprowadzenie prac legislacyjnych w zakresie definicji systemów AI, w miarę możliwości z jak najszerszym udziałem strony publicznej i społecznej, w tym interesariuszy ze świata nauki i nauk informatycznych.
Niejasne zasady klasyfikacji systemów AI wysokiego ryzyka	Projekt nie uwzględnia wszystkich konsekwencji wynikających z powiązania zasad klasyfikacji do grupy systemów AI wysokiego ryzyka z regułami klasyfikacji wyrobów medycznych określonymi m.in. w MDR. Projekt wymaga uzupełnienia w tym zakresie. Wskazane jest również przyjęcie aktu wykonawczego przez Komisję Europejską co do statusu niektórych rodzajów oprogramowania stosowanych w ochronie zdrowia jako wyrobów medycznych lub ich wyposażenia. Wskazane jest także przyjęcie wytycznych przez Europejską Radę ds. Sztucznej Inteligencji (powoływaną przez projektowane rozporządzenie) oraz Grupę Koordynacyjną ds. Wyrobów Medycznych (powołaną na mocy MDR).

Brak systemowej spójności z MDR/IVDR	Projekt jest niespójny systemowo z MDR/IVDR m.in. w zakresie poważnych incydentów. Wskazane jest niezwłoczne opracowanie wytycznych Komisji Europejskiej w zakresie zgłaszania poważnych incydentów oraz skrócenie terminu na ich przyjęcie.
Brak systemowej spójności z RODO	Konieczne jest wprowadzenie do Projektu rozwiązań w zakresie przetwarzania danych osobowych. Bariery w korzystaniu z danych medycznych są obecnie jednymi z głównych powodów spowolnionego rozwoju systemów AI w sektorze ochrony zdrowia. Zawarte w Projekcie rozwiązania są jednak niewystarczające oraz niespójne systemowo.
Brak uregulowania zasad odpowiedzialności cywilnej	Projekt powinien zawierać regulacje w zakresie odpowiedzialności cywilnej związanej z działaniami systemów AI. Wynika to przede wszystkim z wysokiego stopnia złożoności relacji cywilnoprawnych w sektorze ochrony zdrowia, w zakresie w jakim wykorzystywane są nowoczesne narzędzia, takie jak systemy AI. Określenie zasad odpowiedzialności w ramach projektowanego rozporządzenia zapewni jednolity standard ochrony w Unii Europejskiej. Podobne rozwiązanie zastosowano np. w RODO.
Przeregulowanie (*regulatory overload*) – zbyt wiele mechanizmów regulacyjnych stosowanych jednocześnie	Liczba oraz zakres mechanizmów regulacyjnych wprowadzana przez Projekt jest nieuzasadniona. W konsekwencji liczba obowiązków prawnych i wymagań regulacyjnych jest tak duża, a koszt ich realizacji tak znaczący, że będzie prawdopodobnie wywoływał efekt odstraszający, co może skutkować przeniesieniem działalności badawczo-rozwojowej poza terytorium UE.
Wady Projektu w zakresie techniki legislacyjnej	Z uwagi na systemowy charakter Projektu oraz zakres jego obowiązywania wskazane jest doprecyzowanie wskazanych w treści niniejszego stanowiska wad Projektu.

4. UWAGI SYSTEMOWE

4.1. Brak uwzględnienia kwestii dot. systemów AI w sektorze ochrony zdrowia

4.1.1.Opis

Projekt nie zawiera w zasadzie żadnych regulacji dotyczących wykorzystania systemów AI w sektorze ochrony zdrowia, pomimo deklaracji zawartej w pierwszym motywie rozporządzenia.

Motyw 1

„Niniejsze rozporządzenie służy realizacji szeregu nadrzędnych celów interesu publicznego, takich jak wysoki poziom ochrony zdrowia."

Odniesienia do zdrowia znajdują się głównie w motywach projektowanego rozporządzenia. Należy wskazać, że motywy zawarte w preambule do aktu prawa wtórnego nie mają wartości normotwórczej, a zatem nie mają wiążącej mocy prawnej[2]. Ponadto odniesienia te odnoszą się do systemów AI rozpatrywanych bardziej w kategorii zagrożenia np. dla zdrowia i życia pacjenta, niż szansy. W samym rozporządzeniu wyraz „zdrowie" pojawia się w zasadzie wyłącznie jako jedno z kryteriów oceny negatywnego wpływu systemów AI w ramach szacowania ryzyka.

Motyw 28

„Systemy sztucznej inteligencji mogą wywoływać szkodliwe skutki dla zdrowia i bezpieczeństwa osób (…) w sektorze opieki zdrowotnej, w którym chodzi o szczególnie wysoką stawkę, jaką jest życie i zdrowie, coraz bardziej zaawansowane systemy diagnostyczne i systemy wspomagające decyzje podejmowane przez człowieka powinny być niezawodne i dokładne"."

Artykuł 14

„Nadzór ze strony człowieka ma na celu zapobieganie ryzyku dla zdrowia, bezpieczeństwa lub praw podstawowych lub minimalizowanie takiego ryzyka, które może się pojawić, gdy system sztucznej inteligencji wysokiego ryzyka jest wykorzystywany (…)."

W projektowanym załączniku III w kontekście ochrony zdrowia wymienione są jedynie systemy AI przeznaczone do wykorzystania w celu wysyłania lub ustalania priorytetów w wysyłaniu służb ratunkowych w sytuacjach kryzysowych, w tym pomocy medycznej. Z kolei w projektowanym załączniku II w wykazie unijnego prawodawstwa harmonizacyjnego opartego na nowych ramach prawnych znajdują się MDR oraz IVDR. Powyższe oznacza, że na poziomie regulacyjnym dostrzeżona została potrzeba regulacji wzajemnych zależności pomiędzy systemami AI oraz sektorem ochrony zdrowia, przy czym regulacja ta została w dużej mierze ograniczona do kwestii wyrobów medycznych (zob. uwagi dot. zasad klasyfikacji systemów AI wysokiego ryzyka w pkt 4.3 poniżej).

4.1.2.Stanowisko

Wykorzystanie systemów AI to wielka szansa i jedno z głównych wyzwań dla systemów ochrony zdrowia w państwach członkowskich.

Liczne korzyści w tym zakresie omawia raport regulacyjny *„Wykorzystanie danych medycznych w celu rozwoju wykorzystania AI w Polsce i w celu prowadzenia badań naukowych. Prawne uwarunkowania dostępu do danych medycznych i ich jakości."* opracowany przez kancelarię prawną Domański Zakrzewski Palinka sp. k. na zlecenie Koalicji AI w Zdrowiu (Warszawa 2020 r.). Zgodnie z raportem:

> *Rozwój sztucznej inteligencji i robotyki oraz coraz powszechniejsze ich zastosowanie w ochronie zdrowia może przynieść wiele korzyści. Szacuje się, że ułatwi i przyspieszy dostęp do usług ochrony zdrowia oraz pozwoli na ograniczenie ilości błędów popełnianych przez*

[2] Zob. m.in. punkt 54 wyroku Trybunału Sprawiedliwości UE z dnia 19 listopada 1998 r. (C-162/97).

personel medyczny oraz przeprowadzenie operacji i innych czynności z większą dokładnością niż człowiek[2]. Zwolennicy zastosowania sztucznej inteligencji w systemie ochrony zdrowia podnoszą, że jej stosowanie nie wiąże się z większym niebezpieczeństwem dla pacjentów. Jako argumenty podają, że „maszyny" w przeciwieństwie do człowieka nie męczą się, nie pozwalają emocjom wpłynąć na swój osąd oraz uczą się i podejmują decyzje szybciej niż człowiek.

Rozwój sztucznej inteligencji oraz potencjalne korzyści z niego płynące są szczególnie ważne ze względu na starzenie się społeczeństwa. Ponadto zauważalny jest wzrost zachorowań na choroby przewlekłe, które stanowią obecnie 70% przyczyn zgonów na świecie. Wśród tych chorób należy wymienić choroby serca i układu krążenia, nowotwory, choroby płuc oraz cukrzycę. Systemy opieki zdrowotnej muszą więc sprostać rosnącym potrzebom społeczeństwa w zakresie dostępności świadczeń zdrowotnych. Jednocześnie obserwowany jest rosnący deficyt kadr medycznych oraz coraz niższa efektywność systemu opieki zdrowotnej. Najodpowiedniejszą strategią jest więc poszukiwanie, a następnie wdrażanie nowych rozwiązań umożliwiających sprawowanie opieki zdrowotnej przy wykorzystaniu mniejszych zasobów kadrowych, np. opartych na sztucznej inteligencji czy telemedycynie. Jak wynika z przeprowadzonych analiz 54% badanych osób chciałoby zaangażowania systemów sztucznej inteligencji i robotyki w kwestiach związanych z ich zdrowiem.

Ponadto, szacuje się, że zastosowanie sztucznej inteligencji w danych dziedzinach ochrony zdrowia może przynieść wymierne zyski. Prognozuje się, że w 2026 r. Stany Zjednoczone przez wykonywanie operacji z asystą robotów osiągną zyski na poziomie ok. 40 mld dolarów, a upowszechnienie wirtualnej opieki pielęgniarskiej przyniesienie zyski w wysokości ok. 20 mld dolarów. Nieznacznie mniejsze zyski wygeneruje wykorzystanie AI do wsparcia administracyjno-organizacyjnego (ok. 18 mld dolarów), kwalifikacji uczestników na badania kliniczne (ok. 13 mld dolarów), wstępnej diagnozy (ok. 5 mld dolarów), diagnozowania w oparciu o obrazy (ok. 3 mld dolarów).

Warunkiem rozwoju systemów AI w zdrowiu jest utworzenie odpowiednich regulacji prawnych nie tylko umożliwiających, ale i stymulujących ich rozwój. W obecnym stanie prawnym do głównych barier rozwoju europejskich systemów AI w zdrowiu należą:

- **dostęp do danych medycznych i jakość danych medycznych** – w tym m.in. w zakresie przetwarzania danych osobowych (zob. uwagi dot. danych osobowych w pkt 4.5 poniżej), dostępu do danych sektora publicznego, dostępu do danych w dokumentacji medycznej, brak standardów interoperacyjności w systemach HIS;
- **brak regulacji dot. odpowiedzialności –** w tym zasad odpowiedzialności użytkownika oraz dostawcy i innych podmiotów w łańcuchu (zob. uwagi dot. odpowiedzialności cywilnej w pkt 4.6 poniżej);
- **mierzenie korzyści wynikających ze stosowania systemów AI w zdrowiu** – w tym zakresie przy wprowadzaniu do obrotu systemów AI należy również zwracać uwagę na korzyści wynikające z zastosowania niniejszego systemu, a w przypadku, gdy system generuje istotne ryzy-

ko – na korzyści z wyboru odpowiedniego stosunku korzyści do ryzyka, przy uwzględnieniu doświadczeń wynikających np. z obrotu produktami leczniczymi.

4.1.3.Propozycja rozwiązania

Koalicja oraz Grupa postulują szerokie uwzględnienie specyfiki sektora ochrony zdrowia w Projekcie. Systemy AI stosowane w ochronie zdrowia powinny zapewniać bezpieczeństwo ich użytkownikom oraz profesjonalistom medycznym, w tym bezpieczeństwo terapii. Powinny również respektować centralną rolę profesjonalisty medycznego w opiece nad pacjentem i wzbudzać jego zaufanie, a także respektować prawa pacjenta, w tym prawo do prywatności. Konieczne jest jednak również umożliwienie rozwoju europejskich systemów AI szanujących wyżej wymienione wartości. Jednocześnie obszar ochrony zdrowia z natury stanowi obszar wysokiego ryzyka. W związku z powyższym w sytuacji mierzenia jedynie ryzyka i zagrożenia bez ewentualnych korzyści nie będzie możliwe całościowe spojrzenie na wpływ Projektu na rozwój AI. Dlatego jedynie wspólne mierzenie korzyści i ryzyka (z uwzględnieniem odpowiednich proporcji oraz poszanowania fundamentalnych praw jednostki) zapewni całościowe, holistyczne spojrzenie na systemy AI, jak również odpowiednie wykorzystanie ich potencjału.

4.2. Wadliwa definicja systemu AI

4.2.1.Opis

Definicja systemu AI zastosowana w Projekcie jest bardzo szeroka. Obejmuje nie tylko oprogramowanie oparte na mechanizmach uczenia maszynowego, lecz także np. bazy wiedzy oraz metody wyszukiwania. Projektowana definicja systemu AI, poprzez uwzględnienie w niej technik i podejść określonych w załączniku I do rozporządzenia, ma być z założenia okresowo aktualizowana.

Artykuł 3 punkt 1

„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;

Załącznik I

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.

4.2.2.Stanowisko

Z perspektywy naukowej oraz technologicznej definicja systemu AI budzi liczne wątpliwości. Wątpliwości te pogłębia zawarta w Projekcie definicja systemu AI, do której mamy następujące uwagi.

Po pierwsze, definicja ta jest niespójna pod kątem logicznym. Wynika to po pierwsze z błędu definiowania nieznanego przez nieznane (*ignotum per ignotum*), do którego dochodzi w tej definicji. Przy-

kładowo, na gruncie proponowanej definicji systemem sztucznej inteligencji jest oprogramowanie opracowane przy użyciu metody opartej na logice i wiedzy, które może generować wyniki, z którymi wchodzi w interakcję. Pojęcie „*metody oparte na logice i wiedzy*" jest tak szerokie i niejednoznaczne, że może obejmować w zasadzie wszelkie możliwe kody lub języki programowania. **W konsekwencji niemal każde oprogramowanie, które wchodzi w interakcję z generowanymi przez siebie wynikami, stanowi system AI na gruncie ww. definicji**.

Po drugie, definicja pomija inne definicje prawne wypracowane na gruncie prawa UE. Przykładowo, w załączniku I jako jedna z metod opartych na logice i wiedzy jest wskazana „baza wiedzy" (*knowledge base*). Tymczasem dyrektywa 96/9/WE Parlamentu Europejskiego i Rady z dnia 11 marca 1996 r. w sprawie ochrony prawnej baz danych posługuje się pojęciem „bazy danych" (*database*), definiując je jako „*zbiór niezależnych utworów, danych lub innych materiałów uporządkowanych w sposób systematyczny lub metodyczny, indywidualnie dostępnych środkami elektronicznymi lub innymi sposobami*".

W konsekwencji w procesie wykładni projektowanego przepisu definiującego system AI mogą pojawić się m.in. wątpliwości dotyczące:

- znaczenia pojęcia „baza wiedzy" (nie jest ono zdefiniowane ani wyjaśnione),
- relacji pojęcia „baza wiedzy" względem pojęcia „baza danych".

W praktyce może to budzić istotne problemy. Przykładowo: czy program indeksujący błędy w danych treningowych i dokonujący ich korekty w celu przygotowania danych do wykorzystania na potrzeby systemów AI sam stanowi system AI? Czy każde oprogramowanie korzystające z metod statystycznych stanowi system AI? Czy wbudowanie w „zwykłe" oprogramowanie funkcji wyszukiwania zmienia jego status regulacyjny na system AI?

Po trzecie, projektowana definicja narusza zasady techniki legislacyjnej stosowane przez instytucje Unii Europejskiej. Zgodnie z wytycznymi[3]: *„Każdego terminu należy używać w znaczeniu, jakie ma on w języku ogólnym lub specjalistycznym. W dążeniu do osiągnięcia precyzji języka prawnego może jednak okazać się konieczne zdefiniowanie słów użytych w akcie. Jest to istotne, między innymi w przypadku, gdy termin posiada więcej znaczeń (…) Definicja nie może być sprzeczna z powszechnie przyjętym znaczeniem terminu."* Jak wskazano powyżej, definicja jest niezgodna z powszechnie przyjętym w środowisku naukowym i informatycznym rozumieniem terminu „system AI". Wynika to z wymienienia w załączniku I do projektowanego rozporządzenia zarówno „klasycznych" rozwiązań stosowanych w systemach AI (np. uczenie maszynowe) z rozwiązaniami stosowanymi w „zwykłym" oprogramowaniu (np. podejścia statystyczne).

Do konsekwencji wyżej opisanych wad należą między innymi:

- objęcie zakresem regulacji Projektu oprogramowania, które zgodnie ze aktualnym stanem wiedzy naukowej i technicznej nie ma charakteru systemów AI, czego efektem jest narzucenie

[3] Pkt 14.1 wytycznych „Wspólny przewodnik praktyczny Parlamentu Europejskiego, Rady i Komisji przeznaczony dla osób redagujących akty prawne Unii Europejskiej", Luksemburg, Urząd Publikacji Unii Europejskiej, 2015

wymagań regulacyjnych dla systemów AI na dostawców, operatorów, dystrybutorów i użytkowników „zwykłego" oprogramowania;

- wzrost kosztów prowadzenia działalności przez ww. podmioty;
- spowolnienie innowacyjności w sektorze ochrony zdrowia.

4.2.3.Propozycja rozwiązania

Koalicja oraz Grupa postulują ponowne przeprowadzenie prac legislacyjnych w zakresie definicji systemów AI, w miarę możliwości z jak najszerszym udziałem strony społecznej, w tym interesariuszy ze świata nauki ze szczególnym uwzględnieniem nauk informatycznych. Jest to zagadnienie o kluczowym znaczeniu dla całego Projektu.

4.3. Niejasne zasady klasyfikacji systemów AI wysokiego ryzyka

4.3.1.Opis

Projekt wprowadza pojęcie systemów AI wysokiego ryzyka. Są to systemy AI, które albo spełniają przesłanki określone w art. 6 ust. 1 Projektu albo są określone w załączniku III do projektowanego rozporządzenia.

Artykuł 6 ustęp 1

„Bez względu na to, czy system sztucznej inteligencji wprowadza się do obrotu lub oddaje do użytku niezależnie od produktów, o których mowa w lit. a) i b), taki system sztucznej inteligencji uznaje się za system wysokiego ryzyka, jeżeli spełnione są oba poniższe warunki:

a) system sztucznej inteligencji 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 sztucznej inteligencji, lub sam system sztucznej inteligencji 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."

Artykuł 6 ustęp 2

„Oprócz systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w ust. 1, za systemy wysokiego ryzyka uznaje się również systemy sztucznej inteligencji, o których mowa w załączniku III."

Co istotne, na klasyfikację nie ma wpływu to, czy system AI jest wprowadzany do obrotu (lub oddawany do użytku) odrębnie od danego produktu, czy też razem z tym produktem.

4.3.2.Stanowisko

Zgodnie z Projektem za system AI wysokiego ryzyka może być uznany system AI spełniający przesłanki, które można ująć w trzy grupy:

Grupa A	System AI jest określony w projektowanym załączniku III

Grupa B	System AI: ▪ jest przeznaczony do wykorzystania jako związany z bezpieczeństwem element produktu, którego dotyczą unijne przepisy harmonizacyjne określone w projektowanym załączniku II **oraz** ▪ podlega ocenie zgodności na podstawie przepisów UE dotyczących tego produktu.
Grupa C	System AI: ▪ jest produktem, którego dotyczą unijne przepisy harmonizacyjne określone w projektowanym załączniku II **oraz** ▪ podlega ocenie zgodności przeprowadzanej przez osobę trzecią na podstawie przepisów UE dotyczących tego produktu.

Grupa A jest określana wg kryteriów w projektowanym załączniku III, który opisuje zarówno kategorie obszarów stosowania systemów AI (np. *„sprawowanie wymiaru sprawiedliwości i procesy demokratyczne*") jak i kategorie systemów AI (np. *„systemy sztucznej inteligencji, które mają służyć organowi sądowemu pomocą w badaniu i interpretacji stanu faktycznego i przepisów prawa oraz w stosowaniu prawa do konkretnego stanu faktycznego*".)

Grupa B jest określana poprzez powiązanie zastosowania systemu AI jako element bezpieczeństwa produktu regulowanego na poziomie UE (wg wykazu przepisów z załącznika II) oraz obowiazku przeprowadzenia oceny zgodności.

Grupa C jest określana poprzez powiązanie statusu regulacyjnego systemu AI jako produktu regulowanego na poziomie UE (wg wykazu przepisów z załącznika II) oraz obowiazku przeprowadzenia oceny zgodności przez osobę trzecią.

Takie zasady klasyfikacji oznaczają, że regulacje Projektu mogą objąć w kontekście ochrony zdrowia:

- **systemy AI wskazane w projektowanym załączniku III (Grupa A)** – obecnie załącznik III zawiera tylko jedną kategorię takich systemów AI, tj. *„systemy sztucznej inteligencji przeznaczone do wykorzystania w celu wysyłania lub ustalania priorytetów w wysyłaniu służb ratunkowych w sytuacjach kryzysowych, w tym straży pożarnej i pomocy medycznej*";
- **systemy AI będące wyrobami medycznymi albo elementami bezpieczeństwa wyrobów medycznych** (Grupa B oraz C) – z uwagi na zawarcie w wykazie w projektowanym załączniku II zarówno MDR jak i IVDR.

W ocenie Koalicji oraz Grupy powiązanie systemów AI wysokiego ryzyka z wyrobami medycznymi jest, co do zasady, prawidłowym rozwiązaniem. Wymaga ono jednak dopracowania w dwóch kluczowych obszarach.

Po pierwsze, należy doprecyzować status regulacyjny wyposażenia wyrobów medycznych będącego oprogramowaniem. Definicja legalna wyposażenia wyrobu medycznego jest określona w MDR.

> **Artykuł 2 pkt 2 MDR**
>
> *„wyposażenie wyrobu medycznego" oznacza artykuł, który choć sam w sobie nie jest wyrobem medycznym, został przewidziany przez jego producenta do stosowania łącznie z co najmniej jednym określonym wyrobem medycznym specjalnie po to, by umożliwić używanie tego wyrobu medycznego zgodnie z jego przewidzianym zastosowaniem lub aby konkretnie i bezpośrednio wspomagać medyczną funkcjonalność tego wyrobu medycznego na potrzeby jego przewidzianego zastosowania;*

Definicja zakłada:

- bezpośrednią relację pomiędzy wyposażeniem i wyrobem medycznym; oraz
- wpływ na medyczną funkcjonalność wyrobu medycznego.

MDR jako rozporządzenie ustanawia Grupę Koordynacyjną ds. Wyrobów Medycznych („**MDCG**"), której zadaniem jest m.in. przyjmowanie wskazówek i wytycznych dotyczących stosowania MDR[4]. MDCG przyjęło w 2019 r. wytyczne dotyczące kwalifikacji i klasyfikacji oprogramowania[5]. W pkt 3.3 wytycznych MDCG w odniesieniu do wyposażenia wyrobów medycznych wskazało:

> *„(…) software intended to drive or influence the use of a (hardware) medical device and does not have or perform a medical purpose on its own, nor does it create information on its own for one or more of the medical purposes described in the definition of a medical device or an in vitro diagnostic medical device. This software can, but is not limited to:*
>
> *a) **operate, modify the state of, or control the device** either through an interface (e.g., software, hardware) or **via the operator of this device***
>
> *b) or supply output related to the (hardware) functioning of that device*
>
> *Note: Software that is driving or influencing the use of a medical device **is covered by the medical devices regulations** either as a part/component of a device **or as an accessory for a medical device.**"*

Taka interpretacja MDCG powoduje, że za wyposażenie wyrobu medycznego może być uznane także wyposażenie, które:

- jest w pośredniej relacji z wyrobem medycznym *(„via the operator of this device"*);
- wpływa na inne funkcjonalności wyrobu medycznego niż medyczna funkcjonalność (*„operate, modify the state of, or control the device").*

W konsekwencji w praktyce może prowadzić to do wątpliwości interpetacyjnych z uwagi na zastosowanie innych kryteriów na gruncie MDR oraz na gruncie ww. wytycznych. Przykładowo, system AI wy-

[4] Art. 103 ust. 1 w zw. z art. 105 lit. c) MDR.

[5] "Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR" (MDCG, link: https://ec.europa.eu/health/md_sector/new_regulations/guidance_en [dostęp online: 29.07.2021])

korzystywany przez szpital do analizy pracy wyrobów medycznych stosowanych w szpitalu, który nie wpływa bezpośrednio na ich działanie, ale pozwala ustalić, czy pracują one prawidłowo i podejmować odpowiednie i terminowe działania konserwacyjne:

- **nie jest wyposażeniem wyrobu medycznego i nie podlega regulacjom Projektu** – przy zastosowaniu kryteriów określonych w MDR;
- **jest wyposażeniem wyrobu medycznego i podlega regulacjom Projektu** – przy zastosowaniu kryteriów określonych w wytycznych MDCG.

Tak znaczne rozbieżności interpretacyjne nie powinny mieć miejsca, w szczególności z uwagi na niejako automatyczną klasyfikację wyrobów medycznych bedących oprogramowaniem do kategorii systemów AI wysokiego ryzyka (zob. uwagi poniżej). Dodatkowe wątpliwości w tym zakresie budzi motyw 19 MDR, który odróżnia oprogramowanie przewidziane do zastosowań medycznych od oprogramowania do zastosowań ogólnych.

Motyw 19 MDR

Należy doprecyzować, że oprogramowanie odrębne, w przypadku gdy zostało specjalnie przewidziane przez producenta do co najmniej jednego z zastosowań medycznych wyszczególnionych w definicji wyrobu medycznego, kwalifikuje się jako wyrób medyczny, natomiast oprogramowanie do zastosowań ogólnych, nawet jeżeli jest używane w ochronie zdrowia, lub oprogramowanie do zastosowań związanych ze stylem życia i samopoczuciem nie jest wyrobem medycznym. Kwalifikacja oprogramowania - jako wyrobu albo jako wyposażenia - jest niezależna od lokalizacji tego oprogramowania i od typu połączenia między oprogramowaniem a wyrobem.

Po drugie, należy wziąć pod uwagę kryteria klasyfikacji wyrobów medycznych bedących oprogramowaniem do klas wyrobów określonych w MDR w kontekście zasad klasyfikacji do grupy systemów AI wysokiego ryzyka. Reguły klasyfikacji są określone w załączniku VIII do MDR. Wyroby medyczne zaklasyfikowane wg tych reguł do klasy IIa, IIb lub klasy III podlegają ocenie zgodności przeprowadzanej przez osobę trzecią (tj. jednostkę notyfikowaną) w celu wprowadzenia do obrotu. Oznacza to, że z perspektywy Projektu o klasyfikacji do grupy systemów AI wysokiego ryzyka decydują reguły klasyfikacji określone w MDR. Zgodnie z tymi regułami niemal wszystkie wyroby medyczne będące oprogramowaniem są klasyfikowane w klasie IIa, IIb lub klasie III. **W konsekwencji w zasadzie każdy taki wyrób medyczny – o ile może być uznany za system AI, co jest możliwe z uwagi na wadliwą definicję systemu AI (zob. uwagi w pkt 4.2) może być zaklasyfikowany jako system AI wysokiego ryzyka.**

4.3.3.Propozycja rozwiązania

Komisja Europejska dostrzegła potrzebę uwzględnienia specyfiki sektora ochrony zdrowia w ramach regulacji dotyczących systemów AI, co zostało wyraźnie wskazane w dokumencie „Biała księga ws. sztucznej inteligencji - europejskie podejście do doskonałości i zaufania”[6]:

[6] “Biała Księga w sprawie sztucznej inteligencji Europejskie podejście do doskonałości i zaufania” COM/2020/65 final/2, link: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020DC0065 [dostęp online: 29.07.2021r.]

„Komisja bada obecnie te wyzwania związane z bezpieczeństwem i odpowiedzialnością, które są specyficzne dla opieki zdrowotnej (…) nie każde użycie sztucznej inteligencji w wybranych sektorach musi wiązać się ze znaczącym ryzykiem. Na przykład, chociaż sektor opieki zdrowotnej na ogół może być potencjalnie źródłem wysokiego ryzyka, błąd w systemie umawiania wizyt w szpitalu zazwyczaj nie stwarza ryzyka o znaczeniu uzasadniającym interwencję legislacyjną".

Koalicja oraz Grupa popierają przytoczone powyżej stanowisko Komisji Europejskiej. Dla zagwarantowania rozwoju systemów AI w zdrowiu konieczne jest jasne określenie kryteriów klasyfikacji takich systemów do grupy wysokiego ryzyka. Konieczne jest także dostrzeżenie specyfiki związanej z wyrobami medycznymi, w tym kryteriów ich klasyfikacji.

W związku z tym w ocenie Koalicji oraz Grupy należy:

- **przeanalizować w pełni wszystkie konsekwencje regulacyjne powiązania Projektu z MDR** – w tym wynikające z powiązania zasad klasyfikacji do grupy systemów AI wysokiego ryzyka z regułami klasyfikacji wyrobów medycznych określonymi m.in. w MDR;
- **rozważyć określenie przez Komisję Europejską w trybie art. 4 ust. 2 MDR w ramach aktu wykonawczego, czy dany produkt lub dana kategoria lub grupa produktów będących oprogramowaniem wchodzą w zakres definicji "wyrobu medycznego" lub "wyposażenia wyrobu medycznego"** – z uwzględnieniem specyfiki oprogramowania wykorzystywanego w sektorze ochrony zdrowia wyrażonej m.in. w motywie 19 MDR;
- **dokonać aktualizacji wytycznych MDCG dot. wyrobów medycznych będących oprogramowaniem z uwzględnieniem zagadnień związanych z systemami AI określonych w Projekcie oraz przy zapewnieniu konsultacji społecznych** – w tym wytycznych:
    - "Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR" (MDCG 2019-11) oraz
    - „Guidance on Cybersecurity for medical devices" (MDCG 2019-16);
- **rozpocząć niezwłocznie prace nad wytycznymi dotyczącymi systemów AI będących wyrobami medycznymi oraz przy zapewnieniu konsultacji społecznych** – na przykład poprzez ich przyjęcie przez Europejską Radę ds. Sztucznej Inteligencji powoływaną przez Projekt w trybie art. 56 ust. 1 w zw. z art. 58 lit. c) projektowanego rozporządzenia.

4.4. Brak systemowej spójności z MDR/IVDR

4.4.1. Opis

Wadliwa definicja systemu AI w połączeniu z brakiem definicji legalnej oprogramowania na gruncie MDR może prowadzić do istotnych problemów interpretacyjnych.

Artykuł 2 pkt 23 MDR

"wyrób medyczny" oznacza narzędzie, aparat, urządzenie, oprogramowanie, implant, odczynnik, materiał lub inny artykuł przewidziany przez producenta do stosowania - pojedynczo lub łącznie - u ludzi do co najmniej jednego z następujących szczególnych zastosowań medycznych:

- *diagnozowanie, profilaktyka, monitorowanie, przewidywanie, prognozowanie, leczenie lub łagodzenie choroby,*
- *diagnozowanie, monitorowanie, leczenie, łagodzenie lub kompensowanie urazu lub niepełnosprawności,*
- *badanie, zastępowanie lub modyfikowanie budowy anatomicznej lub procesu lub stanu fizjologicznego lub chorobowego,*
- *dostarczanie informacji poprzez badanie in vitro próbek pobranych z organizmu ludzkiego, w tym pobranych od dawców narządów, krwi i tkanek,*

i który nie osiąga swojego zasadniczego przewidzianego działania środkami farmakologicznymi, immunologicznymi lub metabolicznymi w ludzkim ciele lub na nim, ale którego działanie może być wspomagane takimi środkami.

Projekt definiuje pojęcie „*poważnego incydentu*" odmiennie niż MDR.

Artykuł 2 pkt 65 MDR

„poważny incydent" oznacza incydent, który bezpośrednio lub pośrednio doprowadził, mógł doprowadzić lub może doprowadzić do któregokolwiek z niżej wymienionych zdarzeń:

a) zgon pacjenta, użytkownika lub innej osoby;

b) czasowe lub trwałe poważne pogorszenie stanu zdrowia pacjenta, użytkownika lub innej osoby;

c) poważne zagrożenie zdrowia publicznego;

Artykuł 3 pkt 44 Projektu

„poważny incydent" oznacza każdy incydent, który bezpośrednio lub pośrednio prowadzi, mógł prowadzić lub może prowadzić do któregokolwiek z poniższych zdarzeń:

a) śmierci osoby lub poważnego uszczerbku na zdrowiu osoby, uszkodzenia mienia lub szkody dla środowiska,

b) poważnego i nieodwracalnego zakłócenia w zarządzaniu infrastrukturą krytyczną i jej funkcjonowaniu.

Ponadto Projekt nie zawiera definicji ryzyka, podczas gdy MDR zawiera taką definicję legalną.

Artykuł 2 pkt 23 MDR

„ryzyko" oznacza połączenie prawdopodobieństwa wystąpienia szkody oraz jej stopnia ciężkości

4.4.2.Stanowisko

Z uwagi na wady definicji systemu AI (zob. uwagi w pkt 4.2) istnieje ryzyko powstania znacznych wątpliwości co do statusu regulacyjnego wyrobów medycznych będących oprogramowaniem. Jeśli – z uwagi na wadliwą definicję – w zasadzie każde oprogramowanie może być uznane za system AI, to oznacza to, że każdy wyrób medyczny będący oprogramowaniem byłby systemem AI. Co więcej, z uwagi na zasady klasyfikacji (zob. uwagi w pkt 4.3), każdy taki wyrób medyczny byłby systemem AI

wysokiego ryzyka. **W konsekwencji wadliwej definicji istnieje zatem możliwość uznania każdego wyrobu medycznego będącego oprogramowaniem za system AI wysokiego ryzyka ze wszystkimi związanymi z tym konsekwencjami regulacyjnymi (m.in. dla producentów**).

Niezgodność pomiędzy definicjami „poważnego incydentu" w praktyce może prowadzić do wątpliwości dotyczących zakresu raportowania incydentów. Wątpliwości może pogłębiać fakt, że w stosunku do systemów AI z Grupy B oraz C organem nadzorczym będzie organ odpowiedzialny za podejmowanie działań w zakresie nadzoru rynku wyznaczony na podstawie aktów prawnych wskazanych w załączniku II, tj. MDR/IVDR (art. 63 ust. 3 Projektu). Oznacza to, że ten sam organ będzie musiał rozpatrywać zgłoszenia poważnych incydentów w rozumieniu MDR oraz w rozumieniu Projektu. Na poziomie zgłaszających (producentów) problematyczne może być dostosowanie systemów rejestrowania i zgłaszania incydentów i zewnętrznych działań korygujących dotyczących bezpieczeństwa wymaganych na mocy MDR. Systemy takie musiałyby obejmować także incydenty związane z uszkodzeniem mienia, szkody dla środowiska oraz zakłócenia w zarządzeniu infrastrukturą krytyczną, które nie wchodzą w zakres pojęcia poważnego incydentu na gruncie MDR.

Ponadto Projekt w obecnej wersji nie zawiera definicji legalnej pojęcia „ryzyko". W razie wprowadzenia definicji legalnej tego pojęcia należy zadbać o jego zgodność z definicją zastosowaną w MDR. W odmiennym przypadku producenci wyrobów medycznych – systemów AI wysokiego ryzyka musieliby wprowadzić dwa równoległe systemy zarządzania ryzykiem, co byłoby nieuzasadnione.

4.4.3.Propozycja rozwiązania

W ocenie Koalicji oraz Grupy:

- **należy zapewnić szerokie konsultacje ze stroną publiczną oraz podmiotami gospodarczymi podczas opracowywania wytycznych Komisji w zakresie zgłaszania poważnych incydentów, o których mowa w art. 62 ust. 2 Projektu**;
- **należy rozważyć skrócenie terminu na wydanie ww. wytycznych** – obecnie zaproponowany w art. 62 ust. 2 Projektu termin 12 miesięcy od dnia wejścia projektowanego rozporządzenia w życie jest zbyt długi i nie zapewni należytego wsparcia dla producentów oraz organów nadzorczych, co może wpłynąć na obniżenie poziomu bezpieczeństwa w związku ze stosowaniem systemów AI.

4.5. Brak systemowej spójności z RODO

4.5.1.Opis

Projekt reguluje pewne aspekty dotyczące systemów AI związane z przetwarzaniem danych osobowych. Należą do nich m.in.:

- **wprowadzenie ustawowej podstawy przetwarzania danych osobowych szczególnej kategorii, do których należą m.in. dane o stanie zdrowia** (art. 10 ust. 5 Projektu) – przy czym jest to ograniczone wyłącznie do sytuacji, gdy jest to *„ściśle niezbędne do celów zapewnienia monitorowania, wykrywania i korygowania tendencyjności"* systemów AI wysokiego ryzyka;
- **wprowadzenie ustawowej podstawy dalszego przetwarzania danych osobowych** (art. 54 Projektu) – przy czym jest to ograniczone do opracowywania określonych systemów AI w in-

teresie publicznym w *regulatory sandbox* (zob. uwagi w pkt 5.11) oraz poddane bardzo licznym ograniczeniom.

Należy na marginesie zaznaczyć niezgodność ww. projektowanych przepisów z motywem 41 Projektu, który jasno wskazuje, że jego przepisy nie ustanawiają samoistnej podstawy prawnej przetwarzania danych osobowych.

Motyw 41

„Niniejszego rozporządzenia nie należy rozumieć jako ustanawiającego podstawę prawną przetwarzania danych osobowych, w tym w stosownych przypadkach szczególnych kategorii danych osobowych."

4.5.2.Stanowisko

Koalicja popiera kierunkowo wprowadzenie do Projektu rozwiązań w zakresie przetwarzania danych osobowych. Bariery w korzystaniu z danych medycznych są obecnie jednymi z głównych powodów spowolnionego rozwoju systemów AI w sektorze ochrony zdrowia. Zawarte w Projekcie rozwiązania są jednak niewystarczające oraz niespójne systemowo.

W zakresie wprowadzenia podstawy prawnej przetwarzania danych osobowych (art. 10 ust. 5 Projektu) widoczna jest niekonsekwencja. Z jednej strony dostawca systemu AI może przetwarzać dane osobowe (nawet tzw. dane wrażliwe), lecz jedynie na potrzeby monitorowania i korygowania tendencyjności systemów AI (np. nadwrażliwość, jeśli chodzi o prognozowanie zachowań przestępczych osób o określonym kolorze skóry).

Z drugiej strony ten sam dostawca na etapie pozyskiwania danych niezbędnych do stworzenia sytemu AI staje przed obecnymi dziś problemami (np. w niektórych sytuacjach konieczność stosowania jako podstawy przetwarzania zgody pacjenta w trybie art. 9 ust. 2 lit. a) RODO, problemy praktyczne związane z pseudonimizacją oraz anonimizacją danych). W tym zakresie Projekt nie zawiera rozwiązań, które adresowałyby ww. problemy.

Należy wskazać, że art. 10 ust. 5 Projektu określa w obecnym brzmieniu niejako dodatkową podstawę prawną legalizującą przetwarzanie szczególnych kategorii danych osobowych względem art. 9 ust. 1 i 2 RODO. Wydaje się zatem zasadne, aby w treści art. 10 ust. 5 doprecyzować, że niezbędność do celów zapewnienia monitorowania, wykrywania i korygowania tendencyjności systemów AI wysokiego ryzyka mieści się w zakresie jednego z warunków określonych w art. 9 ust. 2 RODO.

Ponadto wydaje się, że pojęcia „pseudonimizacji" oraz „anonimizacji" użyte zostały w treści art. 10 ust. 5 jako tożsame, podczas gdy pseudonimizacja jest procesem odwracalnym, który jest przeprowadzany w celu ograniczenia możliwości identyfikacji osoby fizycznej, podczas gdy anonimizacja jest procesem nieodwracalnym, gdyż polega na przekształceniu danych osobowych w sposób uniemożliwiający przyporządkowanie poszczególnych informacji do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

W zakresie dalszego przetwarzania w ramach *regulatory sandbox* Projekt wprowadza liczne ograniczenia, które w praktyce prawdopodobnie spowodują, że projektowane rozwiązanie – choć kierunkowo zasadne – pozostanie rzadko stosowane. Koalicja popiera wprowadzenie celu przetwarzania w postaci ochrony ważnego interesu publicznego w obszarze „bezpieczeństwo publiczne i zdrowie pu-

bliczne, uwzględniając zapobieganie chorobom, zwalczanie ich i ich leczenie" jako jednej z przesłanek dalszego przetwarzania. W ocenie Koalicji wprowadzone restrykcje są zbyt daleko idące. Należą do nich bowiem między innymi następujące wymagania względem przetwarzanych danych osobowych:

- dane osobowe znajdują się w funkcjonalnie wyodrębnionym, odizolowanym i chronionym środowisku przetwarzania danych podlegającym kontroli uczestników korzystających z *regulatory sandbox*, a dostęp do tych danych posiadają wyłącznie upoważnione osoby;
- dane osobowe nie mogą być przenoszone, przekazywane ani w żaden inny sposób udostępniane osobom trzecim;
- dane osobowe usuwa się po zakończeniu uczestnictwa w *regulatory sandbox* lub po upływie okresu przechowywania danych osobowych.

Ponadto Koalicja podziela stanowisko wyrażone we wspólnej opinii Europejskiej Rady Ochrony Danych oraz Europejskiego Inspektora Ochrony Danych z 18 czerwca 2021 r.[7] w zakresie:

- zasadności przyjęcia podejścia opartego na ocenie ryzyka;
- konieczności doprecyzowania zasad przeprowadzania takiej oceny ryzyka.

Jak słusznie wskazują EROD i EIOD we wspólnym stanowisku, w projektowanym stanie prawnym istnieje ryzyko powstania istotnych rozbieżności w tym zakresie z uwagi na osobne wymagania co do oceny ryzyka pod kątem regulacji dla systemów AI oraz pod kątem wymagań RODO:

> *„20. The Proposal requires the providers of the AI system to perform a risk assessment, however, in most cases, the (data) controllers will be the users rather than providers of the AI systems (e.g., a user of a facial recognition system is a 'controller' and therefore, is not bound by requirements on high-risk AI providers under the Proposal).*
>
> *21. Moreover, it will not always be possible for a provider to assess all uses for the AI system. Thus, the initial risk assessment will be of a more general nature than the one performed by the user of the AI system. Even if the initial risk assessment by the provider does not indicate that the AI system is "high-risk"" under the Proposal, this should not exclude a subsequent (more granular) assessment (data protection impact assessment ('DPIA') under Article 35 of the GDPR, Article 39 of EUDPR or under Article 27 of the LED) that should be made by the user of the system, considering the context of use and the specific use cases."*

W praktyce może mieć to istotne znaczenie przy wprowadzaniu systemów AI w systemie ochrony zdrowia. Przykładowo, może dojść do wątpliwości interpretacyjnych, czy dostawca oprogramowania czy szpital jest odpowiedzialny za wypełnienie obowiązków regulacyjnych związanych z oceną ryzyka.

Należy także podkreślić, że konieczne jest wyjaśnienie na poziomie Projektu, czy każdy system AI wysokiego ryzyka wykorzystujący dane osobowe należy traktować na gruncie RODO jako przetwarzanie danych osobowych powodujące wysokie ryzyko naruszenia praw lub wolności osób fizycznych w rozumieniu art. 35 RODO.

[7] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence(Artificial Intelligence Act)

4.5.3.Propozycja rozwiązania

Projekt powinien w zakresie danych osobowych:

- regulować kwestie pozyskiwania, przetwarzania oraz usuwania danych medycznych;
- określić jakie czynności przetwarzania danych osobowych (w tym danych o stanie zdrowia) w celach badawczych i rozwojowych związanych z systemami AI (np. trenowanie systemu AI) mogą być realizowane, na przykład:
    - na podstawie art. 6 ust. 4 RODO – na zasadzie dalszego przetwarzania danych,
    - na podstawie art. 9 ust. 2 lit. i) RODO – poprzez określenie w Projekcie, że takie przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego (rozwój systemów AI spełniających wysokie standardy jakości i bezpieczeństwa do wykorzystania w sektorze ochrony zdrowia),
    - na podstawie art. 9 ust. 2 lit. j) RODO – poprzez określenie w Projekcie, że takie przetwarzanie stanowi przetwarzanie niezbędne do celów badań naukowych;
- złagodzić wymagania dotyczące dalszego przetwarzania danych osobowych w ramach *regulatory sandbox*.

4.6. Brak regulacji zasad odpowiedzialności cywilnej

4.6.1.Opis

W Projekcie przewidziano liczne obowiązki prawne (np. możliwość kontroli przez organy nadzoru w zakresie procedury oceny zgodności[8] czy kontroli systemów AI na rynku UE[9]) obłożone sankcjami administracyjnymi (m.in. administracyjne kary pieniężne przewidziane w razie niezgodności systemu AI z jakimikolwiek wymogami lub obowiązkami wynikającymi z Projektu[10]).

Projekt, poza zasygnalizowaniem tego zagadnienia w motywach (stanowiących część nienormatywną), nie zawiera natomiast regulacji dotyczących odpowiedzialności cywilnej. W efekcie Projekt w zasadzie pozbawiony jest regulacji w tym zakresie.

Motyw 53

„Należy zapewnić, aby odpowiedzialność za wprowadzenie do obrotu lub oddanie do użytku systemu sztucznej inteligencji wysokiego ryzyka brała na siebie konkretna osoba fizyczna lub prawna określona jako dostawca, niezależnie od tego, czy ta osoba fizyczna lub prawna jest osobą, która zaprojektowała lub opracowała ten system."

4.6.2.Stanowisko

[8] Art. 47 Projektu.

[9] Art. 63 Projektu.

[10] Art. 71 ust.4 Projektu.

Projekt powinien zawierać regulacje w zakresie odpowiedzialności cywilnej związanej z działaniem systemów AI. Wynika to przede wszystkim z wysokiego stopnia złożoności relacji cywilnoprawnych w sektorze ochrony zdrowia, w zakresie w jakim wykorzystywane są nowoczesne narzędzia takie jak systemy AI.

Przykład

Podmiot leczniczy udziela świadczeń zdrowotnych przy wykorzystaniu systemu AI będącego wyrobem medycznym służącym do diagnozy w ściśle określonych przez producenta zastosowaniach. System AI wykona „swoją" usługę udzielenia świadczenia zdrowotnego w postaci postawienia diagnozy. Sposób działania systemu AI ma wyższą skuteczność niż wcześniejsze dotychczasowe działania lekarzy, co zostało poprzedzone badaniami. Jednakże, w tym konkretnym przypadku diagnoza została postanowiona w sposób nieprawidłowy, a pacjent poniósł szkodę.

Konieczna jest regulacja pozwalająca określić, czy odpowiedzialność ponosi producent systemu AI czy świadczeniodawca czy też jeszcze inny podmiot. Ponadto konieczne jest rozstrzygnięcie, czy pacjentowi przysługuje rekompensata, a jeśli tak, to jaka jest podstawa prawna, w oparciu o którą możliwe jest dochodzenie odszkodowania. Konieczne jest określenie czy powinno odbywać się to na podstawie stosunku kontraktowego łączącego pacjenta z lekarzem, który użył takiego oprogramowania, czy wobec lekarza, ale na zasadzie reżimu odpowiedzialności *ex delicto* – na zasadzie winy. Niejasne jest także, czy takie oprogramowanie będzie produktem niebezpiecznym oraz czy możliwe jest dochodzenie odpowiedzialności producenta na zasadzie ryzyka (niejako licząc, że producentowi nie uda się wykazać jednej z okoliczności egzoneracyjnych).

Uregulowanie zasad odpowiedzialności cywilnej w Projekcie jest niezbędne – projektowane rozporządzenie ma wprowadzić jednolite rozwiązania prawne oraz jednolity standard ochrony w całej Unii Europejskiej. Nie jest w związku z tym wskazane pozostawienie tej kwestii całkowicie w gestii państw członkowskich. Nie byłoby to również rozwiązanie nowe – w wielu regulacjach prawa unijnego (np. RODO) określono zasady odpowiedzialności cywilnej by zapobiec powstaniu rozbieżności i ułatwić przepływ produktów i usług na rynku wewnątrzwspólnotowym.

4.6.3.Propozycja rozwiązania

Należy wprowadzić jasne reguły dochodzenia indemnifikacji za szkody powstałe w związku z działaniem systemu AI. Na potrzeby opracowania takiej regulacji można wykorzystać istniejące już rozwiązania, np. określone w art. 82 RODO. Przywołany przepis RODO wprowadza jasne i czytelne zasady odpowiedzialności zgodnie z którymi m.in.:

- każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia RODO, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę;
- odpowiedzialność jest oparta na zasadzie winy (art. 82 ust. 3 RODO);
- określono przesłanki ekskulpacyjne (art. 82 ust. 2 RODO);
- uregulowano kwestię roszczeń regresowych (art. 82 ust. 5 RODO);

- wprowadzono mechanizm odpowiedzialności solidarnej w niektórych przypadkach (art. 82 ust. 4 RODO).

W ocenie Koalicji oraz Grupy wskazane jest określenie podobnie jasnych i czytelnych reguł dotyczących odpowiedzialności cywilnej dla systemów AI z uwzględnieniem następujących okoliczności:

- zasada odpowiedzialności (tj. odpowiedzialność na zasadzie winy, na zasadzie ryzyka, odpowiedzialność absolutna);
- przesłanki zwalniające z odpowiedzialności (np. egzoneracyjne, ekskulpacyjne);
- reguły dot. roszczeń regresowych;
- reguły dot. odpowiedzialności solidarnej;
- regulacje szczegółowe dla niektórych rodzajów systemów AI w sektorze ochrony zdrowia (np. w związku z wyrobami medycznymi).

Takie zasady odpowiedzialności cywilnej mogą być następnie rozbudowane np. o fundusz kompensacyjny, obowiązkowe ubezpieczenie od odpowiedzialności cywilnej i inne rozwiązania, które będą z jednej strony zabezpieczały osoby narażone na szkody związane z systemami AI, a z drugiej strony zapewnią bezpieczeństwo prawne uczestnikom łańcucha dystrybucyjnego od producenta do użytkownika.

4.7. Przeregulowanie (*regulatory overload*) – zbyt wiele mechanizmów regulacyjnych stosowanych jednocześnie

4.7.1.Opis

Projekt wprowadza wiele mechanizmów regulacyjnych mających gwarantować bezpieczeństwo systemów AI. Należą do nich:

MECHANIZM REGULACYJNY	ZAKRES	JEDN. RED. PROJEKTU
Wewnętrzny system compliance (procedury, system jakości, prowadzenie dokumentacji technicznej)	system AI wysokiego ryzyka	Artykuł 17
System zarządzania ryzykiem	system AI wysokiego ryzyka	Artykuł 9
Regulacja obowiązków prawnych każdego uczestnika łańcucha (dostawca, importer, dystrybutor, użytkownik itd.)	system AI wysokiego ryzyka	Artykuł 24-29
Obowiązek uzyskania wpisu w centralnym rejestrze	system AI wysokiego ryzyka	Artykuł 51 Artykuł 60
System oceny zgodności z udziałem jednostek notyfikowanych oraz znaki CE	system AI wysokiego ryzyka	Artykuł 19 Artykuł 43

System nadzoru produktowego po wprowadzeniu oraz obowiązek zgłaszania incydentów	system AI wysokiego ryzyka	Artykuł 61 Artykuł 62
Wymagania techniczne, konstrukcyjne i technologiczne (np. zapewnienie nadzoru człowieka, wymagania jakościowe dla danych treningowych, dokumentacja techniczna)	system AI wysokiego ryzyka	Artykuł 10 Artykuł 11 Artykuł 14
Powiązanie odpowiedzialności ze znakiem towarowym pod którym produkt występuje na rynku	system AI wysokiego ryzyka	Artykuł 28
Możliwość wycofania produktu z rynku przez organ nadzorczy oraz unijna procedura ochronna	system AI	Artykuł 65
Administracyjne kary pieniężne	system AI	Artykuł 71
Obowiązek zapewnienia przejrzystości	system AI	Artykuł 52
Utworzenie organów nadzorczych z kompetencjami kontrolnymi	system AI	Artykuł 63

4.7.2.Stanowisko

Liczba oraz zakres mechanizmów regulacyjnych wprowadzaną przez Projekt są nieuzasadnione, w szczególności z uwagi na:

- niejasne zasady klasyfikacji systemów AI wysokiego ryzyka;
- niejasne zasady zarządzania ryzykiem korzystania z systemów AI wysokiego ryzyka;
- brak dostatecznego zróżnicowania obowiązków regulacyjnych względem wielkości organizacji.

Projekt odnosi się do wielkości podmiotów gospodarczych w kilku przypadkach, przewidując w tym zakresie:

- możliwość proporcjonalnego do wielkości organizacji dostawcy wdrożenia systemu zarządzania jakością (art. 17 ust. 2 Projektu) – bez wskazania jednak, na czym ma ona polegać (m.in. jak określić wielkość organizacji), a także co ulega proporcjonalnemu zwiększeniu lub zmniejszeniu (np. czy nawet jednoosobowy startup musi wdrażać wszystkie elementy systemu zarządzania jakością, jedynie w ograniczonym zakresie, czy też może niektórych z nich nie wdrażać);
- obniżenie opłaty z tytułu oceny zgodności przeprowadzanej proporcjonalnie do wielkości dostawców i do wielkości rynku (art. 55 ust. 2 Projektu) – bez wskazania jednak sposobu określenia wielkości lub rynku, a także relacji pomiędzy opłatą a tak obliczoną wielkością (np. czy firma o obrocie rocznym 1 mln EUR ma płacić 1/100 opłaty uiszczanej przez firmę o obrocie rocznym 100 mln EUR?).

Pośrednio Projekt przewiduje złagodzenie wymagań dla małych i średnich przedsiębiorców poprzez:

- ustanowienie i udokumentowanie systemu monitorowania po wprowadzeniu do obrotu w sposób proporcjonalny do charakteru systemu AI i ryzyka związanego ze stosowaniem danego systemu AI wysokiego ryzyka (art. 61 ust. 1 Projektu) – przy czym brak określenia tej proporcji w zestawieniu z wysokimi sankcjami administracyjnymi w praktyce prawdopodobnie spowoduje, że regulacja ta będzie dla adresatów obojętna.

W konsekwencji liczba obowiązków prawnych i wymagań regulacyjnych jest tak duża, że będzie prawdopodobnie wywoływała efekt odstraszający. **Koszty związane z zapewnieniem zgodności z wymaganiami Projektu w zakresie systemów AI wysokiego ryzyka dla podmiotów SME jest szacowany na ok. € 400.000 (ok. 1.834.000 PLN)[11].** W efekcie podmioty gospodarcze mogą zdecydować o przeniesieniu działalności badawczo-rozwojowej poza terytorium UE. Ponadto tak duże obciążenie regulacyjne stanowi barierę dla powstawania nowych startupów – obecne w Projekcie złagodzenia ww. wymagań są niewystarczające.

4.7.3.Propozycja rozwiązania

Koalicja rekomenduje następujące działania:

- rozważenie, czy nagromadzenie mechanizmów regulacyjnych w Projekcie spełnia swoją rolę (tj. zapewnienie bezpieczeństwa i jakości systemów AI, a nie tworzenie granic dla ich rozwoju),
- rezygnacja z części wprowadzanych wymagań lub ich złagodzenie,
- wprowadzenie na szerszą skalę rozwiązań instytucjonalnych mających wspierać mikro- , małych oraz średnich przedsiębiorców.

4.8. Wady Projektu w zakresie techniki legislacyjnej

4.8.1.Opis

Projekt jest obarczony wadami wynikającymi z braku przestrzegania zasad prawidłowej legislacji. Należą do nich m.in.:

RODZAJ WADY	PRZYKŁAD / KOMENTARZ
Brak definicji legalnych	Projekt nie zawiera definicji legalnej pojęcia „ryzyko", co może mieć istotne znaczenie w przypadku systemów AI klasyfikowanych jako systemy AI wysokiego ryzyka w ramach Grupy B lub C – m.in. wyrobów medycznych. Z uwagi na znaczenie tego pojęcia dla całego Projektu (np. w zakresie obowiązku stworzenia systemu zarządzania ryzykiem) wskazane jest jego zdefiniowanie.

[11] Raport „How Much Will the Artificial Intelligence Act Cost Europe?", Center for Data Innovation, link: https://datainnovation.org/2021/07/how-much-will-the-artificial-intelligence-act-cost-europe/ [dostęp online 29.07.2021]

Pojęcia nieostre	*Systemy sztucznej inteligencji wysokiego ryzyka muszą być odporne na błędy, usterki lub niespójności, które mogą wystąpić w systemie lub w środowisku, w którym działa system, w szczególności w wyniku interakcji z osobami fizycznymi lub innymi systemami. (art. 15 ust. 3)*
	Wdrożenie aspektów, o których mowa w ust. 1, jest proporcjonalne do wielkości organizacji dostawcy. (art. 17 ust. 2)
	Systemy sztucznej inteligencji wysokiego ryzyka projektuje się i opracowuje się w taki sposób, w tym poprzez uwzględnienie odpowiednich narzędzi interfejsu człowiek-maszyna, aby w okresie wykorzystywania systemu sztucznej inteligencji wysokiego ryzyka mogły je skutecznie nadzorować osoby fizyczne. (art. 14 ust. 1)
Odesłania pozasystemowe do praktyk rynkowych (bez ich doprecyzowania)	*Zbiory danych treningowych, walidacyjnych i testowych podlegają odpowiednim praktykom w zakresie zarządzania danymi. (art. 10 ust. 2)*
Obowiązki prawne co do zapewnienia danego standardu bez jego określenia	*Zbiory danych treningowych, walidacyjnych i testowych muszą być adekwatne, reprezentatywne, wolne od błędów i kompletne. (art. 10 ust. 3)*
	Systemy sztucznej inteligencji wysokiego ryzyka projektuje się i opracowuje się w sposób zapewniający wystarczającą przejrzystość ich działania, umożliwiającą użytkownikom interpretację wyników działania systemu i ich właściwe wykorzystanie. (art. 13 ust. 1)
Zbyt krótki okres vacatio legis	*Art. 85 Projektu przewiduje, że (co do zasady) projektowane rozporządzenie wejdzie w życie dwudziestego dnia po jego opublikowaniu w Dzienniku Urzędowym Unii Europejskiej, natomiast stosowane będzie od dnia przypadającego 24 miesiące od dnia wejścia w życie. Tak krótki okres vacatio legis dla regulacji równie kompleksowej co Projekt jest sprzeczny z zasadami prawidłowej legislacji.*

4.8.2.Stanowisko

Z uwagi na systemowy charakter Projektu oraz zakres jego obowiązywania wskazane jest skorygowanie ww. wad Projektu. W praktyce szczególnie istotne znacznie będzie mieć prawdopodobnie doprecyzowanie treści obowiązków prawnych adresatów norm. Przykładowo, Projekt wprowadza obowiązek zapewnienia aby zbiory danych treningowych, walidacyjnych i testowych były adekwatne, reprezentatywne, wolne od błędów i kompletne. Wykładnia tego przepisu napotyka następujące problemy interpretacyjne:

- Projekt definiuje m.in. „dane treningowe", nie definiuje jednak pojęcia „zbiór danych treningowych" – nie jest jasne, co dokładnie ma być wolne od błędów (tj. dane czy metadane na poziomie zbioru);

- Projekt nie definiuje terminów takich jak „wolne od błędów”, co może w praktyce budzić rozbieżności interpretacyjne; przykładowo, pojęcie „wolne od błędów” może oznaczać brak jakichkolwiek błędów, brak istotnych błędów albo bycie wolnym od błędów na poziomie 99,999% zgodnie ze standardem rynkowym.

Ponadto wskazać należy, że Projekt stanowi pierwszą regulację prawną dziedziny społecznej, ekonomicznej i technologicznej obejmującej systemy AI. Aby zapewnić jego przestrzeganie należy zapewnić adresatom regulacji odpowiedni czas na dostosowanie się do jego wymagań. Należy zaznaczyć, że czas ten jest szczególnie istotny dla podmiotów już stosujących lub produkujących systemy AI z uwagi na zmiany jakich doświadczą już w trakcie prowadzenia działalności.

Uzasadnione jest wydłużenie vacatio legis dla stosowania całego projektowanego rozporządzenia – z 24 miesięcy do co najmniej 36 miesięcy od dnia wejścia w życie; przy czym:

- odnośnie tytułu III rozdział 4 (dot. organów notyfikujących i jednostek notyfikowanych) oraz tytułu VI (dot. zarządzania) – z 12 miesięcy od daty wejścia w życie do co najmniej 24 miesięcy od dnia wejścia w życie,
- odnośnie art. 71 (dot. administracyjnych kar pieniężnych) – z 12 miesięcy od daty wejścia w życie do daty wejścia w życie całego projektowanego rozporządzenia (tj. w omawianej propozycji – do co najmniej 36 miesięcy od dnia wejścia w życie).

4.8.3.Propozycja rozwiązania

Koalicja oraz Grupa postulują uważną weryfikację Projektu pod kątem zasad techniki prawodawczej w celu wyeliminowania ww. uchybień Projektu.

5. UWAGI SZCZEGÓŁOWE

5.1. Rejestrowanie zdarzeń (art. 12)

5.1.1.Opis

W Projekcie przewidziano, że systemy AI wysokiego ryzyka projektuje się i opracowuje tak, aby zawierały funkcję umożliwiającą automatyczne rejestrowanie zdarzeń podczas ich działania. Ta funkcja rejestracji zdarzeń musi być zgodna z uznanymi normami lub wspólnymi specyfikacjami. Musi także m.in. zapewniać w całym cyklu życia systemu AI poziom identyfikowalności jego funkcjonowania odpowiedni do jego przeznaczenia.

W przypadku systemów AI wykorzystywanych do identyfikacji biometrycznej wprowadzono dodatkowe wymagania, przykładowo obowiązek zapewnienia ewidencjonowania okresu każdego wykorzystania systemu (data i godzina rozpoczęcia oraz zakończenia każdego wykorzystania) czy danych wejściowych, w których przypadku wyszukiwanie doprowadziło do trafienia[12].

5.1.2.Stanowisko

[12] Art. 12 ust. 4 Projektu.

Należy szerzej uwzględnić odpowiednie wyjątki i dostosować do małych i średnich przedsiębiorców. Obecnie Projekt określa wysokie (choć niezdefiniowane) wymagania, nie odnosząc się do poziomu zaawansowania, pozycji biznesowej czy know-how podmiotu odpowiedzialnego za konkretny system AI.

5.1.3.Propozycja rozwiązania

Rekomendujemy dostosowanie wymogów stawianych małym i średnim przedsiębiorcom, przykładowo poprzez wprowadzenie standardów rejestrowania odpowiednich do stopnia zaawansowania produktu oraz proporcjonalnych do stwarzanego ryzyka.

5.2. Obowiązki w zakresie przejrzystości (art. 13)

5.2.1.Opis

W Projekcie przewidziano, że systemy AI wysokiego ryzyka projektuje się i opracowuje się w sposób zapewniający wystarczającą przejrzystość ich działania, umożliwiającą użytkownikom interpretację wyników działania systemu i ich właściwe wykorzystanie[13]. Do systemów AI wysokiego ryzyka dołącza się instrukcję obsługi w odpowiednim formacie cyfrowym lub innym formacie zawierającą zwięzłe, kompletne, poprawne i jasne informacje, które są istotne, dostępne i zrozumiałe dla użytkowników[14]. Przewiduje się szereg informacji, jakie instrukcje mają obowiązkowo zawierać[15].

5.2.2.Stanowisko

Pozytywnie oceniamy obowiązek należytego informowania użytkowników o działaniu systemu AI oraz dołączania odpowiedniej instrukcji do tychże systemów AI. Istnieją jednak wątpliwości co do zakresu informacji każdorazowo objętych tymi instrukcjami.

Projekt w obecnym brzmieniu nakłada obowiązek przekazania użytkownikom zbyt wielu informacji, których część z punktu widzenia odbiorcy nie ma większego znaczenia. Przykładowo, należy do nich obowiązek udostępniania w „stosownych przypadkach" specyfikacji dotyczących wykorzystywanych zbiorów danych treningowych, walidacyjnych i testowych, uwzględniając przeznaczenie systemu AI[16]. Jednocześnie określenie użyte w Projekcie „odpowiedni rodzaj i stopień przejrzystości" informacji udostępnianych użytkownikom nie jest wystarczająco precyzyjne, co prowadzić może do znacznych rozbieżności w zakresie informacji udostępnianych użytkownikom różnych systemów AI.

Ponadto negatywnie oceniamy obowiązek każdorazowego przedstawiania wszelkich znanych lub dających się przewidzieć okoliczności związanych z wykorzystaniem systemu AI wysokiego ryzyka zgodnie z jego przeznaczeniem lub w warunkach dającego się racjonalnie przewidzieć niewłaściwego wykorzystania, które mogą powodować zagrożenia dla zdrowia i bezpieczeństwa lub praw podstawowy-

[13] Art. 13 ust.1 Projektu.

[14] Art. 13 ust. 2 Projektu.

[15] Art. 13 ust. 3 Projektu.

[16] Art. 13 ust. 3 b) (v) Projektu.

ch[17]. Ponadto z perspektywy systemu ochrony zdrowia za punkt odniesienia należy przyjąć już istniejące obowiązki informacyjne np. względem pacjenta.

5.2.3.Propozycja rozwiązania

Rekomendujemy zawężenie obowiązku informacyjnego w taki sposób, aby uwzględniał istotne i przydatne informacje, np. realne ryzyko, a nie wszelkie znane lub dające się przewidzieć okoliczności związane z wykorzystaniem systemu AI wysokiego ryzyka. Wskazane jest doprecyzowanie kryteriów oceny przejrzystości. Zalecamy również minimalizowanie zakresu informacji przekazywanych nieprofesjonalnym osobom i podmiotom korzystającym z systemów AI, w tym pacjentom. W tym celu w naszej ocenie korzystne byłoby pominięcie szczegółowych specyfikacji dotyczących wykorzystywanych zbiorów treningowych czy walidacyjnych.

5.3. Nadzór ze strony człowieka (art. 14)

5.3.1.Opis

Nadzór ze strony człowieka nad systemami AI wysokiego ryzyka ma na celu zapobieganie ryzyku dla zdrowia, bezpieczeństwa lub praw podstawowych lub minimalizowanie takiego ryzyka, które może się pojawić, gdy system AI wysokiego ryzyka jest wykorzystywany zgodnie z jego przeznaczeniem lub w warunkach dającego się racjonalnie przewidzieć niewłaściwego wykorzystania.

5.3.2.Stanowisko

Obowiązek nadzoru ze strony człowieka został ograniczony wyłącznie do systemów AI wysokiego ryzyka. Należy to ocenić pozytywnie - nadmiar obowiązków związanych z projektowaniem i opracowywaniem systemów AI mógłby wywrzeć negatywny wpływ na rozwój tych systemów w Unii Europejskiej. Jednocześnie Projekt przewiduje klauzule szerokie i niedookreślone w odniesieniu do obowiązku nadzoru, przez co obowiązek ten może być bardzo mocno rozszerzany.

Ponadto Projekt nie przewiduje rozróżnienia obowiązku nadzoru w stosunku do różnych systemów AI. Konieczne są działania mające na celu uatrakcyjnienie inwestowania w systemy AI oraz rozwijania ich, m.in. poprzez różnicowanie obowiązków odpowiednio do rzeczywistego ryzyka i korzyści, jakie przynieść może używanie konkretnego systemu AI.

Z perspektywy systemu ochrony zdrowia Projekt nie zawiera żadnych regulacji dotyczących partycypacji przedstawicieli zawodów medycznych w systemach nadzoru. W naszej ocenie kwestia ta wymaga rozważenia. Z perspektywy zarówno rozwoju systemów AI oraz ich stosowania w warunkach klinicznych zapewnienie udziału przedstawicieli zawodów medycznych może być pożądane.

5.3.3.Propozycja rozwiązania

Należy rozważyć możliwości przyznania właściwym organom krajowym uprawnienia do ustanowienia i podania do wiadomości publicznej wykazu systemów wysokiego ryzyka niepodlegających obowiązkowi nadzoru ze strony człowieka (*whitelist*).

[17] Art. 13 ust. 3 b) (iii) Projektu.

5.4. Brak rozróżnienia na systemy AI dalej uczące się (art. 15)

5.4.1.Opis

W Projekcie przewidziano, że systemy AI wysokiego ryzyka, które po wprowadzeniu na rynek lub oddaniu do użytku nadal się uczą, opracowuje się w taki sposób, aby należycie zaradzić – za pomocą odpowiednich środków ograniczających ryzyko – ewentualnym tendencyjnym wynikom działania spowodowanym tym, że wyniki działania wykorzystuje się jako dane wejściowe w przyszłych operacjach[18].

5.4.2.Stanowisko

Systemy AI stwarzają zupełnie inne szanse oraz zupełnie inne zagrożenie w fazie treningowej oraz po wytrenowaniu. W naszej ocenie Projekt powinien bardziej transparentnie rozróżniać te systemy AI od siebie – obecnie uwzględnia się tę różnicę jedynie w art. 15 ust. 3 oraz art. 43 ust. Projektu.

5.4.3.Propozycja rozwiązania problemu

Wskazane jest wprowadzenie rozróżnienia na systemy AI, które po wprowadzeniu na rynek lub oddaniu do użytku nadal się uczą oraz na te, które już trafiają na rynek lub do użytku wytrenowane oraz zastosowanie tego rozróżnienia w Projekcie (np. poprzez zróżnicowanie wymagań regulacyjnych).

5.5. Systemy zarządzania jakością (art. 17)

5.5.1.Opis

Dostawcy systemów AI wysokiego ryzyka zobowiązani są do wprowadzania systemu zarządzania jakością, który zapewnia zgodność z niniejszym rozporządzeniem. System ten dokumentuje się w systematyczny i uporządkowany sposób w formie pisemnych polityk, procedur i instrukcji oraz obejmuje on obowiązkowo kilkanaście wskazanych w Projekcie aspektów.

5.5.2.Stanowisko

Projektowany art. 17 stanowi w naszej ocenie przykład przeregulowania, które w konsekwencji doprowadzić może do hamowania innowacji. Przewidziano trzynaście obowiązków w zakresie systemów zarządzania jakością, przy czym znaczna część z nich nie jest doprecyzowana. Przykładów, obowiązek dotyczący wprowadzenia systemów i procedur „ewidencjonowania wszelkiej istotnej dokumentacji i wszelkich istotnych informacji" nie określa, czym są takie istotne dokumenty i informacje. Projekt przewiduje, że wdrożenie tych trzynastu aspektów ma być proporcjonalne do wielkości organizacji dostawcy[19]. Brak doprecyzowania, na czym ta proporcjonalność ma polegać, w praktyce może stwarzać liczne problemy interpretacyjna dla przedsiębiorców oraz organów nadzoru.

5.5.3.Propozycja rozwiązania problemu

Proponujemy stworzenie bardziej precyzyjnej oraz przyjaznej dostawcom regulacji poprzez:

[18] Art. 15 ust. 3, „sprzężenie zwrotne".

[19] Art. 17 ust.2 Projektu.

- zmniejszenie ilości obowiązków nakładanych na wszystkich dostawców np. poprzez uzależnienie ilości obowiązków w zakresie systemów zarządzania jakością od możliwych skutków działania systemu AI;
- doprecyzowanie kryterium proporcjonalności jako ułatwienia dla podmiotów gospodarczych, w szczególności z uwzględnieniem specyfiki sektora SME oraz startupów.

5.6. Odpowiedzialność producentów produktów stosowanych razem z systemami AI (art. 24)

5.6.1.Opis

W Projekcie przewidziano, iż w przypadku gdy system AI wysokiego ryzyka powiązany z produktami, do których zastosowanie mają akty prawne wymienione w załączniku II sekcja A, wprowadza się je do obrotu lub oddaje do użytku razem z produktem wytworzonym zgodnie z tymi aktami prawnymi za zapewnienie zgodności systemu AI z Projektem odpowiedzialność ponosi producent produktu, który – w odniesieniu do systemu AI – podlega takim samym obowiązkom jak te nałożone na dostawcę systemu AI.

5.6.2.Stanowisko

Komentowany przepis jest niejasny. Brak kryteriów oceny istnienia lub nie powiązania systemu AI wysokiego ryzyka z innymi produktami (*„system sztucznej inteligencji wysokiego ryzyka powiązany z produktami, do których zastosowanie mają akty prawne wymienione w załączniku II sekcja A*"). W szczególności nie jest jasne, czy powiązanie to ma mieć charakter funkcjonalny (np. system AI można wykorzystać razem z takimi produktami), przeznaczenia systemu AI (np. system AI jest dedykowany do wykorzystania z takimi produktami), prawny (np. system AI jest objęty tą samą transakcją sprzedaży, co te produkty), technologiczny czy właścicielski (np. prawa do systemu AI ma ten sam podmiot, który jest producentem ww. produktów).

Niejasny jest też zakres znaczeniowy sformułowania *„wprowadza się do obrotu lub oddaje do użytku razem z produktem*". Podobnie jak w przypadku sformułowania *„powiązany z*" nie wskazano, co np. oddawania do użytku „razem z" ma oznaczać. W praktyce może rodzić to podobne wątpliwości – np. czy zakup przez szpital wyrobów medycznych od producenta (spółka A) oraz, w oddzielnej procedurze przetargowej, zakup systemu AI wysokiego ryzyka wykorzystujących dane z tych wyrobów od dostawcy (spółka B) spełnia takie wymagania?

Komentowany przepis prowadzi do niezasadnego podziału odpowiedzialności dostawcy za system AI, a producenta za produkt, z którym system AI jest *razem* stosowany lub z którym jest *powiązany*. Analizowany art. 24 Projektu budzi liczne wątpliwości na gruncie praktycznym, przykładowo co do:

- administracyjnych kar pieniężnych – czy dwukrotne (przez dostawcę i przez producenta) naruszenie obowiązków regulacyjnych będzie dwukrotnie osobno karane przez organ nadzorczy, czy też będzie nakładana kara łączna;
- rozkładu kosztów ekonomicznych – w praktyce może być dojść do zawierania umów, które przenoszą ciężar ekonomiczny na dostawców, przy czym producenci mogą unikać zawierania umów z małych podmiotami (np. startupów) z uwagi na brak wypłacalności w razie ew. naruszenia;

- ingerencji producenta w działalność dostawcy – aby producent mógł np. wypełnić obowiązki dotyczące sporządzenia dokumentacji technicznej systemu AI wysokiego ryzyka (art. 16 lit. c Projektu) albo mógł wykazać na żądanie organu krajowego zgodność systemu AI wysokiego ryzyka z wymaganiami rozdziału 2 tytułu III Projektu, np. co do zapewnienia adekwatności danych treningowych, walidacyjnych i testowych (art. 16 lit. j w zw. z art. 10 ust. 3 Projektu), konieczne będzie udostępnienie przez dostawcę w zasadzie wszystkich informacji o systemie AI producentowi; w praktyce może to być utrudnione lub niewykonalne z uwagi na krytyczną wartość biznesową takich informacji dla dostawców;
- potencjalnych konsekwencji ww. ingerencji na gruncie prawa podatkowego i prawa konkurencji – wyżej opisana ingerencja producenta, wymagana przez komentowany przepis, może mieć także istotne konsekwencje w zakresie prawa podatkowego i prawa konkurencji, które należy dokładnie przeanalizować (np. w zakresie wywierania dominującego wpływu na działalność dostawcy przez producenta).

Ponadto część obowiązków nałożonych na producentów wymienionych w załączniku II sekcja A produktów jest niemożliwa do realizacji. Przykładowo, obowiązek rejestracji systemu AI wysokiego ryzyka przed wprowadzeniem do obrotu nałożony na dostawców w art. 51 Projektu jest możliwy do dokonania jedynie przed udostępnieniem na rynku po raz pierwszy. Tymczasem art. 24 Projektu znajduje zastosowanie również w sytuacji, gdy taki kwalifikowany system AI wysokiego ryzyka oddaje się do użytku, co może nastąpić już po wprowadzeniu do obrotu. W efekcie dla producentów, których produkty (np. wyroby medyczne) są powiązane z systemem AI oraz razem z nim oddawane do użytku, wykonanie obowiązków rejestracyjnych określonych w art. 51 Projektu będzie niemożliwe.

Omawiane powyżej projektowane regulacje mogą mieć negatywny wpływ na rozwój startupów w sektorze MedTech. Komentowany przepis – z uwagi na jego wady omawiane powyżej – może wręcz zachęcać producentów produktów (np. wyrobów medycznych) do rozwijania systemów AI wyłącznie *in house*, z pominięciem startupów. W praktyce może to doprowadzić do zahamowania innowacyjności oraz przeniesienia działalności startupów na terytorium państw trzecich (np. Izrael, USA, Kanada).

5.6.3.Propozycja rozwiązania problemu

W ocenie Koalicji należy:

- doprecyzować znaczenie użytych w przepisie terminów tak, by nie wzbudzały wątpliwości co do chwili powstania i zakresu obowiązków producentów produktów,
- wprowadzić zmiany uwzględniające specyfikę działania startupów oraz przedsiębiorstw z sektora SME przy określaniu ich obowiązków,
- doprecyzować przepis w taki sposób, aby kreowane przez niego obowiązki były możliwe do spełnienia.

5.7. Odpowiedzialność uczestników łańcucha dystrybucyjnego „jak producent” (art. 28)

5.7.1.Opis

W Projekcie przewidziano, że dystrybutora, importera, użytkownika lub inną osobę trzecią uznaje się za dostawcę do celów projektowanego rozporządzenia i nakłada się na nich obowiązki równoważne obowiązkom dostawcy określonym w art. 16 Projektu m.in. jeżeli:

- zmieniają przeznaczenie systemu sztucznej inteligencji wysokiego ryzyka, który został już wprowadzony do obrotu lub oddany do użytku;
- wprowadzają istotne zmiany w systemie AI wysokiego ryzyka[20].

5.7.2.Stanowisko

Obowiązki regulacyjne określone w art. 16 Projektu są bardzo rozbudowane. Nałożenie równoważnych obowiązków na podmioty inne niż dostawcy powinno być odpowiednio uzasadnione. Projekt nie definiuje czym są „istotne zmiany" w systemie AI wysokiego ryzyka ani czym jest „zmiana przeznaczenia" takiego systemu. W konsekwencji w praktyce istnieje ryzyko powstania istotnych wątpliwości interpretacyjnych w tym zakresie zarówno po stronie uczestników łańcucha dystrybucyjnego, jak i po stronie organów nadzoru.

5.7.3.Propozycja rozwiązania problemu

Rekomendujemy doprecyzowanie na czym mają polegać „istotne zmiany" oraz „zmiana przeznaczenia" w kontekście projektowanego przepisu, np. poprzez wprowadzenie otwartego wyliczenia jako przykładu, celem ujednolicenia wykładni. Przyniesie to wymierne korzyści z perspektywy pewności prawa, szczególnie, że Projekt zakłada przenoszenie odpowiedzialności za te zmiany również na użytkowników będących osobami fizycznymi korzystającymi z systemów AI zawodowo (np. lekarz).

5.8. Obowiązki użytkowników systemów AI wysokiego ryzyka (art. 29)

5.8.1.Opis

Użytkownicy systemów AI wysokiego ryzyka mają obowiązek przestrzegania instrukcji obsługi systemów AI, oraz w zakresie, w jakim sprawują kontrolę nad danymi wejściowymi, zapewniają adekwatność danych wejściowych w odniesieniu do przeznaczenia systemu AI wysokiego ryzyka[21]. Ponadto użytkownicy mają obowiązek do monitorowania działania systemu AI wysokiego ryzyka w oparciu o instrukcję obsługi[22]. Co więcej, użytkownicy systemów AI wysokiego ryzyka mają obowiązek przechowywać rejestry zdarzeń generowane automatycznie przez dany system AI wysokiego ryzyka w zakresie, w jakim tego rodzaju rejestry zdarzeń znajdują się pod ich kontrolą.

5.8.2.Stanowisko

W naszej ocenie Projekt ustanawia zdecydowanie zbyt wiele obowiązków użytkowników systemów AI wysokiego ryzyka. Jest to niekorzystne z perspektywy tych użytkowników, a w szczególności osób fizycznych, które także zostały objęte regulacją.

---

[20] Art. 28 ust. 1 c).

[21] Art. 26 ust. 2 i ust. 3 Projektu.

[22] Art. 26 ust.4 Projektu.

5.8.3.Propozycja rozwiązania problemu

Jako najbardziej korzystną zmianę rekomendujemy redukcję obowiązków przeniesionych na użytkowników. Alternatywnie sugerujemy uzależnienie obowiązków użytkowników od ich charakteru – np. poprzez wydzielenie obowiązków użytkowników będących osobami prawnymi od obowiązków osób fizycznych szerzej niż obecnie w Projekcie[23], z naciskiem na zmniejszenie obowiązków osób fizycznych.

5.9. Wprowadzenie do obrotu lub oddanie do użytku systemu AI na zasadzie odstępstwa (art. 47)

5.9.1.Opis

W Projekcie przewidziano, że wyjątkowo organ nadzoru rynku może wydać zezwolenie na wprowadzenie do obrotu lub oddanie do użytku konkretnych systemów AI wysokiego ryzyka na terytorium danego państwa członkowskiego w związku z wystąpieniem nadzwyczajnych względów dotyczących bezpieczeństwa publicznego lub ochrony zdrowia i życia osób, ochrony środowiska i ochrony kluczowych aktywów przemysłowych i infrastrukturalnych[24].

Zastrzeżono również, że takie zezwolenie wydaje się wyłącznie wówczas, gdy organ nadzoru rynku stwierdzi, że system AI wysokiego ryzyka spełnia wymogi ustanowione w art. 8 - 15 Projektu, czyli m.in. odnoszące się do cyberbezpieczeństwa, nadzoru ze strony człowieka nad oprogramowaniem czy dokumentacji technicznej oprogramowania.

5.9.2.Stanowisko

Wprowadzenie mechanizmu awaryjnego dopuszczenia systemu AI na rynek oceniamy jako zasadne, zwłaszcza z perspektywy sektora ochrony zdrowia.

Jednakże zastrzeżenie konieczności spełnienia wymogów ze wszystkich wskazanych przepisów w praktyce może powodować trudności. Dotyczy to zwłaszcza wymogu przedstawienia pełnej dokumentacji zgodnie z projektowanym załącznikiem IV. W odniesieniu do oprogramowania używanego w ochronie zdrowia w dokumentacji najczęściej konieczne będzie uwzględnienie wymogów zarówno Projektu, jak i MDR, co przez liczbę wymogów formalnych może spowolnić wprowadzenie systemu AI na rynek.

Niezasadny jest również brak uregulowania kwestii odpowiedzialności w związku z omawianym mechanizmów odstępstwa od procedury zgodności (zob. uwagi dot. odpowiedzialności cywilnej w pkt 4.6).

5.9.3.Propozycja rozwiązania problemu

Rekomendujemy wprowadzenie jasnych reguł odpowiedzialności w przypadku wprowadzania do obrotu lub oddawania do użytku na zasadzie odstępstwa od procedury zgodności systemów AI.

5.10. Obowiązki w zakresie przejrzystości (art. 52)

5.10.1.Opis

[23] W obecnym brzmieniu wyodrębniono jedynie użytkowników będących instytucjami kredytowymi podlegającymi przepisom dyrektywy 2013/36/UE.

[24] Art. 47 ust. 1 Projektu.

W Projekcie przewidziano, że w przypadku systemów AI przeznaczonych do interakcji z osobami fizycznymi postanowienia 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[25]. Przewidziano również osobne obowiązki informacyjne w zakresie technologii identyfikacji biometrycznej[26] oraz technologii generujących obrazy, treści dźwiękowe lub treści wideo, które do złudzenia przypominają istniejące osoby, obiekty, miejsca, inne podmioty lub zdarzenia, lub które tymi obrazami i treściami manipulują, przez co osoba będąca ich odbiorcą mogłaby niesłusznie uznać je za autentyczne lub prawdziwe („*deepfake*")[27].

5.10.2.Stanowisko

Przede wszystkim korzystne byłoby wprowadzenie konkretnych reguł względem przejrzystości stosowania systemu AI. Samo określenie „zapewnianie informowania o prowadzeniu interakcji z systemem" uważamy za nieprecyzyjne.

Ponadto nieuzasadnione jest wyróżnianie regulacyjnie technologii identyfikacji biometrycznej oraz technologii *deepfake* przy jednoczesnym pominięciu osobnych obowiązków informacyjnych w zakresie systemu ochrony zdrowia, np. technologii diagnozujących czy wspomagających diagnozowanie chorób. Sam standard postępowania lekarza i należyta staranność w leczeniu mogą nie być wystarczające, zwłaszcza w przypadku systemu AI – wyrobu medycznego, służącego do samodzielnego stosowania przez pacjenta.

PRZYKŁAD

Pacjent korzysta z aplikacji na smartfon połączonej z jego wagą domową, które służą do monitorowania przebiegu leczenia otyłości u tego pacjenta. Nad procesem leczenia otyłości czuwa lekarz, który monitoruje wyniki pacjenta na bieżąco.

W jaki sposób i gdzie w tej aplikacji powinna znaleźć się informacja o działaniu z użyciem systemu AI? Skoro to na dostawcy ciąży obowiązek poinformowania o użytej technologii, czy informacja powinna zostać zamieszczona w regulaminie korzystania z aplikacji, czy może powinna być widoczna w interfejsie aplikacji? W przypadku odpowiedzi twierdzącej, jaka informacja powinna zostać udostępniona – o konkretnie użytej technologii np. wykorzystaniu rekurencyjnej sieci neuronowej, czy o zbiorczej nazwie grupy technologii?

5.10.3.Propozycja rozwiązania problemu

Rekomendujemy uściślenie sposobu informowania o wykorzystaniu systemu AI np. poprzez wskazanie otwartego wyliczenia informacji, jakie należy przedstawić oraz doprecyzowanie sposobu informowania o wykorzystanej technologii – tj. czy ma to być w widocznym dla użytkownika miejscu, czy w dokumentacji itd.

---

[25] Art. 52 ust. 1 Projektu.

[26] Art. 52 ust. 2 Projektu.

[27] Art. 52 ust. 3 Projektu.

W naszej ocenie korzystne będzie również doprecyzowanie wyjątku przewidzianego w Projekcie – zwolnienia z obowiązku informacyjnego, jeżeli okoliczności i kontekst korzystania z systemu jednoznacznie na to wskazują[28]. Z perspektywy sektora ochrony zdrowia może pojawiać się wiele sytuacji, kiedy korzystanie np. z diagnostyki obrazowej opartej o systemy AI jest powszechnie przyjętym standardem staranności, jednakże z okoliczności i kontekstu nie wynika jednoznacznie, iż stosowany jest system AI.

Dodatkowo należy uściślić okoliczności informowania osób fizycznych o interakcji z systemem AI, w szczególności uwzględniając potrzebę zapewnienia szczególnej ochrony dzieci lub osób z niepełnosprawnościami. Obowiązek informowania powinien ciążyć na dostawcach w każdym przypadku, a ponadto komunikaty kierowane do osoby fizycznej powinny być sformułowane jasnym i prostym językiem, by dziecko czy osoba z niepełnosprawnościami mogła je bez trudu zrozumieć (zob. wymagania w zakresie informowania określone w RODO).

W szczególności rekomendujemy uściślenie obowiązków informacyjnych względem sektora ochrony zdrowia, gdzie chronione dobra (zdrowie i życie) mają szczególne znaczenie , a istniejące już prawne obowiązki informacyjne są szeroko zakrojone.

5.11. Piaskownice regulacyjne (*regulatory sandbox*) (art. 53)

5.11.1.Opis

W Projekcie wprowadzono szereg wymagań dla działania *regulatory sandbox*, w tym włączenie krajowych organów ochrony danych oraz innych organów krajowych w działalność *regulatory sandbox* w zakresie systemów AI m.in. poprzez bezpośredni nadzór nad ich działalnością.

Regulatory sandbox mają nie mieć wpływu na uprawnienia nadzorcze i naprawcze właściwych organów, których wytycznych należy przestrzegać przez cały czas w dobrej wierze w celu ograniczenia wszelkich istotnych zagrożeń dla bezpieczeństwa i praw podstawowych, które mogą powstać podczas eksperymentów w ramach *regulatory sandbox*[29]. Uczestnicy ponoszą również odpowiedzialność za wszelkie szkody wyrządzone osobom trzecim w wyniku eksperymentów w piaskownicy[30].

5.11.2.Stanowisko

W naszej ocenie regulacja w zakresie *regulatory sandbox* nie są wystarczające do pełnienia przez nie zamierzonej funkcji, tj. miejsca do bezpiecznego rozwoju technologii w środowisku testowym. W praktyce może to prowadzić do zminimalizowania ich roli.

W szczególności pozostawienie w pełnym wymiarze odpowiedzialności względem organów nadzorczych oraz odpowiedzialności odszkodowawczej budzi zastrzeżenia . Prace w ramach *regulatory sandbox* mają odbywać się pod bezpośrednim nadzorem profesjonalistów - właściwych organów i zgodnie z ich wytycznymi. Dlaczego zatem podmioty korzystające z *regulatory sandbox* celem sprawdzenia, nauki i rozwoju, maja ponosić pełną odpowiedzialność za działania przeprowadzane zgodnie z wy-

[28] Art. 52 ust. 1 Projektu

[29] Art. 53 ust. 3 Projektu.

[30] Art. 53 ust. 4 Projektu.

tycznymi profesjonalnych, oddelegowanych do tego rodzaju pomiotów? W obecnym brzmieniu Projektu brak reguł przypisywania odpowiedzialności korzystającym z *regulatory sandbox* w taki sposób, aby regulować i ograniczać cedowanie na nich całej odpowiedzialności.

W Projekcie przewidziano, że państwa członkowskie będą musiały podjąć szczególne środki na rzecz sektora SME[31] i przedsiębiorstw rozpoczynających działalność. Te środki to m.in. zapewnienie priorytetowego dostępu do *regulatory sandbox* dotyczących systemów AI czy obniżenie opłat za ocenę zgodności proporcjonalnie do wielkości przedsiębiorstwa i jego udziału w rynku[32]. Powyższe działania nie zapewniają należytego bezpieczeństwa i komfortu stosowania *regulatory sandbox* dla podmiotów gospodarczych rozpoczynających działalność (np. startupów). Tymczasem zapewnienie odpowiednich zachęt dla sektora SME może wpłynąć bardzo korzystnie na rozwój innowacyjnych technologii, zwiększenie przedsiębiorczości społeczeństwa i popularyzowanie stosowania systemów AI.

5.11.3.Propozycja rozwiązania problemu

Należy ponownie przeanalizować rzeczywiste korzyści z regulacji dla sektora SME oraz uwzględnić szerzej jego specyficzne potrzeby.

Konieczne jest uatrakcyjnienie *regulatory sandbox* zarówno od strony regulacyjnej, jak i biznesowej – tak, aby osiągnąć właściwą równowagę polegającą na zapewnieniu bezpieczeństwa bez nadmiernego spowolnienia postępu technologicznego. Niezbędne jest również stworzenie mechanizmów uczciwego przypisywania odpowiedzialności korzystającym z *regulatory sandbox*. Wskazane byłoby również dostosowanie *regulatory sandbox* do poszczególnych branż (w tym sektora ochrony zdrowia) – musiałoby to iść w parze z dostosowaniem reguł odpowiedzialności oraz wsparcia w ramach *regulatory sandbox*.

Znaczenie miałyby ułatwienia oraz zmiany, dzięki którym sektor SME zyskałby realną pomoc, takie jak na przykład:

- obniżenie opłat lub kosztów korzystania z *regulatory sandbox* – nie tylko opłat za ocenę zgodności[33];
- możliwość wydania nakazu dopuszczenia drobnego dostawcy do *regulatory sandbox* organizowanego czy zarządzanego przez większą firmę, dzielenie know-how i czerpanie z doświadczenia większych podmiotów;
- dostosowywanie *regulatory sandbox* do konkretnych branż na poziomie unijnym zapewniając jednolitą politykę w całej UE, w tym zwłaszcza sektora ochrony zdrowia biorąc pod uwagę postulaty standaryzowania i ujednolicania opieki zdrowotnej w Unii Europejskiej – rekomendujemy wprowadzenie szczególnych reguł testowania i weryfikowania oprogramowania wykorzystywanego w ochronie zdrowia, z uwzględnieniem rodzaju dóbr chronionych oraz potencjalnych korzyści z wykorzystania systemów AI;

[31] *Small and Medium-Sized Enterprise*

[32] Art. 55 ust. 1 Projektu.

[33] Art. 55 ust. 2 Projektu.

- stworzenie efektywnych mechanizmów ochrony małych i średnich podmiotów względem uprawnień właściwych organów w zakresie nadzoru i stosowania środków naprawczych – zwłaszcza pod kątem odszkodowawczym czy kar administracyjnych;
- zapewnienie bezpośredniego nadzoru właściwych organów, uwzględniając nie tylko ochronę danych, lecz także i specyfikę oprogramowania, jakie jest badane w ramach *regulatory sandbox*, np. uwzględnienie specyfiki oprogramowania będącego wyrobem medycznym pod kątem ilości i jakości niezbędnych dla jego funkcjonowania danych;
- stworzenie efektywnych mechanizmów oceny, oraz miarkowania i redukcji odpowiedzialności za wszelkie szkody wyrządzone osobom trzecim w wyniku eksperymentów prowadzonych w ramach *regulatory sandbox*.

5.12. Brak wsparcia regulacyjnego dla małych i średnich przedsiębiorców (art. 55)

5.12.1.Opis

Projekt przewiduje pewne środki pomocy na rzecz drobnych dostawców i użytkowników. Państwa członkowskie zobowiązane są do podejmowania następujących działań[34]:

- zapewniania drobnym dostawcom i przedsiębiorstwom typu startup dostępu do *regulatory sandbox* w zakresie systemów AI na zasadzie pierwszeństwa, o ile spełniają oni warunki kwalifikowalności;
- organizowania specjalnych wydarzeń informacyjnych poświęconych stosowaniu przepisów niniejszego rozporządzenia dostosowanych do indywidualnych potrzeb drobnych dostawców i użytkowników;
- w stosownych przypadkach tworzenia specjalnego kanału komunikacji z drobnymi dostawcami i z użytkownikami oraz z innymi innowacyjnymi podmiotami, aby przedstawić im wytyczne i odpowiadać na ich pytania dotyczące wdrażania niniejszego rozporządzenia[35].

5.12.2.Stanowisko

W obecnym brzmieniu Projektu wparcie dla sektora SME jest niewystarczające, w szczególności z perspektywy potrzeb małych i średnich podmiotów w sektorze ochrony zdrowia. Należy jak najszerzej umożliwiać startupom w branży MedTech rozwijanie innowacyjnych projektów wykorzystujących systemy AI, czego stymulatorem może być wsparcie regulacyjne polegające m.in. na zapewnieniu systemu zachęt lub zwolnień (w całości lub części) z niektórych obowiązków prawnych, przy zachowaniu odpowiedniego poziomu bezpieczeństwa.

5.12.3.Propozycja rozwiązania problemu

Należy podjąć działania celem stymulowania innowacyjności, która w dużej części pochodzi od małych i średnich podmiotów, w tym:

[34] Art. 55 ust.1 Projektu.

[35] Art. 55 ust. 1 lit. c) Projektu.

- stworzenie wytycznych oraz innych regulacji *soft law* dostosowanych do konkretnych sektorów gospodarki, wskazujących w jaki sposób mają funkcjonować informacje i kanały komunikacyjne,
- doprecyzowanie na poziomie projektowanego rozporządzenia w jaki sposób miałby funkcjonować specjalny kanał komunikacji wspomniany w Projekcie – zbyt ogólne określenie spowoduje, że w państwach członkowskich podejście do nowych technologii będzie się istotnie różnić (w zależności od funduszy, nastrojów społecznych itd.) nawet pomimo przygotowania wspomnianych wyżej wytycznych sektorowych, prowadząc do narastania nierówności gospodarczych między państwami w UE,
- wprowadzenie realnych udogodnień dla innowacyjnych podmiotów z sektora SME, np. w zakresie odpowiedzialności za projekty w ramach *regulatory sandbox* [por. uwagi w pkt 5.11].

5.13. Szeroki dostęp organów do dokumentacji i danych systemów AI (art. 64)

5.13.1.Opis

Projekt zakłada, że krajowe organy lub podmioty publiczne, które nadzorują lub egzekwują przestrzeganie obowiązków wynikających z prawa UE służącego ochronie praw podstawowych w odniesieniu do stosowania systemów AI wysokiego ryzyka, o których mowa w załączniku III, są uprawnione do żądania wszelkiej dokumentacji sporządzonej lub prowadzonej na podstawie niniejszego rozporządzenia i do uzyskania do niej dostępu, jeżeli dostęp do tej dokumentacji jest niezbędny do wykonywania ich kompetencji w ramach ich mandatu w granicach ich jurysdykcji. Odpowiedni organ lub podmiot publiczny informuje organ nadzoru rynku zainteresowanego państwa członkowskiego o każdym takim żądaniu.

5.13.2.Stanowisko

W naszej ocenie nie jest jasne czy i jak praktycznie ma być zapewniony dostęp do wszelkiej dokumentacji sporządzonej lub prowadzonej na podstawie projektowanego rozporządzenia, jeżeli dostęp do tej dokumentacji jest niezbędny do wykonywania ich kompetencji. W jaki sposób np. Rzecznik Praw Pacjenta powinien żądać dostępu do wskazanych informacji?

5.13.3.Propozycja rozwiązania problemu

Rekomendujemy doprecyzowanie procedur żądania dostępu do informacji w taki sposób, aby kluczowe organy mogły działać na rzecz ochrony obywateli zgodnie z jasnymi i przejrzystymi procedurami.

5.14. Brak gwarancji poufności danych udostępnianych organom nadzoru (art. 70)

5.14.1.Opis

W obecnym brzmieniu Projektu właściwe organy krajowe i jednostki notyfikowane zaangażowane w stosowanie projektowanego rozporządzenia przestrzegają zasady poufności informacji i danych uzyskanych podczas wykonywania swoich zadań i swojej działalności tak, aby m.in. chronić prawa wła-

sności intelektualnej oraz poufne informacje handlowe lub tajemnice przedsiębiorstwa osoby fizycznej lub prawnej, w tym kod źródłowy[36].

5.14.2.Stanowisko

Ujawnienie danych jakimkolwiek podmiotom zewnętrznym, nawet jeśli są one związane poufnością, może wiązać się ze zwiększonym ryzykiem ujawnienia, które jest poza kontrolą firmy – nawet jeśli są to organy regulacyjne. Szczególną uwagę należy zwrócić na systemy AI wysokiego ryzyka, które mogą autonomicznie wytwarzać produkty wynalazcze i które w pewnych okolicznościach mogą wymagać ujawnienia danych właściwym organom krajowym lub jednostkom notyfikowanym wymienionym we wniosku. Ujawnienie takich danych jakimkolwiek podmiotom zewnętrznym, nawet jeśli są one związane poufnością, może wiązać się ze zwiększonym ryzykiem ujawnienia, które jest poza kontrolą firmy.

Projekt nie zapewnia ochrony tajemnicy przedsiębiorstwa w należyty sposób. Ma to szczególnie istotne znaczenie w odniesieniu do systemów AI wysokiego ryzyka, do których należą m.in. wyroby medyczne. W ocenie Koalicji należy rozszerzyć ochronę tajemnicy przedsiębiorstwa m.in. ze względu na potrzebę zapewnienia ochrony prywatności osób, których dane osobowe mogą stanowić element danych wykorzystywanych przez system AI (np. dane treningowe) oraz znaczenie biznesowe informacji objętych tajemnicą, zwłaszcza z perspektywy podmiotów SME. Mocniejsze gwarancje prawne w tym zakresie pośrednio przyczyniłyby się również do promocji rozwoju innowacyjności i konkurencyjności, co byłoby z korzyścią zarówno dla dostawców jak i użytkowników czy beneficjentów systemów AI (np. pacjentów).

5.14.3.Propozycja rozwiązania problemu

Proponujemy rozszerzenie katalogu z art 70 ust. 1 Projektu w taki sposób, aby uwzględnić szerzej kwestie typowo związane z systemami AI, w tym m.in. kwestie ochrony prawnoautorskiej. W szczególności należy odróżnić:

- utwory człowieka wspomagane systemami AI (które w obecnych warunkach prawnych jako wynalazki realizowane za pomocą komputera mogą być chronione patentami lub jako programy komputerowe prawem autorskim), oraz
- twory autonomicznie generowane przez systemy AI, które obecnie są chronione praktycznie wyłącznie przez tajemnice handlowe (tj. systemy AI, które mogą wytworzyć wynalazcze wyjście). Obecnie w europejskich systemach prawnych brak człowieka autora wyklucza takie wytwory z ochrony na podstawie prawa własności przemysłowej lub prawa autorskiego.

Oba rodzaje kreacji należy wziąć pod uwagę np. w przypadku wyrobów medycznych wspieranych przez systemy AI, które w przyszłości mogą pojawić się w komercyjnym portfolio firm i które z definicji należą do systemów AI wysokiego ryzyka. Szczególną uwagę należy zwrócić na systemy AI wysokiego ryzyka, które mogą autonomicznie wytwarzać produkty wynalazcze i które w pewnych okolicznościach mogą wymagać ujawnienia danych właściwym organom krajowym lub jednostkom notyfikowanym wymienionym we wniosku. Konieczne jest zapewnienie norm gwarantujących bezpieczeństwo przepływu danych.

[36] Art. 70 ust. 1 Projektu.

5.15. Administracyjne kary pieniężne (art. 71)

5.15.1.Opis

Projekt przewiduje wysokie kary administracyjne. Przykładowo za nieprzestrzeganie zakazu praktyk w zakresie systemów AI, o których mowa w art. 5 Projektu oraz za niezgodność systemu AI z wymogami określonymi w art. 10 Projektu nakładana jest administracyjna kara pieniężna w wysokości do 30 mln EUR lub – jeżeli naruszenia dopuszcza się przedsiębiorstwo – w wysokości do 6 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego[37]. Natomiast przekazywanie nieprawidłowych, niekompletnych lub wprowadzających w błąd informacji jednostkom notyfikowanym i właściwym organom krajowym w odpowiedzi na ich wezwanie podlega administracyjnej karze pieniężnej w wysokości do 10 mln EUR lub – jeżeli naruszenia dopuszcza się przedsiębiorstwo – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego[38].

5.15.2. Stanowisko

Przewidziane sankcje są zbyt surowe i nieproporcjonalnie zwiększą ryzyko dla biznesu związane z wykorzystaniem i rozwojem systemów AI, co może negatywnie wpłynąć na rozwój tych systemów w Unii Europejskiej.

Po pierwsze, wprawdzie w Projekcie przewidziano, że kary muszą być skuteczne, proporcjonalne i odstraszające, oraz mają w szczególności uwzględniać interesy drobnych dostawców i przedsiębiorstw typu startup oraz ich rentowność[39], jednak interesy mniejszych podmiotów nie są należycie chronione. Wiele innowacji pochodzi wprost od startupów, zwłaszcza w tak szybko rozwijających się branżach jak MedTech. Sankcje finansowe przewidziane w Projekcie mogą być szkodliwe dla rozwoju MedTech w ramach sektora SME, a przy braku należytego sprecyzowania kryteriów oceny w obecnym brzmieniu Projektu pozostawiono szerokie pole do uznania administracyjnego.

Po drugie, Projekt jest nieadekwatny z perspektywy ryzyka regulacyjnego. Nieadekwatny nakład środków do udzielanego zabezpieczenia może doprowadzić do spowolnienia innowacji. Projekt powiela model z RODO, a tym samym jego wady, w tym:

- brak zasad miarkowania na poziomie legislacji UE,
- brak ujednoliconego podejścia w UE mimo potrzeby zapewnienia takiego podejścia,
- brak taryfikatora kar lub modelu ich obliczania przyjętego przez organy nadzorcze[40].

5.15.3.Propozycja rozwiązania problemu

W zakresie dyscyplinowania i kar proponujemy wprowadzenie:

---

[37] Art. 71 ust. 3 Projektu.

[38] Art. 71 ust. 5 Projektu.

[39] Art. 71 ust. 1 Projektu.

[40] Wyjątki m.in. Niemcy, Holandia – jednak wciąż nie jest to regulacja ogólnoeuropejska, a jedynie działanie poszczególnych państw członkowskich.

- przesłanek obciążających i łagodzących, ew. procedury *leniency*,
- taryfikatora kar lub modelu ich obliczania uzależnionego od rodzaju naruszeń.

W naszej opinii kary powinny być nakładane w oparciu o jasny katalog przesłanek oraz konkretnie wymienione naruszenia – konieczne jest zapewnienie adekwatnego nakładu środków do udzielanego zabezpieczenia, co z kolei pozwala na uniknięcie spowolnienia innowacji. W tym zakresie proponujemy rozszerzenie katalogu z art. 71 ust. 6 Projektu o kryteria, jakie będą brane pod uwagę przy ocenie ewentualnych uchybień – obecnie jest on zbyt wąski. Dodatkowo proponujemy, aby te kryteria stanowiły szeroki katalog czynników, które mają być brane pod uwagę – np. w kształcie podobnym do art. 83 RODO. W naszej ocenie rozszerzenie kryteriów oceny pozytywnie wpłynie na efektywność regulacji oraz zredukuje ewentualne problemy interpretacyjne. Przykładowo wskazane byłoby rozszerzenie katalogu czynności branych pod uwagę przy podejmowaniu decyzji o nałożeniu kary czy ustalaniu wysokości kary o:

- uwzględnienie liczby poszkodowanych osób oraz rozmiaru poniesionej przez nie szkody,
- uwzględnienie umyślnego lub nieumyślnego charakteru naruszenia,
- uwzględnienie stopnia współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków.

6. WYKAZ SKRÓTÓW

- **MDR** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych, zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) nr 178/2002 i rozporządzenia (WE) nr 1223/2009 oraz uchylenia dyrektyw Rady 90/385/EWG i 93/42/EWG;
- **IVDR** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/746 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych do diagnostyki in vitro oraz uchylenia dyrektywy 98/79/WE i decyzji Komisji 2010/227/UE;
- **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);

Ligia Kornowska
Liderka Koalicji AI w zdrowiu
Liderka GRAI ds. zdrowia