Dr Artur Romaszewski
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych
artur.romaszewski@uj.edu.pl

Dr hab. med. Wojciech Trąbka
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych
wojciech.trabka@uj.edu.pl

Mgr Mariusz Kielar
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych
mariusz.kielar@uj.edu.pl

Mgr Krzysztof Gajda
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych
krzysztof.gajda@uj.edu.pl

CHMURY OBLICZENIOWE W PRZETWARZANIU DOKUMENTACJI MEDYCZNEJ W POSTACI ELEKTRONICZNEJ

Wstęp

Implementacja nowoczesnych rozwiązań informatycznych w systemie ochrony zdrowia wymaga przestrzegania standardów dotyczących bezpiecznego przetwarzania danych w podmiotach opieki zdrowotnej. Jednym z dostępnych narzędzi w tym zakresie może być technologia tzw. chmury obliczeniowej. W obszarze stosowania rozwiązań chmurowych w przetwarzaniu danych w ochronie zdrowia z jednej strony obserwujemy entuzjazm związany z wieloma zaletami tych rozwiązań, z drugiej jednak strony podkreśla się liczne trudności związane przede wszystkim z problemami:

- zróżnicowanej interpretacji przepisów prawnych, w tym różnicy stanowisk różnych organów państwa, w interpretacji dopuszczalności stosowania rozwiązań chmurowych,
- ochrony prywatności, w tym ochrona danych osobowych, w szczególności danych o stanie zdrowia,
- konsekwencji przetwarzania danych za granicą w związku z faktem, że Internet nie

uwzględnia granic państwowych, a przepisy prawne państw różnicują przetwarzanie danych osobowych,

- braku informacji o podwykonawcach usług w chmurze,
- zmian właścicielskich dostawców usług chmurowych
- zabezpieczenia ciągłości działania, zgodność z międzynarodowymi standardami, itp.

W wielu publikacjach dotyczących chmur obliczeniowych pojawia się ich podział ze względu na grono użytkowników mających dostęp do zasobów określonej chmury. Wyodrębnia się podział chmur na publiczną, prywatną, wspólnotową, hybrydową oraz osobistą[1]. Istotne jest przy tym, żeby każdy typ chmury zapewniał warunki niezbędne do funkcjonowania publicznej chmury obliczeniowej:

- pula zasobów — dostępna dla każdego zarejestrowanego użytkownika
- wirtualizacja — efektywne wykorzystanie sprzętu
- elastyczność — dynamiczne skalowanie bez wydatków inwestycyjnych
- automatyzacja — budowanie, wdrażanie, konfiguracja, zabezpieczanie i przenoszenie bez konieczności ręcznej interwencji
- naliczanie opłat — model biznesowy zależny od realnego zużycia: nie płacisz za niewykorzystane zasoby.

W przypadku chmur prywatnych bez zmian obowiązują trzy zasady dotyczące kwestii technicznych: wirtualizacja, elastyczność i automatyzacja. Dwie pozostałe — pula zasobów i naliczanie opłat — są związane z atrybutami biznesowymi chmury publicznej i nie mają bezpośredniego przełożenia na chmurę prywatną. Chmury prywatne z definicji nie są pulą zasobów obliczeniowych dostępnych na żądanie dla wszystkich zapisanych użytkowników.

Chmury prywatne to wariant chmur obliczeniowych, w których wewnętrzne zasoby firmy, tj. jej centrum danych, nie są udostępniane publicznie. Pula zasobów jest kontrolowana przez daną organizację i dostępna jedynie dla jej członków. Chmura prywatna różni się tym od chmury publicznej, że pula zasobów obliczeniowych nie jest dostępna użytkownikom

[1] Reczek E., *Zastosowanie chmury obliczeniowej w sektorze ochrony zdrowia*. Zeszyt Naukowy - Wyższa Szkoła Zarządzania i Bankowości w Krakowie 2014 nr 33

zewnętrznym (podmiotom spoza firmy będącej właścicielem centrum danych oraz dostępnej w nim mocy obliczeniowej)[2].

Chmura hybrydowa to połączenie dwóch modeli *cloud computing*: wydajnej, sprawnie działającej chmury zewnętrznej i sieci własnej. Oznacza to środowisko *cloud computing*, w którym firma dostarcza i zarządza zasobami wewnątrz organizacji, a inne usługi są do niej dostarczane przez zewnętrznego *providera*. W praktyce takie połączenie polegać może na korzystaniu z *public cloud*, ale trzymaniu danych (np. danych pacjentów) we własnej bazie. O ile *cloud computing* jest uważany za przyszłość przedsiębiorstw, to właśnie model hybrydowy ma być najpopularniejszy. Duże korporacje już mają poczynione znaczące inwestycje w infrastrukturę potrzebną im w celu zarządzania zasobami wewnątrz korporacji. Poza tym wiele organizacji woli trzymać dane specjalne pod własną kontrolą ze względów bezpieczeństwa.

Poprzez integrowanie wielu usług chmurowych użytkownicy mogą łatwiej przechodzić do usług chmury zewnętrznej unikając każdorazowo kwestii zgodności czy autoryzacji dostępu. Hybryda jest zarządzana równolegle, zgodnie z ich kompetencjami, przez dostawcę wewnętrznego i zewnętrznego[3].

W dokumencie „Chmura obliczeniowa – Ekspertyza Komisji Rynku Wewnętrznego i Ochrony Konsumentów Parlamentu Europejskiego możemy znaleźć definicję zarówno chmury prywatnej, jak i chmury osobistej[4]. To ostatnie rozwiązanie może w praktyce mieć formę małego serwera w domu lub niewielkiej sieci komercyjnej, do której dostęp można uzyskać za pośrednictwem Internetu. Zaprojektowane w celu przechowywania i wymiany treści prywatnych chmury osobiste umożliwiają przeglądanie i przesyłanie danych z dowolnego komputera osobistego podłączonego do Internetu, a często również z popularnych smartfonów. Chociaż chmury osobiste funkcjonują w sposób podobny do każdej chmury prywatnej stworzonej przez przedsiębiorstwo, ich główną cechą jest łatwa instalacja dla przeciętnego użytkownika komputera osobistego. Powstaje tylko pytanie czy mały lub średni podmiot leczniczy będzie w stanie na bieżąco dostosowywać zainstalowane w chwili tworzenia systemu narzędzia służące do zabezpieczenia do bieżącej sytuacji.

Jaka chmura obliczeniowa?

[2] Mateos A., Rosenberg J., *Chmura obliczeniowa. Rozwiązania dla biznesu*. Wydawnictwo Helion

[3] http://computingcloud.pl/pl/cloud-przewodnik/219-chmura-prywatna-publiczna-a-moze-hybrydowa

[4] http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_PL.pdf

W publikacjach dotyczących zastosowania rozwiązań chmurowych w podmiotach leczniczych bardzo często pojawia się sugestie, że zastosowanie chmur prywatnych jest jedyną dopuszczalną formą wykorzystania tego typu rozwiązań w przypadku przetwarzania danych o stanie zdrowia. Argumentacja dopuszczalności tego rozwiązania, jako jedynego dopuszczalnego opiera się na fakcie, że tylko takie rozwiązanie umożliwia odpowiednie uwzględnienie w obszarze przetwarzania danych przewidzianym w przepisach obszaru chmury obliczeniowej innej, niż prywatna. Obszar ten należy wskazać w polityce bezpieczeństwa, a tworzy go wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.[5] Oczywiście trzeba pamiętać, że regulujące te kwestie rozporządzenie zostało wprowadzone w życie we wczesnej fazie funkcjonowania w Polsce Internetu[6]. Jego literalna interpretacja uniemożliwia również wykorzystywanie laptopów, tabletów i innych mobilnych urządzeń wykorzystywanych do przetwarzania danych w podmiotach świadczących usługi zdrowotne, jeżeli przetwarzanie danych odbywa się poza ściśle zdefiniowanym obszarem przetwarzania danych.

Od początku rozpoczęcia usług chmurowych w ochronie zdrowia podkreślano, że w zasadzie dane o stanie zdrowia mogą być przetwarzane w obszarach kontrolowanych przez podmioty mające prawo do przetwarzania danych o stanie zdrowia. Przy takim poglądzie dopuszczalne były z zasadzie chmury prywatne (z możliwością stosowania serwerów poza obszarem podmiotu) leczniczego. Zakładano, że chmury publiczne są zbytnio narażone na wszelkie ataki lub błędy powodujące nieuprawniony dostęp do danych lub ich utratę. Mimo tego w placówkach ochrony zdrowia brakuje stosownych procedur wewnętrznych mających na celu ochronę systemów informatycznych, a to z kolei jest bezpośrednią przyczyną niewystarczającego zabezpieczenia wrażliwych danych pacjentów. Jednym z rozwiązań mogących zmienić ten stan rzeczy jest podjęcie decyzji o przeniesieniu całości lub części danych poza obszar swoich systemów informatycznych, przede wszystkim do chmur obliczeniowych. Pozostaje kwestia prawnej dopuszczalności przeniesienia danych i informacji

[5]§ 4. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych

[6] Pierwszy portal internetowy autorstwa Polaków zadebiutował w 1995 roku. Była to Wirtualna Polska. W kwietniu 1996 roku Telekomunikacja Polska uruchomiła dostęp anonimowy do internetu przez modemy. W początkowym okresie w Polsce prasa uznawała internet za narzędzie nieprofesjonalne, nieciekawe oraz zbyt kosztowne - https://pl.wikipedia.org/wiki/Internet_w_Polsce

o stanie zdrowia do zasobów pozostających poza bezpośrednią kontrola administratora, a więc przede wszystkim do chmur obliczeniowych.

Wybór dostawcy usług chmurowych to stosunkowo skomplikowane zagadnienie. Ponieważ w Polsce obowiązuje zasada neutralności technologicznej państwa tzn., że wszystkie podmioty mogą świadczyć usługi, natomiast rolą państwa jest takie przygotowanie i opublikowanie rozwiązań technologicznych przede wszystkim poprzez wskazanie odpowiednich standardów i norm, aby w rezultacie zapewnić interoperacyjność tworzonych systemów. Aby skutecznie oferować usługi w modelu chmurowym trzeba dysponować nie tylko odpowiednimi kompetencjami, produktami, infrastrukturą, ale przede wszystkim skalą, czyli potencjałem organizacyjnym i finansowym.

Takim atutem dysponują firmy działające w skali globalnej, które ze względu na atrakcyjność potencjalnego rynku, w pierwszej kolejności starają sprostać wytycznym Komisji Europejskiej. Przykładem jest chociażby firma Microsoft. Inspektorzy ochrony danych osobowych z 28 krajów Unii Europejskiej (UE) – tzw. Grupa Robocza Art. 29 (w tym polski Generalny Inspektor Ochrony Danych Osobowych), którzy kontrolują firmy prowadzące działalność biznesową na terenie Unii Europejskiej opublikowali wspólne stanowisko, wyrażając swoje poparcie dla prawidłowych rozwiązań kontraktowych firmy Microsoft w zakresie usług chmurowych dla biznesu. W skrócie, w tym konkretnym przypadku dla usługobiorców oznacza to aprobatę unijnego regulatora dla podejścia Microsoftu do ochrony prywatności i bezpieczeństwa danych obywateli europejskich.

Omawiane powyżej problemy zostały stały się przedmiotem regulacji UE, co zaowocowało uchwaleniem w 2016 r. Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji na terytorium Unii (dyrektywa NIS). Państwa UE zostały zobligowane do opracowania krajowych strategii bezpieczeństwa cybernetycznego, zidentyfikowania operatorów tzw. kluczowej infrastruktury (m.in. szpitali) oraz zbudowania krajowych systemów reagowania na cyberataki opartych o Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego. Zakres Dyrektywy NIS ogranicza się do dwóch typów podmiotów: tzw. operatorów usług kluczowych (przedsiębiorców z sektorów energetyki, transportu, bankowości i infrastruktury rynków finansowych, służby zdrowia, zaopatrzenia w wodę pitną, infrastruktury cyfrowej) oraz dostawców usług cyfrowych (internetowych platform handlowych, wyszukiwarek internetowych, usług przetwarzania w chmurze).

Wybór operatorów usług kluczowych zależy tylko od państwa członkowskiego i będzie dokonany albo razem z implementacją Dyrektywy NIS albo bezpośrednio po niej. Nie wiadomo, o które usługi chodzi – każdy kraj musi stworzyć listę usług kluczowych dla każdego sektora wymienionego w dyrektywie.

Wybrane podmioty będą miały głównie dwa obowiązki. Pierwszy nakazuje wprowadzenie środków ochrony (technicznych i organizacyjnych) zależnych od poziomu ryzyka, które być może będzie wyznaczane również przez urzędników. Drugi to konieczność raportowania incydentów[7]. Dyrektywa dotyczy trzech rodzajów dostawców usług cyfrowych: platform handlowych, wyszukiwarek internetowych i usług przetwarzania danych w chmurze. Ponieważ są to operatorzy międzynarodowi zadecydowano, że będą wyznaczeni przez Unię Europejską i podobnie jak w przypadku operatorów usług kluczowych, będą musieli zapewnić poziom bezpieczeństwa zależnie od zidentyfikowanego ryzyka[8] i ogólne rozporządzenie o ochronie danych przewiduje zaostrzone obowiązki podmiotów administrujących danymi oraz je przetwarzającymi (np. szpitali) w zakresie ochrony przechowywanych danych osobowych. Brak adekwatnych do stopnia zagrożenia zabezpieczeń będzie mógł być podstawą do nałożenia przez Głównego Inspektora Ochrony Danych Osobowych surowych kar pieniężnych wynoszących w zależności od rodzaju naruszenia do 10 albo 20 milionów euro, a w przypadku przedsiębiorstwa – 2% albo 4% całkowitego rocznego przychodu w poprzednim roku obrotowym. Państwa unijne mają implementować dyrektywę NIS do 2018 r.

Korzystanie z usług chmurowych może wiązać się z pewnym ryzykiem, np. dotyczącym bezpieczeństwa danych. Pewną pomocą w tym względzie może być norma ISO/IEC 27018:2014, która bazuje na starszej wersji ISO 27001. We wspomnianych regulacjach normalizacyjnych (ISO/IEC 27018:2014 oraz w pierwotnej normie ISO 27001) poruszane są przede wszystkim zagadnienia związane z:

- polityką bezpieczeństwa
- organizacją bezpieczeństwa informacji

[7] Postepowanie w razie incydentów bezpieczeństwa komputerowego opisano normą NIST 800-61 opracowaną przez Narodowy Instytut Standardów i Technologii przy amerykańskim Departamencie Handlu

[8] Grzybowski M., *Dziewięć faktów o Dyrektywie NIS, które powinieneś znać*, https://www.cybsecurity.org/9-faktow-o-dyrektywie-nis-ktore-powinienes-znac/

- bezpieczeństwem zasobów ludzkich
- zarządzaniem aktywami
- kontrolą dostępu
- kryptografią i szyfrowaniem danych wrażliwych
- bezpieczeństwem fizycznym i środowiskowym
- zarządzaniem operacyjnym
- komunikacją i transportem danych w kontekście bezpieczeństwa
- współpracą z dostawcami
- zarządzaniem incydentami związanymi z bezpieczeństwem informacji
- aspektami bezpieczeństwa informacji w zarządzaniu ciągłością działania
- zgodnością z normami krajowymi.

Według wspomnianej normy założenia dla użytkownika usług chmurowych to między innymi transparentność usługi z punktu widzenia użytkownika, ustalenie jasnych standardów w zakresie praw i obowiązków dostawcy usług i użytkownika, a także wdrożenie podstawowych zasad umożliwiających przetwarzanie danych przy zapewnieniu zgodności z obowiązującym prawem.

Dostawcy, którzy chcieliby wdrożyć normę ISO/IEC 27018:2014, powinni przede wszystkim zapewnić użytkownikom (pracownikom) kontrolę nad przetwarzaniem ich danych. Do obowiązków dostawców usług chmurowych należy też zapewnienie ograniczeń w ujawnianiu i dostępie do danych ze strony podmiotów trzecich np. podwykonawców (w tym obowiązek zapewniania poufności i obowiązek ujawnienia podwykonawców użytkownikom). Powołana wyżej norma wymaga również przejrzystości w sprawie wniosków organów państwowych, np. prokuratury i sądów o ujawnienie danych osobowych. Zarejestrowane dane użytkowników mogą być ujawnione takim organom wyłącznie wtedy, gdy dostawca zostanie do tego prawnie zobowiązany. Na podstawie materiału[9] GIODO opracował dokument o nazwie „Dekalog chmuroluba",[10] gdzie można znaleźć wytyczne dotyczące bezpieczeństwa danych w przechowywanych w chmurach. Inną kwestią jest sam format zapisu danych w chmurach obliczeniowych.

[9] Segalis B., *Cloud Computing Legal Risk and Liability*, InfoLawGroup 2011
[10] http://www.giodo.gov.pl/259/id_art/6271/j/pl

Prawne standardy skierowane po wszystkich podmiotów realizujących zadania publiczne zawarte zostały w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[11]. Zgodnie z treścią rozporządzenia wszystkie dane wygenerowane przez system informatyczny (w tym podmiotów leczniczych) powinny być zapisane w formacie XML. W tej sytuacji dane wysyłane do chmur obliczeniowych, jak i dane uzyskane (pobrane) z chmury, powinny zapewnić taki format zapisu danych, co wiąże również się z zapewnieniem możliwości wymiany danych medycznych np. poprzez HL7. Nie ma jednak w dokumentacji norm i standardów precyzyjnego określenia, w jakim formacie dane będą przechowywane w chmurach. Pierwszym podmiotem, który oficjalnie wdrożył normę ISO/IEC 27018:2014 jest Microsoft.

Transgraniczny transfer danych medycznych

Przy zawieraniu umowy o powierzenie, a w szczególności z wykorzystaniem zasobów chmurowych, powinno uwzględniać się obowiązujące zasady transferu danych osobowych. Generalnie zasadą jest, że przepływ danych w obrębie Europejskiego Obszaru Gospodarczego jest traktowany tak samo, jak transfer danych na terytorium Polski. Zasada ta dotyczy wszystkich państw członkowskich Unii Europejskiej oraz tych państw członkowskich Europejskiego Obszaru Gospodarczego, które nie są członkami UE (obecnie to: Norwegia, Islandia i Lichtenstein). Innym słowy zawieranie umów z dostawcą usług, który swoje systemy wykorzystywane do realizowania usług ma zlokalizowane na obszarze Europejskiego Obszaru Gospodarczego jest zgodne z prawem i nie wymaga oddzielnych pozwoleń.

Do pozostałych krajów można przekazywać dane, jeżeli zapewnia one odpowiedni poziom ochrony. Ze względu na duże zróżnicowanie krajowych systemów ochrony danych osobowych Grupa Robocza wskazała trzy cechy, które te systemy powinny spełniać w zakresie środków pozwalających na realizację zasad przetwarzania danych osobowych, a zatem system ten powinien zapewniać wysoki poziom zgodności z zasadami przetwarzania danych osobowych (powinien być on efektywny oraz zapewniać wysoki poziom świadomości swych obowiązków przez administratorów danych). System ten także powinien umożliwiać dochodzenie swoich praw przez poszczególne osoby, których dane dotyczą, co oznacza

[11] http://dziennikustaw.gov.pl/du/2016/113/D2016000011301.pdf

konieczność istnienia mechanizmów zapewniających niezależne rozpatrywanie skarg. System powinien również zapewniać możliwość dochodzenia odpowiedniego odszkodowania w razie naruszenia zasad przetwarzania danych osobowych.

Jest również dopuszczalne przekazywanie danych osobowych do państwa trzeciego, które nie zapewnia odpowiedniej ochrony danych osobowych jest możliwe pod warunkiem spełnienia jednej z przesłanek określonych w ustawie:[12]

- osoba, której dane dotyczą wyraziła pisemną zgodę;
- przekazanie jest niezbędne do wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą, lub jest podejmowane na jej życzenie;
- przekazanie jest niezbędne do wykonania umowy zawartej w interesie osoby, której dane dotyczą, pomiędzy administratorem danych a innym podmiotem;
- przekazanie jest niezbędne ze względu na dobro publiczne lub do wykazania zasadności roszczeń prawnych;
- przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą;
- dane są ogólnie dostępne.

Jeżeli nie zostały spełnione przesłanki ustawy, a państwo docelowe nie zapewnia odpowiednich standardów ochrony, przekazanie danych może mieć miejsce po uzyskaniu zgody Generalnego Inspektora, pod warunkiem, że administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą

Należy podkreślić, że rozpoczęcie przekazywania danych osobowych do państwa trzeciego, które nie zapewnia odpowiednich gwarancji ochrony danych osobowych jest zasadniczo dopiero po wydaniu pozytywnej decyzji przez Generalnego Inspektora. Decyzja ta nie legalizuje bowiem wcześniejszego przekazywania danych osobowych.

[12] W art. 47 ust. 2 i 3 ustawy o ochronie danych.

Zgoda Generalnego Inspektora nie jest jednak wymagana, jeżeli administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą, przez:

- standardowe klauzule umowne ochrony danych osobowych, zatwierdzone przez Komisję Europejską[13]
- wiążące reguły korporacyjne, które zostały zatwierdzone przez Generalnego Inspektora[14].

Nie istnieje obowiązek posługiwania się standardowymi klauzulami. Obecnie, administrator danych osobowych, który posłuży się modelowymi klauzulami umownymi, uznanymi na mocy decyzji Komisji Europejskiej za instrument chroniący w odpowiednim stopniu prawa i wolności osoby, której dane dotyczą, zwolniony jest z obowiązku wystąpienia do GIODO z wnioskiem o wyrażenie zgody na przekazanie danych. Dotychczas Komisja wydała trzy decyzje zawierające zestawy standardowych klauzul. Dwa pierwsze zestawy dotyczą transferu danych pomiędzy administratorami danych (*controller to controller*). Klauzule wprowadzone na podstawie trzeciej decyzji znajdują zastosowanie przy przekazywaniu danych podmiotowi przetwarzającemu dane osobowe na zlecenie (*controller to processor*). Modelowe klauzule mogą stanowić część szerszej umowy transferowej zawartej pomiędzy administratorem danych a odbiorcą lub mogą być zawarte w aneksie do umowy[15].

Zgoda GIODO nie będzie wymagana, gdy administrator oprze transfer danych o zatwierdzone przez GIODO, prawnie wiążące zasady ochrony danych osobowych zwane „wiążącymi regułami korporacyjnymi”**.** Są one instrumentem o charakterze prywatnoprawnym, który ma zagwarantować jednolity, wysoki poziom ochrony praw osób, których dane dotyczą w ramach ich przekazywania w ranach grupy przedsiębiorstw, rekompensując braki w zakresie ochrony danych osobowych na terytorium poszczególnych państw. Przyjęcie takich reguł do stosowania przez całą korporację będzie oznaczało, że wszyscy administratorzy danych należący do tej grupy kapitałowej będą mogli przekazywać między sobą dane osobowe bez uzyskiwania odrębnych zgód GIODO, jeżeli stosują te reguły.

[13] zgodnie z art. 26 ust. 4 Dyrektywy
[14] zgodnie treścią art. 48 ust. 2 ustawy o ochronie danych osobowych,
[15] Wronka K., *Modelowe klauzule umowne, a ochrona danych* http://prawoitechnologia.pl/aktualnosci/dane-osobowe/modelowe-klauzule-umowne-a-ochrona-danych-osobowych.html

Na tej podstawie, dozwolone będzie również przekazanie tych danych podmiotowi przetwarzającemu dane na zlecenie administratora. Może się to odbyć wyłącznie na podstawie pisemnej umowy pomiędzy administratorem oraz „podwykonawcą". Przetwarzanie danych przez ten podmiot może służyć jedynie dla celów wskazanych w umowie. Nie można zapomnieć o tym, że administrator wciąż pozostaje odpowiedzialnym za ochronę przetwarzanych danych. Obecnie, Generalny Inspektor Danych Osobowych zatwierdza uprzednio korporacyjne reguły w zakresie ochrony danych osobowych, co powoduje, że w przypadku planowanego transferu nie ma konieczności ubiegania się o zgodę[16].

Podsumowanie

Wydaje się, że wejście chmury, jako powszechnego mechanizmu przetwarzania danych o stanie zdrowia to tylko kwestia czasu. Z uwagi na to, że większość środowiska osób świadczących usługi lecznicze nie ma przygotowania techniczno-informatycznego do oceny oferowanych rozwiązań dostawców usług chmurowych zdaniem Autorów powinien włączyć się Minister Zdrowia. Powinien przygotować odpowiednie zapisy w akcie prawnym, które wskażą, jakie standardy muszą spełniać dostawcy usług chmurowych, żeby mogli zajmować się przetwarzaniem danych związanych ze stanem zdrowia oraz innych danych wrażliwych takich, jak np. dane genetyczne.

Z drugiej strony firmy zajmujące się dostarczaniem usług opartych na przetwarzaniu w chmurze powinny dążyć do zachowania przejrzystości swoich działań w zakresie prywatności, udostępniania klientom możliwości wyboru opcji związanych z ochroną prywatności oraz odpowiedzialnego zarządzania przechowywanymi danymi. Jako gwarancję tych działań przyjmuje się odpowiednie procedury oraz politykę bezpieczeństwa wdrożone po stronie usługodawcy potwierdzone niezależnymi certyfikatami (np. zgodności z normą 27001/27002: 2013), która jest powszechnie stosowaną międzynarodową normą dotyczącą zarządzania bezpieczeństwem informacji, ISO/IEC 27018 w aspekcie ochrony danych PII czy *atestCloud SecurityAlliance* [CSA] *Cloud ControlsMatrix* [CCM] opisujący podstawowe zasady

[16] Wronka K., *Wiążące reguły korporacyjne w świetle nowelizacji ustawy o ochronie danych* http://prawoitechnologia.pl/aktualnosci/dane-osobowe/wiazace-reguly-korporacyjne-w-swietle-nowelizacji-ustawy-o-ochronie-danych-osobowych.html

zabezpieczeń, którymi powinni kierować się dostawcy) oraz procedurami audytorskimi zgodnymi ze światowymi standardami (np. SOC 1 typu 2 i SOC 2 typu 2 w obszarze audytu)[17]

Piśmiennictwo:

[1.] Gibas A., Gawroński M., Gajda R., *Czas na chmurę w sektorze finansowym w Polsce!,* https://it.projektekf.pl/sites/default/files/prezentacje/CloudComputingInFSIPoland_GAB_Article_online.pdf
[2.] Grzybowski M., Dziewięć faktów o Dyrektywie NIS, które powinieneś znać, https://www.cybsecurity.org/9-faktow-o-dyrektywie-nis-ktore-powinienes-znac/
[3.] http://computingcloud.pl/pl/cloud-przewodnik/219-chmura-prywatna-publiczna-a-moze-hybrydowa
[4.] http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_PL.pdf
[5.] Mateos A., Rosenberg J., *Chmura obliczeniowa. Rozwiązania dla biznesu.* Wydawnictwo Helion
[6.] Postepowanie w razie incydentów bezpieczeństwa komputerowego opisano normą NIST 800-61 opracowaną przez Narodowy Instytut Standardów i Technologii przy amerykańskim Departamencie Handlu
[7.] Reczek E., *Zastosowanie chmury obliczeniowej w sektorze ochrony zdrowia*. Zeszyt Naukowy - Wyższa Szkoła Zarządzania i Bankowości w Krakowie 2014 nr 33
[8.] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych
[9.] Segalis B., *Cloud Computing Legal Risk and Liability,* InfoLawGroup 2011
[10.] Wronka K., *Modelowe klauzule umowne, a ochrona danych* http://prawoitechnologia.pl/aktualnosci/dane-osobowe/modelowe-klauzule-umowne-a-ochrona-danych-osobowych.html
[11.] Wronka K., *Wiążące reguły korporacyjne w świetle nowelizacji ustawy o ochronie danych* http://prawoitechnologia.pl/aktualnosci/dane-osobowe/wiazace-reguly-korporacyjne-w-swietle-nowelizacji-ustawy-o-ochronie-danych-osobowych.html

Streszczenie

W artykule zaprezentowano praktyczne aspekty zastosowania technologii chmury obliczeniowej w obszarze przetwarzania dokumentacji medycznej w formacie elektronicznym.

[17] Gibas A., Gawroński M., Gajda R., *Czas na chmurę w sektorze finansowym w Polsce!,* https://it.projektekf.pl/sites/default/files/prezentacje/CloudComputingInFSIPoland_GAB_Article_online.pdf

Omówione zostały poszczególne rodzaje usług chmurowych, przesłanki wyboru konkretnych rozwiązań z perspektywy placówki medycznej oraz instytucję umowy o powierzenie danych z wykorzystaniem zasobów chmurowych w ramach transgranicznego transferu danych medycznych.