# Cyberbezpieczeństwo - wyciąg z Ustawy

Krajowy system cyberbezpieczeństwa.

Dz.U.2020.1369 t.j. z dnia 2020.08.11

Status: Akt obowiązujący **Wejście w życie:**28 sierpnia 2018 r.

**USTAWA**

z dnia 5 lipca 2018 r.

**o krajowym systemie cyberbezpieczeństwa** [1]

**Art. 2. [Definicje legalne]**

Użyte w ustawie określenia oznaczają:

1) CSIRT GOV - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;

2) CSIRT MON - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej;

3) CSIRT NASK - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy;

4) cyberbezpieczeństwo - odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;

5) incydent - zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo;

6) incydent krytyczny - incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV;

7) incydent poważny - incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej;

8) incydent istotny - incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz. Urz. UE L 26 z 31.01.2018, str. 48), zwanego dalej "rozporządzeniem wykonawczym 2018/151";

9) incydent w podmiocie publicznym - incydent, który powoduje lub może spowodować obniżenie jakości lub

przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny, o którym mowa w art. 4 pkt 7-15;

10) obsługa incydentu - czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu;

11) podatność - właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa;

12) ryzyko - kombinację prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;

13) szacowanie ryzyka - całościowy proces identyfikacji, analizy i oceny ryzyka;

14) system informacyjny - system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 r. poz. 346, 568 i 695), wraz z przetwarzanymi w nim danymi w postaci elektronicznej;

15) usługa cyfrowa - usługę świadczoną drogą elektroniczną w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną ((Dz. U. z 2020 r. poz. 344), wymienioną w załączniku nr 2 do ustawy;

16) usługa kluczowa - usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych;

17) zagrożenie cyberbezpieczeństwa - potencjalną przyczynę wystąpienia incydentu;

18) zarządzanie incydentem - obsługę incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu;

19) zarządzanie ryzykiem - skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka.

**Art. 4. [Podmioty objęte krajowym systemem cyberbezpieczeństwa]**

Krajowy system cyberbezpieczeństwa obejmuje:

1) operatorów usług kluczowych;

2) dostawców usług cyfrowych;

3) CSIRT MON;

4) CSIRT NASK;

5) CSIRT GOV;

6) sektorowe zespoły cyberbezpieczeństwa;

7) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1-6, 8, 9, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2019 r. poz. 869, z późn. zm.);

***(do tej grupy zaliczany jest samorząd powiatowy i jednostki organizacyjne powiatu)***

.....

**Rozdział 5 Obowiązki podmiotów publicznych**

**Art. 21. [Obowiązek wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa]**

1. Podmiot publiczny, o którym mowa w art. 4 pkt 7-15, realizujący zadanie publiczne zależne od systemu informacyjnego jest obowiązany do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
2. Organ administracji publicznej może wyznaczyć jedną osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jednostki jemu podległe lub przez niego nadzorowane.
3. Jednostka samorządu terytorialnego może wyznaczyć jedną osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jej jednostki organizacyjne.

**Art. 22. [Obowiązki w zakresie zgłaszania i obsługi incydentu w podmiocie publicznym]**

1. Podmiot publiczny, o którym mowa w art. 4 pkt 7-15, realizujący zadanie publiczne zależne od systemu informacyjnego:

1) zapewnia zarządzanie incydentem w podmiocie publicznym;

2) zgłasza incydent w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;

3) zapewnia obsługę incydentu w podmiocie publicznym i incydentu krytycznego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe;

4) zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej;

5) przekazuje do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV dane osoby, o której mowa w art. 21, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia jej wyznaczenia, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.

1. Zgłoszenie, o którym mowa w ust. 1 pkt 2, przekazywane jest w postaci elektronicznej, a w przypadku braku możliwości przekazania go w postaci elektronicznej - przy użyciu innych dostępnych środków komunikacji.

**Art. 23. [Zgłoszenie incydentu w podmiocie publicznym]**

1. Zgłoszenie, o którym mowa w art. 22 ust. 1 pkt 2, zawiera:

1) dane podmiotu zgłaszającego, w tym nazwę podmiotu, numer we właściwym rejestrze, siedzibę i adres;

2) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby składającej zgłoszenie;

3) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;

4) opis wpływu incydentu w podmiocie publicznym na realizowane zadanie publiczne, w tym:

a) wskazanie zadania publicznego, na które incydent miał wpływ,

b) liczbę osób, na które incydent miał wpływ,

c) moment wystąpienia i wykrycia incydentu oraz czas jego trwania,

d) zasięg geograficzny obszaru, którego dotyczy incydent,

e) przyczynę zaistnienia incydentu i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne podmiotu publicznego;

5) informacje o przyczynie i źródle incydentu;

6) informacje o podjętych działaniach zapobiegawczych;

7) informacje o podjętych działaniach naprawczych;

8) inne istotne informacje.

1. Podmiot publiczny, o którym mowa w art. 4 pkt 7-15, przekazuje informacje znane mu w chwili dokonywania zgłoszenia, które uzupełnia w trakcie obsługi incydentu w podmiocie publicznym.
2. Podmiot publiczny, o którym mowa w art. 4 pkt 7-15, przekazuje, w niezbędnym zakresie, w zgłoszeniu, o którym mowa w art. 22 ust. 1 pkt 2, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne do realizacji zadań właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV.
3. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może zwrócić się do podmiotu publicznego, o którym mowa w art. 4 pkt 7-15, o uzupełnienie zgłoszenia o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do realizacji zadań, o których mowa w ustawie.
4. W zgłoszeniu podmiot publiczny, o którym mowa w art. 4 pkt 7-15, oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.

**Art. 94. [Wejście w życie]**

Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia. [2]

*[1] Niniejsza ustawa w zakresie swojej regulacji wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, str. 1).*

*[2] Ustawa została ogłoszona w dniu 13 sierpnia 2018 r.*