M A T E R I A Ł P O R Ó W N A W C Z Y

do ustawy z dnia 16 czerwca 2023 r.

o zwalczaniu nadużyć w komunikacji elektronicznej

(druk nr 1011)

U S T A W A z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2022 r. poz. 1648, 1933 i 2581)

Art. 192.

1. Do zakresu działania Prezesa UKE należy w szczególności:

1) wykonywanie, przewidzianych ustawą i przepisami wydanymi na jej podstawie, zadań z zakresu regulacji i kontroli rynków usług telekomunikacyjnych, gospodarki w zakresie zasobów częstotliwości, zasobów orbitalnych i zasobów numeracji oraz kontroli spełniania wymagań dotyczących kompatybilności elektromagnetycznej;

2) wykonywanie zadań:

a) z zakresu regulacji działalności pocztowej, określonych w ustawie z dnia 23 listopada 2012 r. - Prawo pocztowe (Dz. U. z 2022 r. poz. 896),

b) określonych w ustawie:

– z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych,

– z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2021 r. poz. 1376 i 1595 oraz z 2022 r. poz. 32, 655 i 1261),

– z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym (Dz. U. z 2022 r. poz. 503),

– z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami (Dz. U. z 2021 r. poz. 1899)*[;]* **<,>**

<– z dnia 16 czerwca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. poz. ...);>

3) opracowywanie wskazanych przez ministra właściwego do spraw informatyzacji projektów aktów prawnych w zakresie telekomunikacji oraz wskazanych przez ministra właściwego do spraw łączności projektów aktów prawnych w zakresie poczty;

3a) wykonywanie zadań wynikających z przepisów rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1211/2009 z dnia 25 listopada 2009 r. ustanawiającego Organ Europejskich Regulatorów Łączności Elektronicznej (BEREC) oraz Urząd (Dz. Urz. UE L 337 z 18.12.2009, str. 1);

4) analiza i ocena funkcjonowania rynków usług telekomunikacyjnych i pocztowych;

5) podejmowanie interwencji w sprawach dotyczących funkcjonowania rynku usług telekomunikacyjnych i pocztowych oraz rynku aparatury, w tym rynku urządzeń telekomunikacyjnych, z własnej inicjatywy lub wniesionych przez zainteresowane podmioty, w szczególności użytkowników i przedsiębiorców telekomunikacyjnych, w tym podejmowanie decyzji w tych sprawach w zakresie określonym niniejszą ustawą;

5a) kontrolowanie realizacji obowiązków wynikających z przepisów 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 (Dz. Urz. UE L 172 z 30.06.2012, str. 10);

5aa) realizacja obowiązków nałożonych na krajowy organ regulacyjny i kontrolowanie realizacji pozostałych obowiązków, wynikających z przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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 (Dz. Urz. UE L 310 z 26.11.2015, s. 1);

5b) wykonywanie kontroli nad operatorami publicznej sieci telekomunikacyjnej i dostawcami publicznie dostępnych usług telekomunikacyjnych w zakresie realizacji obowiązków, o których mowa w art. 180a ust. 1, z wyjątkiem realizacji obowiązków dotyczących danych osobowych chronionych zgodnie z przepisami o ochronie danych osobowych;

5c) prowadzenie baz danych, o których mowa w art. 71 ust. 4 oraz w art. 180f ust. 2;

6) rozstrzyganie sporów między przedsiębiorcami telekomunikacyjnymi w zakresie właściwości Prezesa UKE;

6a) rozstrzyganie sporów między operatorem multipleksu a nadawcą, o których mowa w art. 131a-131f, oraz sporów, o których mowa w art. 136a;

7) rozstrzyganie w sprawach uprawnień zawodowych w dziedzinie telekomunikacji, określonych w przepisach odrębnych;

8) tworzenie warunków dla rozwoju krajowych służb radiokomunikacyjnych przez zapewnianie Rzeczypospolitej Polskiej niezbędnych przydziałów częstotliwości oraz dostępu do zasobów orbitalnych;

8a) realizacja harmonogramu rozdysponowania zasobów częstotliwości, o którym mowa w art. 111 ust. 4;

9) wykonywanie obowiązków na rzecz obronności, bezpieczeństwa państwa i porządku publicznego;

10) prowadzenie rejestrów w zakresie ujętym w ustawie;

11) koordynacja rezerwacji częstotliwości w zakresach częstotliwości przeznaczonych dla podmiotów, o których mowa w art. 4, w szczególności w zakresach częstotliwości przez nich zwalnianych lub dla nich nowo udostępnianych albo współwykorzystywanych z innymi użytkownikami;

12) (uchylony);

13) współpraca z krajowymi i międzynarodowymi organizacjami telekomunikacyjnymi i pocztowymi oraz właściwymi organami innych państw, w zakresie jego właściwości;

14) współpraca z Prezesem UOKiK w sprawach dotyczących przestrzegania praw podmiotów korzystających z usług pocztowych i telekomunikacyjnych, przeciwdziałania praktykom ograniczającym konkurencję oraz antykonkurencyjnym koncentracjom operatorów pocztowych, przedsiębiorców telekomunikacyjnych i ich związków;

15) współpraca z Krajową Radą Radiofonii i Telewizji w zakresie określonym ustawą i przepisami odrębnymi;

16) wykonywanie zadań w sprawach międzynarodowej i wspólnotowej polityki telekomunikacyjnej z upoważnienia ministra właściwego do spraw informatyzacji;

16a) prowadzenie transgranicznych koordynacji częstotliwości z innymi państwami, w tym zawieranie niezbędnych umów lub porozumień, w sposób i w terminach pozwalających na realizację zobowiązań wynikających z wiążących Rzeczpospolitą Polską umów międzynarodowych lub aktów prawnych Unii Europejskiej, dotyczących gospodarowania częstotliwościami;

17) współpraca z Komisją Europejską i instytucjami Unii Europejskiej, a także z BEREC oraz organami regulacyjnymi innych państw członkowskich;

18) przedstawianie Komisji Europejskiej, BEREC i organom regulacyjnym innych państw członkowskich informacji z zakresu telekomunikacji, w tym wykonywanie obowiązków notyfikacyjnych, obejmujących przekazywanie treści rozstrzygnięć, o których mowa w

art. 23 ust. 1, oraz informacje o przedsiębiorcach telekomunikacyjnych, którzy zostali uznani za posiadających znaczącą pozycję rynkową, świadczących usługę powszechną i realizujących połączenia sieci telekomunikacyjnych oraz nałożonych na nich obowiązkach;

19) przeprowadzanie konsultacji środowiskowych z zainteresowanymi podmiotami, w szczególności z operatorami, dostawcami usług, użytkownikami, konsumentami oraz producentami, w sprawach związanych z zasięgiem, dostępnością oraz jakością usług telekomunikacyjnych;

20) przedstawianie Komisji Europejskiej informacji z zakresu poczty, w tym:

a) o nazwie i adresie operatora wyznaczonego świadczącego usługi powszechne,

b) o sposobie udostępniania korzystającym z usług powszechnych szczegółowych i aktualnych informacji dotyczących charakteru oferowanych usług, warunków dostępu, cen i minimalnych wymagań w zakresie czasu przebiegu przesyłek pocztowych,

c) o przyjętych dla obrotu krajowego minimalnych wymaganiach dotyczących czasu przebiegu przesyłek pocztowych i przyznanym odstępstwie w tym zakresie,

d) o przyznanym odstępstwie od częstotliwości opróżniania nadawczych skrzynek pocztowych i doręczania przesyłek z jednoczesnym przekazaniem tej informacji pocztowym organom regulacyjnym państw członkowskich Unii Europejskiej,

e) danych statystycznych o krajowym rynku pocztowym oraz, na żądanie Komisji Europejskiej, informacji o systemie rachunku kosztów stosowanym przez operatora wyznaczonego;

21) kontrola obowiązku umieszczania oddawczych skrzynek pocztowych zgodnie z obowiązkiem wynikającym z ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe;

22) wykonywanie zadań wynikających z przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/644 z dnia 18 kwietnia 2018 r. w sprawie transgranicznych usług doręczania paczek (Dz. Urz. UE L 112 z 02.05.2018, str. 19).

1a. Prezes UKE, wykonując obowiązek, o którym mowa w ust. 1 pkt 21, ma prawo wstępu na teren nieruchomości, na których znajdują się oddawcze skrzynki pocztowe.

2. (uchylony).

3. Na podstawie informacji uzyskanych od przedsiębiorców telekomunikacyjnych oraz innych podmiotów dysponujących infrastrukturą telekomunikacyjną lub realizujących inwestycje w tym zakresie Prezes UKE, w terminie do dnia 30 czerwca, ogłasza raport o stanie rynku telekomunikacyjnego za rok ubiegły, uwzględniający pokrycie terytorium

Rzeczypospolitej Polskiej zasięgiem stacjonarnych i ruchomych publicznych sieci telekomunikacyjnych oraz przedstawia prognozy inwestycyjne dotyczące rozwoju tych sieci. Raport publikuje się na stronie podmiotowej BIP UKE.

4. Prezes UKE dokonuje, nie rzadziej niż co dwa lata, regularnego przeglądu konieczności stosowania w decyzjach w sprawie rezerwacji częstotliwości ograniczeń, o których mowa w art. 115 ust. 2 pkt 5, oraz publikuje jego wyniki na stronie podmiotowej BIP UKE.

U S T A W A z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2023 r. poz. 57)

Art. 4.

Przepisy ustawy nie naruszają:

1) przepisów o ochronie danych osobowych;

2) ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742);

<**2a) obowiązku korzystania przy realizacji zadań publicznych z poczty elektronicznej wykorzystującej mechanizmy, o których mowa w art. 22 ust. 1 ustawy z dnia 16 czerwca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. poz. ….);**>

3) obowiązków wynikających z potrzeby współpracy z systemami teleinformatycznymi i rejestrami organów innych państw lub organizacji międzynarodowych;

4) obowiązków wynikających z umów międzynarodowych, jak również umów o członkostwo w instytucjach międzynarodowych, w przypadku gdy prawo danego podmiotu do członkostwa w instytucjach międzynarodowych zostało zagwarantowane aktem prawnym o mocy ustawy.

U S T A W A 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913)

Art. 26.

1. CSIRT MON, CSIRT NASK i CSIRT GOV współpracują ze sobą, z organami właściwymi do spraw cyberbezpieczeństwa, ministrem właściwym do spraw informatyzacji oraz Pełnomocnikiem, zapewniając spójny i kompletny system zarządzania ryzykiem na poziomie krajowym, realizując zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewniając koordynację obsługi zgłoszonych incydentów.
2. CSIRT MON, CSIRT NASK i CSIRT GOV w uzasadnionych przypadkach na wniosek operatorów usług kluczowych, dostawców usług cyfrowych, podmiotów publicznych, o których mowa w art. 4 pkt 7-15, sektorowych zespołów cyberbezpieczeństwa lub właścicieli, posiadaczy samoistnych albo posiadaczy zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, mogą zapewnić wsparcie w obsłudze incydentów.
3. Do zadań CSIRT MON, CSIRT NASK i CSIRT GOV, zgodnie z właściwością wskazaną w ust. 5-7, należy:

1) monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym;
2) szacowanie ryzyka związanego z ujawnionym zagrożeniem cyberbezpieczeństwa oraz zaistniałymi incydentami, w tym prowadzenie dynamicznej analizy ryzyka;
3) przekazywanie informacji dotyczących incydentów i ryzyk podmiotom krajowego systemu cyberbezpieczeństwa;
4) wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa;
5) reagowanie na zgłoszone incydenty;
6) klasyfikowanie incydentów, w tym incydentów poważnych oraz incydentów istotnych, jako incydenty krytyczne oraz koordynowanie obsługi incydentów krytycznych;
7) zmiana klasyfikacji incydentów poważnych i incydentów istotnych;
8) przekazywanie do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV informacji technicznych dotyczących incydentu, którego koordynacja obsługi wymaga współpracy CSIRT;
9) przeprowadzanie w uzasadnionych przypadkach badania urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, której wykorzystanie może zagrozić w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, które może mieć wpływ na bezpieczeństwo publiczne lub istotny

interes bezpieczeństwa państwa, oraz składanie wniosków w sprawie rekomendacji dla podmiotów krajowego systemu cyberbezpieczeństwa dotyczących stosowania urządzeń informatycznych lub oprogramowania, w szczególności w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, zwanych dalej "rekomendacjami dotyczącymi stosowania urządzeń informatycznych lub oprogramowania";

10) współpraca z sektorowymi zespołami cyberbezpieczeństwa w zakresie koordynowania obsługi incydentów poważnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej, i incydentów krytycznych oraz w zakresie wymiany informacji pozwalających przeciwdziałać zagrożeniom cyberbezpieczeństwa;

11) przekazywanie do innych państw, w tym państw członkowskich Unii Europejskiej, i przyjmowanie z tych państw informacji o incydentach poważnych i incydentach istotnych dotyczących dwóch lub większej liczby państw członkowskich, a także przekazywanie do Pojedynczego Punktu Kontaktowego zgłoszenia incydentu poważnego i istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej;

12) przekazywanie, w terminie do dnia 30 maja każdego roku, do Pojedynczego Punktu Kontaktowego zestawienia zgłoszonych w poprzednim roku kalendarzowym przez operatorów usług kluczowych incydentów poważnych mających wpływ na ciągłość świadczenia przez nich usług kluczowych w Rzeczypospolitej Polskiej oraz ciągłość świadczenia przez nich usług kluczowych w państwach członkowskich Unii Europejskiej, a także zestawienia zgłoszonych w poprzednim roku kalendarzowym przez dostawców usług cyfrowych incydentów istotnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej;

13) wspólne opracowywanie i przekazywanie ministrowi właściwemu do spraw informatyzacji części Raportu o zagrożeniach bezpieczeństwa narodowego, o którym mowa w art. 5a ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, dotyczącej cyberbezpieczeństwa;

14) zapewnienie zaplecza analitycznego oraz badawczo-rozwojowego, które w szczególności:

a) prowadzi zaawansowane analizy złośliwego oprogramowania oraz analizy podatności,

b) monitoruje wskaźniki zagrożeń cyberbezpieczeństwa,

c) rozwija narzędzia i metody do wykrywania i zwalczania zagrożeń cyberbezpieczeństwa,

d) prowadzi analizy i opracowuje standardy, rekomendacje i dobre praktyki w zakresie cyberbezpieczeństwa,

e) wspiera podmioty krajowego systemu cyberbezpieczeństwa w budowaniu potencjału i zdolności w obszarze cyberbezpieczeństwa,

f) prowadzi działania z zakresu budowania świadomości w obszarze cyberbezpieczeństwa,

g) współpracuje w zakresie rozwiązań edukacyjnych w obszarze cyberbezpieczeństwa;

15) zapewnienie możliwości dokonywania zgłoszeń i przekazywania informacji, o których mowa w art. 11 ust. 1 pkt 4, art. 13 ust. 1, art. 18 ust. 1 pkt 4, art. 20, art. 22 ust. 1 pkt 2, art. 24 i art. 30 ust. 1, oraz udostępnienie i obsługa środków komunikacji pozwalających na dokonywanie tych zgłoszeń;

16) udział w Sieci CSIRT składającej się z przedstawicieli CSIRT państw członkowskich Unii Europejskiej, CSIRT właściwego dla instytucji Unii Europejskiej, Komisji Europejskiej oraz Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji (ENISA).

4. CSIRT MON, CSIRT NASK i CSIRT GOV wspólnie opracowują główne elementy procedur postępowania w przypadku incydentu, którego koordynacja obsługi wymaga współpracy CSIRT, oraz określą we współpracy z sektorowymi zespołami cyberbezpieczeństwa sposób współdziałania z tymi zespołami, w tym sposób koordynacji obsługi incydentu.

5. Do zadań CSIRT MON należy koordynacja obsługi incydentów zgłaszanych przez:

1) podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;

2) przedsiębiorcy realizujący zadania na rzecz Sił Zbrojnych, o których mowa w art. 648 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz. U. poz. 655).

6. Do zadań CSIRT NASK należy:

1) koordynacja obsługi incydentów zgłaszanych przez:

a) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 2-6, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,

b) jednostki podległe organom administracji rządowej lub przez nie nadzorowane, z wyjątkiem jednostek, o których mowa w ust. 7 pkt 2,

c) instytuty badawcze,

d) Urząd Dozoru Technicznego,

e) Polską Agencję Żeglugi Powietrznej,

f) Polskie Centrum Akredytacji,

g) Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej,

h) spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej,

i) dostawców usług cyfrowych, z wyjątkiem wymienionych w ust. 7 pkt 5,

j) operatorów usług kluczowych, z wyjątkiem wymienionych w ust. 5 i 7,

k) inne podmioty niż wymienione w lit. a-j oraz ust. 5 i 7,

l) osoby fizyczne;

2) tworzenie i udostępnianie narzędzi dobrowolnej współpracy i wymiany informacji o zagrożeniach cyberbezpieczeństwa i incydentach;

3) zapewnienie obsługi linii telefonicznej lub serwisu internetowego prowadzących działalność w zakresie zgłaszania i analizy przypadków dystrybucji, rozpowszechniania lub przesyłania pornografii dziecięcej za pośrednictwem technologii informacyjno-komunikacyjnych, o których mowa w dyrektywie Parlamentu Europejskiego i Rady 2011/92/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępującej decyzję ramową Rady 2004/68/WSiSW (Dz. Urz. UE L 335 z 17.12.2011, str. 1)*[.]* <**;**>

<**4) monitorowanie występowania smishingu oraz tworzenie wzorca wiadomości wyczerpującej znamiona smishingu, o którym mowa w art. 4 ustawy z dnia 16 czerwca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. poz. …);**

5) prowadzenie i udostępnianie na swojej stronie internetowej wykazu nazw oraz ich skrótów zastrzeżonych dla podmiotów publicznych jako nadpis wiadomości pochodzącej od podmiotu publicznego oraz wariantów tych nazw i skrótów, mogących wprowadzać odbiorcę w błąd co do pochodzenia wiadomości od podmiotu publicznego, o którym mowa w art. 9 ust. 1 ustawy z dnia 16 czerwca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej.>

7. Do zadań CSIRT GOV należy koordynacja obsługi incydentów zgłaszanych przez:

1) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1, 8 i 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, z wyjątkiem wymienionych w ust. 5 i 6;

2) jednostki podległe Prezesowi Rady Ministrów lub przez niego nadzorowane;

3) Narodowy Bank Polski;

4) Bank Gospodarstwa Krajowego;

5) inne niż wymienione w pkt 1-4 oraz ust. 5 podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;

6) podmioty, o których mowa w ust. 6, jeżeli incydent dotyczy systemów teleinformatycznych lub sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

8. CSIRT MON, CSIRT NASK lub CSIRT GOV, który otrzymał zgłoszenie incydentu, a nie jest właściwy do koordynacji jego obsługi, przekazuje niezwłocznie to zgłoszenie do właściwego CSIRT wraz z otrzymanymi informacjami.

9. Działalność CSIRT NASK jest finansowana w formie dotacji podmiotowej z części budżetu państwa, której dysponentem jest minister właściwy do spraw informatyzacji.

10. CSIRT MON, CSIRT NASK i CSIRT GOV mogą, w drodze porozumienia, powierzyć sobie wzajemnie wykonywanie zadań w stosunku do niektórych rodzajów podmiotów, o których mowa w ust. 5-7. O zawarciu porozumienia CSIRT, który powierzył wykonywanie zadań, informuje podmioty, w stosunku do których nastąpiła zmiana CSIRT.

11. Komunikat o zawarciu porozumienia, o którym mowa w ust. 10, ogłasza się w dzienniku urzędowym odpowiednio Ministra Obrony Narodowej, Ministra Cyfryzacji lub Agencji Bezpieczeństwa Wewnętrznego. W komunikacie wskazuje się informacje o:

1) adresie strony internetowej, na której zostanie zamieszczona treść porozumienia wraz ze stanowiącymi jego integralną treść załącznikami;

2) terminie, od którego porozumienie będzie obowiązywało.