PROTOKÓŁ z IV posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 13 października 2023 roku, o godzinie 13:00 w formie wideokonferencji.

Projekt EUCS (European Cybersecurity Certification Scheme for Cloud Services) – stan projektu oraz odniesienie rządu do projektu – Pan Marcin Wysocki, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa w MC.

Pan Dyrektor Marcin Wysocki na wstępie swojej wypowiedzi wskazał, że prace nad EUCS nadal trwają, a kolejny tekst przedmiotowego projektu nie został opublikowany, w związku z tym nie ma publicznej debaty o tzw. wymogach suwerenności. Ministerstwo Cyfryzacji wskazuje na brak demokratycznego podejścia do tego procesu. W ocenie MC zgłaszane propozycje są za daleko idące – nie jest to proces legislacyjny. Istotnym jest, że certyfikacja nie ma jeszcze charakteru obowiązkowego. Gdy taki program zostanie przyjęty nie jest skomplikowane, aby stał się on obligatoryjny w poszczególnych państwach, czy pozostałych krajach unijnych. Projekt certyfikacji chmury jest trudnym projektem z tego względu, że w ocenie MC zawiera dużo negatywnych rozwiązań, które dotyczą wymogów suwerenności. Pan Dyrektor wymienił zaproponowany wymóg odnoszący się do siedziby dostawcy chmury – siedziba główna powinna znajdować się na terenie państwa członkowskiego. Ten za daleko idący wymóg oznacza, że w najwyższym poziomie dostawcy chmury z innych krajów spoza Europy nie mogliby świadczyć usług chmurowych. Pierwszym globalnym problemem jest zdefiniowanie katalogu danych, które miałyby wiązać się z certyfikacją na najwyższym poziomie. Problemem jest także wskazanie do jakich wartości, przesłanek czy okoliczności należy się odwoływać. W przypadku osiągnięcia konsensusu co do rozróżniania poziomów czy okoliczności przez certyfikację, jest wciąż szereg zastrzeżeń praktycznych mogących mieć wpływ na świadczenie usług chmurowych w Europie, w Polsce oraz na kształtowanie się rynku. Wymóg dotyczący siedziby jest dla MC nieakceptowalny, co zostało wielokrotnie podnoszone. Pan Dyrektor zapewnił członków Rady, że prace nad europejskim programem certyfikacji nie są w MC przeoczone, a przedstawiciele resortu ciągle czuwają nad projektem. MC ma na uwadze również podsumowanie protokołu z dyskusji/spotkania pod kątem sytuacji mogącej wskazywać na osiągnięcie konsensusu, np. do wymogów suwerenności. Poza Polską jest wiele innych krajów, które podzielają przemyślenia w tym zakresie. Pan Dyrektor poinformował, że w pracach Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa biorą udział przedstawiciele MC oraz IŁ i NASK. Na obecnym etapie nie ma jeszcze rządowego stanowiska dotyczącego chmury. Ponadto, dyskusji poddany jest także temat bardziej złożony tj. lokalizacja danych, ponieważ MC wyraża zdanie, by dane były przetwarzane na terytorium UE. Ograniczenie się do przetwarzania danych w Polsce nie zawsze jest właściwe, z uwagi na szereg okoliczności związanych z zarządzaniem kryzysowym czy ze sprawami obronnościowymi. MC dopuszcza możliwość rozróżniania poziomów zapewnienia bezpieczeństwa w odniesieniu do EUCS, natomiast opowiada się za dokładnym rozważeniem i debatą na temat przemyślenia każdego słowa określającego charakter

danych, co do których zastosowanie będą miały rozwiązania, jak również poszczególne przesłanki, uważane przez MC za dyskryminujące.

Odpowiadając na pytania członka Rady Pan Dyrektor wskazał, że obawa przed skierowaniem EUCS na szczebel polityczny jest taka, że konsensus jest bardzo daleko. Minister Cyfryzacji skierował na ECCG pismo, w którym wskazywał zarzut braku transparentności procesu. Sukcesem jest obiecanie przez Komisję Europejską *Impact Assessment* – czy są obecnie moce chmurowe w Europie mogące obsłużyć proces, ocena wpływu na polskich przedsiębiorców, a także małych i średnich podwykonawców w Polsce na przedsięwzięcia chmurowe. Problemem jest, że *Impact Assessment* musi być osadzony w wersji niepublicznej projektu, a wymogi w zakresie suwerenności ulegają zmianom. MC wskazywało, że *Impact Assessment* wynika wprost z przepisów Cybersecurity Act co jest sukcesem MC. W *Impact Assesment* powinna znajdować się m.in. odpowiedź na pytania jaki jest *Impact*, ponieważ przykrywanie dyskusji tym, że certyfikacja jest nieobowiązkowa jest daleko niewystarczające. Co do wymogów Pan Dyrektor wyraził przekonanie, że te dotyczące głównej siedziby są bardzo dyskryminacyjne i zmuszają albo do absurdalnej sytuacji albo do obchodzenia przepisów przez partnerów. Wymogi co do lokalizacji danych muszą być przemyślane. Sytuacja jest skomplikowana, ponieważ nie wiadomo jakiej kategorii są to dane w kontekście lokalizacji - dane zmieniają się i nie są oczywiste. MC nadzoruje niedopuszczenie do sytuacji, w której wymogi byłyby wyższe niż te stawiane dla przetwarzanych informacji z klauzulą zastrzeżone.

W toku dyskusji zadano pytanie czy Pan Dyrektor widzi szanse w dłuższej perspektywie na stworzenie polskiego systemu certyfikacji oraz o szanse, aby UE porozumiała się ze Stanami Zjednoczonymi w kwestii uznawalności certyfikatów. Pan Dyrektor odpowiedział, że certyfikacja jest bardzo ważna, potrzebna i Krajowy System Certyfikacji Cyberbezpieczeństwa jest tworzony w rozumieniu Aktu o cyberbezpieczeństwie, jednak nie jest odpowiedzią na wszystkie okoliczności. Co do uznawalności, EUCS jest drugim programem certyfikacji, prace toczą się nad trzecim dot. 5G.

Jeden z członków Rady wskazał, że dużym problemem jest pojawienie się w EUCS kwestii nietechnicznych w ramach programu certyfikacji, czyli suwerenności, której znaczenie dokładnie nie jest znane, co przekłada się na lokalizację siedziby itd. Precedensem jest, aby do programu certyfikacji wpisywać czynniki nie technologiczne. Pozostaje także zagadnienie Dostawców Wysokiego Ryzyka. Kwestii, które każdy kraj członkowski może wprowadzić ze względu na *National Security Strategy* jest niemało, jednak te mechanizmy muszą znaleźć się w polskim prawodawstwie. Ze strony polskiej administracji widoczne są wysiłki w kierunku niewłączania do programu certyfikacji kwestii innych niż technologiczne oraz w kierunku transparentności.

Pan Przewodniczący uznał, że Rada musi dość szybko podjąć stanowisko w sprawie projektu EUCS, które powinno być wyważone. Projekt jest jedną z bardzo ważnych kwestii dla przyszłego rozwoju UE. Pan Przewodniczący zaproponował lidera grupy redakcyjnej oraz poprosił o kierowanie chęci zgłaszania się członków Rady do grupy.

Dyskusja na temat danych medycznych/dostęp lekarzy do danych pacjentów, status własności danych i dysponowania nimi (zagraniczne firmy), standardy bezpieczeństwa, edukacja dot. danych medycznych.

Pan Przewodniczący na wstępie wskazał, aby w dyskusji ująć główne problemy jakie istnieją w przedmiotowej tematyce według członków Rady.

Jeden z członków Rady omówił przesłane mailowo do pozostałego składu Rady zestawienie obaw i wątpliwości dotyczących fundamentalnych kwestii związanych z szeroko rozumianymi danymi medycznymi w kontekście zbiorów big data, ale jednocześnie spersonalizowanych. Zagadnienie obejmuje bardzo szeroki zakres - jest wrażliwe w najrozmaitszych punktach swojego istnienia. Dodatkowo doszło do uzgodnienia między Komisją Europejską a Parlamentem aktu *REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space*, który stanowi, że najważniejsza jest swoboda dostępu i wymiany międzynarodowej w celach biznesowych, a wszystkie inne elementy są mniej ważne. W rozwiązaniach pojawiają się bardzo słabo reprezentowane interesy człowieka, który jest „źródłem" danych. W akcie szeroko omówiona została strona biznesowa. Trzeci poziom to strona unijna w połączeniu z powołaniem nowych instytucji krajowych. Przytoczono kilka sformułowań z przedmiotowego rozporządzenia. Problem danych medycznych jest bardzo rozległy i dotyczy wielu płaszczyzn. Zauważono trzy poziomy, na których Rada powinna się skoncentrować. Po pierwsze to dane indywidualne. Jednocześnie stygmatyzacja ludzi i zaszeregowanie kastowe ze względu na choroby i predyspozycje do niesprawności, pogorszenie np. pozycji w odniesieniu do ubezpieczycieli, potencjalnych pracodawców czy urzędów. Poprzez profile, które są bardzo słabo wyregulowane (sprawy indywidualnych urządzeń fitness czy medycznych) można wpływać na całe grupy populacji w kierunku inspirowania określonych badań, ponoszenia innych kosztów czy wywoływania określonych nastrojów w tych grupach. Następnym poziomem powinno być spojrzenie na dane grupowe na płaszczyźnie narodowej, co pozwala pozornie anonimowo generować profile genetyczne, a w ślad za tym konstruować celowane środki farmakologiczne, które społeczeństwo będzie musiało nabyć. Najwyższy poziom integracji danych, czyli wieloletnie zestawienie dla całego kraju – predykcja schorzeń i częstości ich występowania, co wpływa na relacje z wielkimi podmiotami produkującymi środki farmakologiczne, szczepionki czy sprzęt diagnostyczny. Rada powinna skupić się na zasadniczych piętrach problemów, a także kwestiach związanych z bezpieczeństwem przetwarzania danych i z dostępem w rozumieniu RODO. Zastanawiano się czy ze względu na wielorakość problemów możliwe jest zawarcie wszystkich aspektów w rekomendacji Rady.

Pan Przewodniczący wskazał, że w temacie danych medycznych zazębiają się interesy polityczne i biznesowe w UE, powodujące zmierzanie legislacji w kierunku ubezwłasnowolniania wpływu człowieka i odbierania mu praw w sposób, o którym się nie wspomina. Kwestia praw pacjenta jest ograniczona do tego, że pod pewnymi warunkami może mieć dostęp do swoich danych medycznych. Regulacje podążają w kierunku pozbywania praw własności i dyspozycji osób fizycznych zwanych pacjentami. Pan

Przewodniczący preferowałby wypowiedzenie się Rady w przedmiotowym temacie nawet jeśli żaden rząd nie podzieli stanowiska Rady z powodów politycznych. Należy wskazać te aspekty problemu, których nikt inny nie pokazuje albo stara się ukryć z powodów biznesowych.

Jeden z członków Rady odniósł się do przepisów unijnych i wskazał, że dyskusja w sprawie danych medycznych toczy się od jakiegoś czasu na unijnym poziomie, a prace legislacyjne wydają się być zaawansowane. Przepisy być może będą przyjęte na początku 2025 roku w czasie polskiej prezydencji. Na większość regulacji wskazano około 3-letni okres przejściowy. To wynika z faktu, że Polska jest jednym z najbardziej zaawansowanych krajów we wdrażaniu różnego rodzaju usług elektronicznych z zakresu zdrowia. Wydaje się, że ostateczny kształt przepisów może być inny niż obecnie. Dyskusja jest dosyć żywiołowa i odbywa się na poziomie *eHealth Network*, w której znajdują się przedstawiciele Komisji Europejskiej, ale przede wszystkim państw członkowskich (Polskie Ministerstwo Zdrowia również ma w niej swój udział). Biorąc pod uwagę, złożoność tematu jest bardzo duża rozbieżność postrzegania przedmiotowych kwestii. Stwierdzone zostało, że warto, aby Rada nie starała się zmierzać w kierunku pewnego uproszczenia i np. wyłącznie skupić się na prawach jednostki albo postrzegać tę materię w kontekście celów stricte biznesowych. Mimo wszystko pewne rozwiązania takie jak wymiana danych medycznych na poziomie unijnym jest niezbędna dla zafunkcjonowania transgranicznej opieki zdrowotnej. Ponadto, bez regulacji unijnych z pewnością wiele krajów nie wdroży nawet na poziomie krajowym licznych rozwiązań, co przy dzisiejszym rozwoju technologii nie znajduje uzasadnienia. Drugą kwestią jest pewien dylemat – z jednej strony prawo człowieka do prywatności, ale z drugiej sprawy związane z interesem takim jak zdrowie i życie człowieka. Trudno jest przyjąć zerojedynkową zasadę, ze względu na złożoność tematu. Zauważono także dylemat pomiędzy interesem jednostki, a interesem społecznym – nie zawsze interes jednostki będzie nadrzędny, bo chociażby w przypadku pandemii przetwarzano dane dotyczące zaszczepienia, co było ważne dla wprowadzenia systemowych rozwiązań i weryfikowania danych. Jednym z pryncypiów przepisów unijnych jest to, że pacjent będzie zarządzał dostępem do swoich danych poprzez podobną aplikację jak Internetowe Konto Pacjenta, które istnieje w Polsce, będą jednak pewne wyjątki. Jest to także rozwiązanie, które funkcjonuje dziś w Polsce ze względu na regulacje ustawowe. To głównie ustawa *o systemie informacji w ochronie zdrowia*, ale także ustawa *o prawach pacjenta i Rzeczniku Praw Pacjenta* stanowiąca o prawie dostępu do danych medycznych pacjentów. W Polsce obowiązuje zasada decydowania o tym przez pacjenta, z pewnymi dosyć wąskimi wyjątkami mającymi swoje uzasadnienie - to sytuacja ratowania życia. Druga kwestia, to dostęp kadry medycznej placówki, w której utworzono daną dokumentację medyczną. Należy jednak mieć na uwadze, że dostęp do danych medycznych musi mieć związek z konkretną usługą medyczną. Lekarz rodzinny posiada dostęp do każdej wytworzonej dokumentacji medycznej także w innych placówkach. Można także wskazać bardzo wyjątkowe sytuacje jak kontrola NFZ w danej placówce.

W toku dyskusji wskazano, że członkowie Rady akcentują różne aspekty, widzą potrzebę wyjątków, a na problem można spojrzeć z perspektywy filozoficznej. Nawiązując do zagrożenia danych genetycznych, w tej sferze prawo jednostki jest wyżej niż inne wartości. Być może RODO nazbyt powierzchownie traktuje kwestię danych, które nazywano wrażliwymi, zwłaszcza w odniesieniu do podstawowych kwestii. Zaakcentowano, że stopień ochrony związany z własnością powinien być odmienny w odniesieniu do różnego rodzaju danych medycznych oraz odróżnialny w odniesieniu do transferu danych do trzech grup krajów tzn. wewnątrz UE, objętych decyzjami adekwatnościowymi oraz krajami, o których można mówić jako dostawcach z kręgów Dostawców Wysokiego Ryzyka.

Zgodzono się z Panem Przewodniczącym, aby w każdy możliwy sposób podkreślać podmiotowość człowieka. Dane jednostki są dobrem ogólnym do potrzeb sprawnego zarządzania państwem czy to w przypadku danych medycznych – dostęp do informacji o ilości zachorowań czy danych osobowych w całokształcie. Ważne jest wyważenie wszystkich aspektów zarówno w ustawodawstwie unijnym, ale także krajowym. Istotne, by na etapie legislacji bardzo szczelnie kontrolować dostęp do danych i ewentualnie wprowadzać odpowiednie zabezpieczenia. Jest to zjawisko bardzo skomplikowane, ponieważ należy wypośrodkować zapewnienie sprawnego funkcjonowania różnych obszarów państwa. Wyrażono zdanie, że postęp w tworzeniu prawa, a postęp technologiczny w obszarze cyfrowym to dwie różne prędkości.

Pan Przewodniczący doprecyzował swoje stanowisko, a mianowicie wskazał, że jest się osobą także ze względu na wspólnotę i to wspólnota czyli np. państwo za każdym razem określa co osobie się należy z punktu widzenia prawa i zasad państwa. Ta relacja jest dynamiczna, a przewaga zaczyna na stałe przechodzić na stronę państwa, co jest pewnym ryzykiem, jednak tak samo przechodzi na korzyść dużego biznesu. Nie ma dużych różnic pomiędzy stanowiskiem Pana Przewodniczącego a legislacją – to polskie rozwiązanie jest słuszne ontologicznie. Problem pojawia się z działaniami państwa w sytuacjach wyjątkowych takich jak pandemia. Być może decyzje podjęte w danym czasie są właściwe, natomiast ich konsekwencje nie są dobre dla państwa i dla społeczeństwa. Rozwój technologiczny i biznesowy powoduje, że duże korporacje mają coraz większą władzę polityczną. Główny problem polega na różnicy pomiędzy stanowiskiem polskim, a unijnym projektem stanowiska omawianym na początku tego punktu posiedzenia. W projekcie nie ma równowagi pomiędzy prawem do decyzji osoby i wspólnoty państwowej – jest ona na korzyść wspólnoty państwowej, która będzie prawem dla dużego biznesu medycznego. Dane medyczne to szczyt danych osobowych i systemowych.

W toku dyskusji zauważono, że obszarem, nad którym warto dyskutować, gdzie legislacja nie nadążyła za rzeczywistością jest tzw. *mHealth* – aplikacje zawierające regulaminy, z którymi użytkownicy nie zapoznają się i w związku z tym nie mają świadomości, że ich dane mogą być przedmiotem handlu.

Ze względu na mnogość zakresu tematyki danych medycznych zastanawiano się w jaki sposób Rada powinna zająć się tą materią. Pojawiło się stwierdzenie, że rolą Rady jest

obserwowanie danych wrażliwych. Warto byłoby wskazać obszary największych zagrożeń, a także wypunktować i wyargumentować sferę przetwarzania informacji o danych medycznych. Zaproponowano zaproszenie do dyskusji w przedmiotowym temacie przedstawicieli m.in. Ministerstwa Zdrowia.

Dyskusja na temat rekomendacji dotyczących bezpieczeństwa informacji - Pan Sławomir Wojciechowski.

Pan Sławomir Wojciechowski zaproponował, aby zwrócić uwagę resortu Cyfryzacji na potrzebę przygotowania roboczo nazwanego dokumentu tj. Rekomendacje bezpieczeństwa informacji w zakresie wdrażania i eksploatacji systemów teleinformatycznych w podmiotach publicznych szeroko rozumianych - nie tylko administracji samorządowej i rządowej. Pan S. Wojciechowski wspominał, że gmina do realizacji zadań własnych wykorzystuje na co dzień dużą liczbę systemów informatycznych różnego rodzaju. W przypadku wykorzystania wielu z nich, odbywa się to na podstawie podpisanej umowy z podmiotem najczęściej komercyjnym. Zauważony został brak kwalifikacji, wiedzy i możliwości skutecznej ochrony interesów podmiotów publicznych w takich relacjach przy wykorzystaniu systemów informatycznych, co za tym idzie właściwego zabezpieczenia przetwarzanych w nim informacji. Przydatnym byłoby, aby MC wypracował rekomendacje w zakresie kwestii na jakie powinien zwrócić uwagę podmiot publiczny nawiązując współpracę przy wykorzystaniu zewnętrznych systemów informatycznych z przykładem wzoru zapisów, także z zakresu wymogów od danej firmy.

Jeden z członków Rady uznał, że przedmiotowy temat jest bardzo powiązany ze skomplikowanym tematem roli Ministerstwa Cyfryzacji w obszarze zorganizowania administracji rządowej oraz samorządowej.

Obecny na posiedzeniu Pan Dyrektor Marcin Wysocki wskazał, że w 2016 r. był realizowany projekt co do wzorcowych klauzul w umowach IT. Projekt zakończył się pozytywnym odbiorem i wiele podmiotów z niego korzysta. Być może wzorcowy dokument dotyczący współpracy czy realizacji umów odnoszący się też do bezpieczeństwa informacji można byłoby rozszerzyć, ponieważ co do przepisów prawa powszechnie obowiązującego jest rozporządzenie KRI i dalsze prace nad tym aktem, z drugiej strony są różne rekomendacje uznanych podmiotów. Trzeba odpowiedzieć na pytanie na jakich kwestiach warto się skupić.

Jeden z członków Rady zauważył, że Departament Cyberbezpieczeństwa MC realizuje program PWC z udziałem podmiotów komercyjnych pozwalający na pogłębienie specjalistycznej wiedzy. To program, w którym Ministerstwo zawiera umowy partnerskie z podmiotami komercyjnymi, czyli z największymi firmami.

W toku dyskusji Pan Sławomir Wojciechowski odpowiedział, że widzi problem w aspekcie bezpieczeństwa informacji. Podano na przykładzie, że trafiające do opiniowania projekty umów z podmiotami komercyjnymi wyraźnie pokazują w bardzo dużej mierze głównie na początku ochronę interesów danej firmy, a w bardzo małym stopniu chronią jednostkę samorządową. Brakuje po stronie podmiotów publicznych specjalistów, którzy mogliby dość

precyzyjnie zdiagnozować problem. Przy obecnej skali ryzyka i zagrożenia z różnych stron, każda pomoc jest bardzo ważna. Ponadto zauważono problem w kompetencjach kadr. Krajowe Ramy Interoperacyjności funkcjonują od kilku lat. Zrozumienie i zastosowanie przepisów w podmiotach publicznych nie tylko w samorządzie oraz przełożenie na działalność i funkcjonowanie organizacji jest istotnym problemem.

Pan Przewodniczący zaproponował, aby zainteresowani dyskutowanym tematem członkowie Rady kierowali swoje uwagi, a także chęć zgłoszenia się do ewentualnego zespołu redakcyjnego prelegentowi tematu oraz o przygotowanie przez prelegenta w punktach najważniejszych zaleceń.

Uczestnicy posiedzenia:

Członkowie Rady:

1. Izabela Albrycht
2. Andrzej Dulka
3. Agnieszka Gryszczyńska
4. Jolanta Jaworska
5. Michał Kanownik
6. Agnieszka Kister
7. Janusz Kosiński
8. Anna Beata Kwiatkowska
9. Dariusz Milka
10. Jarosław Mojsiejuk
11. Józef Orzeł - Przewodniczący
12. Tomasz Rychter
13. Krzysztof Silicki
14. Robert Trętowski
15. Sławomir Wojciechowski

Zaproszeni goście:

16. Krzysztof Głomb, Pełnomocnik Ministra Cyfryzacji do spraw współpracy z administracją samorządową Rzeczpospolitej Polskiej; Pełnomocnik Ministra Cyfryzacji do spraw relacji z podmiotami działającymi na rzecz rozwoju kompetencji cyfrowych
17. Marcin Wysocki, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa w MC
18. Wiesław Paluszyński, ekspert Rady

Sekretariat Rady i pracownicy Ministerstwa Cyfryzacji:

19. Katarzyna Nosalska, Dyrektor Centrum Rozwoju Kompetencji Cyfrowych w MC
20. Aleksandra Ciszewska, Radca, Departament Innowacji i Technologii w MC
21. Ewa Świętochowska, Ekspert, Departament Innowacji i Technologii w MC
22. Sylwia Stefaniak, Ekspertka, Departament Innowacji i Technologii w MC
23. Katarzyna Stopińska, Biuro Ministra w MC
24. Joanna Laskowska, Biuro Ministra w MC