Projekt na dzień 24.01.2020 r.

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I S T R Ó W

z dnia ……. 2020 r.

w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń

Na podstawie art. 176a ust. 5 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2019 r. poz. 2460) zarządza się, co następuje:

§ 1. Rozporządzenie określa:

1) rodzaje, zawartość, tryb sporządzania oraz aktualizacji przez przedsiębiorcę telekomunikacyjnego, zwanego dalej „przedsiębiorcą”, planu działań w sytuacjach szczególnych zagrożeń, zwanego dalej „planem”;
2) organy uzgadniające plany oraz zakres tych uzgodnień;
3) rodzaje przedsiębiorców obowiązanych do uzgadniania zawartości planów;
4) rodzaje działalności telekomunikacyjnej niepodlegającej obowiązkowi sporządzania planu;
5) rodzaje przedsiębiorców telekomunikacyjnych niepodlegających obowiązkowi sporządzania planu.

§ 2. 1. Obowiązkowi sporządzenia planu nie podlega przedsiębiorca, którego roczne przychody z tytułu wykonywania działalności telekomunikacyjnej w poprzednim roku obrotowym były równe lub mniejsze od kwoty 10 milionów złotych lub który wykonuje działalność telekomunikacyjną:

1) polegającą wyłącznie na dostarczaniu udogodnień towarzyszących;
2) wyłącznie na obszarze nie przekraczającym granic administracyjnych jednego powiatu, z wyłączeniem miast na prawach powiatu, w rozumieniu ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2019 r. poz. 511, 1571 i 1815);
3) polegającą wyłącznie na dostarczaniu sieci lub łączy telekomunikacyjnych dzierżawionych od innego przedsiębiorcy;
4) polegającą wyłącznie na sprzedaży we własnym imieniu i na własny rachunek usługi telekomunikacyjnej świadczonej przez innego dostawcę usług;

5) polegającą wyłącznie na rozprowadzaniu lub rozpowszechnianiu programów radiofonicznych lub telewizyjnych;
6) polegającą wyłącznie na świadczeniu usług dostępu do sieci Internet za pośrednictwem sieci telekomunikacyjnej obsługującej do 500 zakończeń sieci posiadających własny adres IP;
7) wyłącznie za pośrednictwem sieci telekomunikacyjnej innego przedsiębiorcy telekomunikacyjnego.

2. Wymienione w ust. 1 kryteria wyłączające obowiązek sporządzenia planu nie mają zastosowania do przedsiębiorców, o których mowa w przepisach wydanych na podstawie art. 6 ustawy z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców (Dz. U. poz. 1320 oraz z 2002 r. poz. 1571), dla których organem nadzorującym jest minister właściwy do spraw informatyzacji oraz Minister Obrony Narodowej.

§ 3. 1. Przedsiębiorca sporządza plan dla całości faktycznego obszaru wykonywanej działalności telekomunikacyjnej.

2. Przedsiębiorcy tworzący grupę kapitałową, o której mowa w art. 3 ust. 1 pkt 44 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2019 r. poz. 351, 1495, 1571, 1655 i 1680), z zastrzeżeniem § 2, mogą sporządzać wspólny plan dla wszystkich przedsiębiorców wchodzących w skład tej grupy.

3. W przypadku sporządzania wspólnego planu dla grupy kapitałowej, jednostka dominująca w grupie kapitałowej informuje Prezesa Urzędu Komunikacji Elektronicznej, zwanego dalej „Prezesem UKE”, o strukturze grupy kapitałowej oraz dokonuje sporządzenia, uzgodnienia i wprowadzenia planu do stosowania.

4. W przypadku braku obowiązku sporządzenia planu działań przez przedsiębiorcę, który jest jednostką dominującą w grupie kapitałowej, wyznacza on jeden z podmiotów zależnych grupy kapitałowej do sporządzenia, uzgodnienia i wprowadzenia planu do stosowania.

5. Do sporządzenia, aktualizacji oraz uzgadniania planów określonych w ust. 2 stosuje się § 4–9.

§ 4. 1. Przedsiębiorca sporządzający plan dokonuje:
1) analizy szczególnych zagrożeń środowiskowych i fizycznych na obszarze, na którym wykonuje działalność telekomunikacyjną, oraz oceny ich wpływu na bezpieczeństwo i integralność własnej sieci lub świadczonych usług;

2) analizy zagrożeń cyberbezpieczeństwa, w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 oraz z 2019 r. poz. 2020 i 2248) zwaną dalej „ustawą o krajowym systemie cyberbezpieczeństwa”, oraz oceny ich wpływu na bezpieczeństwo i integralność własnej sieci lub świadczonych usług;
3) analizy potrzeb w zakresie świadczenia, utrzymania i odtwarzania usług telekomunikacyjnych oraz dostępu telekomunikacyjnego:
   a) podmiotom i służbom wykonującym zadania w zakresie ratownictwa oraz niesienia pomocy ludności,
   b) podmiotom i służbom wykonującym zadania na rzecz obronności, cyberbezpieczeństwa, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego,
   c) podmiotom właściwym w sprawach zarządzania kryzysowego

– wskazanym w ramach uzgodnień planów przez organy, o których mowa w § 6, zwanymi dalej „właściwymi podmiotami i służbami”, a także oceny możliwości zapewnienia tych potrzeb.

2. Analizy i oceny, o których mowa w ust. 1, przedsiębiorca dokonuje na podstawie:

1) danych dotyczących zagrożeń, o których mowa w ust. 1 pkt 1, po uprzednim zwróceniu się o ich udostępnienie do właściwych terytorialnie wojewodów oraz własnych danych o zaistniałych w przeszłości naruszeniach bezpieczeństwa lub integralności sieci lub usług;
2) własnych danych o zaistniałych w przeszłości naruszeniach bezpieczeństwa lub integralności sieci lub usług oraz informacji o zagrożeniach cyberbezpieczeństwa publikowanymi przez CSIRT NASK – w przypadku analiz i ocen, o których mowa w ust. 1 pkt 2.

§ 5. 1. Plan zawiera:

1) podstawowe dane identyfikujące przedsiębiorcę, o których mowa w art. 10 ust. 4 pkt 1, 2, 5 i 6 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, zwanej dalej „ustawą”;
2) stanowiska służbowe, adresy, numery telefonów i adresy poczty elektronicznej osób odpowiedzialnych za sporządzenie planu wraz z określeniem zakresu ich kompetencji;
3) wykaz przeprowadzonych uzgodnień wraz z potwierdzeniem ich dokonania przez organy, o których mowa w § 6;
4) ogólną charakterystykę prowadzonej działalności telekomunikacyjnej, w tym opis świadczonych usług, obszar działalności oraz wykaz obiektów infrastruktury telekomunikacyjnej o znaczeniu kluczowym dla funkcjonowania przedsiębiorcy;

5) opis struktury organizacyjnej właściwej w zakresie zarządzania kryzysowego, w tym wykaz stanowisk przedsiębiorcy obowiązujących w przypadku wystąpienia sytuacji szczególnych zagrożeń wraz z wykazem zadań w zakresie zarządzania sytuacją kryzysową po wystąpieniu naruszenia bezpieczeństwa lub integralności sieci lub usług, z podaniem adresów lub siedzib, numerów telefonów i innych danych kontaktowych;
6) wykaz wdrożonych procedur współpracy przedsiębiorcy w sytuacjach szczególnych zagrożeń z innymi przedsiębiorcami oraz zagranicznymi operatorami telekomunikacyjnymi, w szczególności dotyczące zapewnienia dostępu telekomunikacyjnego;
7) procedury współpracy z organami uzgadniającymi plan, o których mowa w § 6, oraz z właściwymi podmiotami i służbami, w zakresie:
   a) utrzymania ciągłości, a w przypadku jej utraty – odtwarzania świadczenia usług telekomunikacyjnych i dostarczania sieci telekomunikacyjnej, z uwzględnieniem pierwszeństwa dla właściwych podmiotów i służb oraz po dokonaniu analizy, o której mowa w § 4 ust. 1 pkt 3,
   b) sposobów wzajemnego przekazywania informacji, alarmowania i ostrzegania, dotyczących sytuacji szczególnych zagrożeń, a także powiadamiania o konieczności podjęcia lub zaprzestania działań określonych w planie, wraz z wykazem stanowisk służbowych osób albo nazw służb właściwych w sprawach zarządzania kryzysowego, adresów lub siedzib, numerów telefonów i innych danych kontaktowych oraz zakresem ich kompetencji;
8) procedury współpracy z zespołami reagowania na incydenty bezpieczeństwa komputerowego poziomu krajowego, o których mowa w art. 2 pkt. 1–3 ustawy o krajowym systemie cyberbezpieczeństwa, w zakresie wzajemnego przekazywania informacji, ostrzegania i alarmowania, o ile takie zostały ustanowione wraz ze wskazaniem dokumentu normującego stosowanie tych procedur, o ile zostały ustanowione;
9) wyniki analiz i oceny, o których mowa w:
   a) § 4 ust. 1 pkt 1 – mogą być przedstawione w postaci mapy ryzyka lub mapy zagrożeń w rozumieniu ustawy z dnia 26 kwietnia 2007 r. o zarzadzaniu kryzysowym (Dz. U. z 2019 r. poz. 1398), zwanej dalej „ustawą o zarzadzaniu kryzysowym”,

b) § 4 ust. 1 pkt 2 – w postaci mapy ryzyka w rozumieniu ustawy o zarządzaniu kryzysowym,

c) § 4 ust. 1 pkt 3 – w postaci zestawienia tabelarycznego;

10) procedurę udostępniania urządzeń telekomunikacyjnych przedsiębiorcy innym przedsiębiorcom telekomunikacyjnym lub właściwym podmiotom i służbom, niezbędnych do przeprowadzenia akcji ratowniczych, wraz ze wskazaniem dokumentu normującego stosowanie tej procedury, o ile został ustanowiony;

11) opis wdrożonych środków technicznych i organizacyjnych oraz metod zapobiegania zagrożeniom, o których mowa w przepisach wykonawczych wydanych na podstawie art. 175d ustawy wraz ze wskazaniem dokumentu normującego stosowanie tych środków i metod, o ile został ustanowiony;

12) opis rezerw przeznaczonych na utrzymanie ciągłości świadczenia usług oraz ich odtworzenia w sytuacjach szczególnych zagrożeń oraz opis sposobów zapewnienia bezpieczeństwa łańcucha dostaw i usług serwisowych, zgodnie z umowami zawartymi z dostawcami, z uwzględnieniem systemu usług zewnętrznych oraz bezpośrednich inwestycji zagranicznych, wraz ze wskazaniem dokumentu normującego wykorzystanie tych rezerw oraz sposobów, o ile został ustanowiony;

13) wykaz wdrożonych systemów monitorowania i zabezpieczenia, w tym ochrony fizycznej, infrastruktury telekomunikacyjnej oraz świadczonych usług przed zakłóceniami i skutkami naruszenia bezpieczeństwa lub integralności lub incydentów oraz procedur działania i środków wdrażanych w sytuacjach szczególnych zagrożeń dla zabezpieczenia własnej infrastruktury telekomunikacyjnej przedsiębiorcy, wraz ze wskazaniem dokumentu normującego wdrażanie tych systemów, o ile został ustanowiony;

14) opis sposobu zapewnienia zasilania w energię elektryczną infrastruktury telekomunikacyjnej służącej utrzymaniu ciągłości świadczenia usług telekomunikacyjnych i dostarczaniu sieci telekomunikacyjnej, w przypadku przerw w dostawach energii elektrycznej, wraz ze wskazaniem dokumentu określającego sposób zapewnienia takiego zasilania w energię elektryczną, o ile został ustanowiony;

15) wykaz przedsięwzięć technicznych i organizacyjnych podejmowanych w przypadku wprowadzenia ograniczeń w działalności telekomunikacyjnej przewidzianych ustawą, wraz ze wskazaniem dokumentu normującego wprowadzanie takich przedsięwzięć, o ile został ustanowiony;

16) wykaz umów dotyczących realizacji zadań na rzecz obronności państwa, o ile zostały zawarte;
17) informację czy przedsiębiorca sporządza odrębny plan ochrony infrastruktury krytycznej w rozumieniu ustawy o zarzadzaniu kryzysowym.

2. W planie grupy kapitałowej, o której mowa w art. 3 ust. 1 pkt 44 ustawy z dnia 29 września 1994 r. o rachunkowości, informacje, o których mowa w ust. 1 pkt 4, zawiera się w osobno dla każdego z przedsiębiorców wchodzących w skład tej grupy.

§ 6. 1. Przedsiębiorca, o którym mowa w § 2 ust. 2, dokonuje uzgodnień planu z:
1) Ministrem Obrony Narodowej, ministrem właściwym do spraw wewnętrznych, ministrem właściwym do spraw informatyzacji i wojewodami – w zakresie określonym w § 5 ust. 1 pkt 7;
2) Szefem Agencji Bezpieczeństwa Wewnętrznego - w zakresie określonym w § 5 ust. 1 pkt 7 i 8.

2. Przedsiębiorca, z wyłączeniem przedsiębiorcy, o którym mowa w § 2 ust. 2, dokonuje uzgodnień planu z ministrem właściwym do spraw informatyzacji i właściwymi terytorialnie wojewodami - w zakresie określonym w § 5 ust. 1 pkt 7.

3. Organy, o których mowa w ust. 1 i 2, uzgadniają lub odmawiają uzgodnienia planu, określając przyczynę braku uzgodnienia oraz wyznaczają termin jego uzupełnienia i ponownego przesłania do uzgodnienia.

4. Po dokonaniu uzgodnień, o których mowa w ust. 1 lub 2, przedsiębiorca przesyła plan Prezesowi UKE celem:
1) uzgodnienia go w zakresie określonym w § 5 ust. 1 pkt 7 i 15;
2) sprawdzenia jego kompletności.

5. Prezes UKE:
1) uzgadnia plan i stwierdza jego kompletność albo
2) odmawia uzgodnienia planu, określając przyczynę braku uzgodnienia oraz wyznacza termin jego uzupełnienia i ponownego przesłania do uzgodnienia albo
3) w przypadku braku kompletności – określa niezbędny zakres uzupełnienia oraz wyznacza termin ponownego przesłania kompletnego planu.

§ 7. Po dokonaniu uzgodnień, o których mowa w § 6, przedsiębiorca wprowadza plan do stosowania, co potwierdza podpisem osoba uprawniona do prowadzenia spraw przedsiębiorcy w zakresie określonym w rozporządzeniu.

§ 8. 1. Przedsiębiorca przekazuje wprowadzony do stosowania plan ministrowi właściwemu do spraw informatyzacji oraz Prezesowi UKE.

2. Plan, o którym mowa w ust. 1, przekazywany jest w formie dokumentu elektronicznego, opatrzonego przez przedsiębiorcę kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym, zapisanego w formacie .doc(x), .odt albo .pdf, z wyłączeniem elektronicznej kopii stanowiącej obraz pierwotnego dokumentu.

3. W przypadku braku możliwości przekazania planu w formie, o której mowa w ust. 2, plan przekazywany jest w postaci papierowej opatrzonej podpisem własnoręcznym.

4. Na wniosek organów uzgadniających plan przedsiębiorca sporządza i przekazuje nieodpłatnie wyciąg z planu sporządzony w zakresie zagadnień podlegających uzgodnieniom.

§ 9. 1. Plan zachowuje ważność przez 36 miesięcy od daty jego wprowadzenia do stosowania przez przedsiębiorcę. Plan podlega okresowej aktualizacji w trybie określonym w § 3, 4 i 6–8. Przedsiębiorca dokonuje aktualizacji okresowej w terminie zapewniającym dokonanie uzgodnień i wprowadzenie do stosowania zaktualizowanego planu przed datą upływu ważności planu podlegającego aktualizacji. W przeciwnym wypadku uznaje się, że przedsiębiorca nie posiada aktualnego planu działań.

2. Plan podlega bieżącej aktualizacji w przypadku wystąpienia okoliczności wpływających na jego zawartość, a w szczególności:

1) zmian w infrastrukturze telekomunikacyjnej oraz zakresie wykonywanej działalności telekomunikacyjnej, wpływających na zmianę sposobu i formę realizacji planu;
2) zmiany danych identyfikujących przedsiębiorcę, warunków lub procedur współpracy z organami uzgadniającymi zawartość planu;
3) istotnej zmiany danych dotyczących szczególnych zagrożeń;
4) na wniosek właściwych organów administracji publicznej uzgadniających zawartość planu, uzasadniony zmianami potrzeb, o których mowa w § 4 ust. 1 pkt 3.

3. Zmiana treści planu, o których mowa w § 5 pkt 7, wymaga uzgodnienia z organami, o których mowa w § 6, w zakresie ich kompetencji.

4. Do zmiany planu stosuje się przepisy § 8.

5. Analizy i oceny, o których mowa w § 4 ust. 1 pkt 2, przedsiębiorca dokonuje corocznie oraz aktualizuje plan w zakresie określonym w § 5 pkt 9.

6. Do aktualizacji, o której mowa w ust. 5, nie stosuje się przepisów § 8.

§ 10. 1. Przedsiębiorca, z zastrzeżeniem ust. 2, sporządza, uzgadnia i wprowadza do stosowania plan zgodnie z przepisami rozporządzenia w terminie 12 miesięcy od dnia rozpoczęcia świadczenia usług telekomunikacyjnych lub dostarczania sieci telekomunikacyjnej albo od dnia wejścia w życie rozporządzenia, w zależności od tego, który z tych terminów nastąpi później.

2. Plany przedsiębiorców sporządzone przed wejściem w życie rozporządzenia zachowują moc do upływu terminu ich aktualizacji okresowej wynikającego z przepisów dotychczasowych.

§ 11. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.[1)]

PREZES RADY MINISTRÓW

Za zgodność pod względem prawnym, redakcyjnym i legislacyjnym
Iwona Szulc
Zastępca Dyrektora
Departamentu Prawnego
Ministerstwa Cyfryzacji
/-podpisano elektronicznie/

---

1) Niniejsze rozporządzenie było poprzedzone rozporządzeniem Prezesa Rady Ministrów z dnia 4 stycznia 2010 r. w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń (Dz. U. poz. 77, z 2016 r. poz. 1798 oraz z 2017 r. poz. 2307), które traci moc z dniem wejścia w życie niniejszego rozporządzenia zgodnie z art. 92 ust. 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 oraz z 2019 r. poz. 2020 i 2248).

Uzasadnienie

Na skutek wprowadzonych zmian przepisów w art. 176a ust. 1 pkt 3 i ust. 2 pkt 4 ustawy – Prawo telekomunikacyjne (Dz.U. z 2019 r. poz. 2460), w wyniku wejścia w życie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 oraz z 2019 r. poz. 2020 i 2248), nastąpiła konieczność wydania nowego rozporządzenia Rady Ministrów w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń, dotyczących zawartości i zakresu informacji zawartych w planach. W nowym rozporządzeniu pojawiły się regulacje dotyczące m.in. dokonania analizy zagrożeń cyberprzestrzeni istotnych z punktu widzenia przedsiębiorcy, ustanowionych struktur organizacyjnych przedsiębiorcy, procedur wewnętrznych oraz opisu technicznych i organizacyjnych środków zapewnienia bezpieczeństwa i integralności infrastruktury telekomunikacyjnej i świadczonych usług, w przypadku wystąpienia incydentów w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Powyższe wynika także z wystąpienia pokontrolnego NIK przesłanego do Prezesa UKE w dniu 25 października 2018 r. po zakończeniu kontroli pn. „Bezpieczeństwo teleinformatyczne RP”.

Wymagana jest zmiana w zakresie rodzajów planów działań w sytuacjach szczególnych zagrożeń sporządzanych przez przedsiębiorców telekomunikacyjnych wynikająca z podwyższenia kryterium rocznych przychodów z tytułu wykonywania działalności telekomunikacyjnej. Obecna systematyka tj. plany lokalne, rejonowe i ogólne nie w pełni odzwierciedla wielkość i zakres działalności przedsiębiorców oraz poziom i zakres współdziałania przedsiębiorców telekomunikacyjnych z organami administracji rządowej i samorządowej. W związku z tym zrezygnowano z podziału i wprowadzono jeden rodzaj planu, który odzwierciedla całość faktycznego obszaru wykonywania działalności telekomunikacyjnej.

Kwestia korelacji planów działań w sytuacjach szczególnych zagrożeń z innymi rodzajami planów – np. planami ochrony infrastruktury krytycznej jest zagadnieniem należącym do materii ustawowej i nie mogą być rozstrzygane za poziomie aktu wykonawczego.

W nowym projekcie zmiany polegają przede wszystkim na:

1) zwiększeniu obszaru wykonywania działalności telekomunikacyjnej z gminy do granic powiatu oraz podwyższeniu do 10 mln zł. (w § 2) kryterium ograniczającego liczbę przedsiębiorców telekomunikacyjnych obowiązanych do sporządzenia planów. Kryteria po konsultacjach z regulatorem rynku telekomunikacyjnego zostało przyjęte w przedmiotowym projekcie rozporządzenia, jako warunkujące obowiązek opracowania i uzgodnienia planu działań w sytuacjach szczególnych zagrożeń;

2) wyłączeniu z kryteriów (w § 2 ust. 2) przedsiębiorców, o których mowa w przepisach wykonawczych wydanych na podstawie art. 6 ustawy z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców (Dz. U. poz. 1320 oraz z 2002 r. poz. 1571), dla których organem nadzorującym jest minister właściwy do spraw cyfryzacji oraz Minister Obrony Narodowej;

3) zobowiązaniu (w § 3 ust. 1) przedsiębiorców wykonujących działalność telekomunikacyjną na obszarze przekraczającym granice administracyjne powiatu do sporządzenia planu dla faktycznego obszaru wykonywanej działalności.

4) zobowiązaniu (w § 3 ust. 2–4) przedsiębiorcy, który jest jednostką dominującą u przedsiębiorców tworzących grupę kapitałową do poinformowania Prezesa UKE o strukturze grupy kapitałowej oraz sporządzenia, uzgodnienia i wprowadzenia planu do stosowania. W przypadku braku obowiązku sporządzenia planu działań przez przedsiębiorcę, który jest jednostką dominującą w grupie kapitałowej, wyznacza on jeden z podmiotów zależnych grupy kapitałowej do sporządzenia, uzgodnienia i wprowadzenia planu do stosowania. Zmiana ta pozwoli jednoznacznie wyróżnić charakter działalności przedsiębiorcy telekomunikacyjnego i porównać z danymi zawartymi w Rejestrze Przedsiębiorców Telekomunikacyjnych prowadzonym przez Prezesa UKE;

5) doprecyzowaniu (w § 4 ust. 1 pkt 1 i 2) czynności analitycznych (bez niepotrzebnego przepisywania zwartości planów reagowania kryzysowego) przedsiębiorcy telekomunikacyjnego oraz rozszerzono zakres analizy o incydenty mające wpływ na cyberbezpieczeństwo (co wynika z przepisów ustawy o KSC zmieniających przepisy w art. 176a ust. 1 pkt 3 i ust. 2 pkt 4 Prawa telekomunikacyjnego);

6) rozszerzeniu zakresu (w § 4 ust. 1 pkt 3 lit. b) analizy potrzeb w zakresie świadczenia, utrzymania i odtwarzania usług telekomunikacyjnych oraz dostępu telekomunikacyjnego dla podmiotów i służb wykonującym zadania na rzecz cyberbezpieczeństwa.

7) na potrzeby analiz zagrożeń cyberbezpieczeństwa doprecyzowano (§ 4 ust. 2) podstawę uwzględniającą własne zdarzenia oraz incydenty bezpieczeństwa komputerowego publikowane przez CSIRT NASK;

8) określeniu (§ 5 pkt. 1–17) szczegółowej zawartości planu z uwzględnieniem procedur współpracy z zespołami reagowania na incydenty bezpieczeństwa komputerowego poziomu krajowego (§ 5 pkt 8), o których mowa w ustawie o krajowym systemie cyberbezpieczeństwa, w zakresie wzajemnego przekazywania informacji, ostrzegania i alarmowania, jeśli zostały ustanowione;

9) wprowadzeniu (§ 5 pkt 11) opisu wdrożonych środków technicznych i organizacyjnych, metod zapobiegania zagrożeniom oraz zarządzania ryzykiem sieci piątej generacji (5G), o ile przedsiębiorca telekomunikacyjny świadczy usługi w takiej sieci, w zakresie bezpieczeństwa sieci i usług, zgodnie z rozporządzeniem wydanym na podstawie art. 175d ustawy – Prawo telekomunikacyjne;

10) wprowadzeniu (§ 5 pkt 12) opisu rezerw przeznaczonych na utrzymanie ciągłości świadczenia usług oraz procedur (§ 5 pkt 14) zapewnienia zasilania w energię elektryczną infrastruktury telekomunikacyjnej służącej utrzymaniu ciągłości świadczenia usług telekomunikacyjnych i dostarczaniu sieci telekomunikacyjnej w przypadku przerw w dostawach energii elektrycznej;

11) załączeniu (§ 5 pkt 16) wykazu umów dotyczących realizacji zadań na rzecz obronności państwa, w rozumieniu ustawy z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców (Dz. U. poz. 1320 oraz z 2002 r. poz. 1571);

12) zrezygnowaniu z uzgodnień z ministrem spraw zagranicznych, ministrem sprawiedliwości, ministrem finansów, co jest następstwem nowelizacji, w której zniesiono element planu wskazany w § 5 pkt 12 rozporządzenia, który nie powinien być obligatoryjny, ponieważ w zdecydowanej większości przypadków

przedsiębiorcy telekomunikacyjni wskazują, iż nie realizują tego rodzaju inwestycji;

13) doprecyzowaniu katalogu organów uzgadniających plan (w § 6 ust. 1 i 2) ograniczając do organów administracji publicznej, z którymi plan ma zostać uzgodniony, wyłącznie do podmiotów, z którymi uzgadnianie planu jest merytorycznie uzasadnione biorąc pod uwagę kompetencje właściwych organów;

14) doprecyzowaniu (w § 6 ust. 1 i 2) podmiotowego i przedmiotowego zakresu uzgadniania planów oraz trybu ich uzgadniania zachowując tryb administracyjny;

15) w wyniku konsultacji z regulatorem rynku telekomunikacyjnego zostało przyjęte w przedmiotowym projekcie rozporządzenia (w § 6 ust. 5), jako warunkujące obowiązek wdrożenia opracowanego planu działań w sytuacjach szczególnych zagrożeń, uzgodnienie i sprawdzenie jego kompletności przez Prezesa UKE;

16) doprecyzowaniu okresu ważności sporządzanych planów (w § 9 ust. 1) do 36 miesięcy (gwarantując okres przejściowy na aktualizację przed upływem jego ważności), a okresową aktualizację w terminie, który zapewni jego uzgodnienie i wprowadzenie do użytku przed upływem ważności planu obowiązującego;

17) wskazaniu, że zagrożenia cyberbezpieczeństwa przedsiębiorca analizuje i ocenia corocznie (§ 9 ust. 5), z uwagi na szybkozmienność tych zagrożeń. Aktualizacja planu w tym zakresie nie wymaga jednak dokonywania uzgodnień (§ 9 ust.6);

18) określeniu (§ 10 ust. 1) granicznego terminu całego procesu sporządzania przez przedsiębiorcę telekomunikacyjnego planów działań w sytuacjach szczególnych zagrożeń, co jednoznacznie rekomendowała Najwyższa Izba Kontroli (w swoim wystąpieniu pokontrolnym przesłanym do Prezesa UKE dnia 25.10.2018 r.).

Rozporządzenie wejdzie w życie po upływie 14 dni od dnia ogłoszenia, z uwagi na fakt, że nie powoduje znaczących zmian w stosunku do przepisów dotychczas obowiązujących oraz zawiera przepis przejściowy utrzymujący w mocy dotychczas posiadane przez przedsiębiorców plany działań.

Projektowane rozporządzenie nie podlega procedurze notyfikacji w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 i z 2004 r. poz. 597).

Nie zachodzi również konieczność przedstawienia projektu rozporządzenia właściwym organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu.

Przedmiotowy projekt jest zgodny z prawem Unii Europejskiej.

Projektowane rozporządzenie nie będzie mieć wpływu na sytuację ekonomiczną i społeczną rodziny, osób niepełnosprawnych oraz osób starszych.

W celu wykonania obowiązku wynikającego z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) projekt rozporządzenia zostanie zamieszczony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie „Rządowy Proces Legislacyjny” oraz w Biuletynie Informacji Publicznej na stronie podmiotowej urzędu obsługującego ministra właściwego do spraw informatyzacji.

Nazwa projektu Projekt rozporządzenia Rady Ministrów w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** **Marek Zagórski,** Minister Cyfryzacji **Kontakt do opiekuna merytorycznego projektu** **Ireneusz Kisielewski,** tel. 22 245 57 75, ireneusz.kisielewski@mc.gov.pl	**Data sporządzenia** 24.01.2020 **Źródło:** art. 176a ust. 5 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2019 r. poz. 2460) **Nr w wykazie prac legislacyjnych Rady Ministrów RD528**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Zgodnie z art. 81 pkt 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 oraz z 2019 r. poz. 2020 i 2248) zmianie uległy przepisy w ustawie – Prawo telekomunikacyjne dotyczące pojęcia „*sytuacji szczególnych zagrożeń*" oraz zawartości planów działań w sytuacjach szczególnych zagrożeń sporządzanych przez przedsiębiorców telekomunikacyjnych.

W związku z powyższym, istnieje konieczność wydania nowego rozporządzenia na podstawie upoważnienia ustawowego zawartego w art. 176a ust. 5 ustawy – Prawo telekomunikacyjne, dotyczącego planu działania przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Celem wydania nowego rozporządzenia jest przede wszystkim realizacja ustawowej delegacji oraz dostosowanie procedur opracowywania i uzgadniania planów działań przedsiębiorców w sytuacjach szczególnych zagrożeń do rzeczywistych potrzeb związanych z realizacją obowiązków na rzecz obronności, bezpieczeństwa państwa oraz cyberbezpieczeństwa.

Zmiany polegają przede wszystkim na ograniczeniu ilości przedsiębiorców obowiązanych do sporządzenia planów, oraz wyłączenie przedsiębiorców, których infrastruktura i sieć telekomunikacyjna nie mają krytycznego znaczenia dla obronności i bezpieczeństwa państwa oraz bezpieczeństwa porządku publicznego.

Kryterium oceny wielkości przedsiębiorcy telekomunikacyjnego zostanie zwiększone do kwoty 10 milionów zł rocznych przychodów z tytułu wykonywania działalności telekomunikacyjnej w poprzednim roku obrotowym. Spowoduje to ograniczenie liczby przedsiębiorców telekomunikacyjnych sporządzających plany poprzez wyłączenie mikro i małych przedsiębiorców. Jednak wyłączono z kryteriów przedsiębiorców, o których mowa w przepisach wykonawczych wydanych na podstawie art. 6 ustawy z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców (Dz. U. poz. 1320 oraz z 2002 r. poz. 1571), dla których organem nadzorującym jest minister właściwy do spraw cyfryzacji oraz Minister Obrony Narodowej.

Dotychczasowa systematyka tj. plany lokalne, rejonowe i ogólne nie w pełni odzwierciedla wielkość i zakres działalności przedsiębiorców oraz poziom i zakres współdziałania przedsiębiorców telekomunikacyjnych z organami administracji rządowej i samorządowej. W związku z tym zrezygnowano z podziału i wprowadzono jeden rodzaj planu, który odzwierciedla całość faktycznego obszaru wykonywania działalności telekomunikacyjnej.

W nowym rozporządzeniu pojawiły się regulacje dotyczące m.in. dokonania analizy zagrożeń cyberprzestrzeni istotnych z punktu widzenia przedsiębiorcy, ustanowionych struktur organizacyjnych przedsiębiorcy, procedur wewnętrznych oraz opisu technicznych i organizacyjnych środków zapewnienia bezpieczeństwa i integralności infrastruktury telekomunikacyjnej i świadczonych usług, w przypadku wystąpienia incydentów w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa.

Jednoznacznie określono ważność planów uwzględniając okres przejściowy na jego aktualizację – zgodnie bowiem z obecnie obowiązującym rozporządzeniem (§ 11 ust. 1) plany podlegają okresowej aktualizacji nie

rzadziej niż raz na 3 lata. Doprecyzowano czynności analityczne (bez niepotrzebnego przepisywania zwartości planów reagowania kryzysowego) przedsiębiorcy telekomunikacyjnego oraz rozszerzono zakres analizy potrzeb w zakresie świadczenia, utrzymania i odtwarzania usług telekomunikacyjnych oraz dostępu telekomunikacyjnego dla podmiotów i służb wykonującym zadania na rzecz cyberbezpieczeństwa.
Ponadto doprecyzowano katalog organów uzgadniających plan ograniczając do organów administracji publicznej, z którymi plan ma zostać uzgodniony, wyłącznie do podmiotów, z którymi uzgadnianie planu jest merytorycznie uzasadnione biorąc pod uwagę kompetencje właściwych organów.
Zastosowane rozwiązania skutkować będą uproszczeniem procedur w tym zakresie i ograniczeniem zbędnych formalności dla przedsiębiorców telekomunikacyjnych.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Regulacja dotyczy obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Odstąpiono, zatem od analizy porównawczej z innymi państwami.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Minister właściwy do spraw informatyzacji, Minister Obrony Narodowej	2	Nie dotyczy	Ograniczenie uzgodnień wyłącznie do planów ogólnych. Objęcie obowiązkiem, przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, do sporządzania planu ogólnego przez przedsiębiorców w stosunku do, których organem organizującym i nadzorującym wykonywanie zadań jest minister właściwy do spraw informatyzacji i Minister Obrony Narodowej. Zapewnienie przekazywania uzgodnionych i wprowadzonych do działania planów rejonowych przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym.
Przedsiębiorcy telekomunikacyjni obowiązani do sporządzenia planów działań w sytuacjach szczególnych zagrożeń	Zwiększenie obecnego progu z 4 mln do 10 mln zł. rocznych przychodów (co będzie odpowiadać ok. 12-15 tys. abonentów) spowoduje, że	Przedsiębiorcy wpisani w rejestrze przedsiębiorców telekomunikacyjnych prowadzącym przez Prezesa UKE, z wyłączeniem wymienionych w § 2 nowelizowanego rozporządzenia	Przedsiębiorcy telekomunikacyjni będą zobowiązanie do opracowania i uzgodnienia planu działań w sytuacjach szczególnych zagrożeń, skorelowanego z planem zarzadzania kryzysowego i uzgodnionego z

	obowiązki będzie musiało wykonywać nie ok. 220 operatorów (jak obecnie przewiduje projekt rozporządzenia), ale ok. 90 operatorów.		właściwymi organami, natomiast zwiększenie kryterium wielkości przychodów z tytułu wykonywanej działalności telekomunikacyjnej w poprzednim roku pozwoli zdjąć obowiązek z mikro i małych przedsiębiorców.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) projektowane rozporządzenie zostanie zamieszczone w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie „Rządowy Proces Legislacyjny" oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji.

Projekt będzie poddany uzgodnieniom, opiniowaniu i konsultacjom publicznym.

6. Wpływ na sektor finansów publicznych

	Skutki w okresie 10 lat od wejścia w życie zmian [zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem	-	-	-	-	-	-	-	-	-	-	-	-
budżet państwa	-	-	-	-	-	-	-	-	-	-	-	-
JST	-	-	-	-	-	-	-	-	-	-	-	-
pozostałe jednostki (oddzielnie)	-	-	-	-	-	-	-	-	-	-	-	-
Wydatki ogółem	-	-	-	-	-	-	-	-	-	-	-	-
budżet państwa	-	-	-	-	-	-	-	-	-	-	-	-

JST	-	-	-	-	-	-	-	-	-	-	-	-
pozostałe jednostki (oddzielnie)	-	-	-	-	-	-	-	-	-	-	-	-
Saldo ogółem	-	-	-	-	-	-	-	-	-	-	-	-
budżet państwa	-	-	-	-	-	-	-	-	-	-	-	-
JST	-	-	-	-	-	-	-	-	-	-	-	-
pozostałe jednostki (oddzielnie)	-	-	-	-	-	-	-	-	-	-	-	-

Źródła finansowania	-
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Wydanie przedmiotowego rozporządzenia nie będzie wpływało na budżet państwa – zarówno na dochody, jak i wydatki.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

Skutki								
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)	duże przedsiębiorstwa	-	-	-	-	-	-	-
	sektor mikro-, małych i średnich przedsiębiorstw	-	-	-	-	-	-	-
	rodzina, obywatele oraz gospodarstwa domowe	-	-	-	-	-	-	-
	(dodaj/usuń)	-	-	-	-	-	-	-
W ujęciu niepieniężnym	duże przedsiębiorstwa	ograniczenie procedur i formalności						
	sektor mikro-, małych i średnich przedsiębiorstw	ułatwienie rozpoczęcia i prowadzenia działalności, ograniczenie procedur i zbędnych formalności						

	rodzina, obywatele oraz gospodarstwa domowe	Projekt rozporządzenia nie ma wpływu na sytuację ekonomiczną i społeczną rodziny, osób niepełnosprawnych oraz osób starszych, a także na obywateli i gospodarstwa domowe.
	(dodaj/usuń)	-
Niemierzalne	(dodaj/usuń)	-
	(dodaj/usuń)	-
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Efektem będzie usprawnienie wobec przedsiębiorców telekomunikacyjnych procedur i ograniczenie formalności. Wybranie przez przedsiębiorców możliwości przekazywania planów działań w postaci elektronicznej spowoduje dla nich oszczędności w zakresie wydatków na usługi pocztowe oraz przyspieszy procedurę opracowania, uzgadniania i wdrożenia planów działań.	

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☒ nie dotyczy
☒ zmniejszenie liczby dokumentów ☒ zmniejszenie liczby procedur ☒ skrócenie czasu na załatwienie sprawy ☐ inne: -	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne: -
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☒ nie dotyczy

Komentarz: Informatyzacja obowiązujących formularzy skróci czas ich wypełniania oraz znacznie przyspieszy procedurę współpracy z ministrem właściwym do spraw informatyzacji w sytuacjach szczególnych zagrożeń.

9. Wpływ na rynek pracy

Projektowane rozporządzenie nie będzie miało wpływu na rynek pracy.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☒ informatyzacja ☐ zdrowie
Omówienie wpływu	Informatyzacja obowiązujących formularzy skróci czas ich wypełniania oraz znacznie przyspieszy procedurę współpracy z ministrem właściwym do spraw informatyzacji w sytuacjach szczególnych zagrożeń.	

11. Planowane wykonanie przepisów aktu prawnego

Rozporządzenie wejdzie w życie po upływie 14 dni od dnia ogłoszenia.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

Nie dotyczy.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Brak załączników.