M A T E R I A Ł P O R Ó W N A W C Z Y

do ustawy z dnia 5 lipca 2018 r.

o krajowym systemie cyberbezpieczeństwa

(druk nr 893)

USTAWA z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 2017 r. poz. 2198, 2203 i 2361)

Art. 90u.

1. Rada Ministrów może przyjąć rządowy program albo programy mające na celu:
   1) wyrównywanie szans edukacyjnych dzieci i młodzieży oraz innych grup społecznych;
   2) wspieranie powstawania i realizacji regionalnych lub lokalnych programów, o których mowa w art. 90t ust. 1 pkt 1, tworzonych przez jednostki samorządu terytorialnego lub organizacje, o których mowa w art. 3 ust. 2 i 3 ustawy z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie;
   3) wspieranie powstawania i realizacji regionalnych lub lokalnych programów, o których mowa w art. 90t ust. 1 pkt 2, tworzonych przez jednostki samorządu terytorialnego lub organizacje, o których mowa w art. 3 ust. 2 i 3 ustawy z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie;
   4) wspomaganie tworzenia warunków do sprawowania profilaktycznej opieki zdrowotnej nad uczniami;
   5) wspomaganie organów prowadzących szkoły lub placówki w zapewnieniu bezpiecznych warunków nauki, wychowania i opieki lub w podnoszeniu poziomu dyscypliny w szkołach lub placówkach;
   [6) rozwijanie kompetencji, zainteresowań i uzdolnień dzieci i młodzieży oraz innych grup społecznych, w tym wspomaganie organów prowadzących szkoły lub placówki w realizacji przedsięwzięć w tym obszarze;]
   <6) rozwijanie kompetencji, zainteresowań i uzdolnień dzieci i młodzieży oraz innych grup społecznych, w tym wspomaganie organów prowadzących szkoły lub

placówki w realizacji przedsięwzięć w tym obszarze, w szczególności w zakresie bezpiecznego korzystania z technologii informacyjno-komunikacyjnych;>

7) wspieranie przedsięwzięć w zakresie edukacji patriotycznej i obywatelskiej dzieci i młodzieży.

2. [57] (uchylony).

3. [58] (uchylony).

4. W przypadku przyjęcia programu albo programów, o których mowa w ust. 1, Rada Ministrów określi, w drodze rozporządzenia, odpowiednio:

1) szczegółowe warunki udzielania pomocy dzieciom i młodzieży oraz innym grupom społecznym objętym programem, o którym mowa w ust. 1 pkt 1, formy i zakres tej pomocy oraz tryb postępowania w tych sprawach, uwzględniając w szczególności przedsięwzięcia sprzyjające eliminowaniu barier edukacyjnych, a także osoby i grupy osób uprawnione do pomocy;

2) szczegółowe warunki dofinansowania regionalnych lub lokalnych programów, o których mowa w ust. 1 pkt 2, warunki, jakie muszą spełnić te programy, podmioty dokonujące oceny programów oraz udział środków własnych niezbędnych do ubiegania się o udzielenie dofinansowania, a także sposób i tryb wyboru programów, którym zostanie udzielone dofinansowanie, uwzględniając w szczególności potrzeby edukacyjne na danym obszarze, osiągnięcia uczniów, w tym w szczególności wyniki egzaminu ósmoklasisty, egzaminu maturalnego i egzaminu potwierdzającego kwalifikacje w zawodzie, a w przypadku ubiegania się o dofinansowanie przez jednostkę samorządu terytorialnego - także udział nakładów na oświatę w budżecie tej jednostki;

3) szczegółowe warunki dofinansowania regionalnych lub lokalnych programów, o których mowa w ust. 1 pkt 3, warunki, jakie muszą spełnić te programy, podmioty dokonujące oceny programów oraz udział środków własnych niezbędnych do ubiegania się o udzielenie dofinansowania, a także sposób i tryb wyboru programów, którym zostanie udzielone dofinansowanie, uwzględniając w szczególności potrzeby i możliwości edukacyjne uczniów, ich osiągnięcia, bazę dydaktyczną niezbędną do realizacji programu, przygotowanie kadry pedagogicznej i warunki materialne uczniów;

---

4) szczegółowe warunki, formy i tryb wspomagania tworzenia warunków do sprawowania profilaktycznej opieki zdrowotnej nad uczniami, uwzględniając w szczególności tworzenie gabinetów profilaktyki zdrowotnej dla uczniów;

5) formy i zakres wspierania organów prowadzących w zapewnieniu bezpiecznych warunków nauki, wychowania i opieki w szkołach i placówkach lub podnoszeniu poziomu dyscypliny w szkołach lub placówkach, sposób podziału środków budżetu państwa przyznanych na realizację programu, szczegółowe kryteria i tryb oceny wniosków organów prowadzących o udzielenie wsparcia finansowego oraz zakres informacji, jakie powinien zawierać wniosek organu prowadzącego o udzielenie wsparcia finansowego, uwzględniając w szczególności wymóg skuteczności i efektywności przedsięwzięć podejmowanych w ramach programu;

[6) szczegółowe warunki, formy i tryb realizacji przedsięwzięć w zakresie rozwijania kompetencji, zainteresowań i uzdolnień dzieci i młodzieży oraz innych grup społecznych, a także warunki i tryb wspomagania organów prowadzących szkoły lub placówki w realizacji przedsięwzięć w tym obszarze, uwzględniając konieczność rozwijania umiejętności ułatwiających przystosowanie się do zmian zachodzących w życiu społecznym i gospodarczym, możliwość udzielenia wsparcia finansowego organów prowadzących szkoły lub placówki oraz wymóg skuteczności i efektywności wydatkowania środków budżetowych;]

<6) szczegółowe warunki, formy i tryb realizacji przedsięwzięć w zakresie rozwijania kompetencji, zainteresowań i uzdolnień dzieci i młodzieży oraz innych grup społecznych, a także warunki i tryb wspomagania organów prowadzących szkoły lub placówki w realizacji przedsięwzięć w tym obszarze, w szczególności w zakresie bezpiecznego korzystania z technologii informacyjno-komunikacyjnych, uwzględniając konieczność rozwijania umiejętności ułatwiających przystosowanie się do zmian zachodzących w życiu społecznym i gospodarczym, możliwość udzielenia wsparcia finansowego organów prowadzących szkoły lub placówki oraz wymóg skuteczności i efektywności wydatkowania środków budżetowych;>

7) szczegółowe warunki, formy i tryb wspierania przedsięwzięć w zakresie edukacji patriotycznej i obywatelskiej dzieci i młodzieży, uwzględniając w szczególności pomoc w poznawaniu miejsc pamięci narodowej.

Objaśnienie oznaczeń: *[] kursywa – tekst usunięty przez Sejm*

<> druk pogrubiony – tekst wstawiony przez Sejm

USTAWA z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2018 r. poz. 762, 810 i 1090)

Art. 12a.

1. Dział informatyzacja obejmuje sprawy:
   1) informatyzacji administracji publicznej oraz podmiotów wykonujących zadania publiczne;
   2) systemów i sieci teleinformatycznych administracji publicznej;
   3) wspierania inwestycji w dziedzinie informatyzacji;
   4) realizacji zobowiązań międzynarodowych Rzeczypospolitej Polskiej w dziedzinie informatyzacji i telekomunikacji;
   5) udziału w kształtowaniu polityki Unii Europejskiej w zakresie informatyzacji;
   6) rozwoju społeczeństwa informacyjnego i przeciwdziałania wykluczeniu cyfrowemu;
   7) rozwoju usług świadczonych drogą elektroniczną;
   8) kształtowania polityki państwa w zakresie ochrony danych osobowych;
   9) telekomunikacji;
   [10) bezpieczeństwa cyberprzestrzeni;]
   <10) bezpieczeństwa cyberprzestrzeni w wymiarze cywilnym;>
   11) rejestru PESEL, Rejestru Dowodów Osobistych, Rejestru Stanu Cywilnego oraz Centralnej Ewidencji Wydanych i Unieważnionych Dokumentów Paszportowych;
   12) ewidencji pojazdów, ewidencji kierowców oraz ewidencji posiadaczy kart parkingowych;
   13) nadzoru nad świadczeniem usług zaufania w rozumieniu przepisów o usługach zaufania;
   14) infrastruktury informacji przestrzennej.
2. Minister właściwy do spraw informatyzacji sprawuje nadzór nad Prezesem Urzędu Komunikacji Elektronicznej.

Art. 19.

1. Dział obrona narodowa obejmuje, w czasie pokoju, sprawy:
   1) obrony Państwa oraz Sił Zbrojnych Rzeczypospolitej Polskiej, zwanych dalej "Siłami Zbrojnymi",
   <1a) bezpieczeństwa cyberprzestrzeni w wymiarze militarnym,>

Objaśnienie oznaczeń: *[] kursywa – tekst usunięty przez Sejm*

<> druk pogrubiony – tekst wstawiony przez Sejm

2) udziału Rzeczypospolitej Polskiej w wojskowych przedsięwzięciach organizacji międzynarodowych oraz w zakresie wywiązywania się z zobowiązań militarnych, wynikających z umów międzynarodowych,

3) umów offsetowych

- chyba że na mocy odrębnych przepisów określone sprawy należą do zakresu zadań i kompetencji Prezydenta Rzeczypospolitej Polskiej lub innych organów państwowych.

2. Minister właściwy do spraw obrony narodowej wykonuje zadania i kompetencje Ministra Obrony Narodowej określone w art. 134 ust. 2 i 5 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. poz. 483, z 2001 r. poz. 319, z 2006 r. poz. 1471 oraz z 2009 r. poz. 946).

3. Minister Obrony Narodowej sprawuje nadzór nad działalnością Agencji Mienia Wojskowego.

USTAWA z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2017 r. poz. 1920 i 2405 oraz z 2018 r. poz. 138 i 650 i 730)

<Art. 32aa.

1. W celu zapobiegania i przeciwdziałania oraz zwalczania zdarzeń o charakterze terrorystycznym dotyczących istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli, posiadaczy samoistnych i posiadaczy zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, lub danych przetwarzanych w tych systemach oraz zapobiegania i wykrywania przestępstw o charakterze terrorystycznym w tym obszarze oraz ścigania ich sprawców, ABW wdraża w tych podmiotach system wczesnego ostrzegania o zagrożeniach występujących w sieci Internet, zwany dalej „systemem ostrzegania", prowadzi go i koordynuje jego funkcjonowanie.

2. Wdrożenie elementów systemu ostrzegania w podmiotach, o których mowa w ust. 1, następuje zgodnie z rocznym planem wdrożenia, opracowywanym przez Szefa ABW

w terminie do dnia 30 września roku poprzedzającego. W uzasadnionych przypadkach, na wniosek podmiotu, wdrożenie elementów systemu ostrzegania może zostać przeprowadzone z pominięciem planu.

3. ABW niezwłocznie informuje podmiot, o którym mowa w ust. 1, o jego włączeniu do rocznego planu wdrożenia systemu ostrzegania.

4. Podmiot, o którym mowa w ust. 1, ma obowiązek przystąpić do systemu ostrzegania, oraz przekazać ABW niezbędne informacje umożliwiające wdrożenie systemu ostrzegania w tym podmiocie.

5. W podmiotach, o których mowa w ust. 1, podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, wdrożenie systemu ostrzegania może nastąpić za zgodą Ministra Obrony Narodowej.

6. Koszty wdrożenia i utrzymania systemu ostrzegania w podmiotach, o których mowa w ust. 1, pokrywa ABW.

7. ABW, w drodze porozumienia uzgadnia z podmiotem, o którym mowa w ust. 1, techniczne aspekty uczestnictwa w systemie ostrzegania oraz model konfiguracji systemu.

8. W sytuacji braku możliwości zawarcia porozumienia, o którym mowa w ust. 7, z przyczyn leżących po stronie podmiotu, o którym mowa w ust. 1, ABW informuje podmiot go nadzorujący lub ministra właściwego do spraw informatyzacji.

9. Prezes Rady Ministrów określi, w drodze rozporządzenia, warunki i tryb prowadzenia, koordynacji i wdrażania systemu ostrzegania, w szczególności określi czynności niezbędne do jego uruchomienia i utrzymania oraz wzór porozumienia, o którym mowa w ust. 7, kierując się potrzebą zapewnienia bezpieczeństwa systemów teleinformatycznych istotnych z punktu widzenia ciągłości funkcjonowania państwa.>

USTAWA z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2017 r. poz. 1579 i 2018)

Art. 89.

1. Zamawiający odrzuca ofertę, jeżeli:

1) jest niezgodna z ustawą;

---

2) jej treść nie odpowiada treści specyfikacji istotnych warunków zamówienia, z zastrzeżeniem art. 87 ust. 2 pkt 3;
3) jej złożenie stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji;
4) zawiera rażąco niską cenę lub koszt w stosunku do przedmiotu zamówienia;
5) została złożona przez wykonawcę wykluczonego z udziału w postępowaniu o udzielenie zamówienia lub niezaproszonego do składania ofert;
6) zawiera błędy w obliczeniu ceny lub kosztu;
7) wykonawca w terminie 3 dni od dnia doręczenia zawiadomienia nie zgodził się na poprawienie omyłki, o której mowa w art. 87 ust. 2 pkt 3;
7a) wykonawca nie wyraził zgody, o której mowa w art. 85 ust. 2, na przedłużenie terminu związania ofertą;
7b) wadium nie zostało wniesione lub zostało wniesione w sposób nieprawidłowy, jeżeli zamawiający żądał wniesienia wadium;
7c) oferta wariantowa nie spełnia minimalnych wymagań określonych przez zamawiającego;
[7d) jej przyjęcie naruszałoby bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, a tego bezpieczeństwa lub interesu nie można zagwarantować w inny sposób.]
<7d) jej przyjęcie naruszałoby bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, w tym bezpieczeństwo podmiotów objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o której mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2017 r. poz. 209 i 1566 oraz z 2018 r. poz. 1118), a tego bezpieczeństwa lub interesu nie można zagwarantować w inny sposób;>
8) jest nieważna na podstawie odrębnych przepisów.

2. (uchylony).

3. W postępowaniach o udzielenie zamówienia na dostawy lub usługi zamawiający nie może odrzucić oferty wariantowej tylko dlatego, że jej wybór prowadziłby do udzielenia zamówienia na usługi, a nie zamówienia na dostawy, albo do udzielenia zamówienia na dostawy, a nie zamówienia na usługi.

---

4. W przypadku gdy opis przedmiotu zamówienia odnosi się do norm, europejskich ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 30 ust. 1 pkt 2 oraz ust. 3, zamawiający nie może odrzucić oferty tylko dlatego, że roboty budowlane, dostawy lub usługi będące przedmiotem oferty nie są zgodne z normami, europejskimi ocenami technicznymi, specyfikacjami technicznymi i systemami referencji technicznych, do których się ona odnosi, jeżeli wykonawca udowodni w ofercie, w szczególności za pomocą środków, o których mowa w art. 30b ust. 1, że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia.
5. W przypadku gdy opis przedmiotu zamówienia odnosi się do wymagań dotyczących wydajności lub funkcjonalności, o których mowa w art. 30 ust. 1 pkt 1, zamawiający nie może odrzucić oferty zgodnej z Polską Normą przenoszącą normę europejską, normami innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszącymi normy europejskie, z europejską aprobatą techniczną, ze wspólną specyfikacją techniczną, z normą międzynarodową lub z systemem referencji technicznych ustanowionym przez europejski organ normalizacyjny, jeżeli te normy, aprobaty, specyfikacje i systemy referencji technicznych dotyczą wymagań dotyczących wydajności lub funkcjonalności określonych przez zamawiającego. W takim przypadku, wykonawca w ofercie musi udowodnić, w szczególności za pomocą środków, o których mowa w art. 30b ust. 1, że obiekt budowlany, dostawa lub usługa, spełniają wymagania dotyczące wydajności lub funkcjonalności określone przez zamawiającego.

USTAWA z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907 i 2201 oraz z 2018 r. poz. 106, 138, 650 i 1118)

Art. 175a.

1. Przedsiębiorcy telekomunikacyjni są obowiązani niezwłocznie informować Prezesa UKE o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na funkcjonowanie sieci lub usług, o podjętych działaniach zapobiegawczych i środkach naprawczych oraz podjętych przez przedsiębiorcę działaniach, o których mowa w art. 175 i art. 175c.

<1a. Prezes UKE przekazuje informacje, o których mowa w ust. 1, jeżeli dotyczą one zdarzeń będących incydentami w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …), CSIRT właściwemu dla zgłaszającego przedsiębiorcy telekomunikacyjnego, zgodnie z art. 26 ust. 5–7 tej ustawy, z wyłączeniem informacji stanowiących tajemnicę przedsiębiorstwa, zastrzeżonych na podstawie art. 9.

1b. Przekazanie, o którym mowa w ust. 1a, następuje w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji.>

2. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, wzór formularza do przekazywania informacji, o których mowa w ust. 1, kierując się koniecznością zapewnienia Prezesowi UKE informacji niezbędnych do właściwego realizowania jego obowiązków.

<2a. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, kryteria uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług, biorąc pod uwagę w szczególności wartość procentową użytkowników, na których naruszenie bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych miało wpływ, czas trwania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych powodującego niedostępność lub ograniczenie dostępności sieci lub usług telekomunikacyjnych oraz rekomendacje i wytyczne Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji (ENISA).>

Art. 176a.

1. Przedsiębiorca telekomunikacyjny, w celu zapewnienia ciągłości świadczenia usług telekomunikacyjnych lub dostarczania sieci telekomunikacyjnej, jest obowiązany uwzględniać możliwość wystąpienia:
   1) sytuacji kryzysowych,
   2) stanów nadzwyczajnych,
   [3) bezpośrednich zagrożeń dla infrastruktury przedsiębiorcy]
   <3) bezpośrednich zagrożeń dla bezpieczeństwa lub integralności infrastruktury telekomunikacyjnej przedsiębiorcy lub świadczonych przez niego usług>
   - zwanych dalej "sytuacjami szczególnych zagrożeń".

2. Przedsiębiorca telekomunikacyjny, z zastrzeżeniem ust. 5 pkt 2, jest obowiązany posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń, zwane dalej "planami", dotyczące w szczególności:
   1) współpracy z innymi przedsiębiorcami telekomunikacyjnymi;
   2) współpracy z zagranicznymi operatorami telekomunikacyjnymi, a w szczególności państw sąsiadujących;
   3) współpracy z podmiotami i służbami wykonującymi zadania w zakresie ratownictwa, niesienia pomocy ludności, a także zadania na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego oraz z podmiotami właściwymi w sprawach zarządzania kryzysowego, wskazanymi w ramach uzgodnień planów, o których mowa w ust. 3, przez organy uzgadniające plany;
   [4) zabezpieczenia infrastruktury telekomunikacyjnej w sytuacjach szczególnych zagrożeń oraz przed nieuprawnionym dostępem;]
   <4) technicznych i organizacyjnych środków zapewnienia bezpieczeństwa i integralności infrastruktury telekomunikacyjnej i świadczonych usług, w tym ochrony przed wystąpieniem incydentów w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;>
   5) utrzymania ciągłości, a w przypadku jej utraty, odtwarzania:
      a) świadczenia usług telekomunikacyjnych,
      b) dostarczania sieci telekomunikacyjnej
      - z uwzględnieniem pierwszeństwa dla podmiotów i służb, o których mowa w pkt 3;
   6) technicznych i organizacyjnych przygotowań, w przypadku wprowadzenia ograniczeń w działalności telekomunikacyjnej przewidzianych ustawą;
   7) sposobu udostępniania urządzeń telekomunikacyjnych, o którym mowa w art. 177 ust. 3, przez przedsiębiorców telekomunikacyjnych;
   8) ewidencji i gromadzenia rezerw przedsiębiorcy lub współpracy z dostawcami sprzętu oraz usług serwisowych i naprawczych.
3. Z zastrzeżeniem ust. 5 pkt 1 lit. c, przedsiębiorca telekomunikacyjny sporządzający plany dokonuje uzgodnienia ich zawartości z organami, o których mowa w ust. 5 pkt 1 lit. b.
4. Po stwierdzeniu wystąpienia sytuacji szczególnych zagrożeń lub po uzyskaniu informacji o ich wystąpieniu od podmiotów lub służb, o których mowa w ust. 2 pkt 3, przedsiębiorca telekomunikacyjny podejmuje niezwłocznie działania określone w planach.

---

5. Rada Ministrów, mając na uwadze zakres i rodzaj wykonywanej działalności telekomunikacyjnej, wielkość przedsiębiorcy telekomunikacyjnego i jego znaczenie dla gospodarki, obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, a także wymagania, o których mowa w ust. 2, w drodze rozporządzenia:
   1) określi:
      a) rodzaje planów, ich zawartość oraz tryb sporządzania i aktualizacji,
      b) organy uzgadniające plany oraz zakres tych uzgodnień,
      c) rodzaje przedsiębiorców telekomunikacyjnych obowiązanych do uzgadniania zawartości planów;
   2) może określić rodzaje działalności telekomunikacyjnej lub rodzaje przedsiębiorców telekomunikacyjnych niepodlegających obowiązkowi sporządzania planu.

Art. 209.

1. Kto:
   1) nie wypełnia obowiązku udzielania informacji lub dostarczania dokumentów przewidzianych ustawą lub ustawą z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych lub udziela informacji niepełnych lub nieprawdziwych lub dostarcza dokumenty zawierające informacje niepełne lub nieprawdziwe,
   2) wykonuje działalność telekomunikacyjną w zakresie nieobjętym wnioskiem o wpis do rejestru,
   3) (uchylony),
   4) narusza obowiązki informacyjne w stosunku do użytkowników końcowych,
   5) nie wypełnia obowiązków lub wymagań dotyczących ofert określających ramowe warunki umów o dostępie,
   6) nie wypełnia warunków zapewnienia dostępu telekomunikacyjnego oraz rozliczeń z tego tytułu, określonych w decyzji lub w umowie,
   7) nie wykonuje obowiązku świadczenia usługi powszechnej,
   8) (uchylony),
   9) wykorzystuje częstotliwości, numerację lub zasoby orbitalne, nie posiadając do tego uprawnień lub niezgodnie z tymi uprawnieniami,
   9a) używa urządzenia radiowego bez wymaganego wpisu do rejestru urządzeń, o którym mowa w art. 144c ust. 1 albo decyzji, o której mowa w art. 144a lub art. 144b,

9b) nie wykorzystuje, z przyczyn leżących po jego stronie, częstotliwości przyznanych w rezerwacji częstotliwości przez co najmniej 6 miesięcy,

10) nie wypełnia lub nienależycie wypełnia obowiązki lub zadania na rzecz obronności i bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie i na warunkach określonych w ustawie lub decyzjach wydanych na jej podstawie,

11) wprowadza do obrotu lub oddaje do użytku urządzenie radiowe bez wymaganego oznakowania znakiem ostrzegawczym lub nie podaje informacji, o których mowa w art. 154 ust. 1a,

12) nie wypełnia obowiązków lub wymagań dotyczących zapewnienia dostępu telekomunikacyjnego, o których mowa w art. 32,

12a) nie wypełnia lub nienależycie wypełnia szczegółowe warunki regulacyjne zatwierdzone decyzją, o której mowa w art. 43a,

13) nie wypełnia obowiązków regulacyjnych nałożonych na rynkach detalicznych, o których mowa w art. 46-48,

13a) nie wypełnia lub nienależycie wypełnia obowiązki określone w art. 36, art. 56, art. 57 ust. 6, art. 59, art. 60, art. 60a ust. 1, 1b i 4-5 oraz art. 61 ust. 4-6 i 7,

13b) nie wypełnia lub nienależycie wypełnia obowiązki określone w art. 44b-44g,

14) nie wypełnia wymagań dotyczących ustalania cen, o których mowa w art. 61 ust. 2,

14a) nie wypełnia lub nienależycie wypełnia obowiązki określone w art. 64, art. 64a i art. 65,

14b) nie wykonuje w terminie obowiązku określonego w decyzji, o której mowa w art. 62a ust. 5,

15) uniemożliwia abonentom korzystanie z uprawnienia do zmiany przydzielonego numeru, o którym mowa w art. 69,

16) uniemożliwia korzystanie z uprawnień do przeniesienia przydzielonego numeru, o których mowa w art. 70 i art. 71,

17) uniemożliwia abonentom korzystanie z uprawnienia do wyboru dostawcy usług, o którym mowa w art. 72,

18) (uchylony),

18a) nie wypełnia obowiązku, o którym mowa w art. 78 ust. 1, 2 i 5,

19) wykorzystuje numerację niezgodnie z przeznaczeniem, o którym mowa w art. 126,

19a) nie wypełnia nałożonych na niego obowiązków operatora multipleksu, o których mowa w art. 131a,

20) nie wykonuje obowiązków związanych z udostępnianiem lub prowadzeniem oddzielnej rachunkowości, o których mowa w art. 133,

21) nie realizuje obowiązku zapewnienia dostępu do interfejsu programu aplikacyjnego lub elektronicznego przewodnika po programach, o którym mowa w art. 136,

22) nie wypełnia obowiązków lub nie stosuje warunków udostępnienia nieruchomości lub infrastruktury telekomunikacyjnej określonych w decyzji lub w umowie, o których mowa w art. 139,

22a) nie wypełnia warunków współkorzystania i dostępu do infrastruktury technicznej oraz rozliczeń z tego tytułu, określonych w decyzji lub w umowie, zgodnie z ustawą z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych,

22b) nie wypełnia warunków wynikających z decyzji wydawanych w trybie art. 30 ust. 1 i 3 ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych,

23) (uchylony),

24) narusza obowiązek zachowania tajemnicy telekomunikacyjnej, o którym mowa w art. 159,

25) nie wypełnia obowiązków uzyskania zgody abonenta lub użytkownika końcowego, o których mowa w art. 161, art. 166, art. 169 i art. 172-174,

25a) będąc przedsiębiorcą telekomunikacyjnym nie publikuje na swojej stronie internetowej informacji, o których mowa w art. 175e,

26) przetwarza dane objęte tajemnicą telekomunikacyjną, dane abonentów lub dane użytkowników końcowych w zakresie niezgodnym z art. 165,

27) niezgodnie z przepisami art. 173 przechowuje informacje w urządzeniach końcowych abonenta lub użytkownika końcowego lub korzysta z informacji zgromadzonych w tych urządzeniach,

<27¹) nie wypełnia obowiązku, o którym mowa w art. 175a ust. 1,>

27a) nie stosuje się do zakazu określonego w decyzji, o której mowa w art. 175c ust. 3,

28) (uchylony),

29) nie wypełnia obowiązków określonych w art. 3-5 oraz art. 6a-6f, art. 7, art. 9, art. 11, art. 12, art. 14 oraz art. 15 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 531/2012 z dnia 13 czerwca 2012 r. w sprawie roamingu w publicznych sieciach łączności ruchomej wewnątrz Unii,

---

29a) nie wypełnia obowiązków określonych w art. 3, art. 4 i art. 5 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2015/2120 z dnia 25 listopada 2015 r. ustanawiającego środki dotyczące dostępu do otwartego internetu oraz zmieniającego dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, a także rozporządzenie (UE) nr 531/2012 w sprawie roamingu w publicznych sieciach łączności ruchomej wewnątrz Unii,

30) nie wypełnia lub nienależycie wypełnia obowiązki regulacyjne związane z prowadzeniem rachunkowości regulacyjnej lub kalkulacji kosztów,

31) nie wypełnia lub nienależycie wypełnia obowiązki opracowania i przedłożenia do zatwierdzenia przez Prezesa UKE oraz stosowania oferty ramowej o dostępie telekomunikacyjnym,

32) utrudnia lub uniemożliwia wykonywanie czynności kontrolnych przez Prezesa UKE

- podlega karze pieniężnej.

1a. Kara, o której mowa w ust. 1, może zostać nałożona także w przypadku, gdy podmiot zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę, jeżeli Prezes UKE uzna, że przemawiają za tym czas trwania, zakres lub skutki naruszenia.

2. Niezależnie od kary pieniężnej, o której mowa w ust. 1, Prezes UKE może nałożyć na kierującego przedsiębiorstwem telekomunikacyjnym, w szczególności osobę pełniącą funkcję kierowniczą lub wchodzącą w skład organu zarządzającego przedsiębiorcy telekomunikacyjnego lub związku takich przedsiębiorców, karę pieniężną w wysokości do 300% jego miesięcznego wynagrodzenia, naliczanego jak dla celów ekwiwalentu za urlop wypoczynkowy.

3. Kary pieniężne podlegają egzekucji w trybie przepisów o postępowaniu egzekucyjnym w administracji w zakresie egzekucji obowiązków o charakterze pieniężnym.

USTAWA z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 i 1566 oraz z 2018 r. poz. 1118)

Art. 5a.

1. Na potrzeby Krajowego Planu Zarządzania Kryzysowego, ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie sporządzają Raport o zagrożeniach bezpieczeństwa narodowego, zwany dalej "Raportem".

[2. Koordynację przygotowania Raportu zapewnia dyrektor Rządowego Centrum Bezpieczeństwa, a w części dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej, Szef Agencji Bezpieczeństwa Wewnętrznego.]

<2. Koordynację przygotowania Raportu zapewnia dyrektor Rządowego Centrum Bezpieczeństwa, natomiast w części dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej, Szef Agencji Bezpieczeństwa Wewnętrznego, a w części dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej – Pełnomocnik Rządu do spraw Cyberbezpieczeństwa.>

3. Raport jest dokumentem zawierającym następujące elementy:
   1) wskazanie najważniejszych zagrożeń przez stworzenie mapy ryzyka;
   2) określenie celów strategicznych;
   3) określenie priorytetów w reagowaniu na określone zagrożenia;
   4) wskazanie sił i środków niezbędnych do osiągnięcia celów strategicznych;
   5) programowanie zadań w zakresie poprawy bezpieczeństwa przez uwzględnianie regionalnych i lokalnych inicjatyw;
   6) wnioski zawierające hierarchicznie uporządkowaną listę przedsięwzięć niezbędnych do osiągnięcia celów strategicznych.
4. Raport przyjmuje Rada Ministrów w drodze uchwały.
5. Kierunki działania wynikające z wniosków z Raportu stanowią element Krajowego Planu Zarządzania Kryzysowego oraz są uwzględniane w planach zarządzania kryzysowego.
6. Rada Ministrów określi, w drodze rozporządzenia, sposób, tryb i terminy opracowywania Raportu, biorąc pod uwagę konieczność zapewnienia odpowiedniego poziomu bezpieczeństwa narodowego.

Art. 6.

1. Zadania z zakresu ochrony infrastruktury krytycznej obejmują:
   1) gromadzenie i przetwarzanie informacji dotyczących zagrożeń infrastruktury krytycznej;
   2) (uchylony);
   3) opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej;
   4) odtwarzanie infrastruktury krytycznej;

5) współpracę między administracją publiczną a właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej w zakresie jej ochrony.

2. (uchylony).

3. (uchylony).

4. (uchylony).

5. Właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej mają obowiązek ich ochrony, w szczególności przez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury, do czasu jej pełnego odtworzenia.

5a. Właściciele, posiadacze samoistni i zależni, o których mowa w ust. 5, mają obowiązek wyznaczyć, w terminie 30 dni od dnia otrzymania informacji, o której mowa w art. 5b ust. 7 pkt 4, osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej.

<5b. Właściciele, posiadacze samoistni i zależni, o których mowa w ust. 5, będący jednocześnie operatorami usług kluczowych w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …), uwzględniają w planach ochrony infrastruktury krytycznej dokumentację dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych zgodnie z zakresem informacji określonym w przepisach wydanych na podstawie art. 10 ust. 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.>

6. Jeżeli dla obiektów, instalacji, urządzeń i usług infrastruktury krytycznej istnieją, tworzone na podstawie innych przepisów, plany odpowiadające wymogom planu ochrony infrastruktury krytycznej, uznaje się, iż wymóg posiadania takiego planu jest spełniony.

7. Rada Ministrów określi, w drodze rozporządzenia:

1) sposób tworzenia, aktualizacji oraz strukturę planów, o których mowa w ust. 5,

2) warunki i tryb uznania spełnienia obowiązku posiadania planu odpowiadającego wymogom planu ochrony infrastruktury krytycznej

- uwzględniając potrzebę zapewnienia ciągłości funkcjonowania infrastruktury krytycznej.

Art. 8.

1. Przy Radzie Ministrów tworzy się Rządowy Zespół Zarządzania Kryzysowego, zwany dalej "Zespołem", jako organ opiniodawczo-doradczy właściwy w sprawach inicjowania i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego.
2. W skład Zespołu wchodzą:
   1) Prezes Rady Ministrów - przewodniczący;
   2) Minister Obrony Narodowej i minister właściwy do spraw wewnętrznych - zastępcy przewodniczącego;
   2a) minister właściwy do spraw administracji publicznej;
   3) Minister Spraw Zagranicznych;
   4) Minister Koordynator Służb Specjalnych - jeżeli został powołany.
3. W posiedzeniach Zespołu, na prawach członka, biorą udział wyznaczone przez przewodniczącego, w zależności od potrzeb, następujące organy administracji rządowej:
   1) ministrowie kierujący działami administracji rządowej:
      a) (uchylona),
      b) budownictwo, planowanie i zagospodarowanie przestrzenne oraz mieszkalnictwo,
      c) finanse publiczne,
      d) gospodarka,
      e) gospodarka morska,
      f) gospodarka wodna,
      g) instytucje finansowe,
      h) informatyzacja,
      i) kultura i ochrona dziedzictwa narodowego,
      j) łączność,
      k) oświata i wychowanie,
      l) rolnictwo,
      m) sprawiedliwość,
      n) środowisko,
      o) transport,
      p) zdrowie,
      q) praca,
      r) zabezpieczenie społeczne,
      s) (uchylona),

t) energia,

u) gospodarka złożami kopalin,

v) żegluga śródlądowa;

2) Główny Geodeta Kraju;

2a) Główny Inspektor Ochrony Środowiska;

3) Główny Inspektor Sanitarny;

4) Główny Lekarz Weterynarii;

5) Komendant Główny Państwowej Straży Pożarnej;

6) Komendant Główny Policji;

7) Komendant Główny Straży Granicznej;

7a) [(1)] (uchylony);

8) Prezes Państwowej Agencji Atomistyki;

9) Prezes Urzędu Lotnictwa Cywilnego;

10) Szef Agencji Bezpieczeństwa Wewnętrznego;

11) Szef Agencji Wywiadu;

12) Szef Obrony Cywilnej Kraju;

13) Szef Służby Kontrwywiadu Wojskowego;

14) Szef Służby Wywiadu Wojskowego *[.]* **<;>**

<15) Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa.>

4. Prezydent Rzeczypospolitej Polskiej może skierować do prac Zespołu, na prawach członka, Szefa Biura Bezpieczeństwa Narodowego lub innego przedstawiciela.

5. Przewodniczący może zapraszać do udziału w posiedzeniach Zespołu, na prawach członka, inne osoby.

6. W przypadku nieobecności przewodniczącego, pracami Zespołu kieruje wyznaczony przez niego zastępca albo członek Zespołu, w którego właściwości - wynikającej z kierowania danym działem administracji rządowej - pozostaje rodzaj zaistniałej sytuacji kryzysowej.

7. Członkowie Zespołu mogą wyznaczać do udziału w jego pracach swoich przedstawicieli:

1) Prezes Rady Ministrów - wiceprezesa Rady Ministrów;

2) ministrowie - sekretarza lub podsekretarza stanu;

3) organy, o których mowa w ust. 3 pkt 2-14 - swojego zastępcę.

8. (uchylony).

Art. 11.

1. Centrum zapewnia obsługę Rady Ministrów, Prezesa Rady Ministrów, Zespołu i ministra właściwego do spraw wewnętrznych w sprawach zarządzania kryzysowego oraz pełni funkcję krajowego centrum zarządzania kryzysowego.

<1a. Centrum zapewnia obsługę Zespołu do spraw Incydentów Krytycznych, o którym mowa w art. 36 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.>

2. Do zadań Centrum należy:

1) planowanie cywilne, w tym:
   a) przedstawianie szczegółowych sposobów i środków reagowania na zagrożenia oraz ograniczania ich skutków,
   b) opracowywanie i aktualizowanie Krajowego Planu Zarządzania Kryzysowego, we współpracy z właściwymi komórkami organizacyjnymi urzędów obsługujących ministrów oraz kierowników urzędów centralnych,
   c) analiza i ocena możliwości wystąpienia zagrożeń lub ich rozwoju,
   d) gromadzenie informacji o zagrożeniach i analiza zebranych materiałów,
   e) wypracowywanie wniosków i propozycji zapobiegania i przeciwdziałania zagrożeniom,
   f) planowanie wykorzystania Sił Zbrojnych Rzeczypospolitej Polskiej do wykonywania zadań, o których mowa w art. 25 ust. 3,
   g) planowanie wsparcia przez organy administracji publicznej realizacji zadań Sił Zbrojnych Rzeczypospolitej Polskiej;
2) monitorowanie potencjalnych zagrożeń;
2a) uzgadnianie planów zarządzania kryzysowego sporządzanych przez ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych;
3) przygotowanie uruchamiania, w przypadku zaistnienia zagrożeń, procedur związanych z zarządzaniem kryzysowym;
4) przygotowywanie projektów opinii i stanowisk Zespołu;
5) przygotowywanie i obsługa techniczno-organizacyjna prac Zespołu;
5a) zapewnienie koordynacji polityki informacyjnej organów administracji publicznej w czasie sytuacji kryzysowej;
6) współdziałanie z podmiotami, komórkami i jednostkami organizacyjnymi Organizacji Traktatu Północnoatlantyckiego i Unii Europejskiej oraz innych organizacji

międzynarodowych, odpowiedzialnymi za zarządzanie kryzysowe i ochronę infrastruktury krytycznej;

7) organizowanie, prowadzenie i koordynacja szkoleń i ćwiczeń z zakresu zarządzania kryzysowego oraz udział w ćwiczeniach krajowych i międzynarodowych;

8) zapewnienie obiegu informacji między krajowymi i zagranicznymi organami i strukturami zarządzania kryzysowego;

9) realizacja zadań stałego dyżuru w ramach gotowości obronnej państwa;

10) realizacja zadań z zakresu zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym;

10a) współdziałanie z Szefem Agencji Bezpieczeństwa Wewnętrznego w zakresie zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym;

11) realizacja zadań planistycznych i programowych z zakresu ochrony infrastruktury krytycznej oraz europejskiej infrastruktury krytycznej, w tym opracowywanie i aktualizacja załącznika funkcjonalnego do Krajowego Planu Zarządzania Kryzysowego dotyczącego ochrony infrastruktury krytycznej, a także współpraca, jako krajowy punkt kontaktowy, z instytucjami Unii Europejskiej i Organizacji Traktatu Północnoatlantyckiego oraz ich krajami członkowskimi w zakresie ochrony infrastruktury krytycznej;

12) (uchylony);

13) przygotowanie projektu zarządzenia Prezesa Rady Ministrów, o którym mowa w art. 7 ust. 4;

14) informowanie, zgodnie z właściwością, podmiotów, o których mowa w art. 8 ust. 2 i 3, o potencjalnych zagrożeniach oraz działaniach podjętych przez właściwe organy;

15) współdziałanie z centrami zarządzania kryzysowego organów administracji publicznej.

2a. Koszty związane z funkcjonowaniem Centrum są pokrywane z budżetu państwa z części, której dysponentem jest minister właściwy do spraw wewnętrznych.

3. Rada Ministrów lub Prezes Rady Ministrów mogą zlecić Centrum dodatkowe zadania związane z zarządzaniem kryzysowym.