Biuro Rzecznika
Małych i Średnich Przedsiębiorców

Warszawa, 26 września 2020 r.

WPL.631.2020.GG

Pan
Marek Zagórski
Minister Cyfryzacji
ul. Królewska 27
00-060 Warszawa

Szanowny Panie Ministrze

na podstawie art. 8 pkt 1 ustawy z dnia 6 marca 2018 r. o Rzeczniku Małych i Średnich Przedsiębiorców[1], który stanowi, że do zadań Rzecznika MŚP należy opiniowanie projektów aktów normatywnych dotyczących interesów przedsiębiorców oraz zasad podejmowania, wykonywania lub zakończenia działalności gospodarczej na terytorium Rzeczypospolitej Polskiej, w związku z pracami nad projektem ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych[2], w celu uniknięcia wprowadzenia sprzecznych uregulowań z dotyczącymi bezpieczeństwa sieci i usług, zawartymi w projekt ustawy - Prawo komunikacji elektronicznej[3], zwracam się z uprzejmą prośbą o określenie w sposób kompleksowy, jednoznaczny oraz spójny, w jednym akcie prawnym, kwestii z zakresu: bezpieczeństwa sieci i usług oraz cyberbezpieczeństwa odnośnie mikroprzedsiębiorców, małych i średnich przedsiębiorców z branży telekomunikacyjnej.

Jednocześnie zwracam się z uprzejmą prośbą o pilne uzupełnienie dostrzeżonych braków w Projekcie. Pragnę wskazać, że przy opracowaniu Projektu pominięto istotne wymogi dotyczące tworzenia przepisów prawa wynikające z ustawy z dnia 6 marca 2018 r. - Prawo przedsiębiorców (Konstytucja Biznesu)[4]:

---

[1] Dz. U. z 2018 r. poz. 648, dalej: „Rzecznik MŚP".
[2] Nr wykazu: UD68, dalej: „Projekt".
[3] Nr wykazu: UC45.
[4] Dz. U. z 2019 r. poz. 1292 ze zm, dalej: „Prawo przedsiębiorców".

Art. 66 ust 1 pkt 2, który stanowi, że *„Przed rozpoczęciem prac nad opracowaniem projektu aktu normatywnego określającego zasady podejmowania, wykonywania lub zakończenia działalności gospodarczej dokonuje się oceny przewidywanych skutków społeczno-gospodarczych, w tym oceny wpływu na mikroprzedsiębiorców, małych i średnich przedsiębiorców oraz analizy zgodności projektowanych regulacji z przepisami ustawy".*

Ponadto zgodnie z art. 66 ust 2: *„Wyniki oceny i analiz, o których mowa w ust. 1, zamieszcza się w uzasadnieniu do projektu aktu normatywnego lub w ocenie skutków regulacji, stanowiącej odrębną część uzasadnienia projektu aktu normatywnego".*

Konstytucja Biznesu ma charakter gwarancyjny dla ok. 6000 mikroprzedsiębiorców, małych i średnich przedsiębiorców z branży telekomunikacyjnej.

W przypadku stwierdzenia wpływu projektu aktu normatywnego na najmniejsze firmy *„przy opracowaniu projektu aktu normatywnego dąży się do proporcjonalnego ograniczania obowiązków administracyjnych wobec tych przedsiębiorców albo uzasadnia brak możliwości zastosowania takich ograniczeń"* (art. 68 Prawa przedsiębiorców), co należy powiązać z zasadami proporcjonalności i adekwatności, a w szczególności należy: *„dążyć do nienakładania nowych obowiązków administracyjnych, a jeżeli nie jest to możliwe, dążyć do ich nakładania jedynie w stopniu koniecznym do osiągnięcia ich celów"* (art. 67 pkt 1 Prawa przedsiębiorców).

Dodatkowo w art. 40 ust. 1 Europejskiego kodeksu łączności elektronicznej[5] wskazuje się, na konieczność uwzględniania we wprowadzanych uregulowaniach zasady proporcjonalności przez Państwa członkowskie w razie wystąpienia zagrożenia dla bezpieczeństwa sieci lub usług. Art. 40 ust. 2 EKŁE stanowi, że aby określić istotność wpływu danego incydentu związanego z bezpieczeństwem, uwzględnia się w szczególności następujące parametry, gdy są dostępne:

a) liczbę użytkowników, których dotyczy incydent związany z bezpieczeństwem;

b) czas trwania incydentu związanego z bezpieczeństwem;

[5] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona)Tekst mający znaczenie dla EOG (Dz. U. UE. L. z 2018 r. Nr 321, str. 36 ze zm.), dalej: „EKŁE".

c) geograficzny zasięg obszaru dotkniętego incydentem związanym z bezpieczeństwem;

d) zakres wpływu na funkcjonowanie sieci lub usługi;

e) zakres wpływu na działalność ekonomiczną i społeczną.

Dotychczas wprowadzane obowiązki w zakresie obowiązku sporządzania i posiadania planu działań w sytuacjach szczególnego zagrożenia[6] nie obejmują mikroprzedsiębiorców. Uregulowania te powinny zyskać rangę ustawową, ponieważ w obecnej wersji projektu zmiany ustawy o krajowym systemie cyberbezpieczeństwa brak jednoznacznego odniesienia dotyczącego konieczności kontynuacji tych wyłączeń wobec najmniejszych firm. Dodatkowego rozważenia wymagałaby możliwość objęcia tymi wyłączeniami małych i średnich przedsiębiorców oraz zastosowania ww. wyłączenia w powiązanych regulacjach dotyczących bezpieczeństwa sieci i usług.

Nakłady związane z bezpieczeństwem sieci, usług i cyberbezpieczeństwem należą do istotnie obciążających najmniejsze krajowe firmy, które posiadają mniej rozbudowane struktury administracyjne niż międzynarodowe korporacje. Istnienie tych najmniejszych firm gwarantuje jednak istnienie realnej konkurencji na rynku usług komunikacji elektronicznej (w przeciwieństwie do większości państw europejskich, co przekłada się na niższe ceny i wyższą jakość usług oferowanym konsumentom. Jak stwierdzono w uzasadnieniu do samego projektu ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych (UD68) (str. 33): *„Poprzez nałożenie różnych obowiązków na przedsiębiorców będących podmiotami tego systemu ogranicza się konstytucyjną wolność gospodarczą. Zobowiązuje bowiem tych przedsiębiorców do dbania o cyberbezpieczeństwo. Po stronie przedsiębiorców powoduje to koszty związane z koniecznością dostosowania się do wymogów ustawy"*.

W związku z powyższym wymagana jest modyfikacja stwierdzenia na str. 44 uzasadnienia do projektu ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych, że: *„Zawarte w projekcie regulacje nie będą miały*

[6] Rozporządzenie Rady Ministrów z dnia 19 sierpnia 2020 r. w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń, skierowane do podpisu Prezesa Rady Ministrów.

wpływu na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców zgodnie z art. 66 ust. 2 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. 2019 r. poz. 1292, z późn. zm.)." i wprowadzenie stosownych uzupełnień z rozważeniem możliwych wyłączeń lub ograniczeń obowiązków nakładanych na najmniejsze firmy.

Zwracam się także z uprzejmą prośbą o zajęcie stanowiska w odnośnie załączonych uwag w piśmie Związku Pracodawców Mediów Elektronicznych i Telekomunikacji z 16 września 2020 r., zgłoszonych podczas dotychczasowych konsultacji w Zespole ds. Telekomunikacji Rady Przedsiębiorców działającej przy Rzeczniku MŚP, Projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych.

W związku z przedłużeniem terminu konsultacji Rzecznik MŚP zastrzega sobie możliwość złożenia kolejnych pism.

Z poważaniem
Z up. Rzecznika Małych i Średnich Przedsiębiorców
RADCA RZECZNIKA
Wydział Prawno-Legislacyjny
Dr n. pr. Marek Woch

Załącznik – pismo Związku Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM z dnia 16 września 2020 r.

Biuro Rzecznika
Małych i Średnich Przedsiębiorców
rada.przedsiebiorcow@rzecznikmsp.gov.pl

Łódź, dn. 16 września 2020 r.

Związek Pracodawców Mediów
Elektronicznych i Telekomunikacji
MEDIAKOM

reprezentowana przez
adw. Annę Gąsecką
(adres w nagłówku pisma)

dotyczy: Konsultacje RMSP - Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy - Prawo zamówień publicznych (UD68)

Szanowni Państwo,

Działając w imieniu Związku Pracodawców Mediów Elektronicznych i Telekomunikacji Mediakom, uprzejmie dziękuję za umożliwienie zajęcia stanowiska co do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy prawo zamówień publicznych.

ZPMEiT Mediakom zgłasza następujące uwagi do projektowanej ustawy:

1. W pierwszej kolejności podnoszę, że niejasny jest stosunek projektowanych przepisów do zapisów projektu Prawa Komunikacji Elektronicznej (dalej PKE). Oba akty regulują tę samą materię, a część projektowanych przepisów jest tożsama:
   - art. 39 PKE i art. 20a ustawy o krajowym systemie cyberbezpieczeństwa,
   - art.43 ust. 2 i 3 PKE i art. 20e ustawy o krajowym systemie cyberbezpieczeństwa
   - art. 44 ust.1 PKE i art. 20f ustawy o krajowym systemie cyberbezpieczeństwa

   Nadto ustawa o krajowym systemie cyberbezpieczeństwa, równolegle do PKE reguluje obowiązek zgłaszania incydentów bezpieczeństwa, przy czym różny jest krąg podmiotów zobowiązanych i organ właściwy do przyjmowania zgłoszeń:
   - PKE nakłada obowiązek na wszystkich przedsiębiorców telekomunikacyjnych i nakazuje zgłaszać incydenty do UKE (art. 42) , zaś
   - ustawa o krajowym systemie bezpieczeństwa nakłada obowiązki jedynie na tych przedsiębiorców, którzy mają obowiązek sporządzania planów działania w sytuacjach szczególnych zagrożeń i nakazuje zgłaszać incydenty do właściwego CSIRT (art. 20c).

Biorąc pod uwagę powyższe, oraz treść otrzymanego z Ministerstwa Cyfryzacji pisma zawiadamiającego o konsultacjach, z którego wynika, że PKE ma zostać uzupełnione o przepisy regulujące obowiązki przedsiębiorców w zakresie zapewnienia bezpieczeństwa ciągłości świadczenia usług komunikacji elektronicznej oraz dostarczania sieci telekomunikacyjnej poprzez włączenie obowiązków zawartych w konsultowanym projekcie do PKE, nie jest do końca jasne przyjęty sposób regulacji. Czy konsultowane przepisy mają znaleźć się w dwóch równoległych ustawach? Czy też mają one być wprowadzone do PKE i usunięte z konsultowanej ustawy?

Mediakom postuluje, by kwestie bezpieczeństwa sieci i usług uregulowane zostały w jednym akcie prawnym, tak by maksymalnie uprościć przyjęte rozwiązania i zapewnić czytelność i możliwą łatwość stosowania przez przedsiębiorców komunikacji elektronicznej. Zbędne jest też powielanie tożsamych przepisów w dwóch niezależnych ustawach.

Ponadto, wobec wyżej wskazanych rozbieżności pomiędzy projektowanymi art. 42 PKE i art. 20c ustawy o krajowym systemie cyberbezpieczeństwa **Mediakom postuluje, by pozostać przy rozwiązaniu przyjętym w art. 20c – tak, by obowiązek zgłaszania incydentów obciążał wyłącznie tych przedsiębiorców telekomunikacyjnych, którzy są zobowiązani do sporządzania planów działania w sytuacjach szczególnych zagrożeń.** Są to podmioty duże, osiągające ponad 10 mln przychodów, często posiadające rozbudowane sieci i dużą liczbę abonentów. To właśnie incydenty bezpieczeństwa dotykające tych podmiotów, z uwagi na skalę ich działalności, winny być raportowane. Natomiast mniejsi przedsiębiorcy, działający na mniejszą skalę, o znacznie mniejszym zasięgu sieci i liczbie abonentów nie powinni być objęci obowiązkiem raportowania incydentów bezpieczeństwa.

2. W związku z projektowaną treścią art. 4 ustawy o krajowym systemie cyberbezpieczeństwa, poprzez dodanie do niego pkt 2a i tym samym włączenie do krajowego systemu cyberbezpieczeństwa wszystkich przedsiębiorców komunikacji elektronicznej **Mediakom postuluje, by ograniczyć grono przedsiębiorców komunikacji elektronicznej będących częścią systemu cyberbezpieczeństwa do tych tylko, którzy zobowiązani są sporządzać plany działań w sytuacjach szczególnych zagrożeń, o którym mowa w art. 47 ust. 1 PKE.** Jak wskazano powyżej – plany mają obowiązek sporządzać przedsiębiorcy o dużej skali działalności, świadczący własne usługi, z wykorzystaniem własnej sieci i osiągający przychody przekraczające 10 mln złotych. Mają oni realne znaczenie dla krajowego systemu cyberbezpieczeństwa, zaś incydenty bezpieczeństwa, które mogą ich dotknąć z zasady będą miały istotne znaczenie z uwagi na ilość abonentów i obszar, który incydent może dotknąć. Inaczej jest w przypadku mniejszych przedsiębiorców, których liczba jest bardzo znacząca, a jednocześnie znaczenie z uwagi na ilość obsługiwanych abonentów i obszar działania – niewielkie. Przedsiębiorcy ci nie mają realnego znaczenia dla krajowego systemu cyberbezpieczeństwa. Jak pokazała praktyka przedsiębiorcy osiągający przychody do 10 mln złotych nie mieli istotnego znaczenia z punktu widzenia lokalnych podmiotów odpowiedzialnych za zarządzanie kryzysowe – stąd zwolnienie ich z obowiązku tworzenia i uzgadniania z właściwymi podmiotami planów działania, o których mowa w art. 47 ust. 1 PKE. Jednocześnie wielość przedsiębiorców prowadzących działalność na mniejszą skalę jest tak duża – sięgająca aż 6.000 podmiotów, że sama obsługa zgłoszeń incydentów bezpieczeństwa będzie wymagała ogromnej pracy logistycznej. Wobec tego Mediakom proponuje, by dodawany do art. 4 pkt 2a projektowanej ustawy otrzymał brzmienie:

„2a) przedsiębiorców komunikacji elektronicznej sporządzający plan, o którym mowa w art. 47 ust. 1 ustawy Prawo komunikacji elektronicznej"

3. Odnosząc się do planowanej zmiany polegającej na dodaniu przepisów art. 66a, 66b i 66c Mediakom wskazuje, że nie popiera proponowanych zmian w zakresie w jakim uprawniają one do wydawania wiążących rozstrzygnięć skutkujących powstaniem zakazu wprowadzania do użytkowania sprzętu, oprogramowania i usług danego dostawcy oraz obowiązku wycofania ich z obrotu. Mediakom rozumie potrzebę kontroli bezpieczeństwa i jakości sprzętu, oprogramowania i usług dostawców, jednak w jego ocenie proponowana procedura może prowadzić de facto do wykluczenia z rynku dowolnych dostawców i będzie wiązać się z poważnymi kosztami dla przedsiębiorców komunikacji elektronicznej, którzy będą zmuszeni do wymiany być może znacznej części wykorzystywanych urządzeń. Jednocześnie okres wymiany tych urządzeń (5 lat od ogłoszenia komunikatu o ocenie) nie pokrywa się z okresem amortyzacji urządzeń, co dodatkowo wpływa na zwiększenie kosztów nowych urządzeń. Jeśli więc możliwość wydawania wiążących ocen miałaby pozostać, to należy postulować wydłużenie okresu czasu na wymianę urządzeń do 7-8 lat.

Z poważaniem,

Anna Gąsecka
adwokat