AMERYKAŃSKA IZBA HANDLOWA W POLSCE
Spectrum Tower, ul. Twarda 18, 00-105 Warszawa
Tel: +48 22 520-5999, e-mail: office@amcham.com.pl

Warszawa, 11 marca 2024 r.

Pan Krzysztof Gawkowski
Wiceprezes Rady Ministrów, Minister Cyfryzacji

Szanowny Panie Premierze,

działając w imieniu Amerykańskiej Izby Handlowej w Polsce (AmCham) oraz jej firm członkowskich, w związku ze skierowaniem do konsultacji publicznych Ustawy Prawo Komunikacji Elektronicznej (UC7) oraz przepisów wprowadzających (UC8), wdrażających do polskiego systemu prawnego przepisy dyrektywy Parlamentu Europejskiego i Rady ustanawiające Europejski Kodeks Łączności Elektronicznej, niniejszym pragniemy przedstawić uwagi naszych firm członkowskich do Projektu.

AmCham jest organizacją zrzeszającą przedsiębiorców amerykańskich w naszym kraju, reprezentujących jednocześnie jedną z największych grup inwestorów zagranicznych, którzy stworzyli aktywa w Polsce o wartości 239 mld złotych i kreują 327 tysięcy miejsc pracy. Od ponad 30 lat działamy na rzecz rozwoju wzajemnych relacji gospodarczych, a naszą misją jest poprawa klimatu inwestycyjnego i promocji naszego kraju na rynku amerykańskim.

Uwagi firm członkowskich AmCham do ustawy Prawo Komunikacji Elektronicznej

Dot. artykuł 47 ust. 1 pkt 1.

Jeśli obowiązek retencji danych nałożony na przedsiębiorców telekomunikacyjnych jest warunkiem niepodlegającym dyskusji, postulujemy aby owa retencja mogła być realizowana na obszarze całego Europejskiego Obszaru Gospodarczego (EOG). Wobec powyższego, zmodyfikowana wersja artykułu 47 ust. 1 pkt 1) PKE brzmiałaby:

- *„Przedsiębiorca telekomunikacyjny, z wyłączeniem podmiotów, o których mowa w przepisach wydanych na podstawie art. 49 ust. 2, jest obowiązany na własny koszt: 1) zatrzymywać i przechowywać dane, o których mowa w art. 49 ust. 1, generowane w publicznej sieci telekomunikacyjnej lub przez niego przetwarzane, ~~na terytorium Rzeczypospolitej Polskiej,~~ **na terytorium Europejskiego Obszaru Gospodarczego**, przez okres 12 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia, a z dniem upływu tego okresu dane te niszczyć, z wyjątkiem tych, które zostały zabezpieczone, zgodnie z przepisami odrębnymi”*.

Nasz postulat jest zgodny z obowiązywaniem w EOG jednolitych zasad ochrony danych osobowych, w tym danych telekomunikacyjnych, w wyniku obowiązywania przepisów Rozporządzenia o Ochronie Danych Osobowych (RODO).

Uzasadnienie szczegółowe:

1. **Niezgodność z prawem UE**

Zaproponowana w projekcie ustawy obligatoryjność retencji danych na terytorium RP oznacza w praktyce zmuszenie przedsiębiorców telekomunikacyjnych do korzystania tylko z tych centrów danych, które znajdują się w Polsce. Jest to sprzeczne z zasadami funkcjonowania wspólnego rynku UE oraz RODO, które wspiera usuwanie przeszkód w przepływie chronionych danych (osobowych) w ramach EOG. Ponadto, proponowany kształt regulacji nie wynika z obowiązywania innych kluczowych regulacji unijnych, takich jak NIS czy NIS2, ani z Europejskiego Kodeksu Łączności Elektronicznej (EKŁE), którego realizację ma zapewnić PKE.

2. Ograniczenie wyboru rozwiązań i problemy natury organizacyjnej

Wiele firm telekomunikacyjnych działa w więcej niż jednym państwie członkowskim Unii Europejskiej/EOG i używa infrastruktury przetwarzającej dane, która znajduje się w innym kraju unijnym/EOG. Przedsiębiorcy telekomunikacyjni działający w Polsce w przypadku wejścia w życie przepisów w proponowanym kształcie zostaną postawieni w niesprzyjającej sytuacji wyjściowej w zakresie konkurencyjności, bowiem firmy na innych rynkach EOG nie mają takich ograniczeń. Twarda lokalizacja danych oznacza także problemy z zintegrowanym na poziomie grupy zarządzaniem w dziedzinie cyberbezpieczeństwa oraz brak możliwości przysłania danych pomiędzy różnymi podmiotami z grupy, z uwagi na prawne lub organizacyjne ograniczenia w przekazywaniu danych wynikające z obowiązku zatrzymywania i przechowywania ich tylko i wyłącznie na terytorium RP.

3. Wyzwania w zakresie bezpieczeństwa – infrastruktura krytyczna

Twarda lokalizacja danych niesie to ze sobą konkretne ryzyka dla Cyberbezpieczeństwa i wyzwania dla ochrony infrastruktury krytycznej, zwłaszcza w kontekście napiętej sytuacji geopolitycznej i wojny w sąsiedniej Ukrainie. Oprócz wspomnianych wyżej problemów z zintegrowanym zarządzaniem w dziedzinie cyberbezpieczeństwa, oznacza też przeszkody w korzystaniu z najnowocześniejszych technologii i rozwiązań w zakresie ochrony przed cyberatakami opartych np. o rozwiązania chmurowe. Firmy telekomunikacyjne mają określone powinności na rzecz bezpieczeństwa i obronności Rzeczypospolitej Polskiej oraz dysponują własną infrastrukturą i sieciami teleinformatycznymi, definiowanymi jako infrastruktura krytyczna państwa. Tymczasem podmioty infrastruktury krytycznej często padają ofiarą cyberataków. Od kilku lat Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV obserwuje zwiększoną aktywność cyberprzestępców, których celem jest próba przełamania zabezpieczeń systemów teleinformatycznych administracji rządowej oraz infrastruktury krytycznej. Jak czytamy w oficjalnym „Raporcie o stanie bezpieczeństwa cyberprzestrzeni RP w 2022" opublikowanym w sierpniu 2023 r[1] „statystyka incydentów zgłoszonych w systemie obsługi CSIRT GOV z podziałem na poszczególne sektory wskazuje, iż w 2022 roku największa liczba zgłoszeń, w liczbie 1 798, dotyczyła zagrożeń dla systemów i sieci telekomunikacyjnych wykorzystywanych przez operatorów infrastruktury krytycznej". Jest to trend wzrostowy.

Ponadto, restrykcje związane z przymuszaniem operatorów do lokowania danych tylko w Polsce stoją w opozycji do „Narodowego Programu Ochrony Infrastruktury Krytycznej" Rządowego Centrum Bezpieczeństwa[2], a w szczególności Planu Ewakuacji do Chmury Obliczeniowej, który plany ewakuacji infrastruktury krytycznej do chmury obliczeniowej znajdującej się poza granicami RP traktuje jako jeden z filarów bezpieczeństwa teleinformatycznego infrastruktury krytycznej. Dokument postuluje, aby plan ewakuacji do chmury stał się integralną częścią planu ochrony infrastruktury krytycznej powołując się m.in. na przykład wydarzeń w Ukrainie. Jak czytamy w Załączniku 1 NOPIK „Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje" „*Doświadczenia z wojny w Ukrainie wykazały, że informatyczne aktywa* operatorów IK stały się obiektem *hybrydowego ataku obejmującego m.in. zagrożenia cybernetyczne i fizyczne. Praktycznym rozwiązaniem była ewakuacja zasobów, danych i*

[1] https://www.gov.pl/web/baza-wiedzy/raport-csirt-gov-o-stanie-bezpieczenstwa-cyberprzestrzeni-rp-w-2022-roku)
[2] https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej

AMERYKAŃSKA IZBA HANDLOWA W POLSCE
Spectrum Tower, ul. Twarda 18, 00-105 Warszawa
Tel: +48 22 520-5999, e-mail: office@amcham.com.pl

systemów do chmury obliczeniowej, w szczególności do chmury znajdującej się poza terytorium państwa. Liczne przykłady pokazały, że takie przeniesienie zasobów może zostać wykonane szybko i sprawnie, także w warunkach wojennych (…). Aby proces ewakuacji został przeprowadzony sprawnie zaleca się przygotować Plan Ewakuacji poprzedzając go opisanym poniżej procesem przygotowawczym. Plan Ewakuacji do chmury obliczeniowej powinien być integralną częścią planu ochrony IK."

W przypadku jakichkolwiek pytań, pozostajemy do dyspozycji. Osobą do kontaktu jest Karol Witaszek, Manager ds. Prawnych i Polityki Publicznej w AmCham, e-mail: karol.witaszek@amcham.pl, tel. 690 087 660.

Z wyrazami szacunku

Tony Housh, Przewodniczący Rady Dyrektorów Amerykańskiej Izby Handlowej w Polsce