

X kadencja



KANCELARIA SEJMU

Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

- **KOMISJI SAMORZĄDU TERYTORIALNEGO
I POLITYKI REGIONALNEJ
(NR 52)
z dnia 19 marca 2025 r.**

Pełny zapis przebiegu posiedzenia Komisji Samorządu Terytorialnego i Polityki Regionalnej (nr 52)

19 marca 2025 r.

Komisja Samorządu Terytorialnego i Polityki Regionalnej, obradująca pod przewodnictwem posła **Michała Krawczyka (KO)**, przewodniczącego Komisji, zrealizowała następujący porządek dzienny:

– rozpatrzenie informacji na temat bezpieczeństwa przechowywania i zarządzania danymi w chmurze w administracji publicznej.

W posiedzeniu udział wzięli: **Konrad Komornicki** zastępca prezesa Urzędu Ochrony Danych Osobowych wraz ze współpracownikiem, **Marcin Wysocki** zastępca dyrektora Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji wraz ze współpracownikiem, **Andrzej Skrzeczkowski** dyrektor Pionu Rozwoju Cyberbezpieczeństwa NASK oraz **Jarosław Wojciechowski** ekspert Departamentu Bezpieczeństwa Urzędu Komunikacji Elektronicznej.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Mateusz Daszewski** i **Sławomir Jakubczak** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł **Michał Krawczyk (KO)**:

Dzień dobry. Witam państwa serdecznie.

Otwieram 52. posiedzenie Komisji Samorządu Terytorialnego i Polityki Regionalnej.

Witam panie posłanki i panów posłów. Witam gości. Witam pana Konrada Komornickiego, zastępcę prezesa Urzędu Ochrony Danych Osobowych. Witam pana Adriana Potockiego, dyrektora Departamentu Rozwiązań Chmurowych Centralnego Ośrodka Informatyki, pana Marcina Wysockiego, zastępcę dyrektora Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji, pana Alana Koseckiego, starszego specjalistę w Departamencie Cyberbezpieczeństwa Ministerstwa Cyfryzacji, pana Tomasza Ochmińskiego, zastępcę dyrektora Departamentu Prawa i Nowych Technologii Urzędu Ochrony Danych Osobowych, pana Andrzeja Skrzeczkowskiego, dyrektora Pionu Rozwoju Cyberbezpieczeństwa NASK, pana Jarosława Wojciechowskiego, eksperta Departamentu Bezpieczeństwa Urzędu Komunikacji Elektronicznej oraz pana Kamila Wójcika, wiceprezesa Federacji Stowarzyszeń Naukowo-Technicznych NOT. Witam państwa bardzo serdecznie.

Stwierdzam kworum.

Przedmiotem dzisiejszego posiedzenia będzie zgodnie z naszym planem pracy rozpatrzenie informacji ministra cyfryzacji na temat bezpieczeństwa przechowywania i zarządzania danymi w chmurze w administracji publicznej.

Czy są uwagi do porządku dziennego? Nie widzę. Dziękuję. Stwierdzam jego przyjęcie.

Bardzo proszę na początek przedstawiciela Ministerstwa Cyfryzacji pana dyrektora Marcina Wysockiego o przedstawienie informacji.

Zastępca dyrektora Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji **Marcin Wysocki**:

Dzień dobry państwu. Panie przewodniczący, Wysoka Komisjo, kilka słów wstępu à propos przetwarzania w chmurze obliczeniowej przez podmioty administracji publicznej danych i rozwoju usług w tym zakresie. Obecnie w Polsce nie ma takiej kompleksowej regulacji na poziomie ustawowym, która dotyczyłaby przetwarzania danych w chmurze obliczeniowej przez podmioty administracji publicznej. Nie ma również takich wytycznych wiążących podmioty administracji oraz komercyjnych dostawców usług przetwarzania w chmurze co do tego, jakie zabezpieczenia powinny być stosowane. Natomiast na szczęście nie jest tak, że nic nie obowiązuje w tym zakresie, to znaczy, że nie ma wytycznych. Jest uchwała Rady Ministrów w sprawie inicjatywy „Wspólna infrastruktura informatyczna państwa”. Jest to uchwała Rady Ministrów, więc

jej postanowienia wiązą Radę Ministrów, podległe jej podmioty oraz przez nią nadzorowane. Dla pozostałych podmiotów administracji, w tym samorządowej, uchwała jest taką rekomendacją, wskazówką, a nie prawnym obowiązkiem.

W przypadku podmiotów objętych zakresem uchwały WIIP obowiązki nakładane są na podmioty, a nie na samych dostawców. Sprowadza się to do tego, że mogą korzystać wyłącznie z takich usług, które spełniają wymagania wskazane w uchwale i w Standardach Cyberbezpieczeństwa Chmur Obliczeniowych. Tym samym komercyjni dostawcy, aby móc zaoferować swoje usługi podmiotom administracji muszą spełniać te wymagania dotyczące bezpieczeństwa. Pomocniczo oczywiście możemy się posługiwać także odpowiednimi przepisami ustawy o krajowym systemie cyberbezpieczeństwa.

Natomiast w zmianach, które dotyczą kreowania polityki w zakresie korzystania przez administrację z chmury obliczeniowej na tym odcinku, kierujemy się pryncypium polityki *Cloud First*, czyli uwzględniamy korzyści, jakie przynosi wykorzystanie chmury obliczeniowej zarówno dla państwa, jak i dla jego obywateli. Mowa jest o korzyściach ekonomicznych, wydajnościowych, a także dotyczących bezpieczeństwa przetwarzanych danych. Sukcesywnie podejmowane są dalsze działania, które mają na celu upowszechnienie wykorzystania w Polsce usług chmurowych przez administrację.

Pierwszym takim krokiem, który już został wykonany, była nowelizacja uchwały o wspólnej infrastrukturze państwa. Drugim, trwającym krokiem, jest obecnie aktualizacja Standardów Cyberbezpieczeństwa Chmur Obliczeniowych. W dalszych planach minister cyfryzacji ma zamiar przedstawić projekt takiej ustawy właśnie kompleksowej odnoszącej się do chmury obliczeniowej. Wtedy wypełnilibyśmy taką lukę w polskim ustawodawstwie, w zakresie możliwości korzystania z rozwiązań oferowanych w tzw. rządowej chmurze obliczeniowej i publicznej chmurze obliczeniowej, określilibyśmy zarówno obowiązki podmiotów administracji, jak i dostawców, określilibyśmy, jakiego rodzaju dane mogą być przetwarzane, w jakim typie, w jakim modelu chmury obliczeniowej, ponieważ to są różne rozwiązania. Jest rządowa chmura obliczeniowa, której gestorem jest państwo, jak i jest możliwość korzystania z dostawców komercyjnych.

Obecnie analizujemy rozwiązania przyjęte przez państwa z Unii Europejskiej i spoza Unii Europejskiej i jesteśmy przekonani, że m.in. na tej podstawie, a także w konsultacji z podmiotami administracji publicznej oraz z rynkiem wypracujemy takie optymalne rozwiązania zgodne z aktualnymi potrzebami. Wierzymy, że rozpoczęcie prac nad ustawą i jej późniejsze przyjęcie wpłynie pozytywnie na bezpieczeństwo państwa i wspomogą także rozwój gospodarczy w Polsce, ponieważ umieszczanie w centrum przetwarzania danych na terenie kraju, ich lokalizowanie, tworzenie, rozwój takich regionów chmurowych Polsce przez dostawców usług komercyjnych również przełoży się na większe inwestycje w rozwój technologii.

Ta znowelizowana uchwała WIIP, o której wspominałem, weszła w życie 29 października poprzedniego roku. Nowelizacja dokonała szeregu zmian w załączniku nr 2, które koncentrują się na znacznym poszerzeniu możliwości korzystania przez podmioty administracji rządowej z usług przetwarzania w publicznej chmurze obliczeniowej, czyli tej chmurze dostarczanej przez dostawców komercyjnych, ale spełniającej wymagania z zakresu bezpieczeństwa, tzn. zmieniliśmy kryteria systemów teleinformatycznych, z których można korzystać z usług przetwarzania. Przedmiotowa zmiana polega na możliwości umieszczenia poszczególnych systemów teleinformatycznych w jurysdykcji krajowej, czyli w polskiej lub pozostałych państwach Europejskiego Obszaru Gospodarczego, co stanowi wprost odpowiedź na oczekiwania i potrzeby administracji, które były zgłaszane ministrowi cyfryzacji i liczne problemy ze zbyt wąskim podejściem w korzystaniu z usług przetwarzania w chmurze obliczeniowej. Jak wszyscy wiemy taka największa zmiana w naszej optyce i korzystania z rozwiązań chmurowych to oczywiście pandemia COVID-19, którą przeszliśmy zupełnie niedawno, te doświadczenia są wciąż żywe, więc uwzględniamy również oczywiście obecną sytuację międzynarodową.

W ramach nowelizacji zostały wprowadzone także zmiany w zakresie kategorii systemów teleinformatycznych, w których przetwarzane są informacje niejawne i tam jest taka możliwość umieszczenia w rządowej chmurze lub w publicznej chmurze systemów teleinformatycznych oraz rozwiązań informatycznych, w których przetwarzane są informacje niejawne o maksymalnej klauzuli „zastrzeżone” lub równoważnej klauzuli międzynarodowej i w odniesieniu do tych systemów i ich akredytacji nadzór nad funkcjonowaniem tego systemu ochrony informacji niejawnych oczywiście realizuje Służba Kontrwywiadu Wojskowego.

Wszystkie te zmiany zapewnią szerszą dostępność różnego rodzaju oprogramowania dla administracji rządowej, które już nie są często w ogóle dostępne w tradycyjnym modelu *on-premise* albo są dostępne, lecz nie są optymalne kosztowo, a także ze względów bezpieczeństwa, bo kosztować mogą wielokrotnie więcej, przy czym ten przyrost bezpieczeństwa wcale nie zachodzi. Szczególne znaczenie ma poszerzenie dostępności oprogramowania z zakresu cyberbezpieczeństwa właśnie w tym kontekście, że można przetwarzać dane regionalne na obszarze Unii Europejskiej, gdzie obowiązuje prawo unijne, w tym oczywiście RODO.

Uchwała nie zakłada obligatoryjnego korzystania z usług przetwarzania w chmurze, w szczególności z publicznej chmury obliczeniowej. To konkretny gestor systemu sam decyduje, dokonuje analizy ryzyka czy korzystać z rozwiązań przewidzianych w uchwale, a jeżeli zdecyduje się na takie działania, to przed skorzystaniem z tych usług w chmurze publicznej jest zobowiązany do wykonania szeregu czynności, które mają na celu wykluczyć lub zminimalizować ryzyka związane z korzystaniem z publicznej chmury obliczeniowej.

To szersze podejście do możliwości wykorzystania usług bazujących na chmurze powinno przełożyć się na liczniejsze przystępowania do umów ramowych, umieszczania swoich ofert usług w katalogu w tzw. systemie ZUCH, czyli systemie zapewniania usług chmurowych. Domniemyjemy, że całość procesów pozytywnie wpłynie na konkurencyjność i różnorodność ofert zamieszczanych w ramach ZUCH, czyli znowu – szerszy dostęp do usług oferowanych w chmurze obliczeniowej, nowe możliwości skorzystania z usług z zakresu cyberbezpieczeństwa. Ten etap, na którym jesteśmy obecnie – aktualizacja standardów cyberbezpieczeństwa chmur obliczeniowych, to temat jak najbardziej aktualny. Oczywiście decyzja o skorzystaniu z usług chmurowych dostawcy komercyjnego musi zostać podjęta na podstawie wyników analizy z załącznika nr 2 uchwały i zostać potwierdzona przez analizę dokonaną na podstawie właśnie standardów cyberbezpieczeństwa chmur obliczeniowych.

O czym jest ten dokument, który już kilkakrotnie przywołałem? On determinuje poszczególne modele chmur obliczeniowych, kategoryzuje bezpieczeństwo systemu teleinformatycznego, co ma wpływ na wymagania dla samego systemu, dla wyboru odpowiedniego modelu, a co za tym idzie również wyboru konkretnego dostawcy. Aktualnie finalizowane są prace związane z aktualizacją tego dokumentu. W ramach podjętych działań zaktualizowaliśmy tutaj wspólnie we współpracy z Centralnym Ośrodkiem Informacji ten dokument wraz z załącznikami do aktualnej rewizji standardów międzynarodowych National Institute of Standards and Technology. Mam oczywiście te poszczególne normy wypisane, nie będę tutaj państwa nimi zanudzał. Natomiast podkreślę, że jest to, po pierwsze, aktualizacja tych dokumentów, odesłań do aktualnej wiedzy technicznej. W ramach pracy dokonałem także weryfikacji listy zabezpieczeń przy właściwych poziomach wymagań bezpieczeństwa w ścisłym skorelowaniu z zaktualizowanym katalogiem zabezpieczeń.

Celem ministra cyfryzacji i Ministerstwa Cyfryzacji jest jak najszybsze przyjęcie zaktualizowanego dokumentu, bez którego nie jest możliwe jeszcze pełne korzystanie z tych wszystkich zmian, które daje znowelizowana uchwała Rady Ministrów. Dokument został skierowany do ministra spraw wewnętrznych i administracji, ministra obrony narodowej, ministra – koordynatora służb specjalnych w tym miesiącu i oczekujemy na akceptację tych partnerów, z którymi wspólnie na co dzień współpracujemy.

Panie przewodniczący, mam jeszcze informację, jak szczegółowo wygląda zapewnienie bezpieczeństwa danych w chmurze, o jurysdykcji i lokalizacji centrów przetwarzania danych, o własności przetwarzanych w nich danych, migracji danych, przeciwdziałania zjawisku również *vendor lock-in*. Czy kontynuować jeszcze kilka minut?

Przewodniczący poseł Michał Krawczyk (KO):

Bardzo proszę.

Zastępca dyrektora departamentu MC Marcin Wysocki:

Zagwarantowanie bezpieczeństwa danych przetwarzanych w chmurze obliczeniowej stanowi nadrzędny cel w podejmowaniu decyzji o ewentualnej migracji systemu do chmury obliczeniowej. Jest on realizowany przez skategoryzowanie systemów teleinformatycznych oraz informacje jednostek administracji publicznej, które mają być przetwarzane z wykorzystaniem usług modelu chmur obliczeniowych zgodnie z załącznikiem do WIIP, sklasyfikowanie systemów i informacji pod kątem wymagań bezpieczeństwa SCCO.

Jesteśmy przekonani, tak jak wskazałem wcześniej, że Polska potrzebuje przepisów, które umożliwią administracji publicznej korzystanie z usług oferowanych w ramach publicznej chmury obliczeniowej. Jest to kwestia nie tylko rozwoju cyfryzacji, ale i bezpieczeństwa państwa, ponieważ w sytuacji kryzysu musimy zagwarantować ciągłość działania administracji, dostępność jej kluczowych systemów, ich dostępności dla wszystkich obywateli. Jednocześnie mamy na uwadze coraz mniejszą właśnie dostępność usług z zakresu cyberbezpieczeństwa w tej formie *on-premise*, czyli w takim modelu chmury prywatnej. Bezpieczeństwo przetwarzania danych oparte jest o jurysdykcję kraju, w jakim następuje ten proces, więc jest to wyłącznie jurysdykcja polska lub jurysdykcja innego państwa członkowskiego Unii Europejskiej lub Europejskiego Obszaru Gospodarczego, tzn., że państwo EOG musi stosować prawo unijne, czyli mamy przepisy dotyczące cyberbezpieczeństwa, ochrony danych, NIS2, RODO, Data Act. Dostawca usług przetwarzania w publicznych chmurach obliczeniowych umieszczanych przez Ministerstwo Cyfryzacji w katalogu usług publicznej chmury obliczeniowej zobowiązany jest do przedstawienia listy wszystkich fizycznych lokalizacji centrów przetwarzania danych, w których dane mogą być przechowywane i przetwarzane. W tym zakresie absolutnie nie są prawdziwe informacje, że nasze dane w myśl WIIP będą gdzieś przetwarzane lub mogą być przetwarzane poza terytorium Unii i poza jurysdykcją prawa unijnego.

Oczywiście mamy też wskazówki, co powinien zrobić taki podmiot, czego żądać od dostawcy publicznej chmury obliczeniowej, aby faktycznie te warunki wynikające z WIIP dotyczące bezpieczeństwa spełnić. To właściciel systemu decyduje o lokalizacji centrum przetwarzania danych. Może wybrać, czy chce korzystać z usług w ramach publicznej chmury obliczeniowej, z centrum przetwarzania danych na terytorium naszego kraju lub innego kraju Europejskiego Obszaru Gospodarczego Unii Europejskiej. W sytuacji, w której zachodzą wątpliwości co do zagwarantowania suwerenności danych, to z uchwały WIIP i z zaktualizowanych SCCO wynika, że należy korzystać z centrum przetwarzania danych zlokalizowanych na terytorium Rzeczypospolitej Polskiej. Obecnie wielu dostawców komercyjnych oferuje usługi o charakterze *sovereignty*, gdzie klient może wybrać region przetwarzania danych, określając na poziomie kraju czy Europy, grupy poszczególnych państw.

Jeżeli chodzi o własność przetwarzania danych, wszystkie informacje, dane umieszczone lub utworzone przez administrację publiczną w chmurze takiego dostawcy publicznego w tym modelu są własnością właściciela informacji, chyba że została zawarta umowa z dostawcą usług, która stanowi inaczej. Dostawca usług publicznej chmury obliczeniowej nie ma żadnych praw do informacji lub danych administracji publicznej. Informacje i dane obejmują także dzienniki i dane monitorowania tworzone przez aplikację i systemu odbiorcy usług publicznych chmury obliczeniowej, czyli tych jednostek administracji publicznej.

Dostawca usług publicznej chmury obliczeniowej nie może wykorzystywać informacji danych odbiorców usług w żaden inny sposób, aniżeli określone w umowie, nie może oczywiście ujawniać jakichkolwiek danych odbiorców usług korzystających z jego oferty usług chmur obliczeniowych ani organom państw, w których są przetwarzane dane odbiorców tych usług, ani organom państw sprawujących jurysdykcję na dostawcę usług, o ile nie wynika to wprost z umowy zawartej pomiędzy odbiorcą i dostawcą usług.

Ponadto dostawca usług publicznej chmury obliczeniowej zobowiązany jest do niezwłocznego poinformowania odbiorcy usług o obowiązujących prawach lub wprowadzeniu takich praw uniemożliwiających spełnienie powyższych warunków, więc jeżeli zmieniliby się w tym przypadku prawo kraju takiego dostawcy, to jest on zobowiązany wskazać, że nie jest w stanie tych warunków wynikających z umowy z takim podmiotem publicznym dalej dotrzymać. Dopuszcza się jedynie gromadzenie przez dostawcę niezbędnych danych, które są konieczne do prawidłowego świadczenia usługi i te dane muszą być udostępnione odbiorcy na każde jego żądanie. Dostawca komercyjny zobowiązany jest do niezwłocznego usunięcia danych po zakończeniu świadczenia usługi, chyba że coś innego wynika z umowy lub z przepisów prawa powszechnie obowiązującego. Mamy też takie zalecenia, aby w umowie o świadczenie usług chmurowych uregulować, że dostawca usług publicznej chmury obliczeniowej niezwłocznie na każde żądanie odbiorcy przekazuje zawartość wszystkich dzienników i danych monitorowania.

W kwestii migracji danych bezpieczeństwo przetwarzania danych to także zagwarantowanie możliwości swobodnego przeniesienia danych, gdy gestor systemu zadecyduje o migracji danych na przykład do innego dostawcy usług chmur obliczeniowych ze względu na przykład na wygasającą umowę z dostawcą bądź z uwagi na fakt, że dostawca usług przestał świadczyć

usługi chmury obliczeniowej. W związku z tym konieczne jest zagwarantowanie bezpiecznego procesu migracji i kasowania danych, co zostało szeroko sprecyzowane właśnie w standardach cyberbezpieczeństwa chmur obliczeniowych. Tam jest odesłanie do właściwych algorytmów szyfrowania danych w każdej postaci, jak też ich kasowania, również z uwzględnieniem kasowania kryptograficznego, czyli odbywającego się poprzez skasowanie kluczy kryptograficznych używanych do szyfrowania właśnie tych danych.

Ten dokument wspiera również przeciwdziałanie zjawiskom tzw. *vendor lock-in* z procesem migracji ściśle związanym z przeciwdziałaniem temu zjawisku. Zgodnie z SCCO dostawcy usług chmurowych są zobowiązani do stosowania technologii pozwalających na łatwą migrację danych do infrastruktury własnej odbiorcy usługi, gdyby przestał korzystać z takich usług chmurowych lub do infrastruktury innego dostawcy, czyli mamy zapewnić konkurencyjność, odpowiedni poziom bezpieczeństwa i uzależnienia się właśnie od tego jednego odbiorcy usługi. Z tych względów SCCO zobowiązuje do tego by umowa o świadczenie usług chmurowych zawierała część określającą warunki zakończenia korzystania z usług chmury obliczeniowej, zasady i terminy zwrotu lub usunięcia przetwarzania danych.

Co do szyfrowania danych z przedmiotowym zakresem bezpieczeństwa danych ściśle związana jest szeroko pojęta polityka w zarządzaniu kluczami, szyfrowania danych, która jest również uregulowana w tym dokumencie i standardach cyberbezpieczeństwa chmury obliczeniowej. Bezpieczeństwo przetwarzania danych zapewnia korzystanie z silnych algorytmów szyfrowania i stosowania najnowszych bezpiecznych protokołów sieciowych zgodnie z najlepszymi standardami międzynarodowymi. W przypadku systemów przetwarzających informacje niejawne każdorazowo jest wymagane stosowanie oczywiście certyfikowanych rozwiązań kryptograficznych i spełnienie tych wymogów, które wynikają z ustawy o ochronie informacji niejawnych.

Oczywiście, jeżeli chodzi o informacje niejawne, to jest również szczególny rygor. Informacje niejawne przetwarzane w publicznej chmurze obliczeniowej dotyczą wyłącznie klauzuli „zastrzeżone” i tylko ze zgodą Służby Kontrwywiadu Wojskowego w zakresie kopii przetwarzania danych. Zagwarantowanie bezpieczeństwa przetwarzania danych to zapewnienie aktualnych, bezpiecznych i odtwarzalnych kopii danych. W związku z niniejszym dostawcy usług zgodnie z SCCO są zobowiązani do umożliwienia tworzenia kopii zapasowych danych, które mogą być odtwarzane przez odbiorcę usługi. Co więcej, przeprowadzona analiza ryzyka może skutkować koniecznością tworzenia kopii zapasowych u więcej niż jednego dostawcy usług w chmurach obliczeniowych, gwarantując tym samym zmniejszenie utraty danych o tych ryzykach, które są na co dzień i są powszechne w cyberbezpieczeństwie, utrata dostępności danych, a także te doświadczenia, które ma m.in. nasz sąsiad do zapewnienia funkcjonowania systemów teleinformatycznych w danym kraju. Z mojej strony to już tyle. Dziękuję, panie przewodniczący.

Przewodniczący poseł Michał Krawczyk (KO):

Bardzo dziękuję. Czy ktoś jeszcze z państwa gości chciałby zabrać głos w tym miejscu? Nie widzę. Przejdziemy więc do zadawania pytań. Pan przewodniczący Skonieczka, bardzo proszę.

Poseł Marcin Skonieczka (Polska2050-TD):

Panie przewodniczący, Wysoka Komisjo, dzisiaj rzeczywiście żyjemy w takim świecie, że ci, którzy mają informacje, mają władzę. Rozumiem, że mamy pełną kontrolę jako państwo nad tymi usługami świadczonymi w chmurze, świadczonymi centralnie, jak na przykład usługi ZUS czy mObywatel. Jako drugi taki poziom postrzegam to, co dzieje się w samorządach, gdzie powstają systemy do obsługi mieszkańców, które tworzą prywatne firmy i tutaj była mowa o tym, że te firmy muszą spełniać odpowiednie standardy i tutaj te dane są przetwarzane, one są dostępne w chmurze, ale rzeczywiście też jakąś kontrolę nad tym mamy. Tu też w tej kategorii widzę na przykład e-dzienniki, gdzie też bardzo dużo danych jest zbieranych dotyczących naszych dzieci, które uczą się w szkołach. Jest też moim zdaniem taki trzeci poziom, gdzie ta kontrola chyba jest najmniej możliwa i to są programy użytkowe dostarczane przez firmy zagraniczne, na przykład pakiety biurowe. Każdy w biurze ma jakiś taki właśnie program. Bardzo często on jest powiązany z chmurą. Nawet nasze sejmowe tablety przecież też mają usługę iCloud i te dane są wysyłane prawdopodobnie na amerykańskie serwery.

Tu chciałbym podpytać, czy rząd monitoruje bezpieczeństwo tych danych, czy korzystanie z tych systemów ogólnie dostępnych rzeczywiście jest bezpieczne i czy tu nie ma żadnych zagrożeń z tego wynikających dla bezpieczeństwa kraju, bo pewnie z tych programów również

korzystają pracownicy spółek Skarbu Państwa, również tych strategicznie dla nas ważnych, ważnych dla naszego bezpieczeństwa.

Drugi temat, o który chciałbym dopytać, troszeczkę wychodzi poza temat tej Komisji, ale jest ściśle związany z chmurą obliczeniową. Otóż wiemy, że Polska, szerzej Europa, przegrała wyścig, jeśli chodzi o usługi chmurowe z firmami amerykańskimi. Dzisiaj, jak czytamy w raportach, trzy amerykańskie firmy, takie jak Amazon, Microsoft i Google kontrolują większość tego rynku. Znalazłem takie dane, że udział europejskich dostawców zmalał z 27% w 2017 r. do zaledwie 13% w 2022 r. Czyli jesteśmy w totalnej defensywie i autorzy tego raportu wskazują, że to wynika m.in. z tego, że w Europie mamy wyższe ceny energii elektrycznej. Z tego właśnie powodu te firmy, które tutaj świadczą usługi chmurowe są niekonkurencyjne, ale też problemem są skomplikowane i długotrwałe procesy wydawania pozwoleń na budowę takich centrów danych. Tu moje pytanie: Czy ministerstwo w tym zakresie planuje jakieś działania tak, aby wspomóc polskie firmy, aby też budować polską chmurę obliczeniową, żeby wzmacniać jej rozwój, czy są jakieś programy dotacyjne przewidziane albo właśnie zmiany legislacyjne, które by to umożliwiły? Dziękuję bardzo.

Przewodniczący poseł Michał Krawczyk (KO):

Dziękuję. Bardzo proszę, panie dyrektorze.

Zastępca dyrektora departamentu MC Marcin Wysocki:

Bardzo dziękuję za te pytania, panie przewodniczący. Co do kwestii korzystania z usług chmurowych od dostawców komercyjnych zagranicznych – żyjemy w innej rzeczywistości popandemicznej, tzn. wiele podmiotów administracji publicznej zmigrowało się, wzmocniło te narzędzia na przykład do komunikacji zdalnej. Z takiej ogólnej oceny czy pełnej wiedzy na temat bezpieczeństwa i tego, jakie zakupy i z jakich rozwiązań korzysta administracja to niestety minister cyfryzacji w posiadaniu takich danych aktualnie nie jest. Natomiast wierzę, że są rozwiązania i wierzę, że wiele z tych podmiotów publicznych ma tę świadomość i jeszcze więcej w związku z tymi zmianami, panie przewodniczący, będzie miało świadomość, że można wymóc od takiego dostawcy zagranicznego, także z państwa trzeciego, żeby te dane były regionalizowane, czyli jest taka usługa, która mówi „zapewniam ci dane w chmurze, to jest publiczna chmura obliczeniowa” i jeżeli są *data center* w Polsce, to te podmioty też oferują takie usługi, że to jest w Polsce i jak są spełnione te wymogi wynikające z SCCO to jak najbardziej ta usługa jest bezpieczna.

Są też takie rozwiązania regionalne, w których podmiot zobowiązuje się i wierzę, że odpowiednia świadomość, ograniczone zaufanie po stronie zamawiających, ich duża świadomość i też po stronie *vendorów*, które oferują i zakładam, że te rozwiązania, tak jak w Ministerstwie Cyfryzacji, są oparte albo o chmurę prywatną, o chmurę krajową lub to przetwarzanie jest regionalne, gdzie ma zastosowanie jurysdykcja prawa unijnego i absolutnie taki dostawca usługi chmurowej zobowiązuje się do tego, że tych danych nigdzie indziej przekazywać nie będzie. W tym zakresie jest ta zmiana WIIP i zmiana SCCO, panie przewodniczący, że jeżeli przetwarzamy dane, najczęściej te systemy, o których mówił pan przewodniczący, to będą SCCO 2 i teraz zasadą jest przetwarzanie na terytorium EOG, czyli mamy konkurencyjny rynek zapewnienia bezpieczeństwa, ale wciąż gestor systemu nawet na tym poziomie SCCO 2 może powiedzieć „ja chcę decydować o przetwarzaniu danych, ja wybieram dostawcę polskiego”, te dane muszą być ze względu na ich charakter w Polsce i taka decyzja gestora systemu, jest również jak najbardziej uprawniona na podstawie właśnie tych SCCO, które aktualnie aktualizujemy.

Natomiast co do tego stanu rynku to jest tak, jak powiedział pan przewodniczący, najwięksi gracze usług chmurowych, największy udział w rynku to są podmioty ze Stanów Zjednoczonych. W Ministerstwie Cyfryzacji, panie przewodniczący, jesteśmy przekonani, że to nie jest problem w tym, że inwestują w to podmioty spoza Unii. One mają spełniać te wymagania, które są u nas. My jesteśmy w Europie. Tu obowiązuje RODO. Mamy najdalej idące gwarancje i muszą tych zobowiązań dotrzymywać. Jeżeli nasze przepisy mówią „nie ma opcji przetwarzania danych poza Unią Europejską” – a są, panie przewodniczący, scenariusze, w których warto mieć legalną furtkę do tego, żeby mieć na przykład backup systemu w kraju innym europejskim niż w Polsce i tutaj to są doświadczenia m.in. Ukrainy – to znaczy powinniśmy być gotowi również na zachowanie ciągłości działania naszych systemów. Są takie projekty, które są nazywane ambasadą danych, więc jeżeli chodzi o inwestycje, także tych dużych graczy, które wymienił pan przewodniczący, jeżeli to są inwestycje w Polsce, to jest najlepiej, jeżeli to są inwestycje w innych krajach europejskich, które spełniają nasze wysokie wymagania bezpieczeństwa, to też jest dobrze.

Jesteśmy przekonani, że ze względu na różny charakter tych systemów – mówiłem o poziomie SCCO 2, panie przewodniczący, ale są wyższe SCCO, na przykład SCCO 3, tam zasada już jest Polska i jest w ogóle poziom SCCO 4, tam muszą być te systemy posadowione w Polsce – to celem jest właśnie takie uaktualnienie tych rozwiązań do potrzeb administracji. Gdybyśmy na przykład powiedzieli „słuchajcie, podejmujemy decyzję, że wszystkie dane muszą być w Polsce”, to w pewnym momencie wpędzilibyśmy pewnie w nielegalne korzystanie z szeregu rozwiązań chmurowych podmioty administracji publicznej, które korzystają z tych powszechnych rozwiązań. Nie chcę tutaj ich wskazywać i ich reklamować, natomiast tutaj każdy z państwa na pewno ma doświadczenia co do tych usług, które są szczególnie powszechne, one też są oferowane przez tych gigantów cyfrowych, o których powiedział pan przewodniczący.

Przewodniczący poseł Michał Krawczyk (KO):

Dziękuję. Czy ktoś z państwa jeszcze chce zadać pytanie? Nie widzę. To ja zapytam jeszcze o jedną rzecz w kontekście samorządów. Jeśli ma pan taką wiedzę czy mógłby pan nam przybliżyć, jak powszechne jest korzystanie przez samorządy z chmur? Jakie kategorie danych samorządy tam przechowują? Już nie pytam o bezpieczeństwo, ale też i czy to są też usługi komercyjne.

Zastępca dyrektora departamentu MC Marcin Wysocki:

Panie przewodniczący, oczywiście, że korzystają z rozwiązań chmurowych, bo my wszyscy obywatele korzystamy i również urząd, nawet jak nie z tej usługi publicznej jakiejś tam korowej, która jest na przykład częścią systemu rejestrów państwowych, to też korzystają na pewno z rozwiązań chmurowych. Widzimy potrzebę zapewnienia im też tej możliwości, wszystkim samorządom. Natomiast, panie przewodniczący, Centralny Ośrodek Informatyki prowadzi taką ankietę, bo my powinniśmy kształtować od potrzeb, zapewniamy bezpieczeństwo, pytamy samorządy czego potrzebują i na tej podstawie podejmiemy decyzję o rozwoju rządowej chmury obliczeniowej, pozostaniu naszych zasobów kluczowych systemów na terytorium Polsce w tej inwestycji i też w kategorii pozostałych systemów, które może już nie przetwarzają tak istotnych danych, albo potrzebny jest na przykład backup systemu z odpowiednio wysokimi gwarancjami i wtedy te możliwości dla gestorów systemów trzeba...

Jeżeli tutaj szanowna Wysoka Komisja ma jakieś informacje, ma jakieś dane, to my oczywiście prosimy o podzielenie się z Ministerstwem Cyfryzacji, jest ankieta Centralnego Ośrodka Informatyki i na pewno będziemy podejmować taką politykę zgodną z oczekiwaniami, ze wsparciem wszystkich interesariuszy, także tych przede wszystkim odpowiedzialnych za bezpieczeństwo państwa, z którymi jesteśmy zobowiązani ustalić standardy chmury obliczeniowej. Tak jak wskazałem, to będzie akceptacja ministra spraw wewnętrznych i administracji, ministra – koordynatora służb specjalnych i oczywiście ministra obrony narodowej.

À propos przetwarzania usług oczywiście przez wojsko informacji niejawnych, o których wspomniałem, to całe NATO pracuje nad tym, żeby mieć zdolność, żeby przynajmniej do tych informacji niejawnych o najniższej klauzuli mieć taką zdolność w sojuszu do przetwarzania tych danych, ponieważ obieg informacji, co Komisja i wszyscy goście wiedzą, jest szczególnie istotne w dzisiejszych czasach, żeby mieć takie wiarygodne środki komunikacji.

Przewodniczący poseł Michał Krawczyk (KO):

Dziękuję.

Czy ktoś z państwa jeszcze chce zadać pytanie? Nie widzę.

W związku z tym dziękuję państwu bardzo. Wyczerpaliśmy porządek dzienny Komisji. Zamykam posiedzenie.