PROTOKÓŁ z XXXV posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 10 czerwca 2022 roku, o godzinie 12:00 w formie wideokonferencji.

Spotkanie z Panem Michałem Potoczkiem, Prezesem Operatora Chmury Krajowej; Panem Pawłem Ławeckim, Wiceprezesem Operatora Chmury Krajowej oraz Panem Wiesławem Wilkiem, Prezesem Stowarzyszenia Polska Chmura na temat przedstawienia wizji chmury dla Polski.

Pan Wiceprezes Paweł Ławecki przybliżył cztery zidentyfikowane przez Operatora Chmury Krajowej główne aspekty z zakresu pozycji gospodarki cyfrowej na świecie:

1. Rosnący poziom konkurencyjności na zglobalizowanym cyfrowym rynku - tradycyjne biznesy nie mogą się już rozwijać bez wykorzystania nowoczesnych technologii;
2. Rosnące tempo wprowadzania nowych produktów i usług cyfrowych;
3. Powszechne wykorzystanie narzędzi pracy zdalnej - wysoce zaawansowane narzędzia pozwalające na pracę zdalną funkcjonują obecnie tylko w chmurze;
4. Ekspansja zagraniczna polskich firm ze wsparciem technologii to szansa i konieczność, aby zapewnić wzrost polskiej gospodarki.

OChK wyraża przekonanie co do wysokiego poziomu korelacji pomiędzy adopcją chmury w danym kraju, a poziomem jego innowacyjności. Polska ma bardzo dużo do nadrobienia w tej materii. Jest na dalszej pozycji wśród innych krajów w zakresie współczynnika innowacyjności oraz na dalszej pozycji wśród krajów w aspekcie adopcji chmury.

W dalszej części wypowiedzi wskazano czym jest chmura. Jest wysoce skalowalna, a jej podstawową cechą jest płatność za to, czego używamy. W chmurze znajduje się bardzo dużo rozwiązań do wspomagania procesu rozwoju aplikacji i oprogramowania oraz najbardziej innowacyjnych na świecie rozwiązań m.in. do pracy zdalnej, z zakresu Internetu rzeczy, sztucznej inteligencji, procesowania obrazu, generowania mowy z tekstu, platformowych usług skalowalnych baz danych. Zauważono, że obecnie mamy ogromny potencjał wzrostu usług chmurowych w Polsce. W krajach najbardziej zaawansowanych usługi chmurowe jednostkowo są tańsze, z uwagi na efekt skali.

Pan Wiceprezes nakreślił krótko, że Chmura Krajowa powstała w 2018 r. z inicjatywy PKO Banku Polskiego i Polskiego Funduszu Rozwoju. Jest to firma komercyjna z misją współpracowania ze spółkami skarbu państwa, z jednostkami administracji centralnej, a także z misją dostosowania usług chmurowych hyperscaler'ów takich jak Google czy Microsoft do lokalnych realiów, dostosowania do wymogów KNF procesu zakupowego i zbudowania odpowiednich kompetencji w Polsce dla efektywności korzystania z tych narzędzi przez firmy. OChK realizuje dwa duże globalne partnerstwa z Google oraz Microsoft. Dzięki temu, że takie partnerstwa zostały podpisane, w Warszawie utworzył się region Google. Do końca tego roku planowane jest otwarcie regionu Microsoft Azure. Wspomniano,

że powstanie OChK znacznie redukuje wiele z barier zewnętrznych. Do momentu otwarcia regionu Google w Polsce toczyła się często dyskusja m.in. o miejscu rezydowania danych, ich wysyłki oraz sposobie dostosowania tych kwestii do regulacji prawnych. Obecnie umowy, które są już zaakceptowane przez regulatorów, pozwalają na konsumpcję usług chmurowych. OChK funkcjonuje aktywnie, by wspierać firmy w adresowaniu ich barier wewnętrznych. Chmura Krajowa oferuje m.in. odpowiednie dostosowanie usługi w zakresie poziomu bezpieczeństwa oraz zgodności regulacyjnej. Posiada rozwiązanie zbudowania wirtualnego środowiska chmurowego, w sposób spełniający wymogi KNF, a także swoją platformę chmurową i doradza klientowi najlepsze rozwiązanie technologiczne w danym kontekście.

W dalszej części przedstawiono model biznesowy OChK. Fundamentem jest odsprzedaż subskrypcji – OChK sprzedaje usługi Google Cloud, Microsoft Azure, ale oferuje m.in. migrację aplikacji na chmurę, zarządzanie tym procesem, monitorowanie stałe pod kątem bezpieczeństwa. Rozwija także swoje rozwiązania – oferuje projekty dla administracji publicznej wokół kryzysu ukraińskiego, jednostek administracji centralnej czy lokalnej. Współpracuje także z firmami mającymi swoje rozwiązania biznesowe i razem z takim dostawcą oferuje chmurową wersję zabezpieczoną. OChK posiada ok. 200 klientów – od jednostek administracji centralnej, przez duże spółki skarbu państwa, duże i średnie firmy prywatne po jednostki najmniejsze. Oferuje projekty dla klientów z obszaru zdrowia, sektora usług finansowych, ubezpieczeniowych, a także z obszaru turystyki, produkcji żywnościowej, usług cyfrowych. OChK ma kilka flagowych projektów: m.in. budowa systemu obsługującego Narodowy Program Szczepień przeciwko Covid-19 (e-Rejestracja), projekt dla PGNiG – wykorzystanie nowoczesnych technologii do przyspieszenia analizy zasobów węglowodorów w złożach oraz zwiększenia efektywności wydobycia, a także projekt dla firmy „Booksy" – rezerwacja usług online – dostosowanie infrastruktury do zwiększającego się, ale zmiennego zainteresowania ze strony klientów i ekspansji na nowe rynki.

Wspomniano o problemach, z jakimi mierzy się OChK, z zakresu wzrostu usług chmurowych i poziomu innowacyjności w Polsce. Jednym z najważniejszych tematów jest proces PZP, który wprost nie uwzględnia tego, że usługi IT można kupować chmurowo. Brakuje także dobrych praktyk opublikowanych przez Urząd Zamówień Publicznych w jaki sposób kupować usługi chmurowe. Według OChK pomocne byłoby stworzenie jednego centrum usług wspólnych chmurowych dla jednostek administracji centralnej, które zawrą umowę ramową z dostawcami usług chmurowych i wynegocjują lepsze stawki z dostawcami, a także doprowadzą do mocnego wzrostu efektywności. Pomocne może być także porozumienie spółek skarbu państwa w zakresie szukania synergii w obszarze technologii. Ponadto w ramach Krajowego Planu Odbudowy można także zdefiniować szereg inicjatyw transformacyjnych i chmurowych.

Pan Prezes Michał Potoczek podkreślił, że chmura posiada element efektywności kosztowej, czyli pozwala robić pewne rzeczy taniej. Z obserwacji rynku wynika, że głównym motorem napędowym do korzystania z chmury są innowacje. Istotne jest traktowanie chmury nie jako

wehikułu zastępującego infrastrukturę, lecz jako wehikułu do zwiększenia innowacyjności polskich firm oraz gospodarki, dla tworzenia lepszych produktów oraz konkurowania z bardziej rozwiniętymi krajami.

Głos zabrał Pan Prezes Wiesław Wilk i zadał pytanie na jakiej podstawie OChK przyjął zobowiązanie do konsumpcji części polskiego rynku. Zauważył, że trwają konsultacje w ramach nowego prawa zamówień publicznych, w których kwestia chmury stanowiącej wyzwanie dla PZP jest poruszana. Zapytano także, jak przedstawiciele OChK widzą możliwość pogodzenia umowy typu adhezyjnego zawieranej z reguły w przypadku zamawiania usług z Microsoft Azure, Google, Amazon ze specyfiką i istotą zamówień publicznych, w których to zamawiający określa dość precyzyjnie zapisy tych umów według swojego uznania.

Pan Prezes Michał Potoczek odpowiedział, że w kwestii PZP widać postęp. W styczniu Rada Ministrów przyjęła nową strategię zakupową państwa, która w sposób otwarty wskazuje na elementy dotyczące chmury oraz optymalizację, jaką administracja centralna może osiągnąć kupując usługi chmurowe zamiast standardowych usług infrastrukturalnych. W ślad za tą strategią dokonały się pewne rekomendacje w PZP, jednak OChK uważa, że są one niewystarczające, ponieważ nie odpowiadają na proste, codzienne problemy klientów chmury. OChK również uczestniczy w konsultacjach PZP. Co do kwestii komercyjnej i zobowiązań, podpisano umowy z hyperscaler'ami, aby zbudowali w Polsce regiony i dostarczali usługi. Umowy są objęte tajemnicą przedsiębiorstwa. To typowe umowy komercyjne – z jednej strony jest inwestycja, z drugiej jest pewnego rodzaju gwarancja kupowania tych usług przez OChK. Co do umowy adhezyjnej – te umowy są bardzo jednostronne, a warunki są dyktowane przez hyberscaler'ów. Aby ułatwić dużym regulowanym podmiotom kupowanie usług chmurowych, OChK stworzyło model, w którym wynegocjowało z hyperscaler'ami inne warunki, bardziej przystające do potrzeby rynku regulowanego i administracji publicznej.

Pan Wiceprezes Paweł Ławecki odpowiedział na pytanie dotyczące wizji chmury dla Polski. Wskazał, że ta wizja to wykorzystywanie jako fundamentu oferty dużych graczy, dostosowanie tego do polskich realiów, budowanie na tym i osiąganie przewagi konkurencyjnych przez dodawanie nowych innowacyjnych „klocków" w ramach istniejących ekosystemów. Obecnie chmura to nie tylko infrastruktura – jest to także AI, Internet rzeczy, platformy baz danych itd. Pan Prezes Michał Potoczek dodał, że cel powstania OChK to zapewnienie rezydencji danych - aby polscy przedsiębiorcy mogli korzystać w sposób maksymalnie efektywny z usług chmurowych, jednocześnie mając gwarancję, że dane które powierzają do przetwarzania w chmurze nie opuszczają terytorium Polski. Po drugie, aby te usługi były świadczone na zasadach partnerskich oraz po trzecie, aby zbudować i akcelerować wehikuł do pojawiania się na rynku kompetencji. Zdaniem OChK udało się zrealizować cel rezydencji danych – posiadamy inwestycje w Polsce, a także własną infrastrukturę, z której OChK świadczy usługi dla klientów w Polsce, gdzie bezpieczeństwo danych jest najwyższym priorytetem. W ramach programów partnerskich przeszkolonych zostało kilkadziesiąt tysięcy inżynierów w Polsce przez Google i Microsoft. OChK kontynuuje

działania wokół budowania edukacji, dostarczania innowacyjnych rozwiązań oraz wspierania polskiego biznesu z zakresu budowania wartości biznesowych, konkurowania z bardziej zaawansowanymi firmami z zagranicy.

Pan Prezes Michał Potoczek odpowiedział na pytanie dotyczące relacji pomiędzy OChK a chmurą rządową. OChK jest dostawcą komercyjnym chmury. Chmura rządowa budowana przez Centralny Ośrodek Informatyki jako element administracji centralnej. W ramach tej chmury znajdzie się element komercyjny, to tzw. platforma ZUCH. OChK to jeden z dostawców chmury rządowej dostarczający swoje usługi, z których potem zamawiający mogą korzystać na platformie ZUCH.

Europejskie regulacje chmurowe – spotkanie z Panem Łukaszem Wojewodą, Dyrektorem Departamentu Cyberbezpieczeństwa w KPRM; Panem Krzysztofem Silickim, Zastępcą Dyrektora NASK, Dyrektorem ds. Cyberbezpieczeństwa i Innowacji; Panem Tadeuszem Chomickim, Ambassador for Cyber & Tech Affairs; Panią Katarzyną Prusak-Górniak, Radcą/attaché ds. cyfrowych SPRP Bruksela; Panem Wiesławem Wilkiem, Prezesem Stowarzyszenia Polska Chmura.

Jako pierwszy głos zabrał Pan Dyrektor Krzysztof Silicki. Wskazał, że bazą dla architektury certyfikacji w cyberbezpieczeństwie jest „Cybersecurity Act", obowiązujący jako rozporządzenie z 2019 r. Akt przewiduje powstawanie tzw. programów certyfikacji dla produktów, usług lub procesów i definiuje metodykę postępowania w przypadku powstania w określonych grupach produktów, usług czy procesów europejskiego schematu czy programu certyfikacji. Kraje członkowskie, szczególnie te bardziej rozwinięte, mają swoje systemy, w których dokonują certyfikowania - głównie produktów. Rozwijanie się tego systemu europejskiego będzie powodowało, że jeśli pojawi się w danej grupie produktowej europejski program certyfikacji, wówczas krajowy program certyfikacji w danej dziedzinie przestaje działać. W ramach tego procesu została powołana Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa (ECCG), składająca się z reprezentantów wszystkich krajów, w której decydują się najważniejsze kwestie. W pierwszej kolejności podlegały opracowaniu programy certyfikacji. Po przyjęciu *road map* zleca się przygotowanie draftowego programu certyfikacji ENISIE, która otrzymała rolę przygotowywania programów kandydackich. Następnie programy trafiają do konsultacji publicznych oraz do grupy ECCG. Obecnie na *road mapie* są trzy takie programy. Jeden dot. Common Criteria**,** drugi - usług cloudowych, a trzeci - 5G. Co do programu certyfikacji dot. usług chmurowych, ENISA wiele miesięcy temu przygotowała pierwszy draft poddany istotnej analizie przez wszystkich interesariuszy na poziomie UE. Obecnie na ukończeniu jest wersja kolejna, która zostanie wniesiona na posiedzenie grupy ECCG pod koniec czerwca br., gdzie odbędzie się właściwa dyskusja na temat kształtu programu certyfikacji. W tej chwili ta wersja nie jest znana - obecnie nie ma żadnego przyjętego programu certyfikacji.

Jeden z członków Rady zapytał o projekt KSO3C. Pan Dyrektor Krzysztof Silicki odpowiedział, że projekt jest w fazie końcowej - zakłada stworzenie w naszym kraju podstawy do rozwijania

certyfikacji w cyberbezpieczeństwie. W ramach KSO3C powstała jednostka certyfikująca w NASK, która jest akredytowana przez Polskie Centrum Akredytacji. Powstały także dwa akredytowane laboratoria w Instytucie Łączności i w EMAG. W ramach tej współpracy międzynarodowej istotny jest etap końcowy, polegający na tym, że inne kraje bardziej zaawansowane w certyfikacji potwierdzają operacyjną gotowość tego, co zostało stworzone w tym przypadku w naszym kraju. W ramach KSO3C obecnie wykonywana jest certyfikacja w ramach normy Common Criteria.

Wskazano, że Europejski Schemat Certyfikacji wchodzi w życie, nawet jeśli w naszym prawodawstwie nie zostanie wprowadzona dodatkowa legislacja. W nowelizacji KSC jest opisany dość szczegółowo Krajowy System Certyfikacji wzorowany na wskazaniach zawartych w europejskim akcie. Do decyzji kraju członkowskiego należy kwestia posiadania swoich krajowych schematów.

Mówiąc o certyfikacji bardzo ważne jest zrozumienie, że są potrzebne pewne normy i standardy, w oparciu o które dokonuje się oceny zgodności. W przypadku Common Criteria jest to norma, która jest znana od lat. W przypadku usług chmurowych czy 5G są różne dobre praktyki/standardy/podejścia. Europejskie organy standaryzacyjne współpracują z ENISĄ i całym środowiskiem związanym z certyfikacją, żeby w momencie gdy program certyfikacji powstaje, istniały także dojrzałe normy zwane standardami. Jednak w samych założeniach zostało wskazane, że rozwiązaniem może być lekka certyfikacja, oparta nie na długich przepisach norm, ale na zdefiniowanych kryteriach pozwalających dokonać certyfikacji.

Pan Dyrektor odniósł się do kwestii propozycji Francji w postaci tzw. „non paper", do której przyłączyły się Hiszpania i Włochy. Zaprezentowano podejście, że w ramach certyfikacji być może potrzebne jest wprowadzenie innych, mniej technicznych kryteriów z zakresu m.in. lokalizacji danych. Przeciwwagą do „non paper" jest stanowisko innych krajów, takich jak Holandia, Irlandia czy Polska, krytykujące takie podejście i przedstawiające pogląd, że certyfikacja to działanie w oparciu o techniczne wskaźniki/kryteria.

Pan Dyrektor wspomniał o dokumencie „5G Toolbox", który dotyczy europejskiego podejścia w cyberbepieczeństwie. Zostało ono wypracowane pomiędzy krajami członkowskimi, KE, ENISĄ i wskazuje, że w ramach oceny zagrożenia czy wpływu produktów stosowanych w sieciach nowej generacji oraz wpływu na cyberbezpieczeństwo, należy rozważyć kryteria co najmniej z dwóch kategorii – warstwa techniczna i warstwa strategiczna. Trwa dyskusja na ten temat, która będzie rzutowała na całą przyszłość europejskiego podejścia do certyfikacji. W kwestii dotyczącej włączenia pojęcia suwerenności do certyfikacji będzie musiała się odbyć dyskusja, a decyzje nie powinny być podejmowane wyłącznie w roboczych grupach eksperckich, ale także na poziomie strategicznym/politycznym.

Pan Dyrektor Łukasz Wojewoda odpowiedział na pytanie dot. narzucania francuskiej wizji cybersuwerenności w innych gremiach, np. European Alliance for Industrial Data, Edge and Cloud Computing w ramach grupy skupiającej wyłącznie państwa członkowskie. Wskazał, że w razie uzyskania niepokojących informacji na ww. temat, poinformuje o tym Radę.

Pan Ambasador Tadeusz Chomicki odniósł się w szerszej perspektywie (niż tylko ograniczonej do rozwiązań chmurowych) do wątku geopolitycznego. Wskazał, że należy mieć na uwadze kontekst pomysłów budowania suwerenności zgłaszanych przez Francję. Patrząc na cel działania chmury - nawiązując do wypowiedzi przedstawicieli OChK - wskazano, że chmura ma bardzo ścisły związek z innowacyjnością. Natomiast innowacyjność i digitalizacja są warunkami rozwoju gospodarki, a rozwój gospodarki określa nasze miejsce w łańcuchu pokarmowym świata. Wychodząc z tego założenia trzeba widzieć wszystkie pomysły dotyczące suwerenności, autonomii, ponieważ chmura z tej perspektywy daje dostęp do danych i budowania zbiorów danych, które mogą zasilać rozwój sztucznej inteligencji. Jest jednym z narzędzi tworzenia silniejszych podstaw do szybszego rozwoju własnej gospodarki i ostatecznie do określania naszego miejsca w tym łańcuchu pokarmowym. W tym sensie wiele z zabiegów wokół chmury, które mają ograniczyć dostęp firm spoza Europy, wiąże się z zamysłem gromadzenia danych, w oparciu o które będzie można budować własne kompetencje i pozycję rynkową. Procesy dotyczące chmury trzeba widzieć w szerszym kontekście dyskusji. Polska ma wypracowane stanowisko przez KPRM w kwestii suwerenności i autonomii europejskiej w obszarze gospodarki cyfrowej. Chce rozwijać europejskie zdolności w kwestiach cyfrowych, podnosić je, aby europejskie firmy rozwijały się, były silniejsze, miały lepsze miejsce na rynku, m.in. w tym kontekście Polska popiera rozwój Europejskiego Centrum Kompetencji w Cyberbezpieczeństwie. Pan Ambasador uznał, że Europa musi budować swoją samowystarczalność, jednak jest to bardzo długi proces. Brak jest w Europie zasobów technicznych, finansowych, kompetencyjnych, aby odciąć się od partnerów transatlantyckich, w związku z tym nie jest to w naszym interesie. Dobrym kierunkiem, nad którym trzeba popracować także w administracji jest rozgraniczenie prac dotyczących certyfikacji rozwiązań chmurowych pod kątem technicznym (które powinny być skupione na standardach bezpieczeństwa i technicznych – te kwestie należą do ENISY), od dyskusji geopolitycznych/strategicznych, które powinny się odbywać w innych organach politycznych związanych z UE.

Pani Dyrektor Katarzyna Prusak – Górniak nawiązała do pytania jednego z członków Rady wskazując sygnatariuszy „non paper". Inicjatorami są Holendrzy, podpisani są Szwedzi i Irlandczycy. Dyskusje prowadzone są także z Duńczykami i Grekami - są to dyskusje zaawansowane (prowadzone także w szerszym gronie) i obecnie trwa oczekiwanie na ostateczną decyzję.

Pan Dyrektor Łukasz Wojewoda odniósł się do pytania dotyczącego uchwały Rady Ministrów nr 97 w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa"[1] z zakresu dot. cyberbezpieczeństwa. Wskazał, że idea Wspólnej Infrastruktury Informatycznej Państwa jest kontynuowana. KPRM Cyfryzacja przygotowuje się do przeglądu załącznika nr 2, który w niektórych gremiach administracji publicznej jest wskazywany jako trudny do

[1] Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy "Wspólna Infrastruktura Informatyczna Państwa" (M.P. 2019 poz. 862).

zinterpretowania. Pan Dyrektor wspomniał, że istnieje pewne niezrozumienie zagadnienia – nawet jeśli przeniesiemy zasoby do usług chmurowych, to odpowiedzialność za dany system zostaje na wskazanym podmiocie. W „ZUCHU" podjęte jest staranie upraszczania niektórych mechanizmów czy udostępnienie rozwiązania wprowadzającego pewną automatykę. KPRM podejmie się uproszczenia załącznika nr 2 w zakresie stosowania zawartych w nim tabel, tak aby zapisy nie stwarzały wątpliwości.

Pan Wiceprzewodniczący wspomniał, że ww. tematach Rada będzie dążyć do wypracowania stanowiska.

Uczestnicy posiedzenia:

Członkowie Rady:

1. Izabela Albrycht
2. Katarzyna Chałubińska-Jentkiewicz
3. Agnieszka Gryszczyńska
4. Janusz Kosiński
5. Karol Krawczyk
6. Anna Beata Kwiatkowska
7. Mirosław Maj
8. Dariusz Milka - Wiceprzewodniczący
9. Aleksandra Musielak
10. Paweł Śniatała
11. Robert Trętowski
12. Mateusz Tykierko

Zaproszeni goście:

13. Michał Potoczek, Prezes Operatora Chmury Krajowej
14. Paweł Ławecki, Wiceprezes Operatora Chmury Krajowej
15. Wiesław Wilk, Prezes Stowarzyszenia Polska Chmura
16. Krzysztof Silicki, Zastępca Dyrektora NASK, Dyrektor ds. Cyberbezpieczeństwa i Innowacji
17. Tadeusz Chomicki, Ambassador for Cyber & Tech Affairs
18. Katarzyna Prusak-Górniak, Radca/attaché ds. cyfrowych SPRP Bruksela
19. Łukasz Wojewoda, Dyrektor Departamentu Cyberbezpieczeństwa w KPRM
20. Tomasz Wlaź, Główny specjalista ds. międzynarodowych aspektów cyberbezpieczeństwa w Ministerstwie Spraw Zagranicznych

Sekretariat Rady i pracownicy Kancelarii Prezesa Rady Ministrów:

21. 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
22. Michał Pukaluk, Dyrektor Departamentu Polityki Cyfrowej w KPRM
23. Ewa Świętochowska, Ekspertka, Departament Tożsamości Cyfrowej w KPRM

24. Katarzyna Stopińska, KPRM
25. Joanna Laskowska, KPRM