ZESZYT NAUKOWY
Wyższa Szkoła Zarządzania i Bankowości w Krakowie

dr Artur Romaszewski
dr hab. Mariusz Duplaga, prof. UJ
mgr Szczepan Jakubowski
Zakład Promocji Zdrowia, Instytut Zdrowia Publicznego, Wydział Nauk o Zdrowiu, Uniwersytet Jagielloński Collegium Medicum
artur.romaszewski@uj.edu.pl

DANE O STANIE ZDROWIA W NOWYCH ROZWIĄZANIACH PRAWNYCH I DOKUMENTACH STRATEGICZNYCH POLSKI I UNII EUROPEJSKIEJ

Wprowadzenie

Pandemia jest źródłem wyzwań nie tylko o charakterze medycznym, ale także związanych z przetwarzaniem danych w systemie ochrony zdrowia. Obciążenia ponoszone przez społeczeństwa z powodu pandemii sprawiają, że na dalszy plan schodzą inicjatywy i regulacje odnoszące się do bardziej ogólnych kwestii. Przykładem na gruncie krajowym może być rozporządzenie dotyczące dokumentacji medyczne [1]. Warto też pamiętać, że przynajmniej część regulacji sprowokowanych pandemią i wprowadzających w pierwotnym zamiarze tylko czasowe zmiany w przetwarzaniu danych, może ostatecznie mieć charakter długoterminowy. Ważnym rozwiązaniem jest wejście do systemu prawnego usługi e-doręczenia. Jest ono konsekwencją wdrożenia w Polsce usług zaufania zawartych w Rozporządzeniu dotyczącym elektronicznej identyfikacji i usług zaufania (*Electronic Identification and Trust Services Regulation, eIDAS*)[2]. Wszystko wskazuje na to, że to nowe rozwiązanie będzie można wykorzystywać do przesyłania elektronicznej dokumentacji medycznej. Przyczyni się ono do skutecznej ochrony przesyłanych dokumentów elektronicznych, w tym dokumentacji medycznej w postaci elektronicznej, przed ryzykiem utraty lub jakiejkolwiek nieupoważnionej zmiany. W efekcie proces przesyłania dokumentów będzie bezpieczny, a nadawca i odbiorca zostaną jednoznacznie wskazani[3]. Należy także odnotować działania związane z cyberbezpieczeństwem[4]. Jest to problematyka, która w krótkim czasie będzie miała bardzo duże

[1] Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2020 poz. 666).
[2] Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz.U. 2020 poz. 2320).
[3] Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz.U. 2020 poz. 2320).
[4] Projekt Rekomendacji Ministra Cyfryzacji dotyczących warunków technicznych i organizacyjnych powierzenia danych administracji publicznej do przetwarzania w publicznej chmurze obliczeniowej (Projekt 2018.07.09).

znaczenie szczególnie w obszarze transmisji danych i przetwarzania danych w chmurach obliczeniowych[5,6].

1. Jednolita Europejska Przestrzeń Danych

Rozwiązania krajowe są uzależnione w dużym stopniu od działalności legislacyjnej Unii Europejskiej (UE). Wśród najistotniejszych regulacji i dokumentów należy wymienić Rozporządzenie w sprawie swobodnego przepływu danych nieosobowych[7], Dyrektywę w sprawie otwartych danych[8], Zalecenia Komisji w sprawie europejskiego formatu wymiany elektronicznej dokumentacji medycznej[9] oraz „Europejską strategię w zakresie danych"[10].

Celem strategii w zakresie danych jest budowa Jednolitej Europejskiej Przestrzeni Danych – wspólnego, otwartego rynku danych, opartego na jasnych zasadach obejmujących:

- swobodny przepływ danych w ramach UE i poza UE, także pomiędzy sektorami;
- pełne poszanowanie dla europejskich praw, zasad i wartości, w szczególności ochrona danych osobowych, ochrona konsumentów i prawo konkurencji;
- sprawiedliwe zasady dostępu do danych i transparentne mechanizmy zarządzania danymi.

We wspomnianej strategii znajduje się odniesienie do medycyny personalizowanej jako jednego z obszarów szczególnie ważnych dla społeczeństwa, w kontekście wykorzystania dużych zbiorów danych. W dokumencie strategii można znaleźć zapis, że: „Medycyna personalizowana będzie lepiej reagować na potrzeby pacjentów, umożliwiając lekarzom podejmowanie trafnych decyzji w oparciu o dane. Umożliwi to dostosowanie właściwej strategii terapeutycznej do potrzeb danej osoby we właściwym czasie, określenie predyspozycji do choroby lub zapewnienie szybkiej i ukierunkowanej profilaktyki"[11].

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Tekst mający znaczenie dla EOG), s. 881.
[6] Chmury obliczeniowe to model, w którym, w czasie rzeczywistym użytkownik dzierżawi zasoby obliczeniowe takie jak pamięć masowa, moc obliczeniowa i inne zasoby sieciowe mając jednocześnie minimalną interakcję z dostawcą.
[7] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej (Tekst mający znaczenie dla EOG).
[8] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego.
[9] Zalecenie Komisji (UE) 2019/243 z dnia 6 lutego 2019 r. w sprawie europejskiego formatu wymiany elektronicznej dokumentacji medycznej (Tekst mający znaczenie dla EOG).
[10] Communication from the Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions A European strategy for data. COM/2020/66 final, s. 66.
[11] European Commission website, „European Data Strategy".

W „Europejskiej strategii zakresie danych" określono cztery najważniejsze filary związane z przetwarzaniem danych[12]:

I Filar – Zarządzanie danymi. Obejmuje takie kwestie jak standardy gromadzenia danych, przejrzyste zasady określające przez kogo, które dane mogą być użyte oraz ułatwienie obywatelom dzielenia się generowanymi przez nich danymi.

II Filar – Rozwój gospodarki opartej na danych. Rozwiązania wdrażane w ramach tego filaru mają na celu budowę europejskich przestrzeni danych i wspólnej infrastruktury chmurowej.

III Filar – Decyzyjność obywateli, kompetencje i wsparcie małych i średnich przedsiębiorstw. Celem tej grupy działań jest zwiększenie uprawnień obywatelom w odniesieniu do podejmowana decyzji w sprawie ich danych osobowych, ale również zapewnienie wpływu na dane nieosobowe np. generowane przez domowe urządzenia Internetu Rzeczy (*ang. Internet of Things, IoT*), w tym urządzenia monitorujące stan zdrowia.

IV Filar – Wspólne europejskie przestrzenie danych. Głównym zadaniem tego filaru jest stworzenie europejskiej infrastruktury dla danych w strategicznych sektorach gospodarki – wśród nich „Wspólną europejskiej przestrzeni danych dla zdrowia" (*ang. A Common European health data space*). Zaplanowano opracowanie narzędzia i architektury umożliwiającej gromadzenie i wykorzystywanie danych, a także dzielenie się nimi pomiędzy sektorami.

Według założeń przestrzenie zostaną zaprojektowane w pełnej zgodności z europejskimi zasadami ochrony danych i najwyższymi standardami bezpieczeństwa teleinformatycznego.

W najbliższym czasie przewiduje się opracowanie w Unii Europejskiej, specyficznych dla sektora ochrony zdrowia środków ustawodawczych i innych rozwiązań potrzebnych do utworzenia i funkcjonowania europejskiej przestrzeni danych dotyczących zdrowia. Ich celem będzie zwiększenie dostępu obywateli do danych dotyczących zdrowia, zagwarantowanie możliwości przenoszenia tych danych oraz likwidacja barier dla transgranicznego oferowania cyfrowych usług i produktów zdrowotnych. Ważnym założeniem strategii jest wprowadzenie zasady przewidującej przyznanie większej decyzyjności obywatelom w odniesieniu do ich danych osobowych. Przewidziano mianowicie utworzenie osobistych przestrzeni danych (*ang.*

[12] European Commission website.

personal data spaces), w których obywatele będą mogli kontrolować swoje dane, a także udzielać zgody na ich wykorzystanie[13].

W związku z tworzeniem europejskiej przestrzeni danych dotyczących zdrowia, przewiduje się wprowadzenie infrastruktury danych oraz zapewnienie odpowiednich narzędzi i zdolności obliczeniowych na potrzeby tego rozwiązania. Mowa przede wszystkim o wsparciu krajowych elektronicznych kart zdrowia oraz interoperacyjność danych dotyczących zdrowia poprzez zastosowanie jednolitego formatu wymiany elektronicznych kart zdrowia. Rozwijana będzie transgraniczna wymiana danych dotyczących zdrowia. Nastąpi połączenie i wykorzystanie za pośrednictwem bezpiecznych, stowarzyszonych repozytoriów, określonych rodzajów informacji dotyczących zdrowia, takich jak elektroniczne karty zdrowia, informacje genomiczne oraz cyfrowe obrazy medyczne.

Strategia przewiduje także zapewnienie dokumentów elektronicznych. Dotyczy to elektronicznych kartotek pacjentów i recept między 22 państwami członkowskimi uczestniczącymi w europejskiej infrastrukturze usług cyfrowych w dziedzinie e-zdrowia (*ang. eHealth Digital Service Infrastructure, eHDSI*),[14,15] a także rozpoczęcie transgranicznej elektronicznej wymiany za pośrednictwem eHDSI obrazów medycznych, wyników badań laboratoryjnych i raportów na zakończenie opieki. Planowane jest rozszerzenie modelu wirtualnych konsultacji oraz rejestrów europejskiej sieci referencyjnej. Będą promowane i wspierane projekty w dziedzinie dużych zbiorów danych wspierające: profilaktykę; diagnostykę i leczenie (w szczególności w odniesieniu do chorób nowotworowych, chorób rzadkich oraz chorób powszechnych i złożonych); badania naukowe i innowacje; oraz kształtowanie polityki i działań regulacyjnych w państwach członkowskich w obszarze zdrowia publicznego[16].

2. Nowa forma Elektronicznej Dokumentacji Medycznej

Rozwój technologii informatycznych wymusza ostatecznie całkowite odstąpienie od tworzenia i prowadzenia dokumentacji w postaci papierowej i przejście do dokumentacji w postaci elektronicznej. W Polsce elektroniczna dokumentacja medyczna jako podstawowa

[13] Communication from the Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions A European strategy for data. COM/2020/66 final, s. 66.
[14] Do 2021 r. te dwa rodzaje usług cyfrowych będą stopniowo wdrażane w 22 krajach UE: w Austrii, Belgii, Chorwacji, na Cyprze, w Czechach, Estonii, Finlandii, Francji, Grecji, Hiszpanii, Holandii, Irlandii, na Litwie, w Luksemburgu, na Malcie, w Niemczech, Polsce, Portugalii, Słowenii, Szwecji, na Węgrzech i we Włoszech.
[15] European Commission website, „Electronic Cross-Border Health Services".
[16] European Commission website, „European Data Strategy".

postać prowadzenia dokumentacji medycznej wprowadziło Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania[17].

Ważnym dokumentem dotyczącym funkcjonowania elektronicznej dokumentacji medycznej są Zalecenie Komisji (UE) 2019/243 z dnia 6 lutego 2019 r. w sprawie europejskiego formatu wymiany elektronicznej dokumentacji medycznej[18]. Określono w nim zasadnicze funkcje, które ma spełniać elektroniczna dokumentacja medyczna. Akceptowany i wdrożony we wszystkich krajach format wymiany elektronicznej dokumentacji medycznej umożliwi jej łatwą wymianę między państwami członkowskimi UE. Poza tym przewidziano zapewnienie możliwości obywatelom UE transgranicznego dostępu do ich elektronicznych danych dotyczących zdrowia oraz bezpiecznego transgranicznego udostępniania tych danych[19]. Docelowo osoby na ternie Unii Europejskiej ma przysługiwać możliwość wyboru, komu udostępnią swoje elektroniczne dane dotyczące zdrowia oraz w jakim zakresie. Co ważne. państwa członkowskie mają za zadanie wprowadzić odpowiednie środki, by wesprzeć stosowanie interpretacyjnych systemów elektronicznej dokumentacji medycznej.

Elektroniczna dokumentacja medyczna powinna być zgodna z zasadami określonymi w załączniku do Zaleceń Komisji. Nadrzędną zasadą przetwarzania danych dotyczących zdrowia zawartych w dokumentacji medycznej jest podstawa prawna lub wyraźna zgoda osoby, której dane są przetwarzane. Każdy kogo dane dotyczą, powinien mieć zagwarantowane wszystkie prawa wynikające z Rozporządzenia o ochronie danych osobowych (RODO)[20], w tym możliwość korzystania z przysługującego mu prawa dostępu do swoich danych dotyczących zdrowia, poprzez wgląd do swojej elektronicznej dokumentacji medycznej, również w wymiarze transgranicznym.

Ponadto elektroniczna dokumentacja medyczna powinna być kompleksowa. Każdy przypadek przetwarzania danych dotyczących zdrowia należy zarejestrować i zweryfikować do celów kontroli, korzystając z odpowiednich technik, takich jak prowadzenie dzienników i

[17] Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2020 poz. 666).
[18] Zalecenie Komisji (UE) 2019/243 z dnia 6 lutego 2019 r. w sprawie europejskiego formatu wymiany elektronicznej dokumentacji medycznej (Tekst mający znaczenie dla EOG).
[19] Zalecenie Komisji (UE) 2019/243 z dnia 6 lutego 2019 r. w sprawie europejskiego formatu wymiany elektronicznej dokumentacji medycznej (Tekst mający znaczenie dla EOG).
[20] 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).

tworzenie ścieżki audytu, na potrzeby prowadzenia dokładnej ewidencji dostępu do dokumentacji elektronicznej, jej wymiany lub jakiejkolwiek innej operacji przetwarzania.

Dane dotyczące zdrowia wprowadzone do elektronicznej dokumentacji medycznej powinny nadawać się do odczytu maszynowego w takim zakresie, w jakim jest to konieczne z uwagi na rozsądne zamierzone ponowne wykorzystanie tych danych. Informacje powinny być usystematyzowane i opatrzone kodami, w jak najbardziej użyteczny sposób tak, aby dane dotyczące zdrowia były interoperacyjne, również na poziomie międzynarodowym. Dodatkowo systemy elektronicznej dokumentacji medycznej muszą gwarantować poufność danych osobowych dotyczących zdrowia i być zgodne ze wszystkimi aspektami przepisów w dziedzinie ochrony danych już od etapu ich opracowywania.

3. Bezpieczeństwo danych o stanie zdrowia

Konieczne jest wdrożenie odpowiednich środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa systemów elektronicznej dokumentacji medycznej. Powinny one uwzględniać ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem danych dotyczących zdrowia oraz przed ich przypadkową utratą, zniszczeniem lub uszkodzeniem. Odpowiednie przygotowanie edukacyjne personelu obsługującego systemy elektronicznej dokumentacji medycznej musi zagwarantować zaistnienie odpowiedniej świadomości zagrożeń dla bezpieczeństwa cybernetycznego.

Ważny problem to solidna i rzetelna identyfikacja i uwierzytelnianie wszystkich zainteresowanych stron (podmiotów medycznych, pacjentów pracowników). Jest to element gwarantujący zaufanie do wymiany danych między systemami elektronicznej dokumentacji medycznej. Państwa członkowskie UE powinny podjąć działania w celu zapewnienia, by następujące dziedziny informacji dotyczących zdrowia stanowiły część europejskiego formatu wymiany elektronicznej dokumentacji medycznej jako informacje podstawowe:

- Kartoteka pacjenta;
- E-recepta/realizacja e-recepty;
- Wyniki badań laboratoryjnych;
- Obrazowanie medyczne i raporty medyczne;
- Wypisy ze szpitala.

Warto zauważyć, że państwa członkowskie zaczęły już udostępniać niektóre elementy elektronicznej dokumentacji medycznej i zapewniać ich wymianę między wybranymi

państwami. Od stycznia 2019 r. obywatele Finlandii mogą przy użyciu elektronicznych recept kupować leki w Estonii, a luksemburscy lekarze wkrótce będą mieli dostęp do kartotek pacjentów z Czech[21].

Ochrona zdrowia to jedna z tych dziedzin, której funkcjonowanie jest związane z szerokim wykorzystaniem Internetu oraz stworzonymi i funkcjonującymi w związku z jego wykorzystaniem chmurami obliczeniowymi. Ocena się, że chmury obliczeniowe będą w niedalekiej przyszłości stanowiły podstawowe miejsce przetwarzania danych w ochronie zdrowia. Wynika to z faktu, że zapewniają one już teraz praktycznie nieograniczone miejsce do przetwarzania i magazynowania danych. Jednak wykorzystywanie tego typu rozwiązań też podlega pewnym ograniczeniom. Największą barierą nie są wymogi technologiczne, ale fakt zróżnicowania przepisów prawnych krajów utrzymujących infrastrukturę chmurową, co powoduje zróżnicowane podejście do danych przetwarzanych w chmurze w zależności od zarejestrowania podmiotów bądź miejsca przetwarzania danych. Podejście do prywatności danych i sposobu dostępu do nich jest zróżnicowane w zależności od kraju, w którym dokonano rejestracji podmiotów posiadających infrastrukturę sieciową, bądź miejsca przetwarzania danych. Szczególnie jest to widoczne w relacjach dotyczących przetwarzania danych osobowych między USA a UE po wyroku uchylającym dotychczas stosowane rozwiązania dwustronne oparte na programie tarczy prywatności (*ang. Privacy Shield).* Program ten miał na celu zagwarantowanie analogiczną do europejskiej, ochronę danych osobowych przetwarzanych przez podmioty amerykańskie. Trybunał Sprawiedliwości Unii Europejskiej stwierdził jednak jego nieważność uzasadniając to faktem, że regulacje amerykańskie zapewniały zbyt łatwy dostęp do danych dla amerykańskich służb[22]. Było to następstwem wejścia w życie w USA legislacji pt. *Clarifying Lawful Overseas Use of Data Act (*potocznie nazywanej „*Cloud Act").*

Regulacja ta daje możliwości amerykańskim organom ścigania dostępu do cyfrowych danych przetwarzanych przez firmy z USA, niezależnie od reżimu prawnego państw, gdzie zlokalizowane są dane, obywatelstwa, w tym miejsca zamieszkania osób, których dane dotyczą. Umożliwia także na zawieranie umów USA z innymi państwami (*ang. executive agreements*) dających tym krajom prawo dostępu do danych osobowych przetwarzanych przez

[21] Gazeta Prawna, „KE chce ułatwić dostęp do dokumentacji medycznej w całej UE".
[22] Sprawa C-311/18: Wyrok Trybunału (Wielka Izba) z dnia 16 lipca 2020 r. - Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems.

amerykańskie podmioty (z wyjątkiem obywateli Stanów Zjednoczonych, gdzie podstawę inwigilacji nadal będzie stanowił nakaz sądowy)[23].

Próbą szybkiego wyjścia z impasu jest inicjatywa GAIA-X – **Europejskie Stowarzyszenie na rzecz Danych i Chmury**[24]**.** Jej celem jest uniezależnienie się od podmiotów amerykańskich i chińskich w zakresie usług chmurowych. GAIA-X jest projektem komercyjnym. Zadaniem projektu jest wsparcie innowacji i transformacji cyfrowej UE. Jego koncepcja ma być oparta na europejskich wartościach i regulacjach dotyczących przetwarzania danych. Docelowo ma być stworzona platforma łącząca usługi chmurowe dziesiątek firm, umożliwiająca usługobiorcom swobodne przenoszenie danych – federacyjne usługi oparte na wspólnych standardach zapewniających przejrzystość i interoperacyjność.

Główne cele projektu GAIA-X to[25]:

- Budowanie wartości usług federacyjnych poprzez oparcie na wspólnych standardach zapewniających przejrzystość i interoperacyjność;
- Integracja dostawców sieci i połączeń międzysystemowych, dostawców rozwiązań chmurowych (ang. *Cloud Service Provider, CSP*);
- Integracja wysokowydajnych mocy obliczeniowych (*ang. High-Performance Computing, HPC*), chmur specyficznych dla sektora i systemów brzegowych;
- Opracowanie mechanizmów wyszukiwania, zestawiania i łączenia usług od uczestniczących dostawców w celu stworzenia przyjaznego dla użytkownika ekosystemu infrastruktury;
- Określenie minimalnych wymagań technicznych i usług niezbędnych do obsługi sfederowanego ekosystemu GAIA-X;
- Rozwój usług zgodnych z zasadami zaaranżowanie bezpiecznej przestrzeni[26] (ang. *Secure by Design*);
- Zapewnienia najwyższych wymagań bezpieczeństwa i ochrony prywatności dzięki koncepcji ochrona danych osobowych już w fazie projektowania (*ang. Privacy by Design*).

[23] P. Opitek, „Clarifying Lawful Overseas Use Data Act – nowy model pozyskiwania danych cyfrowych w sprawach karnych", *BRIEF PROGRAMOWY INSTYTUTU KOŚCIUSZKI*, 2018, s. 6.
[24] GAIA-X została ustanowiona jako podmiot prawny wraz z końcem stycznia 2021 roku. Organizacja posiada teraz osobowość prawną jako międzynarodowe stowarzyszenie non-profit podlegające prawu belgijskiemu (AISBL).
[25] „GAIA-X: A Federated Data Infrastructure for Europe".
[26] *Secure by design* – program, którego naczelnym założeniem jest odpowiednie zaaranżowanie przestrzeni jeszcze w fazie projektu tak

Do zadań stowarzyszenia GAIA-X należy stworzenie warunków ramowych w następujących obszarach: architektura, interfejsy, klasyfikacja danych, procesy między zaangażowanymi stronami, interoperacyjność i łączność[27]. Oznacza to, że w stosunkowo krótkim czasie wszystkie dane, w tym dotyczące zdrowia, przetwarzane będą w krajach członkowskich w chmurze zlokalizowanej w Europie, zapewniającej przestrzeganie obowiązujących tu zasad prawnych.

Warto zauważyć, że część krajów azjatyckich wdraża rozwiązania zbliżone do RODO. Przykładem może być Japonia[28], która znowelizowała swoją ustawę o ochronie danych osobowych (*ang*. *Protection of Personal Information Act*), która obowiązuje tam od 2005 r[29].

Zapewnienie bezpieczeństwa danych o stanie zdrowia jest jednym z kluczowych wyzwań zarówno w Polsce, jak i krajach UE. W Polsce do końca września 2020 roku odnotowano ponad 90 incydentów związanych z bezpieczeństwem danych. Pojawiają się doniesienia o odkryciu kilku groźnych podatności w urządzeniach medycznych różnych producentów. Dotyczyło to m.in. urządzeń regulujących pracę serca jednej z amerykańskich firm, które miały luki w protokołach służących do radiowej transmisji danych (*ang. Radio-Frequency Identification, RFID*). Dane można było „podsłuchać" z niewielkiej odległości. Podatności wykryto również w urządzeniach przeznaczonych do zabiegów elektrochirurgicznych tej samej firmy oraz aparaturze anestezjologicznej innego producenta. O ile kradzież środków z konta czy zaszyfrowanie istotnych danych może być problematyczne, o tyle niekontrolowana zmiana parametrów pracy urządzenia medycznego może doprowadzić do utraty zdrowia lub życia pacjentów, którzy obok personelu medycznego stanowią najistotniejszą grupę użytkowników tych urządzeń. Incydenty cyberbezpieczeństwa mogą skutecznie uniemożliwić przeprowadzanie planowanych operacji, czy zagrozić prywatności danych pacjentów. Jak nie dopuścić do ataków i co robić w momencie ich wystąpienia - zaleca Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (*ang. European Union Agency for Cybersecurity, ENISA*)[30].

Na poziomie UE aktem prawnym określającym zasady bezpieczeństwa przetwarzania danych w chmurze jest Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego, wspólnego poziomu bezpieczeństwa sieci

[27] Kancelaria Prezesa Rady Ministrów, „Federacja Chmur Obliczeniowych - podsumowanie spotkania - Cyfryzacja KPRM - Portal Gov.pl".
[28] Od 23 stycznia 2019 r. zaczęła obowiązywać decyzja Komisji Europejskiej stwierdzająca adekwatny stopień ochrony danych osobowych w Japonii do systemu obowiązującego w państwach należących do Europejskiego Obszaru Gospodarczego.
[29] E. Woollacott, „Changes to Japan's Data Privacy Law Echo Europe's GDPR".
[30] NASK, „Cyberbezpieczeństwo w ochronie zdrowia – kluczowe dla zdrowia i życia pacjentów".

i systemów informatycznych na terytorium Unii[31]. Przepisy zawarte w tej dyrektywie ustanawiają:

- obowiązki dla wszystkich państw członkowskich dotyczące przyjęcia krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych;
- grupy współpracy i zespołów reagowania na incydenty bezpieczeństwa komputerowego;
- wymogi bezpieczeństwa i zgłaszania incydentów dla operatorów usług kluczowych i dostawców usług cyfrowych, a także obowiązki dla państw członkowskich dotyczące wyznaczania właściwych organów krajowych, pojedynczych punktów kontaktowych oraz sieci zespołów reagowania[32].

W celu wdrożenia w Polsce wyżej omawianej dyrektywy uchwalono stawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[33]. Polski system ochrony zdrowia dosyć sprawnie implementuje założenia procesu cyfryzacji – przykładowo brytyjski system z dużo większą ostrożnością podchodzi do przekazywania danych pacjentów serwerom zewnętrznym. W Polsce przekazywanie danych osobowych zawartych w dokumentacji medycznej do chmury przez przychodnie czy szpitale jest już praktycznie powszechną praktyką[34].

Podsumowanie

Jesteśmy świadkami reorganizacji systemów przetwarzających dane elektroniczne w różnych sektorach. Zbiory danych dają początek innowacjom i umożliwiają monitorowanie wielu ważnych obszarów w tym zdrowia populacji. Modyfikacje tak skomplikowanych systemów są możliwe tylko dzięki wprowadzeniu odgórnych wytycznych legislacyjnych. Głowna postępującą zmianą jest standaryzacja elektronicznych systemów przetwarzania danych, po to, aby różni uczestnicy mogli swobodnie, bez barier przesyłać dane (np. pomiędzy krajami) – koncepcja Jednolitej Europejskiej Przestrzeni Danych. Jednak chcąc wprowadzić takie zmiany nie wolno zapominać o cyberbezpieczeństwie, dlatego konieczne jest wdrożenie odpowiednich środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa systemów – dobrym przykładem jest inicjatywa GAIA-X.

[31] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.
[32] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560).
[33] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560).
[34] M. Wach, M. Puto, „Dane medyczne w chmurze – przyszłość czy rzeczywistość".

Potrzebne są dalsze badania w kierunku oceny efektywności wprowadzanych rozwiązań za równo na szczeblu krajowym jak i europejskim.

Literatura

[1] Communication from the Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions A European strategy for data. COM/2020/66 final (2020).
[2] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (b.d.).
[3] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (b.d.).
[4] European Commission website. „Electronic Cross-Border Health Services". Public Health - European Commission, 17 styczeń 2019. https://ec.europa.eu/health/ehealth/electronic_crossborder_healthservices_en.
[5] „European Data Strategy". European Commission. Udostępniono 5 marzec 2021. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.
[6] „GAIA-X: A Federated Data Infrastructure for Europe". Udostępniono 5 marzec 2021. https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html.
[7] Gazeta Prawna. „KE chce ułatwić dostęp do dokumentacji medycznej w całej UE", 6 luty 2019. https://serwisy.gazetaprawna.pl/zdrowie/artykuly/1396362,ke-chce-ulatwic-dostep-do-dokumentacji-medycznej-w-calej-ue.html.
[8] Kancelaria Prezesa Rady Ministrów. „Federacja Chmur Obliczeniowych - podsumowanie spotkania - Cyfryzacja KPRM - Portal Gov.pl". Cyfryzacja KPRM, 31 sierpień 2020. https://www.gov.pl/web/cyfryzacja/federacja-chmur-obliczeniowych---podsumowanie-spotkania.
[9] NASK. „Cyberbezpieczeństwo w ochronie zdrowia – kluczowe dla zdrowia i życia pacjentów". NASK. Udostępniono 5 marzec 2021. https://www.nask.pl/pl/aktualnosci/3988,Cyberbezpieczenstwo-w-ochronie-zdrowia-kluczowe-dla-zdrowia-i-zycia-pacjentow.html.
[10] Opitek P., „Clarifying Lawful Overseas Use Data Act – nowy model pozyskiwania danych cyfrowych w sprawach karnych", *BRIEF PROGRAMOWY INSTYTUTU KOŚCIUSZKI*, 2018, s. 6.
[11] Projekt Rekomendacji Ministra Cyfryzacji dotyczących warunków technicznych i organizacyjnych powierzenia danych administracji publicznej do przetwarzania w publicznej chmurze obliczeniowej (Projekt 2018.07.09) (b.d.).
[12] Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2020 poz. 666) (b.d.).
[13] 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) (b.d.).

[14] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej (Tekst mający znaczenie dla EOG) (b.d.).
[15] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Tekst mający znaczenie dla EOG) (b.d.).
[16] Sprawa C-311/18: Wyrok Trybunału (Wielka Izba) z dnia 16 lipca 2020 r. - Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems. (b.d.). http://curia.europa.eu/juris/liste.jsf?num=C-311/18.
[17] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560) (b.d.).
[18] Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz.U. 2020 poz. 2320) (b.d.).
[19] Wach M., Puto M. „Dane medyczne w chmurze – przyszłość czy rzeczywistość". *Cloud Community Europe Polska* (blog), 4 czerwiec 2020. https://cloudeurope.pl/dane-medyczne-w-chmurze/.
[20] Woollacott E. „Changes to Japan's Data Privacy Law Echo Europe's GDPR". The Daily Swig | Cybersecurity news and views, 10 październik 2020. https://portswigger.net/daily-swig/changes-to-japans-data-privacy-law-echo-europes-gdpr.
[21] Zalecenie Komisji (UE) 2019/243 z dnia 6 lutego 2019 r. w sprawie europejskiego formatu wymiany elektronicznej dokumentacji medycznej (Tekst mający znaczenie dla EOG) (b.d.).

Streszczenie

Dane o stanie zdrowia ze względu na swoją specyficzność i ważność są regulowane w wielu prawno-strategicznych dokumentach. Wdrożenie Koncepcji Jednolitej Europejskiej Przestrzeni Danych daje możliwość wymiany danych pomiędzy krajami pozostając tym samym transparentna i z prawem użytkowników do zarządzania własnymi informacji. Dane dotyczące zdrowia wprowadzone do elektronicznej dokumentacji medycznej powinny nadawać się do odczytu maszynowego w takim zakresie, w jakim jest to konieczne z uwagi na ponowne wykorzystanie tych danych. W odpowiedzi na rozwiązania cyberbezpieczeństwa z innych krajów UE zainicjowała projekt GAIA-X, celem uniezależnienie się od podmiotów amerykańskich i chińskich w zakresie usług chmurowych. Zadaniem projektu jest przede wszystkim wsparcie innowacji i transformacji cyfrowej na terenie UE.

Słowa kluczowe

dane zdrowotne, dokumentacja medyczna, przestrzeń danych, cyberbezpieczeństwo, jednolity rynek cyfrowy