Warszawa, 10 stycznia 2023 r.

Szanowna Pani Poseł
Elżbieta Witek
Marszałek Sejmu RP

Szanowna Pani Marszałek,

W imieniu Związku Cyfrowa Polska branżowej organizacji pracodawców, która zrzesza największe firmy z branży nowoczesnych technologii działające w Polsce, w tym producentów, importerów i dystrybutorów sprzętu elektrycznego oraz usług komunikacji elektronicznej przekładamy stanowisko do ***Druk nr 2861 Rządowy projekt ustawy - Prawo komunikacji elektronicznej (PKE)*** oraz ***Druk nr 2862 Rządowy projekt ustawy - Przepisy wprowadzające ustawę - Prawo komunikacji elektronicznej.***

Najważniejszymi zmianami merytorycznymi wprowadzonymi do nowego projektu PKE z dnia 17.11.2022 r. (wobec poprzedniego projektu poddawanemu konsultacją publicznym) jest rozszerzenie części zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego **na nową grupę podmiotów**, tzn. przedsiębiorców komunikacji elektronicznej (obok przedsiębiorców telekomunikacyjnych). Opinia dotyczy przepisów z trzech artykułów budzących wątpliwości (art. 43, 47 i 53).

Należy zauważyć, że opisywane przepisy zostały dodane na ostatnim etapie prac rządowych, bez jakichkolwiek konsultacji z rynkiem i które skutkować będą **fundamentalną zmianą zasad funkcjonowania rynku cyfrowego w Polsce**. Dodatkowo, przepisy te **nie wynikają z treści dyrektywy Europejski Kodeks Łączności Elektronicznej** (EKŁE). Taki tryb stanowienia prawa jest sprzeczny z zasadami transparentnego i uczciwego procesu legislacyjnego, w którym przepisy mające ogromny wpływ zarówno na przedsiębiorców, jak też odbiorców ich usług powinny podlegać szerokim konsultacjom społecznym i spotkaniom warsztatowym celem wypracowania przemyślanych rozwiązań nie naruszających zasady swobody prowadzenia działalności gospodarczej i uwzględniających realia ekonomiczne oraz technologiczne.

1. **<u>Przejrzystość definicji (Druk nr 2861)</u>**

Stoimy na stanowisku, że w zakresie regulacji obowiązków przedsiębiorców świadczących usługi komunikacji elektronicznej opartej na numerach (dalej: NB-ICS) oraz świadczących usługi komunikacji elektronicznej niewykorzystującej numerów (dalej: NI-ICS), powinien istnieć klarowny rozdział, co do zakresu tych obowiązków. Definicje wykorzystywane w ustawie nie powinny budzić wątpliwości. Jednocześnie, ustawa wprowadza następujące pojęcia, które potencjalnie mogą rodzić wiele pytań w zakresie ich stosowania:
– przede wszystkim, ustawa wykorzystuje zbiorczą kategorię oznaczoną jako **„przedsiębiorca komunikacji elektronicznej”,** która obejmuje dwa różne rodzaje przedsiębiorców i usług przez nich świadczonych, tj. przedsiębiorcę telekomunikacyjnego (który świadczy między innymi usługę NB-ICS) oraz podmiot świadczący usługę NI-ICS (który nie został już oznaczony jako przedsiębiorca, a objęty szeroką i otwartą kategorią „podmiotu”). Z punktu widzenia praktyki, należy wziąć pod uwagę, że **są to radykalnie różne rodzaje podmiotów**, funkcjonujące na innych zasadach, mające zupełnie inne portfolio produktów, korzystające z różnych systemów, opierające się na innych procedurach wewnętrznych oraz podlegające nierzadko zupełnie innym przepisom prawa. **Stosowanie kategorii łącznej i nakładanie jednakowych obowiązków na te dwa rodzaje podmiotów <u>nie jest uzasadnione z punktu widzenia efektywności stosowania prawa oraz proporcjonalności nakładanych obciążeń.</u>**

Dodatkowo, zdefiniowanie „publicznej dostępności” jako „dostępności dla ogółu użytkowników” nie wyjaśnia, jak ta dostępność ma się do modeli subskrypcyjnych, które również są jedną z kategorii produktów umożliwiających komunikacją wskazaną w projekcie.

2. **<u>Obowiązki wynikające z art. 43 i n. projektu (Druk nr 2861)</u>**

Przede wszystkim, należy wskazać, co również zaznaczone zostało w punkcie 1. niniejszych uwag – obowiązek ten nałożony jest zbiorczo na kategorię podmiotów obejmujących usługi o radykalnie różnym charakterze. Ustanowienie obowiązków o tak daleko idącym charakterze powoduje sytuację, w której te same obowiązki powodują różną skalę obciążeń nałożonych na przedsiębiorców i tym samym są nieproporcjonalne.

Należy wskazać, że komunikatory oparte o model NI-ICS, tj. pozwalające na swobodną komunikację przez sieć bez konieczności wykorzystywania numerów, zostały skonstruowane w swoim założeniu przede wszystkim jako urządzenia zapewniające użytkownikom prywatność i bezpieczeństwo. Dla wielu użytkowników wybór konkretnego komunikatora jest podyktowany tym, w jaki sposób przedsiębiorca świadczący usługę wykorzystuje dane użytkownika, w jakim stopniu zapewnione jest jego bezpieczeństwo i jak dużą kontrolę może mieć nad własną komunikacją w sieci. To pod kątem tych właśnie właściwości dostosowane

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

zostały systemy, którymi dysponują przedsiębiorcy świadczący usługę NI-ICS, bez względu na to, czy mowa tutaj o czatach, wideokonferencjach, czy innych formach komunikacji bez numerów. **Krótko mówiąc, obowiązkiem przedsiębiorcy jest zapewnienie jak największego poszanowania prawa użytkowników, tj. ich bezpieczeństwa i prywatności.** Wszelkie odstępstwa od tego obowiązku, których przedsiębiorca może dokonywać na rzecz ingerencji organów władzy publicznej, **otwiera furtkę również do wykorzystywania tych luk przez cyberprzestępców.**

To, w jaki sposób dane systemy zapewniają ochronę użytkowników, jest związane z ich konstrukcją tworzoną przez tysiące inżynierów na całym świecie, którzy zajmują się między innymi zachowywaniem szczelności i sprawnego funkcjonowania tych systemów. Projekt ustawy obciąża kosztami wykonywania obowiązków przedsiębiorcę (tj. przede wszystkim przygotowania technicznych możliwości i pozostałymi wymienionymi w art. 47 projektu), co jest procesem **wymagających znacznych nakładów operacyjnych, finansowych i przede wszystkim wymagających czasu.** Jednocześnie omawiane przepisy zdają się nie brać tych okoliczności pod uwagę:

- **art. 43 ust. 4 wskazuje**, że uprawnione podmioty, tj. wymienione w przepisie służby, wraz z przedsiębiorcą w ciągu 24 godzin od momentu zgłoszenia zapotrzebowania dostępu do danych wskazanych w ustawie – termin ten może nie być możliwy do zrealizowania w szczególności, gdy mowa o podmiotach operujących w sferze wirtualnej i zapewniających funkcjonowanie systemów w obrębie wielu krajów świata,
- **Problemu tego nie mityguje fakt**, że w art. 44 przyznano możliwość złożenia wniosku o zawieszenie obowiązku udostępniania danych na okres nie dłuższy niż 6 miesięcy. Wniosek składany jest w terminie 14 dni, a do wniosku należy dołączyć harmonogram osiągnięcia przed przedsiębiorcę zdolności do udostępnienia danych, co po pierwsze – wymaga przewidzenia w ciągu dwóch tygodni niemożliwych często w przestrzeni wirtualnej okoliczności, a po drugie – i tak nie zwalnia przedsiębiorcy z wykonywania obowiązków, jeśli zdaniem organów władzy publicznej, przedsiębiorca ten posiada możliwości do ich realizacji.

Ponadto, należy zauważyć, że art. 43 projektu wskazuje bardzo szeroki katalog służb mogących mieć **dostęp do danych wrażliwych związanych z komunikacją** (ujętych równie szeroko, w tym m.in. do treści komunikatów elektronicznych, danych abonentów oraz danych o lokalizacji), **nie precyzując jednocześnie określenia okoliczności**, w jakich te dane mogą być uzyskane przez podmioty. Za podmioty uprawnione zostały uznane: Policja, Biuro Nadzoru Wewnętrznego, Straż Graniczna, Służba Ochrony Państwa, Agencja Bezpieczeństwa Wewnętrznego, Służba Kontrwywiadu Wojskowego, Żandarmeria Wojskowa, Centralne Biuro Antykorupcyjne i Krajowa Administracja Skarbowa. Norma prawna, przyznając określone kompetencje władzy publicznej, **powinna określać wszystkie niezbędne elementy pozwalające na określenie granic stosowania tej normy, co wynika z podstawowych zasad ustrojowych zakładających, że organy władzy publicznej mogą działać tylko na podstawie**

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

i w granicach prawa. Nie można domniemywać swobody działania organu władzy publicznej, nie wspominając o sytuacji, w której chodzi o uzyskiwanie dostępu do wrażliwych danych obywateli, co jest istotnym ograniczeniem korzystania z konstytucyjnych wolności i praw. Takie ograniczenia w ustawie wymagają wskazania jasnych kryteriów, które mogą uzasadniać ich zastosowanie.

Konstrukcja obowiązków z art. 43 oraz skomplikowanie zapisów mogą budzić wątpliwości interpretacyjne dotyczące tego, których przedsiębiorców obejmują wymienione obowiązki, jak również jak w praktyce powinny być one realizowane przez nową grupę podmiotów zobowiązanych. Dodatkowo, zwracamy uwagę, iż szeroki katalog podmiotów, które otrzymały ww. uprawnienia bez kontroli sądowej **może doprowadzić do naruszeń zagwarantowanych konstytucji praw i wolności.**

3. **Art. 47 (Druk nr 2861)**

Proponowane rozszerzenie obowiązku retencji danych wynikające z art. 47 nakłada na przedsiębiorców komunikacji elektronicznej obowiązek zatrzymywania i przechowywania (wyłącznie) na terytorium Rzeczypospolitej Polskiej danych, generowanych w publicznej sieci telekomunikacyjnej lub przez niego przetwarzane, przez okres 12 miesięcy. **Nakładanie ww. obowiązku na wszystkie podmioty świadczące usługi komunikacji elektronicznej jest nadmiarowe, a jednocześnie nie jest transparentne** (wynika to z tego, że decyzję, które podmioty nie będą objęte tym obowiązkiem - zgodnie z art. 49 ust. 2 - ma podejmować Minister właściwy ds. Informatyzacji w formie rozporządzenia), co prowadzi do braku pewności prawnej.

Dodatkowo, wątpliwości budzi obowiązek przechowywania danych komunikacyjnych w kraju, jako warunek oferowania określonej usługi w Polsce, w tym przez dostawców zagranicznych. Jest to nie tylko sprzeczne z dotychczas artykułowanymi celami Rządu RP wspierającego wolny obieg danych w UE, ale jest również **zaprzeczeniem idei jednolitego rynku cyfrowego** oraz znacząco ogranicza swobodę przedsiębiorczości. Co więcej, przepis ten nie wynika z EKŁE, ani też z innych regulacji unijnych. Wprost przeciwnie – **w naszej opinii stoi on w sprzeczności z innymi projektami i obowiązującymi regulacjami, w szczególności z Rozporządzeniem o Ochronie Danych Osobowych (RODO)**. Należy podkreślić, iż jednym z głównych założeń RODO jest bowiem likwidacja barier w swobodnym przepływie chronionych danych osobowych na obszarze Europejskiego Obszaru Gospodarczego.

Naszym zdaniem rozwiązanie przyjęte w art. 47 spowoduje również komplikacje w zakresie funkcjonowania usług komunikacji elektronicznej, bazujących na rozwiązaniach chmurowych i **jest ono niezgodne z uwarunkowaniami technicznymi.** Gdyby przedmiotowy obowiązek wszedł w życie w obecnym kształcie, dostęp przedsiębiorców z innych państw członkowskich

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

UE do polskiego rynku zostałby częściowo ograniczony, gdyż nałożony na nich obowiązek lokowania centrów danych na terytorium RP **mógłby zostać uznany za dyskryminujący i nieproporcjonalny do osiągnięcia zamierzonych celów**. Ponadto, nie wszystkie przedsiębiorstwa komunikacji elektronicznej korzystają z centrów danych zlokalizowanych na terenie RP, więc nałożenie na nie takiego wymogu mogłoby wiązać się ze znacznymi kosztami. Przedsiębiorcy mogą nie mieć wystarczającego czasu na przeniesienie swojej infrastruktury lub zmianę podwykonawców w okresie 6 miesięcy jako przewidzianego okresu wejścia w życie PKE.

Z tzw. twardą lokalizacją danych (ang. hard data localization) wpisaną do obecnej wersji art. 47 ust. 1 wiąże się również **ryzyko dla bezpieczeństwa cybernetycznego**. Przedsiębiorcy telekomunikacyjni, zobligowani do wypełniania obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, których infrastruktura oraz sieci teleinformatyczne są zaliczane do infrastruktury krytycznej państwa, stanowią potencjalny cel cyberataków. **Fizyczna lokalizacja danych na terytorium danego państwa nie chroni ich przed nieuprawnionym dostępem i utrudnia ich ochronę oraz możliwość ich przeniesienia w przypadku zagrożeń.** Takie restrykcyjne podejście utrudnia zintegrowane zarządzanie ryzykiem cyberbezpieczeństwa, ogranicza dostęp do najnowocześniejszych technologii i rozwiązań w zakresie ochrony przed cyberatakami, a także oznacza brak warunków dla dzielenia się danymi pomiędzy różnymi organizacjami.

Dodatkowo, niejasny jest zakres, co obejmują "dane generowane w publicznej sieci telekomunikacyjnej". **Naszym zdaniem, powinna zostać określona konkretna lista kategorii danych wymagających retencji.** W innym przypadku przedsiębiorcy będą mieli trudności interpretacyjne dotyczące tego jakie dane mają zatrzymywać i przechowywać. Wskazujemy również, że **konieczne jest zagwarantowanie, aby żaden przedsiębiorca nie był zobowiązany do gromadzenia danych, które nie są przetwarzane w ramach prowadzonej przez niego standardowo działalności.**

Postulujemy zatem powrót do poprzedniego zakresu podmiotowego (tj. „przedsiębiorca telekomunikacyjny" i zniesienie wymogu retencji danych, o których mowa w art. 47 ust 1. wyłącznie na terytorium RP.

4. **Art. 53 (Druk nr 2861)**

Zgodnie z projektowanym przepisem, art. 53 przyznaje prawo Prezesowi UKE, na uzasadnione żądanie uprawnionego podmiotu, niezwłocznego nakładania na przedsiębiorcę komunikacji elektronicznej, w drodze decyzji w formie ustnej, obowiązku blokowania, nie później niż w terminie 6 godzin liczonych od otrzymania decyzji, połączeń lub komunikatów elektronicznych przesyłanych w związku ze świadczoną publicznie dostępną usługą telekomunikacyjną, jeżeli mogą one zagrażać obronności, bezpieczeństwu państwa oraz bezpieczeństwu i porządkowi publicznemu, albo umożliwienia dokonania takiej blokady przez

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

uprawnione podmioty. Co więcej, przepis nadaje rygor natychmiastowej wykonalności takiej decyzji.

Nie jest tutaj jasne, dlaczego ustawodawca użył sformułowania „przedsiębiorca komunikacji elektronicznej" (czyli obejmującego zarówno usługi NB-ICS oraz NI-ICS), ale wskazał, że blokowane mogą być tylko określone komponenty wchodzące w skład publicznie dostępnej usługi telekomunikacyjnej, w której zakres, zgodnie ze słownikiem projektu, NI-ICS nie wchodzi. **Sugerowane byłoby tu jasne rozdzielenie wskazanych kategorii podmiotów.**

Uznając konieczność przeciwdziałaniu zagrożeniom bezpieczeństwa kraju uważamy, że **6 godzinny nakaz zatrzymania świadczenia usług może być niewykonalny**. Usługi komunikacji elektronicznej są świadczone często spoza terytorium RP i ich zablokowanie w tak krótkim czasie może być trudne. W praktyce może to oznaczać, że przedsiębiorca komunikacji elektronicznej nie będzie miał możliwości dokładnej analizy treści decyzji. Co więcej, przedsiębiorca taki będzie zobowiązany do wykonania jej w ciągu kilku godzin, co może również oznaczać, że decyzja będzie musiała zostać wykonana w nocy, **kiedy nie będzie dysponował personelem niezbędnym do podjęcia odpowiednich kroków technicznych.** Przedsiębiorca nie będzie również dysponować skutecznymi środkami sprzeciwu w celu zakwestionowania legalności decyzji w rozsądnym terminie.

Ponadto, wątpliwość budzi **tryb przekazania takiej decyzji (możliwość 'ustna').** Wobec powyższego, **obowiązek taki można uznać za sprzeczny z zasadami konstytucyjnymi**. Zastosowane środki wydają się nieproporcjonalne i nieracjonalne, a często wręcz niemożliwe do spełnienia. **Nie spełniają one zasady pewności prawa, ani nie gwarantują skutecznego środka odwoławczego od wydanej decyzji.**

5. **Art. 10 (Druk nr 2862)**

Proponowana regulacja w art. 10 ustawy przepisy wprowadzające PKE dot. sposobu wprowadzania instytucji must carry / must offer z punktu widzenia prawnego, budzi bardzo poważne wątpliwości zgodności z Konstytucją RP. Obowiązki tego rodzaju nie mogą być nakładane na przedsiębiorców w drodze rozporządzenia KRRiT, a jedynie w drodze ustawy.

Z wyrazami szacunku,

Michał Kanownik

Prezes Zarządu

Związek Cyfrowa Polska

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