

## PROTOKÓŁ z XXXIV posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 20 maja 2022 roku, o godzinie 12:00 w Kancelarii Prezesa Rady Ministrów.

Projekt stanowiska Rady: Strategia dot. narodowego zasobu informacyjnego – Pan Jarosław Mojsiejuk, ekspert Rady.

Projekt Uchwały został uprzednio wysłany do członków Rady do zapoznania się i zgłoszenia uwag. Decyzją Przewodniczącego zostało przeprowadzone głosowanie nad przyjęciem projektu Uchwały – wszyscy członkowie obecni na posiedzeniu opowiedzieli się za przyjęciem Uchwały. Nie zgłoszono uwag.

### Wolne wnioski.

Jeden z członków Rady omówił raport na temat chmury i cyberbezpieczeństwa wśród średnich i dużych firm oraz w sektorze GovTech w Polsce, przygotowany na zlecenie Polskiej Chmury. Zostały wskazane obszary analizy, tj. gotowość firm produkcyjnych do przejścia do chmury w szczególności z elementami związanymi z zarządzaniem i produkcją oraz ocena poziomu nasycenia systemami informatycznymi w firmach.

Metodyka badania opierała się na badaniu ilościowym i telefonicznym. Najważniejsze wnioski z przeprowadzonego raportu przedstawiają się następująco:

- 2/3 badanych firm korzysta już rozwiązań chmurowych z sektora gospodarczego,
- niewiele ponad 1/3 zasobów jest przechowywana w chmurze,
- firmy zatrudniające ponad 250 pracowników częściej używają chmury,
- 3/4 firm korzysta z chmury prywatnej,
- większe firmy częściej korzystają z chmur publicznych i hybrydowych, najczęściej w modelu SaaS,
- tylko 2/5 badanych firm deklaruje dalsze inwestycje.

Większość przedsiębiorstw preferuje rozwiązania dostawców z polskim kapitałem. Głównymi kryteriami, którymi kierują się firmy w wyborze dostawcy usług chmurowych są: certyfikaty, całkowita cena rozwiązania, elastyczność oraz przejrzystość oferty. Dla firm ważne jest, aby Data Center zlokalizowane było w kraju należącym do UE, a najlepiej w Polsce.

Jeśli chodzi o GovTech, to co czwarty podmiot deklaruje korzystanie z chmury, co dziesiąty korzysta z usług Samorządowego Centrum Usług Wspólnych. Instytucje, które nie korzystają z chmury, uzasadniają to brakiem potrzeb. Chmury najczęściej są wykorzystywane w formie prostego oprogramowania biurowego oraz finansowo-księgowego. Co czwarty podmiot planuje w ciągu kolejnych 24 miesięcy inwestycje w rozwiązania chmurowe. 12% spodziewa się, że w tym czasie do chmury zostanie przeniesione przynajmniej część zasobów. Dla ośmiu na dziesięć badanych krytyczna jest również kwestia suwerenności danych. Kwestia lokalizacji Data Center w naszym kraju jest istotna dla zdecydowanej większości podmiotów.

Po zakończeniu prezentacji raportu członkowie Rady rozpoczęli dyskusję. Podkreślono, że jeśli chodzi o wnioski związane z raportem, to powinno zwrócić się uwagę na suwerenność. Natomiast nawiązując do administracji publicznej, szczególnie organów samorządowych, to istnieje tu problem nowych technologii i nowych rozwiązań, które przynoszą zmiany w sposobie realizacji zadań publicznych.

Podkreślono, że jeśli chodzi o chmurę, to istnieją dwa różne obszary. Pierwszy obszar to budowanie usług w architekturze publicznej, drugi zaś to budowa centrum przetwarzania danych, gdzie ma być umieszczony zasób informacyjny państwa. Te systemy, które są przekazywane samorządom na poziomie powiatów, czy też gminy, wiążą się z zadaniami zleconymi przez państwo i powinny być wykonane w tej samej architekturze.

Podczas dyskusji zwrócono również uwagę na Departament Architektury Informacyjnej Państwa w KPRM i całą instytucję nadzorowania i realizacji Architektury Informacyjnej Państwa. Rada postanowiła zająć stanowisko w tej sprawie.

[Regulacja chmurowa w Unii Europejskiej – Pan Jarosław Mojsiejuk, ekspert Rady oraz Pan Michał Kanownik.](#)

W prezentacji pokazano dwa główne problemy: tsunami legislacyjne UE w zakresie cyberbezpieczeństwa chmury oraz prace nad European Cybersecurity Certification Scheme for Cloud Services (EUCS). Wskazane zostało, że jeśli chodzi o podstawy prawne, to nie ma specjalnej regulacji prawnej dotyczącej chmury w UE. Zapisy odnoszące się do usług chmurowych są zapisane w wielu różnych aktach prawnych. Usługi chmurowe charakteryzuje outsourcing oraz wielodzierżawa, które polegają na dzieleniu zasobów między wielu usługobiorców, w tym samym czasie. Kluczową cechą rozwiązań chmurowych jest skalowanie i wirtualizacja.

W przypadku konstrukcji umów dostawca, ze względu na mnogość odbiorców i ich rozproszenie, jest zmuszony jak najbardziej ujednoczyć ich wzorzec tak, aby odpowiadał on potrzebom wszystkich użytkowników, a jednocześnie spełniał oczekiwania ekonomiczne i biznesowe. EUCS wynika z wdrożenia Cybersecurity Act. Przygotowany jest przez ENISA; oczekuje się, że uzgodniona wersja zostanie przekazana do Komisji Europejskiej latem 2022 r. Wdrożenie EUCS, czyli pierwsze certyfikaty będą wydawane już w 2023 r.

Do istniejących i stosunkowo niedawno przyjętych aktów - jak Cybersecurity Act, NIS, RODO, a także rozporządzenie o swobodnym przepływie danych nieosobowych - dochodzą nowe, z których najistotniejsze znaczenie mają projekty: Digital Governance Act (DGA), NIS 2, Data Act (DA). Komisja Europejska przygotowała propozycję nowej dyrektywy w sprawie odporności podmiotów krytycznych - dyrektywę CER. Na podstawie tej dyrektywy ma zostać opracowany jednolity sposób identyfikacji podmiotów krytycznych oraz sposoby ochrony podmiotów identyfikowanych jako krytyczne, w tym ustalenie zasad przeciwdziałania wszystkim zagrożeniom.

KE przedstawiła też propozycję rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego, tzw. rozporządzenie DORA. Cybersecurity Act nie nakłada obowiązku

stosowania, ale Dyrektywa NIS2 wskazuje już, że trzeba będzie stosować certyfikaty obowiązkowo.

Praktyczne wdrożenie Cybersecurity Act odbywa się powoli, potrzebna jest certyfikacja usług chmurowych. Polscy dostawcy chmury mogą mieć problem z procesem certyfikacji „C5” dla poziomu Basic/Substantial oraz „SecNumCloud” dla poziomu High. Pojawiają się wątpliwości, czy mając suwerenne certyfikaty rzeczywiście podnosi się poziom bezpieczeństwa, zwłaszcza na poziomie High. Powinna zostać wprowadzona synchronizacja certyfikacji unijnych z certyfikacjami NATO. EUCS zakłada wprowadzenie kryterium „wymagań suwerenności” jako warunku koniecznego dla przyznania certyfikatu wysokiego poziomu.

Zwrócono również uwagę na brak jednolitej klasyfikacji danych w UE (Data Classification). Wyparcie „nieeuropejskich” dostawców chmury oznaczać może załamanie na rynku cyfrowym.

Wspomniano, że uzyskanie harmonizacji certyfikacji technologii chmurowych na poziomie europejskim – zgodnie z przyjętymi celami EUCS – jest wysoce pożądane, podobnie jak transparentność procesu powstawania programu standaryzacji i jego późniejszego wdrożenia. Nadrzędnym celem regulacji dotyczących technologii cyfrowych powinna być odporność na upływ czasu i ograniczenia ryzyka niedostosowania regulacji do realiów rynku cyfrowego oraz postępu technologii. Istotne jest, aby program EUCS powstał z uwzględnieniem głosów nie tylko największych państw UE, lecz szerszego grona zainteresowanych stron oraz zachował dobrowolny charakter.

#### [Spotkanie z Panem Ministrem Januszem Cieszyńskim.](#)

Pan Minister odpowiadał na pytania zadawane przez Członków Rady.

Pan Przewodniczący przekazał, że według Rady jest potrzebna polska strategia chmurowa, ze względu na zmierzanie europejskich regulacji chmurowych w kierunku dyskryminacji firm amerykańskich i równoległe wpływanie na wskazanie standardów charakterystycznych dla Francji oraz Niemiec, co jest niebezpieczne nie tylko dla Polski. Rada będzie budować stanowisko w tej sprawie i zapraszać przedstawicieli reprezentujących Polskę w negocjacjach z tego zakresu. Jeśli chodzi o regulacje chmurowe to Pan Minister wspominał o przeprowadzonej rozmowie z ówczesnym Ministrem Cyfryzacji Francji.

Pan Minister odniósł się do kwestii informacyjnego państwa. Zakomunikował, że wszędzie tam, gdzie jest potencjał, powinny rozwijać się zespoły technologiczne. Jeżeli coś powstaje bez konsultacji z Departamentem Architektury Informacyjnej Państwa KPRM, ale z dobrą, użyteczną, działającą, ekonomiczną e-usługą to dobrze, że to powstaje. Pan Minister podkreślił, że cieszy się, iż są tworzone kolejne zespoły, które realizują takie projekty.

Jeden z członków Rady poruszył kwestie współpracy z Ukrainą. Pan Minister odpowiedział, że na chwilę obecną nikt nie myśli strategicznie, Ukraina na bieżąco jest wspierana w wielu dyplomatycznych, praktycznych inicjatywach.

Zapytano Pana Ministra o kwestie komunikacji elektronicznej, jeżeli chodzi o usługi przedpłacone. Jakiś czas temu uzgodniono kompromisową wersję między KPRM, UKE i UOKiK dotyczącą nieprzekazywania numeru rachunku bankowego podczas realizacji usług przez konsumentów. Po czym na posiedzeniu Stałego Komitetu Rady Ministrów nastąpiła zmiana i opcja podawania tego numeru rachunku została w ustawie przywrócona. Pan Minister odpowiedział, że jest to już jednoznaczne stanowisko Prezesa UOKiK.

Kolejne pytanie dotyczyło kręgu podmiotów uprawnionych do świadczenia teleinformatycznego, czy planowane są zmiany w tym zakresie. Pan Minister odpowiedział, że w tej chwili trwa nowelizacja ustawy. Jest to jeden z wniosków po wykonaniu pierwszej rundy świadczeń teleinformatycznych. W tym temacie ma zostać przygotowane stanowisko Rady.

Poruszone zostały także kwestie dotyczące współpracy z różnymi podmiotami, m.in. z Facebookiem i Twitterem, w kwestii dezinformacji i cyberprzestępczości oraz realizacji prac nad Aktem o usługach cyfrowych. Pan Minister wskazał, że w kraju nie ma instytucji, przygotowanej merytorycznie, która mogłaby wypełniać te zadania. Podkreślił również, że nie należy obawiać się Rady Wolności Słowa. Rada powinna działać w oparciu o merytorycznie przygotowane materiały - działania te powinny być inicjowane przez zewnętrznych ekspertów. Najważniejsze jest, żeby Rada pracowała w sposób, który odzwierciedla głos większości społeczeństwa.

## Uczestnicy posiedzenia:

### Członkowie Rady:

1. Izabela Albrycht
2. Andrzej Dulka
3. Agnieszka Gryszczyńska
4. Michał Kanownik
5. Janusz Kosiński
6. Karol Krawczyk
7. Mirosław Maj
8. Dariusz Milka - Wiceprzewodniczący
9. Aleksandra Musielak
10. Józef Orzeł - Przewodniczący
11. Paweł Śniatała
12. Mateusz Tykierko

### Zaproszeni goście:

13. Janusz Cieszyński, Sekretarz Stanu w KPRM; Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
14. Wiesław Paluszyński, ekspert Rady
15. Jarosław Mojsiejuk, ekspert Rady

### Sekretariat Rady i pracownicy Kancelarii Prezesa Rady Ministrów:

16. Krzysztof Głomb, Pełnomocnik Ministra Cyfryzacji do spraw współpracy z administracją samorządową Rzeczypospolitej Polskiej; Pełnomocnik Ministra Cyfryzacji do spraw relacji z podmiotami działającymi na rzecz rozwoju kompetencji cyfrowych
17. Katarzyna Stopińska, KPRM
18. Anna Supeł, KPRM
19. Joanna Laskowska, KPRM