Projekt z 15 czerwca 2022 r.

USTAWA

z dnia ………………………… 2022 r.

o zwalczaniu nadużyć w komunikacji elektronicznej[[1]](#footnote-2))

Art. 1. Ustawa określa:

1) prawa i obowiązki przedsiębiorców telekomunikacyjnych związane z zapobieganiem oraz zwalczaniem nadużyć w komunikacji elektronicznej;

2) zasady wnoszenia sprzeciwu przez nadawcę krótkiej wiadomości tekstowej (SMS), wobec uznania treści takiej wiadomości za wyczerpującą znamiona nadużycia w komunikacji elektronicznej;

3) obowiązki dostawcy poczty elektronicznej oraz podmiotu publicznego związane ze świadczeniem i korzystaniem z poczty elektronicznej w celu zapobiegania nadużyciom w komunikacji elektronicznej;

4) szczególne zasady przetwarzania informacji objętych tajemnicą telekomunikacyjną związane z zapobieganiem oraz zwalczaniem nadużyć w komunikacji elektronicznej.

**Art. 2.** Określenia użyte w ustawie oznaczają:

1) CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, o którym mowa w art. 2 pkt 3 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z 2021 r. poz. 2333 i 2445 oraz z 2022 r. poz. 655);

2) dostawca poczty elektronicznej – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która prowadząc, chociażby ubocznie, działalność zarobkową lub zawodową świadczy usługę poczty elektronicznej;

3) komunikat elektroniczny – każdą informację wymienianą lub przekazywaną między określonymi użytkownikami za pośrednictwem publicznie dostępnych usług telekomunikacyjnych lub usług komunikacji interpersonalnej niewykorzystujących numerów; nie obejmuje on informacji przekazanej jako część transmisji radiofonicznych lub telewizyjnych transmitowanych przez sieć telekomunikacyjną, z wyjątkiem informacji odnoszącej się do możliwego do zidentyfikowania użytkownika otrzymującego informację;

4) nadużycie w komunikacji elektronicznej – świadczenie usługi telekomunikacyjnej lub korzystanie z urządzeń telekomunikacyjnych niezgodnie z ich przeznaczeniem lub przepisami prawa, których celem lub skutkiem jest wyrządzenie szkody przedsiębiorcy telekomunikacyjnemu, użytkownikowi końcowemu lub osiągnięcie nienależnych korzyści;

5) operator – operatora, o którym mowa w art. 2 pkt 27 lit. b ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. 2021 r. poz. 576 oraz z 2022 r. poz. 501);

6) podmiot publiczny – podmiot, o którym mowa w art. 4 pkt 7–15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;

7) przedsiębiorca telekomunikacyjny – przedsiębiorcę, o którym mowa w art. 2 pkt 27 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;

8) poczta elektroniczna – usługę komunikacji interpersonalnej niewykorzystującą numerów, która umożliwia przekazywanie komunikatu elektronicznego z wykorzystaniem standardu SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol), lub IMAP4 (Internet Message Access Protocol);

9) połączenie głosowe – połączenie ustanowione za pomocą publicznie dostępnej usługi komunikacji interpersonalnej, pozwalające na dwukierunkową komunikację głosową;

10) sieć telekomunikacyjna – sieć o której mowa w art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;

11) tajemnica telekomunikacyjna – tajemnicę, o której mowa w art. 159 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;

12) usługa komunikacji interpersonalnej – usługę umożliwiającą bezpośrednią interpersonalną i interaktywną wymianę informacji za pośrednictwem sieci telekomunikacyjnej między skończoną liczbą osób, gdzie osoby inicjujące połączenie lub uczestniczące w nim decydują o jego odbiorcy lub odbiorcach, z wyłączeniem usług, w których interpersonalna i interaktywna komunikacja stanowi wyłącznie funkcję podrzędną względem innej usługi podstawowej;

13) usługa komunikacji interpersonalnej niewykorzystująca numerów – usługę komunikacji interpersonalnej, która nie umożliwia realizacji połączeń z numerami z planu numeracji krajowej lub międzynarodowych planów numeracji;

14) usługa telekomunikacyjna – usługę, o której mowa w art. 2 pkt 48 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;

15) użytkownik – podmiot, o którym mowa w art. 2 pkt 49 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;

16) użytkownik końcowy – podmiot, o którym mowa w art. 2 pkt 50 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

Art. 3. 1. Zakazane są nadużycia w komunikacji elektronicznej, w szczególności dotyczące:

1) inicjowania wysyłania lub odbierania komunikatów elektronicznych lub połączeń głosowych w sieci telekomunikacyjnej z wykorzystaniem urządzeń telekomunikacyjnych lub programów, których celem nie jest skorzystanie z usługi telekomunikacyjnej, lecz ich zarejestrowanie na punkcie połączenia sieci telekomunikacyjnych bądź przez systemy rozliczeniowe (sztuczny ruch);

2) wysyłania krótkich wiadomości tekstowych (SMS), w których nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem, przekierowania na stronę internetową, żądania kontaktu telefonicznego lub instalacji oprogramowania (smishing);

3) nieuprawnionego posłużenia się przez użytkownika wywołującego połączenie głosowe informacją adresową wskazującą na osobę lub jednostkę organizacyjną inną niż ten użytkownik, służące podszyciu się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem lub instalacji oprogramowania (CLI spoofing).

2. Przedsiębiorca telekomunikacyjny jest obowiązany do podejmowania proporcjonalnych środków technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie.

Art. 4. 1. CSIRT NASK na podstawie otrzymanych od odbiorców krótkich wiadomości tekstowych (SMS) monitoruje występowanie smishingu.

2. CSIRT NASK na podstawie monitorowania, o którym mowa w ust. 1, tworzy wzorzec wiadomości wyczerpującej znamiona smishingu.

3. CSIRT NASK przekazuje informację o wystąpieniu smishingu, za pomocą systemu teleinformatycznego, Komendantowi Głównemu Policji, Prezesowi Urzędu Komunikacji Elektronicznej, zwanego dalej „Prezesem UKE” i przedsiębiorcom telekomunikacyjnym, wraz ze wzorcem wiadomości wyczerpującej znamiona smishingu.

4. Wzorzec wiadomości, o którym mowa w ust. 2, CSIRT NASK udostępnia na swojej stronie internetowej, w terminie 14 dni nie później jednak niż w terminie 21 dni od dnia jego przekazania przedsiębiorcy telekomunikacyjnemu w sposób, o którym mowa w ust. 3.

5. CSIRT NASK, w przypadku gdy uzna, że treść zawarta we wzorcu wiadomości nie stanowi smishingu lub niecelowe jest dalsze blokowanie krótkich wiadomości tekstowych (SMS) zgodnie z wzorcem wiadomości niezwłocznie informuje o tym podmioty, o których mowa w ust. 3.

6. Przedsiębiorca telekomunikacyjny po otrzymaniu informacji, o której mowa w ust. 3 lub 5, jest obowiązany do:

1) niezwłocznego blokowania krótkich wiadomości tekstowych (SMS) zawierających treści zawarte we wzorcu wiadomości, za pomocą systemu teleinformatycznego pozwalającego na automatyczną identyfikację krótkich wiadomości tekstowych (SMS);

2) zaprzestania blokowania krótkich wiadomości tekstowych (SMS) w przypadku uzyskania informacji, że treść zawarta we wzorcu wiadomości nie nosi znamion smishingu lub niecelowe jest dalsze blokowanie krótkich wiadomości tekstowych (SMS) zawierających treści wskazane we wzorcu wiadomości.

**Art. 5.** 1. Nadawca krótkiej wiadomości tekstowej (SMS) może wnieść do Prezesa UKE sprzeciw wobec uznania treści takiej wiadomości za wyczerpującą znamiona smishingu.

2. Sprzeciw zawiera:

1) uzasadnienie wyjaśniające dlaczego treść krótkiej wiadomości tekstowej (SMS) nie wyczerpuje znamion smishingu;

2) wskazanie numeru wykorzystanego do nadania krótkiej wiadomości tekstowej (SMS).

3. Sprzeciw opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym i wnosi się do Prezesa UKE, za pomocą środków komunikacji elektronicznej.

4. Sprzeciw niespełniający wymagań, o których mowa w ust. 2 lub 3, pozostawia się bez rozpoznania.

**Art. 6.** 1. Prezes UKE:

1) rozpatruje sprzeciw, w terminie 14 dni od dnia jego otrzymania, oraz

2) niezwłocznie informuje nadawcę krótkiej wiadomości tekstowej (SMS) o sposobie rozpatrzenia sprzeciwu za pomocą środków komunikacji elektronicznej, których użył nadawca krótkiej wiadomości tekstowej (SMS) składając sprzeciw.

2. W przypadku uwzględnienia sprzeciwu przez Prezesa UKE, CSIRT NASK przekazuje informację o której mowa w art. 4 ust. 5, podmiotom, o których mowa w art. 4 ust. 3.

**Art. 7.** Przedsiębiorca telekomunikacyjny może blokować krótkie wiadomości tekstowe (SMS) zawierające treści wyczerpujące znamiona smishingu, inne niż zawarte we wzorcu wiadomości, o którym mowa w art. 4 ust. 3, za pomocą systemu teleinformatycznego pozwalającego na automatyczną identyfikację takich krótkich wiadomości tekstowych (SMS).

**Art. 8.** W celu zapobiegania i zwalczania CLI spoofing przedsiębiorca telekomunikacyjny blokuje połączenie głosowe albo ukrywa identyfikację numeru wywołującego dla użytkownika końcowego.

**Art. 9.** 1. Prezes UKE, prowadzi jawny wykaz numerów telefonów służących wyłącznie do odbierania połączeń głosowych, i udostępnia go w Biuletynie Informacji Publicznej na swojej stronie podmiotowej.

2. Prezes UKE dokonuje wpisu do wykazu, o którym mowa w ust. 1, na wniosek:

1) jednostki sektora finansów publicznych, o której mowa w art. 9 z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. 2021 r. poz. 305, z późn. zm.[[2]](#footnote-3))),

2) banku

– w zakresie wykorzystywanych przez te podmioty numerów.

3. Prezes UKE na wniosek przedsiębiorcy telekomunikacyjnego dokonuje wpisu do wykazu, o którym mowa w ust. 1, wyłącznie numerów wykorzystywanych przez przedsiębiorcę telekomunikacyjnego na potrzeby biura obsługi klientów lub infolinii.

4. Wniosek, o którym mowa w ust. 2 i 3, zawiera wskazanie podmiotu, od którego pochodzi oraz numeru, który ma służyć wyłącznie do odbierania połączeń głosowych.

5. W przypadku gdy wniosek, o którym mowa w ust. 2 i 3, nie zawiera informacji, o których mowa w ust. 4, Prezes UKE wzywa podmiot do ich uzupełnienia w terminie 7 dni od dnia otrzymania wezwania pod rygorem pozostawienia wniosku bez rozpoznania.

6. Prezes UKE dokonuje wpisu numeru do wykazu, o którym mowa w ust. 1, w terminie 5 dni od dnia otrzymania wniosku.

7. Wpis do wykazu, o którym mowa w ust. 1, jest czynnością materialno-techniczną.

8. Prezes UKE odmawia wpisu do wykazu, o którym mowa w ust. 1, w drodze decyzji, jeżeli wniosek został złożony przez podmiot nieuprawniony lub dotyczy on numeru niewykorzystywanego przez ten podmiot.

9. Podmiot, który złożył wniosek, o którym mowa w ust. 2 i 3, może w każdym czasie go wycofać. W takim przypadku Prezes UKE niezwłocznie, jednak nie później niż w terminie 5 dni od dnia złożenia wniosku o wycofanie numeru z wykazu, wykreśla numer z wykazu, o którym mowa w ust. 1.

10. Wniosek, którym mowa w ust. 2 i 3, oraz wniosek o wycofanie numeru z wykazu opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym i wnosi się do Prezesa UKE za pomocą środków komunikacji elektronicznej.

11. Wniosek niespełniający wymagań, o których mowa w ust. 10, pozostawia się bez rozpoznania.

12. Przedsiębiorca telekomunikacyjny świadczący usługę połączeń głosowych blokuje połączenia inicjowane z wykorzystaniem numeru wpisanego do wykazu.

**Art. 10.** 1. Operatorzy mogą zawrzeć z Prezesem UKE porozumienie określające środki organizacyjne i techniczne, które będą stosowali przy realizacji obowiązków, o których mowa w art. 8.

2. Zawarcie porozumienia i jego prawidłowe wykonywanie stanowi spełnienie przez strony porozumienia obowiązku podejmowania proporcjonalnych środków technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie w zakresie o którym mowa w art. 3 ust. 1 pkt 3.

3. Operator prawidłowo wykonujący porozumienie, o którym mowa w ust. 1, nie ponosi odpowiedzialności za niewykonanie lub nienależyte wykonanie usługi telekomunikacyjnej będącej skutkiem wprowadzonych środków technicznych i organizacyjnych, o których mowa w ust. 1.

4. Prezes UKE kontroluje prawidłowość stosowania środków organizacyjnych i technicznych określonych w porozumieniu, o którym mowa w ust. 2. Przepisy ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne dotyczące kontroli stosuje się.

**Art. 11.** 1. W celu ochrony użytkowników internetu przed stronami internetowymi wyłudzającymi dane, w tym dane osobowe oraz doprowadzającymi użytkowników internetu do niekorzystnego rozporządzenia ich majątkiem, może zostać zawarte porozumienie w zakresie prowadzenia i utrzymywania jawnej listy ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i środków finansowych użytkowników internetu oraz uniemożliwienia dostępu do tych stron.

2. W celu ochrony użytkowników internetu przed CLI spoofing,elementem porozumienia, o którym mowa w ust. 1, może być jawna lista ostrzeżeń dotyczących domen internetowych, które służą do nieuprawnionego wykorzystania numeru lub identyfikatora użytkownika wywołującego połączenie głosowe oraz uniemożliwienia dostępu do tych stron.

3. CSIRT NASK opracowuje, prowadzi i utrzymuje jawną listę ostrzeżeń dotyczącą domen internetowych, o których mowa w ust. 1 i 2. Lista ostrzeżeń jest udostępniana na stronie internetowej CSIRT NASK.

4. Stronami porozumienia są:

1) Prezes UKE;

2) minister właściwy do spraw informatyzacji;

3) Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy, oraz

4) przedsiębiorca telekomunikacyjny lub przedsiębiorcy telekomunikacyjni.

5. Porozumienie określa co najmniej zasady współpracy między stronami, w tym zasady zgłaszania domen internetowych, wpisania oraz usuwania ich z listy ostrzeżeń, o której mowa w ust. 1.

6. Przedsiębiorca telekomunikacyjny może uniemożliwić użytkownikom internetu dostęp do stron internetowych wykorzystujących nazwy domen internetowych wpisanych na listę, o której mowa w ust. 1.

**Art. 12.** 1. Dostawca poczty elektronicznej:

1) dla co najmniej 500 000 użytkowników,

2) dla podmiotu publicznego, lub

3) obsługujący co najmniej 500 000 aktywnych kont pocztowych

– ma obowiązek stosowania mechanizmu SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication Reporting and Conformance) oraz DKIM (DomainKeys Identified Mail).

2. Podmiot publiczny jest obowiązany do korzystania z poczty elektronicznej wykorzystującej mechanizmy, o których mowa w ust. 1.

3. Prezes UKE może przeprowadzić kontrolę:

1) wykonywania obowiązku, o którym mowa w ust. 1, przez dostawcę poczty elektronicznej oraz

2) wykonywania obowiązku, o którym mowa w ust. 2, przez podmiot publiczny.

4. Przepisy ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne dotyczące kontroli stosuje się.

**Art. 13.** 1. Przedsiębiorca telekomunikacyjny jest obowiązany do rejestracji danych o usługach telekomunikacyjnych, które nie zostały przez tego przedsiębiorcę wykonane w związku z realizacją:

1) obowiązku, o którym mowa w art. 4 ust. 6,

2) uprawnienia, o którym mowa w art. 7

– w zakresie umożliwiającym rozpatrzenie reklamacji, o której mowa w art. 106 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

2. Przedsiębiorca telekomunikacyjny przechowuje dane, o których mowa w ust. 1, co najmniej przez okres 12 miesięcy, a w przypadku wniesienia reklamacji – przez okres niezbędny do rozstrzygnięcia sporu.

**Art. 14.** 1. Przedsiębiorcy telekomunikacyjni mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą telekomunikacyjną, z wyłączeniem komunikatu elektronicznego, w celu identyfikacji, zapobiegania i zwalczania nadużyć w komunikacji elektronicznej, z uwzględnieniem ust. 2.

2. Przedsiębiorcy telekomunikacyjni mogą przetwarzać i wzajemnie udostępniać również komunikat elektroniczny w celu identyfikacji, zapobiegania i zwalczania smishingu.

3. Przedsiębiorca telekomunikacyjny może przetwarzać:

1) treści krótkich wiadomości tekstowych (SMS), oraz

2) dane o usługach telekomunikacyjnych, które nie zostały przez tego przedsiębiorcę wykonane w związku z realizacją obowiązku, o którym mowa w art. 4 ust. 6 lub uprawnienia, o którym mowa w art. 7

– w celu realizacji obowiązku, o którym mowa w art. 3 ust. 2, art. 4 ust. 6 i art. 8 oraz realizacji uprawnienia, o którym mowa w art. 7, a także na cele związane z dochodzeniem roszczeń. Przetwarzanie to dopuszczalne jest tylko do końca okresu, w którym możliwe jest dochodzenie roszczeń.

4. Do przetwarzania danych osobowych przez przedsiębiorców telekomunikacyjnych, przepisu art. 14 i 15 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.) nie stosuje się w zakresie, w jakim jest to niezbędne dla identyfikacji, zapobiegania oraz zwalczania przestępstw na szkodę przedsiębiorcy telekomunikacyjnego.

Art. 15. 1. Kto dokonuje nadużyć w komunikacji elektronicznej, o których mowa w art. 3 ust. 1 pkt 1, 2 lub 3, podlega karze pieniężnej.

2. Na przedsiębiorcę telekomunikacyjnego, który nie wypełnia obowiązków, o których mowa w:

1) art. 4 ust. 6,

2) art. 8,

3) art. 9 ust. 12

– może zostać nałożona kara pieniężna.

3. Na dostawcę poczty elektronicznej, który nie wypełnia obowiązków, o których mowa w art. 12 ust. 1, może zostać nałożona kara pieniężna.

4. Kary, o których mowa w ust. 1–3, nakłada Prezes UKE w drodze decyzji. Do kar nakładanych na podstawie ust. 1–3 stosuje się odpowiednio przepisy art. 209 ust. 1a–3 oraz art. 210 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

5. Prezes UKE może, w drodze decyzji, nałożyć karę pieniężną na kierownika podmiotu publicznego, jeżeli nie został wykonany obowiązek, o którym mowa w art. 11 ust. 2. Kara pieniężna nakładana jest w wysokości do jednokrotności przeciętnego wynagrodzenia w gospodarce narodowej, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego, w ostatnim komunikacie, o którym mowa **w** art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2022 r. poz. 504).

6. Wpływy z tytułu kar pieniężnych, o których mowa w ust. 1-3, stanowią przychód Funduszu Cyberbezpieczeństwa, o którym mowa w art. 1 pkt 1 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2021 r. poz. 2333 oraz z 2022 r. poz. 655).

**Art. 16.** 1. Kto w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody dopuszcza się:

1) inicjowania wysyłania lub odbierania komunikatów elektronicznych lub połączeń głosowych w sieci telekomunikacyjnej z wykorzystaniem urządzeń telekomunikacyjnych lub programów, których celem nie jest skorzystanie z usługi telekomunikacyjnej, lecz ich zarejestrowanie na punkcie połączenia sieci telekomunikacyjnych bądź przez systemy rozliczeniowe,

2) wysyłania krótkich wiadomości tekstowych (SMS), w których podszywa się pod inny podmiot, w celu nakłonienia odbiorcy tej wiadomości do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem, przekierowania na stronę www, żądania kontaktu telefonicznego lub instalacji oprogramowania,

3) nieuprawnionego posłużenia się przy wywoływaniu połączenia głosowego informacją adresową wskazującą na inną osobę lub jednostkę organizacyjną, służącego podszyciu się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do określonego działania, w szczególności przekazania danych osobowych lub instalacji oprogramowania

– podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

3. Jeżeli działanie, o którym mowa w ust. 1 pkt 1–3, popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

**Art. 17.** Prezes UKE przedstawia sejmowej komisji właściwej w sprawach nowych technologii roczne sprawozdanie z wykonywania swoich obowiązków i uprawnień określonych w niniejszej ustawie. Sprawozdanie składa się do dnia 31 marca za rok poprzedni.

**Art. 18.** W ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. poz. 2333 oraz z 2022 r. poz. 655) w art. 2 w ust. 4 po pkt 1 dodaje się pkt 1a w brzmieniu:

„1a) wpływy z kar pieniężnych, o których mowa w art. 15 ustawy z dnia … o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. poz. …);”.

Art. 19. 1. CSIRT NASK uruchomi system, o którym mowa w art. 4 ust. 3, i poinformuje ministra właściwego do spraw informatyzacji, w terminie nie później niż w 3 miesięcy od dnia wejścia w życie ustawy.

2. Minister właściwy do spraw informatyzacji niezwłocznie po otrzymaniu informacji, o której mowa w ust. 1, udostępnia, w Biuletynie Informacji Publicznej, informację o uruchomieniu systemu, o którym mowa w art. 4 ust. 3.

3. Komendant Główny Policji, Prezes UKE i przedsiębiorcy telekomunikacyjni obowiązani są do podłączenia się do systemu, o którym mowa w art. 4 ust. 3, w terminie 3 miesięcy od dnia udostępnienia przez ministra właściwego do spraw informatyzacji w Biuletynie Informacji Publicznej na swojej stronie podmiotowej informacji o uruchomieniu tego systemu.

Art. 20. Kary pieniężnej:

1) o której mowa w art. 15 ust. 2 pkt 1, nie nakłada się przed upływem 6 miesięcy od dnia wejścia w życie ustawy;

2) o której mowa w art. 15 ust. 2 pkt 2, nie nakłada się przed upływem 12 miesięcy od dnia wejścia w życie ustawy.

**Art. 21.** Przedsiębiorcy telekomunikacyjni są obowiązani do wdrożenia rozwiązań umożliwiających podejmowanie proporcjonalnych działań mających na celu zapobieganie i zwalczanie nadużyć w komunikacji elektronicznej, o których mowa w:

1) art. 3 ust. 1 pkt 1 i 2 – w terminie 6 miesięcy od dnia wejścia w życie ustawy;

2) art. 3 ust. 1 pkt 3 – w terminie 12 miesięcy od dnia wejścia w życie ustawy.

**Art. 22.** 1. Z dniem wejścia w życie ustawy porozumienie o współpracy w zakresie ochrony użytkowników internetu przed stronami wyłudzającymi dane, w tym dane osobowe oraz doprowadzających użytkowników internetu do niekorzystnego rozporządzenia ich środkami finansowymi w okresie stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego w Rzeczypospolitej Polskiej, zawarte w dniu 23 marca 2020 r., staje się porozumieniem, o którym mowa w art. 11 ust. 1.

2. Z dniem wejścia w życie ustawy lista ostrzeżeń dotycząca domen internetowych, które służą do wyłudzeń danych i środków finansowych użytkowników internetu, prowadzona przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy na podstawie zawartego w dniu 23 marca 2020 r. porozumienia o współpracy w zakresie ochrony użytkowników internetu przed stronami wyłudzającymi dane, w tym dane osobowe oraz doprowadzających użytkowników internetu do niekorzystnego rozporządzenia ich środkami finansowymi w okresie stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego w Rzeczypospolitej Polskiej, staje się listą, o której mowa w art. 11 ust. 3.

3. Postanowienia porozumienia, o którym mowa w ust. 1, ograniczające stosowanie porozumienia do stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego w Rzeczypospolitej Polskiej stają się bezskuteczne z dniem wejścia w życie ustawy.

Art. 23. Ustawa wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

ZA ZGODNOŚĆ POD WZGLĘDEM PRAWNYM,

LEGISLACYJNYM I REDAKCYJNYM

Anna Markowska

Zastępca Dyrektora

Departamentu Regulacji Cyfrowych

Kancelarii Prezesa Rady Ministrów

/podpisano elektronicznie/

1. ) Niniejszą ustawą zmienia się ustawę z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa. [↑](#footnote-ref-2)
2. ) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2021 r. poz. 1236, 1535, 1773, 1927, 1981, 2054 i 2270 oraz z 2022 r. poz. 583, 655 i 1079. [↑](#footnote-ref-3)