Warszawa, 31.08.2022 r.

Szanowny Pan
Janusz Cieszyński
Sekretarz Stanu,
Kancelaria Prezesa Rady Ministrów

Szanowny Panie Ministrze,

W imieniu Związku Cyfrowa Polska, branżowej organizacji pracodawców, która zrzesza największe firmy z branży RTV i IT działające w Polsce, a w tym producentów, importerów i dystrybutorów sprzętu elektrycznego i elektronicznego, przedkładam naszą opinię do projektu *ustawy o przygotowaniu i realizacji inwestycji w zakresie Krajowego Centrum Przetwarzania Danych (UD 424).*

Poniżej znajdą Państwo zagadnienia, które naszym zdaniem należy uszczegółowić lub zmodyfikować na dalszym etapie procedowania rzeczonej ustawy.

1. **Wyłączanie zastosowania przepisów prawa zamówień publicznych (PZP) oraz Prawa budowalnego**

W uzasadnieniu projektowanej ustawy (Projekt, str. 63 i nast.) możemy przeczytać, że:

Stosowanie terminów i procedur z ustawy Pzp uniemożliwiłoby zapewnienie terminowej realizacji wysokospecjalistycznych zamówień finansowanych w ramach Krajowego Planu Obudowy i Zwiększenia Odporności, a także dochowania kamieni milowych.

Proponowana struktura wydatków (str. 103) również to potwierdza:

(ceny stałe z 2022 r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł brutto]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Wydatki ogółem (brutto)	1,37	135,52	275,13	397,55	255,36	49,58	54,53	59,99	65,99	96,78	106,46	1498,25
budżet Państwa*	0,00	0,00	0,00	0,00	45,07	49,58	54,53	59,99	65,99	96,78	106,46	478,40
KPO	1,37	135,52	275,13	397,55	210,29	0,00	0,00	0,00	0,00	0,00	0,00	1019,86

www.zipsee.pl
Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

Struktura wydatków wskazuje, że 1019 mln złotych z KPO zostanie wydane w ciągu trzech lat, zaś z budżetu państwa 433 mln złotych (z budżetu 478 mln złotych) to będą wydatki od 5 do 10 roku trwania projektu.

Rozumiejąc oczywiście zamysł projektodawcy by większość inwestycji zrealizować ze środków europejskich w ramach KPO, w naszym przekonaniu projekt ustawy w obecnym kształcie wywrze jednak negatywny wpływ na transparentność i zwiększy uznaniowość zamówień publicznych. Wyłączając w szerokim zakresie stosowanie przepisów PZP, planowane zmiany umożliwiają zamawiającemu wybór wykonawcy bez konieczności przeprowadzania przetargu, czy skierowania zaproszenia do negocjacji. Naszym zdaniem, proponowane zmiany ram prawnych w wyraźny sposób narażają bezstronność i niezależność procesu doboru wykonawcy. Wymóg zaproszenia co najmniej trzech wykonawców (art. 4 ust. 4) stanowi środek mitygujący, niemniej projekt ustawy nie przewiduje sankcji za naruszenie tego zobowiązania i dopuszcza zaproszenie mniejszej liczby w wyjątkowych sytuacjach.

Proponujemy także, aby w projektowanych przepisach ustawy rozważyć możliwość przeprowadzenia zamówienia w jednym z trybów występujących już w ustawie prawo zamówień publicznych, tj. w trybie przetargu ograniczonego, w trybie negocjacji z ogłoszeniem, lub w trybie dialogu konkurencyjnego (jedną z pierwszych przesłanek tego trybu jest udzielenie zamówienia na podstawie kryteriów jakościowych). Z pewnością przyczyni się to do zwiększenia procedury transparentności zamówienia oraz nie wpłynie negatywnie na harmonogram realizacji tej inwestycji.

W tym miejscu warto także zauważyć, że większe inwestycje związane z budową centrów przetwarzania danych były wykonywane w Polsce, nawet w krótszym czasie niż zakładana budowa KCPD.

Polska stała się miejscem inwestycji i budowy tzw. regionów chmurowych dla wielu komercyjnych dostawców z Europy i ze świata. Inwestycje firm, m.in. Google, w stworzenie regionu chmurowego w Polsce to 2 mld dolarów, zaś firmy Microsoft to 1 mld dolarów. Region chmurowy, to podobnie jak w projekcie ustawy, co najmniej trzy centra przetwarzania danych. Obie inwestycje są kilkukrotnie większe niż wskazany w projekcie ustawy koszt stworzenia KCPD.

www.zipsee.pl
Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

Co więcej, uruchomienie regionu Google – co oznacza nie tylko przygotowanie lokalizacji i postawienie budynków, ale dostępność usług dla klientów – zostało osiągnięte w dwa lata, zaś później ogłoszona inwestycja Microsoft ma się ku końcowi (obecnie od chwili rozpoczęcia prac minęło nieco ponad dwa lata). Obydwie inwestycje były bardzo dobrze przyjęte przez polski rząd, czego dowodem było osobiste zaangażowanie się Prezesa Rady Ministrów, Pana Mateusza Morawieckiego.[1]

2. Brak sprecyzowania zakresu przechowywanych danych w Krajowym Centrum Przetwarzania Danych

Projekt ustawy wraz z uzasadnieniem i OSR nie precyzuje zakresu danych, które mają być przechowywane w projektowanym centrum danych, ani jasno nie określa grupy podmiotów, które będą z jednej strony beneficjentami tego rozwiązania, z drugiej – których dane będą podlegały takiemu przechowywaniu. Tymczasem podstawowym krokiem w wyborze odpowiednich narzędzi oraz w zarządzaniu ryzykiem cyberbezpieczeństwa jest klasyfikacja danych. Polega ona na identyfikacji typów danych, które są przetwarzane i przechowywane w systemie informacyjnym będącym własnością lub obsługiwanym przez określoną organizację. Wiąże się to również z określeniem wrażliwości danych i prawdopodobnego wpływu, jeśli dane zostaną naruszone, utracone lub wykorzystane niezgodnie z przeznaczeniem. W Polsce obowiązują poziomy SCCO, na których oparty jest m.in. system ZUCH. Lista kontroli bezpieczeństwa opiera się na klasyfikacji NIST SP 800-53, która tworzy warunki niezbędne do spełnienia wymagań sektora publicznego i infrastruktury krytycznej określonych w polskim ustawodawstwie. Według tej klasyfikacji danych jedynie kontrolowane wrażliwe informacje urzędowe (poziom SCCO3) oraz informacje niejawne (poziom SCCO4) powinny być przetwarzane w Rządowej Chmurze Obliczeniowej. Zdecydowana jednak większość danych administracji publicznej (niekontrolowane informacje nieklasyfikowane SCCO1 oraz kontrolowane informacje urzędowe SCCO2) może być hostowana również przez dostawców usług publicznych (komercyjnych) chmur obliczeniowych. Postulujemy, aby projekt KCPD uwzględniał istniejącą klasyfikację danych oraz zwracamy uwagę, jak ważne jest zachęcanie organów administracji publicznej i samorządowej do dywersyfikowania dostępnych metod przechowywania i przetwarzania

[1] https://www.radiomaryja.pl/informacje/inwestycja-google-w-polsce-moze-byc-warta-2-mld-dolarow/ oraz https://www.tvp.info/47889231/microsoft-inwestuje-w-baze-danych-w-polsce-premier-mateusz-morawiecki-niech-z-chmury-danych-spadnie-deszcz-pomyslow-wieszwiecej

www.zipsee.pl
Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

danych w celu zwiększania bezpieczeństwa, podnoszenia dostępności i innowacyjności e-administracji, jak również oszczędności

3. **Budowa i lokalizacja centrów przetwarzania danych, a poziom bezpieczeństwa cybernetycznego państwa**

Istnieje szereg analiz ekspertów z dziedziny prawa oraz cyberbezpieczeństwa, które wskazują na poważne ryzyka związane z tzw. „twardą / stałą lokalizacją danych" (ang. *hard data localization*) dla bezpieczeństwa cybernetycznego i zdolności organizacji (np. agencji rządowych) do obrony przed cyberatakami. Wśród tych ryzyk należy wymienić m.in. trudności w zintegrowanym zarządzaniu ryzykiem cyberbezpieczeństwa, przeszkody w korzystaniu przez dany kraj z najnowocześniejszych technologii i rozwiązań w zakresie ochrony przez cyberatakami, a także brak warunków dla dzielenia się danymi pomiędzy różnymi organizacjami, z uwagi na prawne lub organizacyjne ograniczenia w przekazywaniu danych. Podzielamy wypływający z tych analiz wniosek, że fizyczna lokalizacja danych na terytorium danego państwa nie chroni ich przed nieuprawnionym dostępem, a co więcej, dodatkowo zwiększa podatność takiego niezależnego, krajowego centrum danych na wszelkie zagrożenia cybernetyczne, pozbawiając je bieżącego i aktualnego dostępu do najnowszych środków bezpieczeństwa, oferowanych przez komercyjnych dostawców.

W tym kontekście szczególnie istotne wnioski wypływają także z analizy działań podejmowanych w zakresie ochrony systemów i infrastruktury cyfrowej podejmowanych przez rząd Ukrainy w toku przygotowania oraz trwania konfliktu zbrojnego z Rosją. Analiza ostatnich wydarzeń na Ukrainie ukazuje jak istotną rolę odgrywają nowe technologie i usługi chmurowe w zakresie ochrony danych i informacji sektora publicznego nie tylko w czasie pokoju, a także w okresie zagrożenia militarnego. Doświadczenia rządu Ukrainy, którego obiekty czy centra danych stanowiły istotny cel ataków rosyjskich, ukazały jak ważna jest dywersyfikacja źródeł przechowywania danych, jeśli chodzi o miejsce i dostawcę usługi, jak również stosowanie rozwiązań publicznej (komercyjnej) chmury obliczeniowej. Sukces obrony Ukrainy wynika bowiem, jak się wydaje (bazując na dostępnych aktualnie informacjach), w znacznym stopniu z jej zdolności do sprawnego przenoszenia danych ze zlokalizowanych fizycznie na jej terytorium serwerów i uzyskania do nich dostępu poza granicami własnego państwa.

www.zipsee.pl
Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

Co więcej, koncentracja danych w fizycznych centrach z zasady zwiększa ryzyko ich utraty. W przypadku wystąpienia np. klęski żywiołowej czy wskutek wspomnianych już działań wojskowych, serwerownie są wyjątkowo narażone, podobnie jak reszta infrastruktury. Przykładowo, w 2021 r. w Strasburgu doszło do pożaru w serwerowni jednego z francuskich dostawców technologii przetwarzania w chmurze, który spowodował paraliż znaczącej części sieci internetowej. Wiele firm, w tym z Polski, straciło swoje dane, a ich strony internetowe przestały działać. Z tego powodu korzystanie z usług oferowanych przez przedsiębiorstwa globalne (np. usługi chmurowe) potencjalnie podwyższa, a nie obniża, poziom cyberbezpieczeństwa jednostek administracji rządowej.

W celu przeciwdziałaniu zagrożeniom kinetycznym, fizycznym albo szerzej militarnym dla krytycznej infrastruktury informatycznej państwa, należy też rozważyć budowę rozwiązań typu e-Ambasada i/lub mobilnych CPD, dla których być może konieczna byłaby regulacja ustawowa związana z transferem danych do miejsc bezpiecznych, nawet poza terytorium UE. W tego typu analizach dotyczących bezpieczeństwa danych, trzeba szukać różnych rozwiązań w tym wspomnianych mobilnych CPD, które w razie zagrożenia można łatwo spakować i przenieść w dowolne, bezpieczne miejsce.

4. Relacja między Projektem ustawy a obowiązującym ustawodawstwem krajowym

Rozważając utworzenie krajowej infrastruktury chmurowej, należy mieć także na uwadze obowiązujące w polskim porządku prawnym istotne regulacje w zakresie cyberbezpieczeństwa. Do takich należą m.in. Uchwała Rady Ministrów z dnia 11 września 2019 r. w sprawie Wspólnej Infrastruktury Informatycznej Państwa (dalej: „**WIIP**"). Przyjęciu WIIP przyświecała potrzeba zapewnienia bezpieczeństwa danych przetwarzanych w systemach teleinformatycznych podmiotów administracji publicznej oraz optymalizacji kosztów utrzymania tych systemów, a także konieczność wspierania podmiotów administracji publicznej w utrzymaniu tych systemów oraz zapewnienia wysokiego poziomu usług świadczonych społeczeństwu przez administrację publiczną. Istotnym elementem WIIP jest System Zapewniania Usług Chmurowych ZUCH, który powinien służyć do promowania, wyszukiwania i zakupu zweryfikowanych pod względem bezpieczeństwa rozwiązań chmurowych przez szeroko rozumiany sektor publiczny. WIIP oraz ZUCH jasno wskazują, że dla bezpiecznego przechowywania i przetwarzania tak dużej ilości danych, jakie są gromadzone przez administrację rządową i samorządową nie ma innej alternatywy niż chmura, w tym

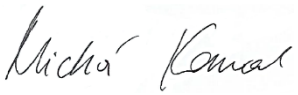
www.zipsee.pl
Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

chmura publiczna gwarantująca oszczędność, bezpieczeństwo, elastyczność i skalowalność. Tymczasem, analiza udostępnionego Projektu ustawy wraz z uzasadnieniem i OSR nie umożliwia ustalenia jasnej relacji pomiędzy zakresami unormowań WIIP, ZUCH oraz innymi wymogami dla funkcjonowania rządowej chmury obliczeniowej, a planowanym KCPD.

Konkludując, w naszej opinii projektodawca jeszcze raz powinien rozważyć i sprecyzować tak fundamentalne kwestie całej inwestycji, jak: wyłączenie stosowania prawa zamówień publicznych, zakres przechowywanych danych, cyberbezpieczeństwo w ujęciu lokalizacji i rozproszenia oraz dywersyfikacji serwerów, odniesienia do istniejących już regulacji prawnych w przedmiotowym zakresie.

Pozostajemy do dyspozycji na dalszym etapie procedowania ustawy.

Z wyrazami szacunku,
Michał Kanownik



Prezes Zarządu
Związek Cyfrowa Polska