Stanowisko ZPP w sprawie konsultacji Prawa komunikacji elektronicznej

Ministerstwo Cyfryzacji rozpoczęło konsultacje projektu ustawy Prawo komunikacji elektronicznej oraz ustawy wdrażającej. Projektowane ustawy stanowią implementację Europejskiego Kodeksu Łączności Elektronicznej i wprowadzają nowe rozwiązania dla branży i korzyści dla konsumentów. Na wstępie Związek Przedsiębiorców i Pracodawców pragnie podziękować za wznowienie prac nad projektem ustawy oraz możliwość zabrania głosu w procesie konsultacji nowej wersji projektu.

Nowe rozwiązania dla branży, m.in. kontrakty zawierane między dostawcami usług a ich klientami, mają stać się bardziej zrozumiałe i transparentne, przede wszystkim przez dołączenie krótkiego streszczenia kluczowych zapisów umownych. W naszej opinii nowe przepisy wprowadzą większą swobodę w zakresie podpisywania i anulowania umów, umożliwiając m.in. wykorzystanie zdalnej weryfikacji tożsamości abonenta podczas autoryzacji u usługodawcy. Dzięki temu klienci zyskają dostęp do niezawisłego mechanizmu porównywania ofert usług komunikacyjnych. Jednak chcielibyśmy zwrócić uwagę na konieczność zmiany w zakresie obowiązku przechowywania danych, która stoi w sprzeczności z ideą wspierania jednolitego rynku europejskiego. Liczymy na uwzględnienie naszych uwag w procesie konsultacji.

TWARDA LOKALIZACJA DANYCH

Na podstawie przedstawionego projektu ustawy Prawo komunikacji elektronicznej oraz ustawy wprowadzającej te przepisy, pragniemy zwrócić uwagę na konieczność zmiany w zakresie obowiązku przechowywania danych przez przedsiębiorców telekomunikacyjnych. Sugerujemy rewizję art. 47 ust. 1 pkt 1) PKE w taki sposób, aby umożliwić przechowywanie danych w ramach całego Europejskiego Obszaru Gospodarczego (EOG), zamiast ograniczać je wyłącznie do terytorium Rzeczypospolitej Polskiej.

Postulujemy aby art. 47 ust. 1 pkt 1) PKE brzmiał:

- *„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,~~ 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”*.

lub, jeśli retencja danych ma pozostać i dane mają być zatrzymywane i przechowywane na jakimś określonym obszarze, postulujemy rozszerzenie tego obszaru do Europejskiego Obszaru Gospodarczego. W zw. z powyższym, zmieniona wersja art. art. 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”*.

Zmiana ta bierze pod uwagę fakt, że w Europejskim Obszarze Gospodarczym obowiązują jednolite przepisy dotyczące ochrony danych osobowych, włączając w to dane telekomunikacyjne, zgodnie z zasadami określonymi w Rozporządzeniu o Ochronie Danych Osobowych (RODO). Poniżej przedstawiamy

NIEZGODNOŚĆ Z PRAWEM UE

Pragniemy podkreślić, że wymóg, aby przedsiębiorstwa telekomunikacyjne wykorzystywały wyłącznie centra danych umiejscowione na terenie Polski, stoi w sprzeczności z ideą wspierania jednolitego rynku europejskiego. Taka polityka nie jest odzwierciedlona w Europejskim Kodeksie Łączności Elektronicznej (EKŁE), który jest implementowany przez PKE. Ograniczenie to koliduje z unijnymi przepisami, takimi jak rozporządzenie o ochronie danych (RODO), którego głównym założeniem jest ułatwienie przepływu danych osobowych wewnątrz Europejskiego Obszaru Gospodarczego (EOG). Ponadto, ten narzucony obowiązek fizycznego umiejscowienia danych na obszarze Polski nie znajduje uzasadnienia w obecnych ani przyszłych regulacjach unijnych, w tym w dyrektywach typu NIS 2.0 czy w Europejskim Kodeksie Łączności Elektronicznej. Również nowe regulacje oraz ich projektowane zmiany nie wprowadzają ograniczeń co do lokalizacji przechowywania danych, pozwalając na ich umieszczenie w dowolnym kraju członkowskim – przykłady to rozporządzenie DORA czy różne Akty dotyczące danych, zarządzania danymi, czy sztucznej inteligencji.

OCHRONA INFRASTRUKTURY KRYTYCZNEJ

Wymóg utrzymywania danych wyłącznie w Polsce, znany jako "twarda lokalizacja danych", może stwarzać ryzyka dla cyberbezpieczeństwa i ochrony infrastruktury krytycznej, szczególnie w obliczu geopolitycznych napięć i konfliktu na Ukrainie. Operatorzy telekomunikacyjni, posiadający kluczowe dla bezpieczeństwa państwa sieci i infrastrukturę, są narażeni na cyberataki. Taka polityka utrudnia skuteczne zarządzanie cyberbezpieczeństwem, korzystanie z nowych technologii ochronnych i wymianę danych wewnątrz grupy, ze względu na bariery prawne i organizacyjne.

Ograniczenia te kolidują z "Narodowym Programem Ochrony Infrastruktury Krytycznej", który promuje plany ewakuacji do chmury obliczeniowej za granicą jako element bezpieczeństwa. Niejasne jest, dlaczego takie restrykcje nie dotyczą infrastruktury krytycznej, podczas gdy są nałożone na sektor telekomunikacyjny. Doświadczenia z konfliktu na Ukrainie pokazują, że przeniesienie danych do chmury za granicą jest skutecznym sposobem na ochronę przed atakami, co powinno być integralną częścią planowania bezpieczeństwa.