Stanowisko ZPP w sprawie Projektu ustawy o przygotowaniu i realizacji inwestycji w zakresie Krajowego Centrum Przetwarzania Danych (UD424)

Na stronach Rządowego Centrum Legislacji 22 sierpnia 2022 r. opublikowano Projekt ustawy o przygotowaniu i realizacji inwestycji w zakresie Krajowego Centrum Przetwarzania Danych (KCPD). Celem zaproponowanego projektu jest stworzenie ram prawnych umożliwiających realizację inwestycji wzmacniającej bezpieczeństwo cybernetyczne zasobów administracji rządowej. Realizacja ta będzie polegać na budowie usług cyfrowych dla systemów teleinformatycznych administracji publicznej wraz z zabezpieczeniem infrastruktury krytycznej.

Związek Przedsiębiorców i Pracodawców aktywnie uczestniczy w pracach legislacyjnych dotyczących gospodarowania i zarządzania danymi. Monitorujemy także możliwe zmiany regulacji w obszarze polityki cyfrowej. Stąd, po przeprowadzonej analizie zaproponowanych przepisów, chcielibyśmy zwrócić uwagę na kilka kluczowych elementów projektu ustawy, które mogą prowadzić do efektów odwrotnych, niż te założone przez ustawodawcę. W naszej opinii część przedstawionych rozwiązań może obniżyć poziom bezpieczeństwa przechowywanych danych, a także zmniejszyć możliwość zarządzania danymi w przypadku zaistnienia sytuacji kryzysowej.

WYŁĄCZENIE ZASTOSOWANIA PRZEPISÓW USTAWY PRAWO ZAMÓWIEŃ PUBLICZNYCH (PZP)

W pierwszej kolejności chcielibyśmy zwrócić uwagę na artykuły 10 oraz 49 powyższego projektu ustawy. Wprowadzają one wyłączenie zastosowania przepisów ustawy Prawo Zamówień Publicznych (PZP) w stosunku do "do zamówień związanych z przygotowaniem, realizacją i użytkowaniem inwestycji w zakresie Krajowego Centrum Przetwarzania Danych (...)".[1] Ponadto, na podstawie artykułu 49, z podlegania przepisom PZP zwolnione zostaną także umowy dotyczące realizacji KCPD, które zostały zawarte przed wejściem w życie omawianej ustawy. Ustawodawca wprowadzając specjalną procedurę udzielania zamówień powołuje się w uzasadnieniu szczegółowym projektu ustawy na rozdział I, oddział 2 Ustawy Prawo Zamówień Publicznych o wyłączeniach zastosowaniu tego aktu prawnego.

W naszej ocenie wyłączenie zastosowania przepisów PZP doprowadzi do zmniejszenia transparentności procesu inwestycyjnego oraz zwiększy uznaniowość wydatkowania środków budżetowych w ramach prowadzonych zamówień publicznych. Zawarta obecnie propozycja wyłączenia przygotowania i inwestycji w zakresie KCPD z przeprowadzania przetargu czy skierowania zaproszenia do negocjacji jest nieproporcjonalna do specyfiki planowanej inwestycji.

Uważamy, że zamówienia powinny być udzielane z uwzględnieniem kryteriów jakościowych, dlatego sugerujemy, aby projekt ustawy powiązał możliwość wyboru wykonawcy z jednym z trybów przewidzianych przepisami ustawy PZP, tj. przetargu ograniczonego, negocjacji z ogłoszeniem czy dialogu konkurencyjnego. Pozwoli to na utrzymanie wiarygodności niezależnego wyboru wykonawcy dzięki przejrzystym procedurom składania zamówienia.

[1] Artykuł 10 Projektu ustawy o przygotowaniu i realizacji inwestycji w zakresie Krajowego Centrum Przetwarzania Danych (UD424)

Z uwagi na wysokospecjalistyczny charakter planowanej inwestycji pożądana jest konkurencja zainteresowanych podmiotów oparta na jasnych i przejrzystych zasadach. Ilość podmiotów mogących się podjąć rzeczonego przedsięwzięcia jest ograniczona, zatem zastosowanie procedur ustawy PZP nie będzie prowadziło do mnogości ofert, których rozpatrzenie mogłoby okazać się czasochłonne. Na rynku funkcjonuje ograniczony katalog podmiotów prywatnych, które z powodzeniem oraz dochowaniem najwyższych standardów realizują przedsięwzięcia tworzenia centrów przetwarzania danych. Wobec powyższego przeprowadzenie konkurencyjnego postępowania z zastrzeżonymi maksymalnymi wymogami jakościowymi oraz dotyczącymi bezpieczeństwa zapewni lepszy środek wyboru wykonawcy inwestycji niż wyłączenie przepisów PZP.

Projekt ma być realizowany ze środków budżetowych oraz europejskich uzyskanych w ramach Krajowego Planu Odbudowy. W związku z tym niezbędne może być rozliczenie otrzymanych funduszy oraz wykazanie, że zostały one wydane w sposób możliwie efektywny i nie budzący wątpliwości co do bezstronności wyboru wykonawcy.

Dotychczasowe inwestycje sektora prywatnego w zakresie budowy centrów przetwarzania danych były realizowane w Polsce w relatywnie krótkim czasie - do dwóch lat. Komercyjni dostawcy, którzy zdecydowali się utworzyć w Polsce swoje centra przetwarzania danych, tworzą przestrzeń chmurową większą niż ta zakładana w ramach KCPD, zatem nie należy spodziewać się przewlekłości przy inwestycji mniejszych rozmiarów.

Podsumowując, powyższy środek nie spowoduje wydłużenia realizacji inwestycji, a zapewni transparentność wydatkowania pieniędzy publicznych, więc jego wyłączenie należy uznać za zbyteczne.

NIESPRECYZOWANY ZAKRES DANYCH JAKIE MAJĄ BYĆ PRZECHOWYWANE W KRAJOWYM CENTRUM PRZECHOWYWANIA DANYCH

Projekt ustawy nie zawiera informacji o zakresie ani rodzaju danych jakie mają być przechowywane w KCPD. Co więcej, projekt ustawy nie określa grupy podmiotów, które mają korzystać z danych zgromadzonych w KCPD. W związku z powyższym nie wiadomo, czy przechowywaniu będą podlegały jedynie pewne kategorie danych osobowych, takie jak dane wrażliwe, czy zakres ten będzie rozszerzony także na inne rodzaje danych. Nie podano także, kto będzie mógł korzystać z danych zgromadzonych z KCPD. Zatem nie ma możliwości ukształtowanie protokołów bezpieczeństwa związanych z dostępem do danych na tym etapie.

Należy podkreślić, że jest to informacja niezbędna dla określenia procedur związanych z bezpieczeństwem przechowywanych danych. Ponadto przyjęcie takich standardów powinno też precyzować sposób postępowania z danymi w przypadku zagrożenia cybernetycznego lub fizycznego związanego z ryzykiem wystąpienia klęski żywiołowej czy ataku militarnego na budynek KCPD. Zarządzanie danymi w przypadku zagrożeń cybernetycznych jest oparte na ich odpowiednim sklasyfikowaniu. Właściwa identyfikacja pozwala na ich powiązanie z podmiotem zawiadującym danymi oraz należyte określenie wpływu jaki może mieć ich nieuprawnione przejęcie bądź rozpowszechnienie.

Ponadto należy zwrócić uwagę, że w Polsce funkcjonuje System Zapewniania Usług Chmurowych (ZUCH). Jest on uregulowany obowiązującymi Standardami Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO), które stanowią zbiór wymagań prawnych, technicznych i organizacyjnych mających na celu zapewnienie bezpieczeństwa we wdrażaniu rozwiązań chmurowych do celów obliczeniowych będących częścią szerszej inicjatywy Wspólnej Inicjatywy Informatycznej Państwa (WIIP).

Polskie prawodawstwo ukształtowało warunki jaki muszą zostać spełnione przez sektor publiczny oraz infrastrukturę krytyczną. Są one zawarte w liście kontroli bezpieczeństwa NIST SP 800-53, która kategoryzuje dane mające być przetwarzane w Rządowej Chmurze Obliczeniowej. Zgodnie z powyższą systematyzacją są to kontrolowane wrażliwe informacje urzędowe (poziom SCCO3) oraz informacje niejawne (poziom SCCO4).[2] Pozostałe rodzaje danych, czyli kontrolowane informacje urzędowe (SCCO2) oraz niekontrolowane informacje nieklasyfikowane (poziom SCCO1) nie muszą zatem być przechowywane w Rządowej Chmurze Obliczeniowej, takiej jaką ma być KCPD. Ich przetwarzaniem mogą zajmować się podmioty komercyjne zapewniające chmury obliczeniowe.

Aby umożliwić ustalenie odpowiednich standardów technicznych i zasad bezpieczeństwa, jakie muszą być zachowane przy przechowywaniu danych, konieczna jest klasyfikacja danych mających się znaleźć w KCPD. Z tego powodu rekomendujemy uściślenie w projekcie ustawy zakresu tych danych, uwzględnienie w pracach nad ustawą istniejącej w Polsce klasyfikacji danych oraz stworzenie ram prawnych zachęcających do dywersyfikacji zdolności przetwarzania danych tak, aby przyczyniało się to do zwiększenia bezpieczeństwa, innowacji administracji publicznej oraz generowało oszczędności dla budżetu państwa.

KONCENTRACJA DANYCH JAKO CZYNNIK ZWIĘKSZAJĄCY POZIOM ZAGROŻENIA DLA BEZPIECZEŃSTWA CYBERNETYCZNEGO PAŃSTWA

Trwająca wojna w Ukrainie unaoczniła wiele zjawisk związanych z bezpieczeństwem cybernetycznym państw, w tym z centrami przetwarzania danych. Podmioty te stają się łatwym celem ataków militarnych. Uszkodzenie takiej jednostki może skutkować utratą dostępu do danych strategicznych dla funkcjonowania państwa. Co więcej, zwiększa to jednoczesne ryzyko utraty znacznych ilości danych, co może zostać wykorzystane przeciwko bezpieczeństwu państwa. Podobnie sytuacja się kształtuje w przypadku żywiołów i klęsk żywiołowych, które mogą wstrzymać funkcjonowanie centrum przetwarzania danych.

Biorąc pod uwagę powyższe ZPP opowiada się za zwiększaniem dywersyfikacji miejsc fizycznego przechowywania danych. W naszej ocenie zdekoncentrowanie możliwości przetwarzania danych administracji publicznej pozwoli na bezpieczniejsze zarządzanie nimi oraz obniżenie kosztów. Warto zwrócić uwagę na dostępność usług przechowywania danych przez podmioty komercyjne. Część z nich funkcjonuje na rynku globalnie co przy posiadanej wielości centrów przetwarzania danych pozwala na rozproszenie ich położenia, mogące zapobiec zagrożeniom cyberbezpieczeństwa na dużą skalę. Oprócz tego przedsiębiorstwa zajmujące się realizacją inwestycji z zakresu przetwarzania danych oferują stale aktualizowane środki bezpieczeństwa przed cyberzagrożeniami oraz posiadają

[2] https://chmura.gov.pl/zuch/static/media/SCCO_v_1.00.pdf

doświadczenie w przedmiocie optymalizacji kosztów i procesów tworzenia chmurowych centrów obliczeniowych.

Rekomendujemy, aby jednostki administracji rządowej dekoncentrowały miejsca przechowywania danych poprzez ich fizyczne rozlokowanie oraz korzystanie z powierzchni ośrodków obliczeniowych oraz serwerowni na rynku komercyjnym. Poza tym opowiadamy się za stworzeniem strategii przenoszenia danych do miejsc bezpiecznych w przypadku wystąpienia zagrożeń dla bezpieczeństwa cybernetycznego. Miejsca takie mogłyby funkcjonować zarówno w kraju jak i poza granicami na wypadek zaistnienia rozległego zagrożenia.

RAMY PRAWNE ZAWARTE W PROJEKCIE USTAWY W STOSUNKU DO ISTNIEJĄCEGO PRAWODAWSTWA W POLSCE

Wspomniana wcześniej Wspólna Inicjatywa Informatyczna Państwa (WIIP) została przyjęta przez Radę Ministrów w celu zagwarantowania bezpieczeństwa przetwarzania danych administracji publicznej. Dodatkowo przyświecał jej cel optymalizacji procesów i redukcji kosztów w utrzymaniu chmur obliczeniowych na potrzeby administracji publicznej. Biorąc pod uwagę największą wydajność rozwiązań chmurowych, utworzony został System Zapewniania Usług Chmurowych (ZUCH). Jego istotą jest znajdowanie bezpiecznych rozwiązań chmurowych dla sprawniejszego i przyjaźniejszego dla społeczeństwa funkcjonowania sektora publicznego.

Powyższe funkcjonujące już mechanizmy zarządzania danymi administracji publicznej nie znajdują swojego miejsca w zaproponowanym projekcie ustawy. Budzi zatem nasze wątpliwości, w jaki sposób proponowany Projekt ustawy o przygotowaniu i realizacji inwestycji w zakresie Krajowego Centrum Przetwarzania Danych wpłynie na dotychczasowe działania państwa mające na celu zapewnienie bezpiecznej chmury obliczeniowej dla danych gromadzonych przez instytucje publiczne państwa polskiego.

Reasumując, w naszej opinii warte rozważenia są założenia przyjęte dla przygotowania i realizacji inwestycji w zakresie Krajowego Centrum Przetwarzania Danych (KCPD). Opisane powyżej rozwiązania przyjęte przez projekt ustawy mogą mieć niekorzystne skutki dla cyberbezpieczeństwa państwa, co stoi w kontrze do założeń przyjętych w uzasadnieniu oraz ocenie skutków regulacji przedmiotowego projektu.