WARMIŃSKI WSPÓLNICY

AI w wyrobach medycznych

W PYTANIACH I ODPOWIEDZIACH

LISTOPAD 2024

Wstęp

Technologia na naszych oczach zmienia medycynę – co paradoksalnie w dużej mierze zawdzięczamy pandemii Covid-19.

W skali makro to jeden z filarów, który ma przywrócić konkurencyjność Europy i Polski na globalnym rynku. W skali mikro dzieje się to dzięki odważnym firmom, szczególnie medtechowym i biotechowym, które opracowują i wprowadzają na rynek innowacyjne rozwiązania, dające zupełnie nowe możliwości w obszarze diagnostyki, leczenia czy też funkcjonowania opieki zdrowotnej.

Otoczenie prawne jest niezwykle dynamiczne i wyzwań prawnych ciągle przybywa, od regulacyjnych (zgodność z MDR – Medical Device Regulation i AI Act), poprzez ochronę danych medycznych, aż po kwestie związane z ochroną własności intelektualnej.

Zamiast pisać o przepisach prawa, dzielimy się z Wami hipotetycznym *casem*, pokazując, jak można by podejść do regulacyjnej „ośmiornicy" oplatającej nowy produkt medtechowy. Odpowiadamy na ponad 30 pytań z czterech kluczowych obszarów – ale potencjalnych wątpliwości może być jeszcze więcej.

Zapraszamy do lektury, kontaktu i dialogu!

Joanna Krakowiak
radca prawny, partner,
life sciences i ochrona zdrowia

Krzysztof Wojdyło
adwokat, wspólnik
nowe technologie

Opis przypadku

Polska firma Medical Software chce wprowadzić na rynek aplikację mobilną wykorzystującą algorytm AI do generowania zaawansowanych raportów nt. zmian miażdżycowych w naczyniach krwionośnych. Firma Algorithmics z siedzibą w USA opracowała wielofunkcyjny algorytm, a następnie udzieliła firmie Medical Software wyłącznej, globalnej, odpłatnej licencji na korzystanie z tego oprogramowania w obszarze zastosowań medycznych na kolejne 5 lat pod prawem stanu Delaware. Firma Medical Software dostosowała algorytm, tak aby generował raporty medyczne nt. zmian miażdżycowych.

Oprogramowanie wymaga współpracy z fizycznym detektorem – czujnikiem, który zawiera mikroakumulator oraz mikrokartę SIM. Kompatybilny detektor został opracowany przez firmę Smart Detectors we współpracy z Medical Software.

Oprogramowanie i detektor są przewidziane do medycznego zastosowania – monitorowania pracy tętnic szyjnych.

Firmy Smart Detectors i Medical Software zawarły ponadto umowę o współpracy z właścicielem znanej sieci sklepów jubilerskich (firma Golden Necklace). Umowa zakłada, że detektor kompatybilny z oprogramowaniem będzie mocowany na wybranych, dostosowanych do tego naszyjnikach firmy Golden Necklace. Dostępne będą różne wzory oraz modele – niektóre ze złota, srebra oraz kamieni szlachetnych.

Zamierzeniem umowy o współpracy jest to, że konsument, który kupił **naszyjnik** od Golden Necklace, będzie mógł dokupić do niego **detektor** od Smart Detectors. Posiadając taki zestaw, będzie mógł następnie pobrać aplikację wykorzystującą algorytm AI (**oprogramowanie**) od Medical Software.

Oprogramowanie tworzy raporty, których zakres definiuje użytkownik naszyjnika. Cały czas dodawane są nowe opcje w tym zakresie. Raporty są płatne (możliwa jest opłata jednorazowa, miesięczna lub roczna). Użytkownik definiuje również ewentualnych odbiorców raportów. Poniżej przykłady dostępnych raportów oraz ich odbiorców:

1. Raport o zmianach miażdżycowych – odbiorcą raportu może być użytkownik, wskazany lekarz lub producent leków na miażdżycę.
2. Raport o ryzyku udaru – odbiorcą raportu może być użytkownik oraz wskazany lekarz.
3. Raport o bezpośrednim zagrożeniu życia – odbiorcą może być użytkownik, członek jego rodziny oraz system powiadamiania ratunkowego (w takim

przypadku z serwera firmy Medical Software jest wysyłana do systemu informacja o geolokalizacji użytkownika, podstawowe dane użytkownika oraz numer telefonu, pod którym można próbować się z nim kontaktować). Dodatkowo naszyjnik można sparować z samochodem, którym kieruje użytkownik. W przypadku raportu o bezpośrednim zagrożeniu życia odpowiednia informacja trafia do systemu pokładowego pojazdu, który uruchamia tryb awaryjny (w zależności od modelu pojazdu tryb awaryjny może wiązać się np. z przejęciem częściowej kontroli nad pojazdem przez autonomicznego pilota lub przymusowym, kontrolowanym zatrzymaniem pojazdu).

System ma zdolność do samodoskonalenia, tj. algorytm sam w sposób autonomiczny dostraja swoje parametry w oparciu o analizowane dane oraz feedback przekazywany od użytkowników i odbiorców raportów.

Oprogramowanie jest stworzone w 60% z oprogramowania *open source*.

Analiza przypadku

W omawianym przypadku należy sobie zadać kilka pytań dotyczących regulacji z zakresu wyrobów medycznych, AI, ochrony danych osobowych oraz własności intelektualnej.

Regulacje dotyczące wyrobów medycznych

1. Czy oprogramowanie wykorzystujące dane z detektora jest wyrobem medycznym?

Definicja wyrobu medycznego zawarta w rozporządzeniu 2017/745 w sprawie wyrobów medycznych (**MDR**) przewiduje, że oprogramowanie może być uznawane za wyrób medyczny.

Szczegółowe zasady dotyczące kwalifikowania software'u jako wyrobu medycznego w kontekście definicji z MDR można znaleźć w wytycznych Grupy Koordynacyjnej ds. Wyrobów Medycznych – MDCG 2019-11. Oprogramowanie jest w tych wytycznych definiowane jako zestaw instrukcji przetwarzających dane wejściowe i tworzących dane wyjściowe. O uznaniu oprogramowania za wyrób medyczny decyduje to, czy spełnia ono wszystkie wymogi wskazane w wytycznych (m.in. ma przeznaczenie medyczne, a jego celem jest przysparzanie korzyści indywidualnym pacjentom).

Omawiane oprogramowanie spełnia te kryteria (generuje raporty o ryzykach medycznych dotyczące indywidualnego pacjenta w oparciu o dane z odczytów), a zatem stanowi wyrób medyczny.

2. Jak traktować detektor (komponent hardware) z perspektywy regulacji o wyrobach medycznych i co go różni od strony regulacyjnej od smartwatchów?

Software będący wyrobem medycznym nierzadko wymaga komponentu hardware do prawidłowego działania. Tak też jest w omawianym przypadku.

Detektor podlega obowiązkom wynikającym z MDR z uwagi na swoje medyczne przeznaczenie. W świetle wytycznych Grupy Koordynacyjnej ds.

Wyrobów Medycznych – MDCG 2023-4 hardware współpracujący z omawianym oprogramowaniem:

- może być wprowadzany jako wyposażenie wyrobu medycznego (hardware jako wyposażenie wyrobu medycznego – software'u),
- może stanowić integralną część wyrobu medycznego (hardware i software razem jako jeden wyrób medyczny),
- może stanowić odrębny wyrób medyczny (hardware jako wyrób medyczny i software jako odrębny wyrób medyczny).

Ponieważ w omawianym stanie faktycznym software i hardware wprowadzają dwie różne firmy, naturalną konsekwencją byłoby traktowanie ich jako odrębnych wyrobów medycznych.

Detektor został przez producenta przewidziany do stosowania w celu medycznym. Z kolei producenci popularnych smartwatchów nierzadko podkreślają, że ich produkt – smartwatch –jest do zastosowań ogólnych, związanych ze stylem życia i samopoczuciem, a nie do zastosowań medycznych (nawet jeśli posiada detektory umożliwiające wykorzystanie go do celów medycznych). W konsekwencji smartwatch nie kwalifikuje się jako wyrób medyczny.

Przewidziane przez producenta zastosowanie jest kluczowe dla klasyfikowania hardware'u jako wyrobu medycznego. Z uwagi na definicję prawną hardware nie będzie wyrobem medycznym, jeżeli dokumentacja producenta i materiały dla użytkowników nie wskazują na to, że hardware został przewidziany do zastosowania medycznego. Od hardware'u należy jednak odróżnić software o przeznaczeniu medycznym – np. aplikację EKG na smartwatch, która jest traktowana jako wyrób medyczny, z uwagi na jej medyczne zastosowanie przewidziane przez producenta.

Zakładając, że naszyjnik będzie prezentowany jako ozdoba, a nie jako produkt przeznaczony do zastosowania medycznego, nie należy go uznawać za wyrób medyczny, nawet jeżeli wspomniana zostanie jego kompatybilność z detektorem, który można, ale nie trzeba dokupić.

3. Jak ustalić klasę ryzyka produktu z perspektywy regulacji o wyrobach medycznych?

MDR wyróżnia cztery zasadnicze klasy ryzyka wyrobów medycznych: klasa I, klasa IIa, klasa IIb, klasa III. Im wyższa klasa, tym większe ryzyko i tym większy zakres wymogów regulacyjnych. Wyrób klasyfikuje się do danej klasy ryzyka zgodnie z regułami klasyfikacji określonymi w załączniku do MDR.

Zgodnie z tymi regułami oprogramowanie przeznaczone do monitorowania procesów fizjologicznych należy do klasy IIa, z wyjątkiem przypadków, gdy jest ono przeznaczone do monitorowania życiowych parametrów fizjologicznych, a zmiana tych parametrów może powodować bezpośrednie zagrożenie dla pacjenta – w takim przypadku oprogramowanie należy do klasy IIb.

Z uwagi na charakter parametru badanego przez wyrób (prawidłowość pracy tętnic szyjnych) wyrób należy przyporządkować do klasy ryzyka IIb (zmiana badanego parametru może bowiem powodować bezpośrednie zagrożenie dla pacjenta).

Analogicznie należy zaklasyfikować detektor współpracujący z oprogramowaniem – jako wyrób medyczny klasy ryzyka IIb. W tym wypadku zastosowanie znajduje reguła, zgodnie z którą do klasy IIb należą produkty przeznaczone specjalnie do monitorowania życiowych parametrów fizjologicznych, a charakter zmian tych parametrów może powodować bezpośrednie zagrożenie dla pacjenta.

4. Czy to jedyna ocena ryzyka, jaka musi być przeprowadzona wobec produktu?

Po rozpoczęciu stosowania unijnego rozporządzenia dotyczącego AI (tzw. AI Act) konieczne będzie ponadto ustalenie ryzyka produktu w świetle tej regulacji (zob. odpowiedź na pytanie nr 2 w części poświęconej regulacjom dotyczącym AI poniżej).

5. Jakie są obowiązki producenta wprowadzającego produkt na rynek (z perspektywy regulacji o wyrobach medycznych)?

Producent wprowadzający wyrób medyczny na rynek ma obowiązek w szczególności:

- pozyskać osobę odpowiedzialną za zgodność regulacyjną,
- przygotować niezbędną dokumentację, procedury i systemy,
- przeprowadzić ocenę kliniczną wyrobu,
- nadać kody UDI wyrobom medycznym, przekazać je do bazy Eudamed (obligatoryjne w perspektywie najbliższych lat, ale możliwe do wykonania już teraz, na zasadzie dobrowolności) oraz umieścić je na wyrobach,
- przeprowadzić ocenę zgodności, tj. uzyskać certyfikat MDR wydawany przez jednostkę notyfikowaną,

- sporządzić deklarację zgodności i oznakować wyroby znakiem CE,
- zgłosić zamiar wprowadzenia wyrobu na rynek.

6. Czy trzeba przeprowadzić badania kliniczne?

Przeprowadzenie badania klinicznego jest bezwzględnie obowiązkowe, z pewnymi wyjątkami, wobec wyrobów do implantacji i wyrobów klasy III. Produkt (ani oprogramowanie, ani detektor) nie należy zaś do tych kategorii.

Jednakże badanie kliniczne i tak może okazać się konieczne, jeżeli brakuje danych klinicznych dotyczących zgodności wyrobu z zasadniczymi wymaganiami dotyczącymi bezpieczeństwa i skuteczności stosowania, na których można by się oprzeć, i zachodzi potrzeba ich wygenerowania.

7. Czy trzeba zaangażować jednostkę certyfikującą?

Tak, w przypadku wyrobów klasy IIa i IIb wymagany jest udział jednostki notyfikowanej w ramach przeprowadzania oceny zgodności.

Udział jednostki notyfikowanej nie jest wymagany jedynie w przypadku wyrobów klasy I (innych niż wprowadzane do obrotu w stanie sterylnym, mające funkcję pomiarową lub będące narzędziami chirurgicznymi wielokrotnego użytku).

8. Jakie są możliwości w zakresie komunikacji o zdrowotnych funkcjach produktu i reklamowania go wobec użytkowników (laików i profesjonalistów)?

Reklamowanie wyrobów medycznych jest co do zasady możliwe, ale podlega szczególnym regułom przewidzianym przez przepisy ustawy o wyrobach medycznych i polskiego rozporządzenia w sprawie reklamy wyrobów medycznych.

Produkt jest przeznaczony do stosowania przez laików, dlatego może być reklamowany zarówno wobec profesjonalistów, jak i laików. Zakazane jest w szczególności wprowadzanie odbiorcy reklamy w błąd. Komunikatom reklamowym kierowanym do publicznej wiadomości musi ponadto towarzyszyć stosowne ostrzeżenie.

9. Czy będzie można ubiegać się o refundację produktu, jeżeli jego używanie będzie prowadziło do oszczędności w systemie ochrony zdrowia?

W Polsce nowoczesne technologie są już niekiedy finansowane ze środków publicznych (np. zawansowane roboty do operacji chirurgicznych).

Temat wspierania technologii AI w zdrowiu jest obecny w debacie publicznej. W Sejmie funkcjonuje obecnie podkomisja stała do spraw sztucznej inteligencji i przejrzystości algorytmów (CNT01S). W kwietniu 2024 r. dyskutowała ona na temat systemu refundacji stosowania nielekowych technologii cyfrowych wykorzystujących sztuczną inteligencję, jako metody na poprawę organizacji systemu ochrony zdrowia i opieki zdrowotnej społeczeństwa.

Funkcjonują także organizacje postulujące przygotowanie ram organizacyjno-prawnych, które w przyszłości umożliwią publiczne finansowanie wykorzystania AI w ochronie zdrowia.

10. Czy organy nadzoru weryfikują klasyfikację produktu? Jakie sankcje grożą za błędy w procesie wprowadzania do obrotu, sprzedaży czy też reklamy produktów?

Co do zasady za ustalenie klasy ryzyka odpowiada sam producent, a gdy w ocenę zgodności zaangażowana jest jednostka notyfikowana – weryfikuje ona klasyfikację dokonaną przez producenta. Przepisy przewidują natomiast, że spory pomiędzy producentem a jednostką notyfikowaną co do klasyfikacji wyrobów rozstrzyga Prezes URPL. W tych sprawach Prezes wydaje decyzję określającą to, do której klasy ryzyka należy wyrób.

Jeśli wyrób nie jest zgodny z wymaganiami prawnymi, Prezes URPL wzywa do usunięcia niezgodności – a gdy nie zostaną one usunięte, może wycofać wyrób z rynku. Nieprawidłowości związane z obowiązkami producenta i reklamą są ponadto obwarowane niezwykle surowymi karami pieniężnymi, które zgodnie z ustawą o wyrobach medycznych mogą sięgać nawet do 5 000 000 zł.

Regulacje dotyczące AI

1. Czy omawiany system jest systemem AI w rozumieniu rozporządzenia w sprawie sztucznej inteligencji (AI Act)?

W świetle rozporządzenia w sprawie sztucznej inteligencji „system AI" to system maszynowy, zaprojektowany do działania z różnym poziomem autonomii, który może po wdrożeniu wykazywać zdolność adaptacji i który – do wyraźnych lub dorozumianych celów – wnioskuje, jak generować na podstawie danych wejściowych wyniki, takie jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne.

Definicję systemu AI wyróżniają trzy cechy:
- zdolność wnioskowania (cecha niezbędna),
- autonomiczność, tj. zdolność działania w pewnym zakresie bez zaangażowania ze strony człowieka (cecha niezbędna),
- zdolność adaptacji, tj. zdolność do samouczenia się (cecha fakultatywna).

Omawiane oprogramowanie spełnia te cechy:
- przetwarza surowe dane z detektora na raporty z predykcjami i konkluzjami (tj. wnioskuje),
- generuje raporty bez udziału człowieka (autonomiczność),
- dostraja się, tj. udoskonala (samouczenie).

Z kolei detektor wprawdzie funkcjonuje autonomicznie, jednak nie ma zdolności wnioskowania – jedynie zbiera i przekazuje dalej zebrane dane, bez analizowania ich ani wyciągania konkluzji. Nie stanowi zatem systemu AI i nie podlega związanym z tym restrykcjom.

Również naszyjnik nie podlega wymogom wynikającym z rozporządzenia w sprawie sztucznej inteligencji – nie spełnia on bowiem cech, o których mowa w definicji systemu AI.

2. Do jakiej klasy ryzyka można przyporządkować omawiany system?

System AI może zostać zakwalifikowany jako system AI wysokiego ryzyka z uwagi na to, że:

1 jest produktem (lub związanym z bezpieczeństwem elementem produktu) wymienionym w Załączniku I do AI Actu (np. wyrobem medycznym) oraz podlega ocenie zgodności z udziałem jednostki notyfikowanej; lub
2 jest wykorzystywany w obszarze wymienionym w Załączniku III do AI Actu.

Omawiane oprogramowanie należy uznać za system AI wysokiego ryzyka w oparciu o pkt 1 powyżej. Wynika to z tego, że po pierwsze oprogramowanie stanowi wyrób medyczny w świetle przepisów, a po drugie podlega ono ocenie zgodności z udziałem jednostki notyfikowanej (zob. pytania 1 i 7 w części poświęconej regulacjom dotyczącym wyrobów medycznych). Spełnienie tych warunków przesądza na gruncie rozporządzenia w sprawie sztucznej inteligencji o tym, że oprogramowanie należy uznać za system AI wysokiego ryzyka.

Oprogramowanie można też uznać za system AI wysokiego ryzyka w oparciu o pkt 2 powyżej. Wynika to z tego, że w Załączniku III do AI Actu wskazano m.in.:

- systemy AI przeznaczone do wykorzystania przy kategoryzacji biometrycznej, według wrażliwych lub chronionych atrybutów lub cech na podstawie wywnioskowania tych atrybutów lub cech. Można uznać, że oprogramowanie wyświetla monit zdrowotny po tym, gdy ustali, że naczynia krwionośne użytkownika odpowiadają kategorii osób zagrożonych udarem;
- systemy AI przeznaczone do oceny i klasyfikacji zgłoszeń alarmowych dokonywanych przez osoby fizyczne lub do wykorzystywania w celu wysyłania lub ustalania priorytetów w wysyłaniu służb pierwszej pomocy, w tym policji, straży pożarnej i pomocy medycznej, a także w ramach systemów oceny stanu zdrowia pacjentów w nagłych wypadkach. Można uznać, że oprogramowanie jest tego rodzaju systemem z uwagi na funkcjonalność polegającą na ocenie stanu zdrowia pacjenta w nagłym wypadku i powiadamianiu służb ratunkowych.

Uznanie, że mamy do czynienia z systemem AI wysokiego ryzyka wymienionym w Załączniku III do AI Actu, ma skutki praktyczne. Rozporządzenie w sprawie sztucznej inteligencji różnicuje bowiem sytuację prawną systemów wysokiego ryzyka z Załącznika I i III. Jeśli produkt podlega obu załącznikom, należy naszym zdaniem stosować normy bardziej restrykcyjne.

3. Jaką rolę na gruncie AI Act można przypisać firmie Medical Software, a jaką firmie Algorithmics?

W opisanej sytuacji można przyjąć, że firma Algorithmics opracowała model AI ogólnego przeznaczenia, a w związku z udzieleniem licencji Medical Software udostępniła go na rynku, stając się dostawcą modelu AI ogólnego przeznaczenia.

Ponieważ jednak Algorithmics jest podmiotem spoza UE, będzie ona musiała wyznaczyć upoważnionego przedstawiciela w UE, któremu powierzy unijne obowiązki związane z rolą dostawcy modelu AI ogólnego przeznaczenia. Takim przedstawicielem mogłaby być firma Medical Software.

Niezależnie od dostarczania modelu przyjąć można, że Medical Software, dostosowując algorytm do konkretnej roli, adaptując go do pracy z detektorem i aplikacją – utworzyła system AI, który markuje swoją nazwą i odpłatnie udostępnia. W takim przypadku firmę tę należałoby uznać za dostawcę systemu AI.

4. Czy trzeba zgłosić wprowadzenie do obrotu omawianego oprogramowania?

Tak. Systemy AI wymienione w Załączniku III przed wprowadzeniem do obrotu muszą zostać zarejestrowane w bazie danych UE.

Z uwagi na to, że omawiane oprogramowanie jest pośrednio wspomniane w Załączniku III, konieczne jest dokonanie w jego przypadku takiego zgłoszenia (rejestracji).

5. Jakie inne obowiązki na gruncie AI Actu wiążą się z wprowadzeniem takiego systemu do obrotu w UE?

Zgodnie z nowymi przepisami dostawcy systemów AI wysokiego ryzyka muszą w szczególności:

- ustanowić system zarządzania ryzykiem,
- ustanowić system zarządzania jakością,
- opracować dokumentację techniczną i instrukcje używania systemu AI,
- przeprowadzić ocenę zgodności z wymogami rozporządzenia w sprawie sztucznej inteligencji (jest ona elementem oceny zgodności dokonywanej na podstawie przepisów o wyrobach medycznych i jest prowadzona z udziałem

jednostki notyfikowanej oceniającej zgodność z przepisami dotyczącymi wyrobów medycznych),
- sporządzić deklarację zgodności,
- odpowiednio oznakować system AI (w tym znakiem CE),
- zaprojektować system AI w odpowiedni sposób (tak aby umożliwiać wdrożenie nadzoru człowieka, a także aby zapewnić odpowiednią dokładność, solidność i cyberbezpieczeństwo),
- zadbać o to, aby system AI korzystał z odpowiednich danych treningowych,
- ustanowić system monitorowania systemu AI po wprowadzeniu do obrotu,
- zgłaszać poważne incydenty związane z systemem AI.

6. Jakie obowiązki oraz uprawnienia wiążą się z budowaniem oraz testowaniem systemu AI jeszcze przed jego wprowadzeniem do obrotu?

AI Act reguluje nie tylko obszar wprowadzania systemów AI do obrotu, ale także ich budowanie oraz testowanie przed wprowadzeniem.

Państwa członkowskie UE mają ustanawiać tzw. piaskownice regulacyjne. Piaskownice regulacyjne zapewniają kontrolowane ŚRODOWISKO sprzyjające innowacjom oraz ułatwiające rozwój, trenowanie, testowanie i walidację innowacyjnych systemów AI przez ograniczony czas przed ich wprowadzeniem do obrotu lub oddaniem ich do użytku zgodnie z określonym planem działania piaskownicy uzgodnionym między dostawcami lub potencjalnymi dostawcami a właściwym organem.

Systemy AI wysokiego ryzyka można rozwijać także poza piaskownicami regulacyjnymi w ramach tzw. testów w warunkach rzeczywistych. Dla systemów AI wysokiego ryzyka z Załącznika III do AI Actu trzeba jednak spełnić szereg warunków, m.in. przygotować plan testów, uzyskać zatwierdzenie od organu, ograniczyć czas trwania testów, uzyskać świadomą zgodę od uczestników i zapewnić odpowiedni nadzór.

Regulacje dotyczące ochrony danych osobowych, w tym danych medycznych (RODO)

1. Czy działanie produktu wiąże się z przetwarzaniem danych osobowych? Jeśli tak, jakiego rodzaju i przez kogo?

Tak, działanie produktu wiąże się z przetwarzaniem danych zwykłych oraz danych szczególnych kategorii.

W przetwarzanie danych w różnym stopniu zaangażowane są Smart Detectors i Medical Software oraz potencjalnie również Algorithmics (w zależności od tego, czy poza licencją świadczy na rzecz Medical Software usługi, które wiążą się z przetwarzaniem danych osobowych).

2. W jakim zakresie RODO będzie mieć zastosowanie do przetwarzania danych osobowych, do którego dochodzi w związku z działaniem produktu?

RODO będzie miało zastosowanie do przetwarzania danych osobowych w następujących kontekstach:

- przetwarzanie danych „zwykłych" użytkownika w związku z pobraniem i korzystaniem przez niego z aplikacji (dane potrzebne do założenia profilu i korzystania z niego: login, hasło, logi, dane związane z płatnościami (o ile będą) itp.),
- przetwarzanie danych o zdrowiu użytkownika w związku z działaniem produktu (detektora + aplikacji) – przy założeniu, że detektor nie będzie działał bez instalacji aplikacji i utworzenia konta przez użytkownika,
- przetwarzanie danych o zdrowiu użytkownika gromadzonych przez detektor dla celów rozwoju systemu,
- przetwarzanie danych o zdrowiu użytkownika dla celów tworzenia raportów i udostępniania ich podmiotom trzecim (w zależności od sposobu udostępniania, tj. w zależności od tego, czy aplikacja będzie bezpośrednio wykorzystywana do takiego udostępniania).

3. Kto jest, w rozumieniu RODO, administratorem danych osobowych przetwarzanych w związku z działaniem produktu? Na kim spoczywają główne obowiązki wynikające z RODO związane z produktem?

Rodzaj i cel przetwarzania danych	Role w świetle RODO
przetwarzanie danych zwykłych użytkownika w związku z pobraniem i korzystaniem z aplikacji (dane potrzebne do założenia profilu i korzystania z niego: login, hasło, logi itp.)	administrator danych: Medical Software
przetwarzanie danych o zdrowiu użytkownika w związku z działaniem produktu	administrator danych: Medical Software podmiot przetwarzający: potencjalnie Smart Detectors; Algorithmics (w zależności od ustaleń pomiędzy stronami i faktycznie wykonywanych czynności, np. jeśli Smart Detectors będzie miał dostęp do danych w ramach usługi maintenance)
przetwarzanie danych o zdrowiu dla celów rozwoju systemu	administrator danych: Medical Software (chyba że ustalenia umowy o współpracy z Algorithmics oraz Smart Detectors będą prowadziły do innych wniosków)
przetwarzanie danych o zdrowiu użytkownika dla celów tworzenia raportów i udostępniania ich podmiotom trzecim (w zależności od sposobu udostępniania)	administrator danych: Medical Software podmiot przetwarzający: potencjalnie Smart Detectors lub Algorithmics (w zależności od ustaleń pomiędzy stronami i faktycznie wykonywanych czynności)

4. Na jakiej podstawie wynikającej z RODO może dochodzić do przetwarzania danych osobowych w związku z działaniem produktu i jakie ma to znaczenie dla podmiotów prowadzących przetwarzanie danych?

Rodzaj przetwarzania danych	Podstawa przetwarzania
przetwarzanie danych zwykłych użytkownika w związku z pobraniem i korzystaniem przez niego z aplikacji (dane potrzebne do założenia profilu i korzystania z niego: login, hasło, logi itp.)	Niezbędność przetwarzania danych osobowych w celu wykonania umowy z użytkownikiem (art. 6 ust. 1 lit. b RODO). Prawnie uzasadniony interes administratora (art. 6 ust. 1 lit. f RODO), np. w związku z roszczeniami.

przetwarzanie danych o zdrowiu użytkownika w związku z działaniem produktu	Wyraźna zgoda (art. 9 ust. 1 lit. a RODO) (zakładamy, że działanie produktu **nie może** być traktowane jako prowadzenie działalności leczniczej)
przetwarzanie danych o zdrowiu dla celów rozwoju systemu	Wyraźna zgoda (art. 9 ust. 1 lit. a RODO) AI Act i rozporządzenie UE w sprawie europejskiej przestrzeni danych dotyczących zdrowia (EHDS) w przyszłości potencjalnie mogą dawać dodatkowe podstawy w tym zakresie.
przetwarzanie danych o zdrowiu użytkownika dla celów tworzenia raportów i udostępniania ich podmiotom trzecim wskazanym przez użytkownika (w zależności od sposobu udostępniania)	Wyraźna zgoda (art. 9 ust. 1 lit. a RODO)

5. Czy w związku z działaniem produktu będzie dochodziło do transferu danych osobowych poza EOG? Jakie są tego skutki?

Opis przypadku nie zawiera informacji w tym zakresie. Jeżeli jednak do działania aplikacji konieczne jest korzystanie z serwerów firmy Algorithmics, które znajdują się w USA, działanie aplikacji będzie wiązało się z transferem danych poza EOG, który będzie musiał być zalegalizowany (zasadniczo albo poprzez przystąpienie Algorithmics do programu EU-US privacy framework, albo poprzez zawarcie umowy opartej o standardowe klauzule umowne, tzw. SCCs).

6. Czy i kto powinien przeprowadzić ocenę skutków dla ochrony danych (DPIA) w związku z działaniem produktu?

Tak – będą argumenty, by twierdzić, że przeprowadzenie DPIA będzie wymagane. DPIA powinien przeprowadzić administrator danych osobowych przetwarzanych przez produkt, czyli Medical Software.

Jeżeli system AI zostanie uznany za system wysokiego ryzyka z Załącznika III do AI Actu, trzeba też będzie przygotowywać ocenę skutków systemu AI dla praw podstawowych na podstawie art. 27 AI Actu.

7. Kto i w jaki sposób powinien zapewnić przekazanie użytkownikom produktu informacji o przetwarzaniu ich danych osobowych?

Taką informację powinien przekazać administrator danych: Medical Software.

W tym celu może np. umieścić odpowiednie informacje w polityce prywatności udostępnianej przy pobieraniu / instalacji / korzystaniu z aplikacji powiązanej z produktem (przed rozpoczęciem działania detektora).

8. Czy dane osobowe przetwarzane w związku z działaniem produktu powinny być przechowywane w postaci dokumentacji medycznej?

Nie – o ile działanie produktu nie będzie równoznaczne z prowadzeniem działalności leczniczej.

9. Kto i w jakich okolicznościach będzie mógł udostępnić dane zebrane przez produkty podmiotom trzecim, np. w celach komercyjnego wykorzystania do trenowania AI?

Jeśli chodzi o dane niezanonimizowane – będzie mógł je udostępniać administrator danych, czyli Medical Software, ale tylko jeśli spełni dodatkowe warunki, tzn. przede wszystkim:

- uprzednio zidentyfikuje podstawę przetwarzania danych w tym celu – np. wyraźną zgodę użytkownika,
- zapewni użytkownikom odpowiednią informację dotyczącą przetwarzania ich danych w tym celu,
- przeprowadzi stosowne DPIA.

Do danych zanonimizowanych (skutecznie i nieodwracalnie) lub zagregowanych RODO nie ma zastosowania. Podmiot posiadający takie dane może nimi dysponować na zasadach ogólnych.

Rozporządzenie w sprawie sztucznej inteligencji (AI Act), rozporządzenie w sprawie sprawiedliwego dostępu do danych (Data Act) i rozporządzenie w sprawie europejskiej przestrzeni danych dotyczących zdrowia (EHDS) w przyszłości potencjalnie mogą dawać dodatkowe możliwości w tym zakresie.

10. Czy użytkownik aplikacji może żądać od Medical Software oraz Smart Detector danych generowanych przez detektor oraz oprogramowanie?

W zakresie, w jakim dane przetwarzane przez produkt będą stanowić dane osobowe użytkownika, użytkownik będzie miał prawo domagać się od administratora danych (co do zasady od Medical Software) otrzymania kopii przetwarzanych przez produkt danych osobowych na podstawie art. 15 ust. 3 RODO. Dodatkowo użytkownik będzie mógł domagać się od administratora otrzymania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych jego dotyczących, które dostarczył administratorowi. Konieczność zapewnienia możliwości realizacji ww. praw powinna być uwzględniona na etapie projektowania produktu.

Ponadto, w celu realizacji zobowiązań wynikających z Data Actu, firma Medical Software powinna zapewnić, że produkt i usługa będą zaprojektowane i będą działały w taki sposób, że dane z produktu, w tym stosowne metadane niezbędne do interpretacji i wykorzystania danych, będą dostępne dla użytkownika:

- domyślnie łatwo, bezpiecznie, bezpłatnie,
- w całościowym, ustrukturyzowanym, powszechnie używanym i nadającym się do odczytu maszynowego formacie,
- w stosownym przypadku i jeśli jest to technicznie możliwe – bezpośrednio.

11. W jaki sposób Medical Software może pozyskiwać dane do trenowania swoich algorytmów jeszcze przed wprowadzeniem systemu na rynek?

Ponieważ produkt przetwarza dane o zdrowiu, pozyskanie rzeczywistych danych na potrzeby trenowania algorytmu używanego w produkcie przed wprowadzeniem systemu na rynek może być dość problematyczne. Przepisy rozporządzenia w sprawie sztucznej inteligencji dają jednak pewne możliwości w tym zakresie.

Art. 59 AI Actu przewiduje bowiem możliwość korzystania w celu trenowania algorytmów z danych osobowych zebranych zgodnie z prawem w innych celach (a więc zebranych niekoniecznie w celu trenowania algorytmów), w ramach tzw. piaskownicy regulacyjnej w zakresie AI, wyłącznie do celów rozwoju, trenowania i testowania w ramach piaskownicy niektórych systemów AI, gdy spełnione są wszystkie następujące warunki:

a systemy AI rozwija się w celu zabezpieczenia przez organ publiczny lub inną osobę fizyczną lub prawną istotnego interesu publicznego w co najmniej jednym z następujących obszarów:
   i. bezpieczeństwo publiczne i zdrowie publiczne, w tym wykrywanie, diagnozowanie, profilaktyka, kontrola i leczenie chorób oraz poprawa systemów opieki zdrowotnej;
   ii. wysoki poziom ochrony ŚRODOWISKA i poprawa jego jakości, ochrona różnorodności biologicznej, ochrona przed zanieczyszczeniem, środki w zakresie transformacji ekologicznej, środki w zakresie łagodzenia zmiany klimatu i przystosowania się do niej;
   iii. zrównoważoność energetyczna;
   iv. bezpieczeństwo i odporność systemów transportowych i mobilności, infrastruktury krytycznej i sieci;
   v. wydajność i jakość administracji publicznej i usług publicznych;
b przetwarzane dane są niezbędne do zapewnienia zgodności z co najmniej jednym z wymogów, o których mowa w rozdziale III sekcja 2 AI Act, przy czym wymogów tych nie można skutecznie spełnić, przetwarzając dane zanonimizowane, dane syntetyczne lub innego rodzaju dane nieosobowe;
c ustanowiono skuteczne mechanizmy monitorowania pozwalające zidentyfikować wszelkie wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą, określone w art. 35 RODO i art. 39 rozporządzenia (UE) 2018/1725, jakie może wystąpić w trakcie przeprowadzania doświadczeń w ramach piaskownicy, a także mechanizmy reagowania zapewniające możliwość szybkiego ograniczenia tego ryzyka oraz – w stosownych przypadkach – wstrzymania przetwarzania;
d wszelkie dane osobowe, które mają być przetwarzane w kontekście piaskownicy, znajdują się w funkcjonalnie wyodrębnionym, odizolowanym i chronionym ŚRODOWISKU przetwarzania danych podlegającym kontroli potencjalnego dostawcy, a dostęp do tych danych posiadają wyłącznie upoważnione osoby;
e dostawcy mogą udostępniać dalej pierwotnie zebrane dane wyłącznie zgodnie z prawem UE o ochronie danych; wszelkie dane osobowe stworzone w piaskownicy nie mogą być udostępniane poza piaskownicą;
f przetwarzanie danych osobowych w kontekście piaskownicy nie prowadzi do wdrożenia środków lub podjęcia decyzji wywierających wpływ na osoby, których dane dotyczą, ani nie wpływa na stosowanie ich praw określonych w prawie UE o ochronie danych osobowych;
g dane osobowe przetwarzane w kontekście piaskownicy chroni się za pomocą odpowiednich środków technicznych i organizacyjnych oraz usuwa się po zakończeniu uczestnictwa w piaskownicy lub po upływie okresu przechowywania danych osobowych;

h rejestry przetwarzania danych osobowych w kontekście piaskownicy przechowuje się przez cały czas uczestnictwa w piaskownicy, o ile prawo UE lub prawo krajowe nie stanowią inaczej;

i w dokumentacji technicznej, o której mowa w załączniku IV do AI Act, zamieszcza się wyczerpujący i szczegółowy opis procesu trenowania, testowania i walidacji systemu AI wraz ze stosownym uzasadnieniem oraz wyniki przeprowadzonych testów;

j krótkie streszczenie projektu w zakresie AI rozwiniętego w ramach piaskownicy, jego celów i oczekiwanych rezultatów zostało opublikowane na stronie internetowej właściwych organów; obowiązek ten nie obejmuje wrażliwych danych operacyjnych związanych z działaniami organów ścigania, organów kontroli granicznej, organów imigracyjnych lub azylowych.

Dodatkowe możliwości w zakresie pozyskiwania danych dla celów trenowania algorytmów będą dostępne dla Medical Software w przyszłości, po wejściu w życie EHDS.

Regulacje dotyczące własności intelektualnej

1. Co zrobić, aby konkurencja nie wprowadziła na rynek naszyjnika o podobnym wyglądzie?

Najprostszym sposobem jest zgłoszenie wzoru naszyjnika do rejestracji i uzyskanie wzoru wspólnotowego (ewentualnie krajowego wzoru przemysłowego). Ochrona wynikająca z rejestracji jest ograniczona terytorialnie. Oznacza to, że uzyskanie rejestracji wzoru wspólnotowego daje uprawnionemu ochronę we wszystkich krajach Unii Europejskiej, a rejestracja wzoru krajowego daje ochronę jedynie na terytorium danego kraju.

Rejestracja wzoru do ochrony wymaga sprawdzenia w dostępnych rejestrach, czy wcześniej nie został udostępniony publicznie inny identyczny lub podobny wzór (w przepisach definiowany jako wzór niewywołujący na zorientowanym użytkowniku odmiennego ogólnego wrażenia). Ochronę mogą bowiem uzyskać jedynie takie wzory, które łącznie spełniają przesłanki nowości i indywidualnego charakteru. Urząd, dokonując rejestracji wzoru, nie bada spełniania ww. przesłanek. Oznacza to, że dany wzór, mimo że został zarejestrowany, może nie korzystać z ochrony, a konkurent może doprowadzić do unieważnienia przyznanego prawa (albo w samodzielnym postępowaniu przed odpowiednim urzędem, albo w drodze powództwa wzajemnego w wytoczonym przeciwko niemu postępowaniu o ochronę wzoru).

Konkurencyjną podstawą ochrony wzoru naszyjnika mogą być przepisy ustawy o prawie autorskim i prawach pokrewnych, które nie wymagają, aby dany wzór charakteryzował się nowością na poziomie światowym, a jedynie, aby stanowił przejaw działalności twórczej o indywidualnym charakterze.

Ostatnią możliwością ochrony wzoru jest jego ochrona na podstawie przepisów ustawy o zwalczaniu nieuczciwej konkurencji (w szczególności art. 13 ust. 1 oraz art. 3 ust. 1 u.z.n.k.). Ustawa o zwalczaniu nieuczciwej konkurencji chroni interesy gospodarcze przedsiębiorców przed tzw. niewolniczym naśladownictwem oraz pasożytnictwem. Aby skorzystać z ochrony, powód musi wykazać tzw. pierwszeństwo rynkowe, a także – w zależności od wybranej podstawy prawnej – albo wykazać, że konkurent wykonał identyczną (niewolniczą) kopię, albo wykazać renomę swojego produktu (uzyskaną np. poprzez ponoszenie znacznych nakładów na promocję i marketing swojego

wyrobu) oraz uzyskanie przez dany wyrób znacznej rozpoznawalności na rynku podobnych wyrobów.

2. Jakie postanowienia chroniące własność intelektualną powinna zawierać umowa joint venture pomiędzy Medical Software, Smart Detectors i Golden Necklace?

Umowy joint venture nie są przedmiotem szczegółowych regulacji Kodeksu cywilnego ani innych aktów prawnych. Dopuszczalność ich zawarcia nie budzi jednak wątpliwości w oparciu o zasadę swobody umów. W omawianym przypadku umowa joint venture jest umową trójstronną zawartą między spółką Smart Detectors (współtwórca detektora), Medical Software (twórca aplikacji i współtwórca detektora) oraz Golden Necklace (zakład jubilerski projektujący naszyjniki).

Umowa powinna przede wszystkim definiować, jak strony rozumieją własność intelektualną związaną z projektem oraz kto ma prawa i jakie do poszczególnych komponentów naszyjnika (np. prawa autorskie do oprogramowania detektora, oprogramowania aplikacji, projektów i wzorów naszyjników).

Umowa musi:
- wskazywać, jakich uprawnień na korzystanie z własności intelektualnej (w praktyce licencji) każda ze stron udziela pozostałym stronom,
- określać zakres używania (pola eksploatacji, terytorium, czas trwania licencji, np. tylko na czas współpracy stron) i ograniczenia.

W omawianym przypadku kluczowe wydaje się zagwarantowanie, aby strony korzystały z własności intelektualnej pozostałych stron tylko w ramach tej konkretnej współpracy. Nie powinny móc wykorzystywać, a tym bardziej rozwijać własności intelektualnej pozostałych stron poza wspólnym projektem.

W projektach joint venture zwykle zdarza się, że współpracujące strony tworzą wspólnie udoskonalenia lub modyfikacje lub nowe wytwory które mogą być chronione prawami własności intelektualnej. Warto zatem określić, kto ma być właścicielem wspólnie wytworzonej nowej własności intelektualnej i ustalić zasady dzielenia się związanymi z nią kosztami – np. kto będzie ponosił koszty zgłoszenia do formalnej ochrony (np. jako znak towarowy) i kto będzie wskazany jako właściciel (jedna ze stron czy wspólny znak towarowy). W omawianej sytuacji strony nie ustaliły np. nazwy handlowej dla finalnego naszyjnika i prawdopodobnie będą musiały to niebawem zrobić.

W umowie joint venture należy też określić, kto ponosi odpowiedzialność, jeśli własność intelektualna narusza prawa osób trzecich, i jak strony dzielą tę odpowiedzialność. Warto ustalić też związane z tym ewentualne koszty. Należy uregulować procedury rozstrzygania sporów dotyczących własności intelektualnej i wykorzystania wspólnie tworzonej własności intelektualnej.

Warto wprowadzić zobowiązania do zachowania poufności informacji ujawnianych w ramach joint venture i określić sposób ochrony informacji poufnych (np. ograniczenia dostępu, szyfrowanie, ograniczenia dotyczące publikowania informacji bez zgody wszystkich stron joint venture czy procedury zatwierdzania publikacji). Warto też ustalić procedury reagowania na naruszenia praw własności intelektualnej przez podmioty trzecie.

Niezwykle ważne, a często pomijane są postanowienia dotyczące wyjścia z joint venture, w tym określenie procedur zaprzestania wykorzystywania przez stronę wycofującą się własności intelektualnej licencjonowanej od pozostałych stron. Warto pamiętać o klauzulach konkurencyjnych, by ograniczyć działalność strony wycofującej się po opuszczeniu joint venture.

3. Do kogo należą prawa do wzorów naszyjników stworzonych w ramach umowy o współpracę z Golden Necklace?

Odpowiedź na to pytanie zależy od przebiegu procesu twórczego, który doprowadził do stworzenia produktu (naszyjnika z komplementarnym detektorem), a także od treści zawartej umowy. Co do zasady, jeśli w pracach nad produktem uczestniczyło kilka podmiotów, prawa do produktu powinny przysługiwać im łącznie.

Przedstawiony stan faktyczny nie daje odpowiedzi na pytanie, czy detektor (komplementarny z naszyjnikiem, który może być także noszony bez detektora) wpływa na wygląd zewnętrzny naszyjnika i modyfikuje jego design. Jeśli tak jest, należałoby przyjąć, że obu podmiotom przysługują łącznie prawa do wzoru naszyjnika z detektorem. Strony mogły jednak w zawartej umowie odmiennie ustalić, komu mają przysługiwać te prawa, a także udzielić sobie wzajemnie licencji na korzystanie z własności intelektualnej wytworzonej przez każdą ze stron lub przenieść przysługujące jednej stronie prawa na inne strony.

4. Na co powinna zwrócić szczególną uwagę firma Medical Software jako licencjobiorca modelu AI ogólnego przeznaczenia, rozwijająca na jego podstawie własny system AI?

Umowa pomiędzy Medical Software a Algorithmics, poza określeniem wzajemnych obowiązków stron typowych dla relacji licencjodawca – licencjobiorca (np. zakres używania, terytorium czy czas trwania licencji), powinna odnosić się do obowiązków wynikających z zakwalifikowania Algorithmics jako dostawcy modelu AI ogólnego przeznaczenia, a Medical Software – jako dostawcy systemu AI wysokiego ryzyka.

Firma Medical Software powinna w szczególności zadbać o to, aby Algorithmics udostępnił jej i aktualizował informacje oraz dokumentację dotyczące licencjonowanego modelu AI ogólnego przeznaczenia. W szczególności Algorithmics musi dostarczyć dokumenty i informacje, dzięki którym firma Medical Software będzie mogła:

- dobrze zrozumieć możliwości i ograniczenia licencjonowanego modelu AI,
- spełnić liczne obowiązki ciążące na tej spółce w związku z zakwalifikowaniem jej jako dostawcy systemu AI wysokiego ryzyka.

Dokumenty, które ma dostarczyć Algorithmics, muszą zawierać co najmniej informacje określone w załączniku XII do AI Act, tj.:

- ogólny opis modelu AI ogólnego przeznaczenia, w tym:
  - zadania, które dany model ma wykonywać, oraz rodzaj i charakter systemów AI, z którymi może zostać zintegrowany,
  - mające zastosowanie dopuszczalne zasady wykorzystania,
  - datę wydania modelu i metody jego dystrybucji,
  - sposób, w jaki model, w stosownych przypadkach, współdziała lub może być wykorzystywany do współdziałania ze sprzętem lub oprogramowaniem, które nie są częścią samego modelu,
  - w stosownych przypadkach wersje odpowiedniego oprogramowania związanego z wykorzystaniem modelu AI ogólnego przeznaczenia
  - architekturę i liczbę parametrów,
  - formę oraz format danych wejściowych i wyjściowych,
- opis elementów modelu oraz procesu jego rozwoju, w tym:
  - środki techniczne wymagane do integracji modelu z systemami AI,
  - informacje na temat danych wykorzystywanych do trenowania, testowania i walidacji, w stosownych przypadkach, w tym rodzaj pochodzenia danych oraz metody ich porządkowania.

Ma to szczególne znaczenie, biorąc pod uwagę fakt, że licencja będzie regulowana prawem Delaware, a Algorithmics jest podmiotem mającym siedzibę w USA, do którego AI Act stosuje się wyłącznie w związku z wprowadzaniem modeli AI ogólnego przeznaczenia na rynku unijnym.

Strony mogą też umownie uregulować kwestię wykorzystywania danych pozyskiwanych od użytkowników końcowych do dalszego trenowania modelu przez Algorithmics.

5. Czy fakt, że w produkcie wykorzystano oprogramowanie open source, ma jakiekolwiek znaczenie dla uprawnień przysługujących właścicielowi praw do oprogramowania?

W zależności od tego, jakiego rodzaju oprogramowanie typu *open source* zostało wykorzystane, fakt jego użycia może wpływać na kwestię dystrybucji całego oprogramowania i możliwości jego komercjalizowania. Niektóre fragmenty kodu źródłowego udostępniane są bowiem na zasadzie tzw. licencji *copyleft*, która nakłada na podmioty korzystające z oprogramowania *open source* obowiązek udostępnienia oprogramowania wykorzystującego *open source* na takich samych warunkach. Do licencji o skutku *copyleft* zalicza się m.in. licencje GNU GPL, GNU LGPL oraz GNU FDL.

Autorzy

Joanna Krakowiak
radca prawny, partner,
life sciences i ochrona zdrowia

Krzysztof Wojdyło
adwokat, wspólnik
nowe technologie

Marcin Rytel
adwokat,
life sciences i ochrona zdrowia

Natalia Nieróbca
prawnik,
life sciences i ochrona zdrowia

Karolina Romanowska
adwokat,
ochrona danych

Łukasz Rutkowski
radca prawny,
ochrona danych

Ewa Nagy
radca prawny,
własność intelektualna