Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz

Ustawa o krajowym systemie cyberbezpieczeństwa[1]

z dnia 5 lipca 2018 r. (Dz.U. z 2018 r. poz. 1560)

Tekst jednolity z dnia 29 grudnia 2025 r. (Dz.U. z 2026 r. poz. 20)[2]

(zm.: Dz.U. 2026, poz. 252)

Rozdział 1. Przepisy ogólne

Art. 1. [Zakres przedmiotowy]

1. Ustawa określa:

1) organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu;

2) sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy;

3) zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej;

4)[3] zakres Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, zwanego dalej „Krajowym planem".

2. Ustawy nie stosuje się do:

1)[4] (*uchylony*)

2)[5] (*uchylony*)

3) podmiotów wykonujących działalność leczniczą, tworzonych przez Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu.

---

[1] Treść odnośnika publikujemy na końcu ustawy.

[2] Tekst jednolity ogłoszono dnia 9.01.2026 r.

[3] Art. 1 ust. 1 pkt 4 dodany ustawą z dnia 23.01.2026 r. (Dz.U. z 2026 r. poz. 252), która wchodzi w życie 3.04.2026 r.

[4] Art. 1 ust. 2 pkt 1 uchylony ustawą z dnia 23.01.2026 r. (Dz.U. z 2026 r. poz. 252), która wchodzi w życie 3.04.2026 r.

[5] Art. 1 ust. 2 pkt 2 uchylony ustawą z dnia 23.01.2026 r. (Dz.U. z 2026 r. poz. 252), która wchodzi w życie 3.04.2026 r.

Spis treści

1 1. **Rys historyczny.** Artykuł 1 CyberbezpU w swojej pierwotnej treści wszedł w życie 13.8.2018 r. i składał się z art. 1 ust. 1 pkt 1–3 oraz art. 1 ust. 2 pkt 1–3. W początkowej wersji projektu z 31.10.2017 r. (https://legislacja.rcl.gov.pl/docs//2/12304650/12466702/12466703/dokument314511.pdf, dostęp: 24.3.2026 r.), implementującego dyrektywę NIS2, nie uwzględniono ust. 2 regulującego kwestię wyłączeń stosowania ustawy. Wyłączenia przewidziane dla przedsiębiorców telekomunikacyjnych i dostawców usług zaufania zostały dodane do projektu ustawy z 13.3.2018 r. (https://legislacja.rcl.gov.pl/docs//2/12304650/12466734/12466735/dokument337541.pdf, dostęp: 24.3.2026 r.) wdrażającego dyrektywę NIS2, z kolei wyłączenie dla „podmiotów wykonujących działalność leczniczą, tworzonych przez Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu" zostało wprowadzone w projekcie datowanym na 5.4.2018 r. (https://orka.sejm.gov.pl/Druki8ka.nsf/Projekty/8-020-963-2018/$file/8-020-963-2018.pdf, dostęp: 24.3.2026 r.).

Po uchwaleniu i wejściu w życie CyberbezpU jej art. 1 nie był nowelizowany aż do 10.11.2024 r., kiedy to nastąpiła zmiana ust. 2 pkt 1 polegająca na zastąpieniu wyłączenia dla przedsiębiorców telekomunikacyjnych w rozumieniu *PrTelekom* (utraciła moc z dniem 10.11.2024 r.), analogicznym wyłączeniem odnoszącym natomiast do nowej PrKomElektr. Wchodzące w życie 3.4.2026 r. zmiany, obejmujące dodanie ust. 1 pkt 4 oraz uchylenie ust. 2 pkt 1–2, zostały zaproponowane już na etapie wersji projektu z 23.4.2024 r., opracowanej w toku rządowych prac legislacyjnych. W takim kształcie projektowana zmiana doczekała się uchwalenia.

2 2. **Zakres przedmiotowy ustawy.** Artykuł 1 ust. 1 CyberbezpU określa w czterech punktach zakres przedmiotowy ustawy.

Punkt 1 ogólnie dotyczy pozostałych, względem punktów 2–4 tego ustępu, rozdziałów ustawy stwierdzając, że jej zakres przedmiotowy dotyczy organizacji krajowego systemu cyberbezpieczeństwa oraz zadań i obowiązków podmiotów wchodzących w skład tego systemu. Wynika z takiej redakcji, że ustawa nie określa żadnych praw dla podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa, co jednak wydaje się zbyt kategorycznym stwierdzeniem, gdyż ustawa przyznaje im m.in. prawo do wymiany informacji o zagrożeniach oraz prawo do wsparcia w obsłudze incydentów przez zespoły CSIRT.

Punkt 2 dotyczy rozdziału 11 pt. „Nadzór i kontrola podmiotów kluczowych lub podmiotów ważnych", obejmującego art. 53–59c CyberbezpU. W stosunku do poprzedniego brzmienia przepisów (obowiązującego do 3.4.2026 r.) zmieniono (rozbudowano) w szczególności zakres art. 53 CyberbezpU, w którym wskazano, że nadzór mają sprawować organy właściwe do spraw cyberbezpieczeństwa w zakresie wykonywania przez podmioty kluczowe i podmioty ważne wynikających z ustawy obowiązków (w poprzedniej wersji ustawy była mowa o Ministrze Cyfryzacji, a dopiero potem – w ograniczonym zakresie – innych organach właściwych ds. cyberbezpieczeństwa).

Przepis rozszerzono o szczegółowe uprawnienia organów właściwych do spraw cyberbezpieczeństwa, w tym możliwość kontroli, żądania informacji i dokumentów, nakazywania audytów oraz korzystania ze wsparcia CSIRT. Dodano również mechanizmy egzekwowania obowiązków i procedurę nadzorczą, obejmującą ostrzeżenia, decyzje i środki sankcyjne, a także zasady odwołania do sądu administracyjnego i gwarancje proceduralne dla nadzorowanych podmiotów. W literaturze przedmiotu zwracano uwagę, że uwzględniając znaczenie nadawane w nauce prawa administracyjnego terminom „kontrola" i „nadzór", można też przyjąć, że regulacja sposobu sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy obejmuje dodatkowo przepisy rozproszone w wielu innych rozdziałach ustawy [zob. *G. Szpor*, w: *K. Czaplicki*, *A. Gryszczyńska*, *G. Szpor* (red.), Ustawa o krajowym systemie cyberbezpieczeństwa, komentarz do art. 1].

Punkt 3 dotyczy rozdziału 13 pt. „Strategia" (art. 68–72 CyberbezpU).

Punkt 4 – obowiązujący od 3.4.2026 r. – odnosi się do rozdziału 13a pt. „Krajowy plan reagowania na incydenty i sytuacje kryzysowe cyberbezpieczeństwa na dużą skalę" (art. 72a–72f CyberbezpU). Krajowy plan zawiera w szczególności:

1) cele działań w zakresie zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę;
2) zadania organów zaangażowanych w zarządzanie kryzysowe w cyberbezpieczeństwie;
3) procedury zarządzania kryzysowego w cyberprzestrzeni oraz kanały wymiany informacji;
4) krajowe środki służące zapewnieniu gotowości na wypadek wystąpienia incydentów w cyberbezpieczeństwie na dużą skalę, w tym ćwiczenia i szkolenia;
5) zasady współpracy między sektorem publicznym i prywatnym w obszarze zarządzania kryzysowego;
6) kryteria oceny infrastruktury informatycznej pod kątem jej znaczenia dla zarządzania kryzysowego;
7) krajowe procedury i ustalenia między odpowiednimi organami i instytucjami krajowymi mające na celu zapewnienie efektywnego uczestnictwa danego państwa członkowskiego UE w skoordynowanym zarządzaniu incydentami i zarządzaniu kryzysowym w cyberbezpieczeństwie na dużą skalę;
8) postanowienia dotyczące zarządzania kryzysami i reagowania na nie w odniesieniu do transgranicznych przepływów energii elektrycznej;
9) uporządkowaną listę działań na rzecz ograniczenia ryzyka wystąpienia incydentu krytycznego w zakresie organizacyjnym i technicznym, z uwzględnieniem:
   a) hierarchii działań,
   b) ram czasowych ich realizacji,
   c) podmiotów wiodących oraz współpracujących przy ich wykonywaniu,
   d) sposobów finansowania oraz wysokości nakładów finansowych,
   e) oceny osiągniętych efektów oraz wniosków z wdrożonych działań.

3. **Wyłączenia ze stosowania ustawy.** W art. 1 ust. 2 CyberbezpU określono wyłączenia z zakresu stosowania ustawy. Od 4.4.2026 r. uchylono wyłączenia do dostawców usług komunikacji elektronicznej (pkt 1) – wcześniej przedsiębior- **3**

ców telekomunikacyjnych – oraz dostawców usług zaufania publicznego (pkt 2). Z uzasadnienia projektu nowelizacji CyberbezpU (uzasadnienie do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, https://orka.sejm.gov.pl/Druki10ka.nsf/0/EAE89BDA7AEC8DECC1258D450063FA62/%24File/1955.pdf, dostęp: 24.3.2026 r.) wynika, że obydwie te grupy podmiotów podlegają obecnie pod przepisy CyberbezpU i należy je również uwzględnić w ustawie. Pozostało obowiązujące jedynie wyłącznie z art. 1 ust. 2 pkt 3 CyberbezpU odnoszące się do niestosowania ustawy do podmiotów wykonujących działalność leczniczą, tworzonych przez Szefa ABW lub Szefa AW. W doktrynie zwraca się uwagę na brak konsekwencji ze strony ustawodawcy, a mianowicie dlaczego analogicznego rozwiązania nie zastosowano w stosunku do pozostałych podmiotów leczniczych o szczególnej regulacji, tj. jednostek tworzonych przez ministra właściwego do spraw wewnętrznych, Ministra Obrony Narodowej, Ministra Sprawiedliwości lub Szefa CBA, o których mowa w art. 40 ust. 1 i 2 DziałLeczU [zob. *F. Radoniewicz*, w: *W. Kitler*, *J. Taczkowska-Olszewska*, *F. Radoniewicz* (red.), Ustawa o krajowym systemie cyberbezpieczeństwa, komentarz do art. 1].

Art. 2. [Objaśnienie pojęć]

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;

3a)[6] **CSIRT sektorowy – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, działający na poziomie sektora lub podsektora, ustanowiony przez organ właściwy do spraw cyberbezpieczeństwa dla danego sektora lub podsektora;**

3b)[6] **abonent nazwy domeny – podmiot będący stroną umowy o utrzymywanie nazwy domeny zawartej z rejestrem nazw domen najwyższego poziomu (TLD), za pośrednictwem podmiotu świadczącego usługi rejestracji nazw domen;**

3c)[6] **adres do doręczeń elektronicznych – adres, o którym mowa w art. 2 pkt 1 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz.U. z 2026 r. poz. 3);**

3d)[6] **bezpieczeństwo systemów informacyjnych – odporność systemów informacyjnych, przy danym poziomie pewności, na zdarzenia naruszające pouf-**

[6] Art. 2 pkt 3a–3d dodane ustawą z dnia 23.01.2026 r. (Dz.U. z 2026 r. poz. 252), która wchodzi w życie 3.04.2026 r.

ność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;

4)[7] **cyberbezpieczeństwo – cyberbezpieczeństwo w rozumieniu art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.Urz. UE L 151 z 07.06.2019, str. 15, z późn. zm.), zwanego dalej „rozporządzeniem 2019/881";**

4a)[8] **cyberzagrożenie – cyberzagrożenie w rozumieniu art. 2 pkt 8 rozporządzenia 2019/881;**

4b)[8] **dostawca sieci dostarczania treści – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która dostarcza treści i usługi cyfrowe do sieci rozproszonych geograficznie serwerów służących zapewnieniu wysokiej i łatwej dostępności tych treści i usług cyfrowych lub ich szybkiego dostarczania na rzecz użytkowników Internetu w imieniu dostawców treści i usług, z wyłączeniem przedsiębiorców komunikacji elektronicznej;**

4c)[8] **dostawca sprzętu lub oprogramowania – producenta, upoważnionego przedstawiciela, importera lub dystrybutora, w rozumieniu odpowiednio art. 2 pkt 3–6 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającego wymagania w zakresie akredytacji i uchylającego rozporządzenie (EWG) nr 339/93 (Dz.Urz. UE L 218 z 13.08.2008, str. 30, z późn. zm.), produktu ICT, usługi ICT lub procesu ICT;**

4d)[8] **dostawca internetowej platformy handlowej – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która dostarcza internetową platformę handlową, o której mowa w art. 2 pkt 8 ustawy z dnia 30 maja 2014 r. o prawach konsumenta (Dz.U. z 2024 r. poz. 1796 oraz z 2025 r. poz. 1172);**

4e)[8] **dostawca chmury obliczeniowej – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługę umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników;**

4f)[8] **dostawca platformy sieci usług społecznościowych – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługę świadczoną drogą elektroniczną w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elek-**

[7] Art. 2 pkt 4 w brzmieniu ustawy z dnia 23.01.2026 r. (Dz.U. z 2026 r. poz. 252), która wchodzi w życie 3.04.2026 r.

[8] Art. 2 pkt 4a–4l dodane ustawą z dnia 23.01.2026 r. (Dz.U. z 2026 r. poz. 252), która wchodzi w życie 3.04.2026 r.

troniczną (Dz.U. z 2024 r. poz. 1513), która umożliwia użytkownikom końcowym łączenie się z innymi osobami oraz komunikowanie się i wymianę, udostępnianie i odkrywanie treści za pomocą wielu urządzeń;

4g)[8] **dostawca usług DNS – podmiot, który świadczy dostępne publicznie rekurencyjne usługi rozpoznawania nazw domen na rzecz ogółu użytkowników końcowych Internetu lub autorytatywne usługi rozpoznawania nazw domen do użytku ogółu użytkowników końcowych Internetu, z wyjątkiem głównych serwerów nazw;**

4h)[8] **dostawca usługi centrum przetwarzania danych – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługę obejmującą struktury lub grupy struktur przeznaczone do scentralizowanego hostingu, zapewniania wzajemnego połączenia i eksploatacji produktów ICT, usług ICT lub procesów ICT służącego do świadczenia usług przechowywania, przetwarzania i transportu danych wraz ze wszystkimi obiektami i całą infrastrukturą, zapewniającymi dystrybucję energii elektrycznej i kontrolę środowiskową;**

4i)[8] **dostawca usług zarządzanych – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługi związane z instalacją, eksploatacją lub konserwacją produktów ICT, usług ICT, procesów ICT lub systemów informacyjnych przez wsparcie lub aktywną administrację przeprowadzane u usługobiorcy na miejscu lub zdalnie;**

4j)[8] **dostawca usług zarządzanych w zakresie cyberbezpieczeństwa – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługi polegające na realizacji lub wsparciu dla realizacji działań związanych z zarządzaniem ryzykiem w cyberbezpieczeństwie, w tym obsługę incydentów, testów bezpieczeństwa, audytów systemów informacyjnych, doradztwo;**

4k)[8] **dostawca usług zaufania – dostawcę usług zaufania w rozumieniu art. 3 pkt 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz.Urz. UE L 257 z 28.08.2014, str. 73), zwanego dalej „rozporządzeniem 910/2014";**

4l)[8] **dostawca wyszukiwarki internetowej – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługę wyszukiwarki internetowej, o której mowa w art. 2 pkt 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1150 z dnia 20 czerwca 2019 r. w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego (Dz.Urz. UE L 186 z 11.07.2019, str. 57);**

5)[9] **incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych;**

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)[10] **incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi przez podmiot kluczowy lub podmiot ważny, straty finansowe dla tego podmiotu lub wpływa na inne osoby fizyczne, osoby prawne, jednostki organizacyjne nieposiadające osobowości prawnej przez wywołanie poważnej szkody materialnej lub niematerialnej;**

8)[11] **incydent w cyberbezpieczeństwie na dużą skalę – incydent, którego skutki przekraczają możliwości reagowania państwa lub który ma poważny wpływ na inne państwo członkowskie Unii Europejskiej;**

8a)[12] **kierownik podmiotu kluczowego lub podmiotu ważnego – kierownik jednostki w rozumieniu art. 3 ust. 1 pkt 6 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz.U. z 2023 r. poz. 120, z późn. zm.) kierujący podmiotem kluczowym lub podmiotem ważnym, a w przypadku podmiotu kluczowego lub podmiotu ważnego będącego jednostką sektora finansów publicznych – kierownik jednostki sektora finansów publicznych, o którym mowa w art. 53 ust. 1 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. z 2025 r. poz. 1483, 1844 i 1846);**

9)[13] **(*uchylony*)**

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

10a)[14] **organizacja badawcza – niebędącą podmiotem kluczowym osobę prawną, albo jednostkę organizacyjną nieposiadającą osobowości prawnej, której podstawową działalnością jest działalność, o której mowa w art. 4 ust. 2 pkt 2 lub ust. 3 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyż-**

[9] Art. 2 pkt 5 w brzmieniu ustawy z dnia 23.01.2026 r. (Dz.U. z 2026 r. poz. 252), która wchodzi w życie 3.04.2026 r.

[10] Art. 2 pkt 7 w brzmieniu ustawy z dnia 23.01.2026 r. (Dz.U. z 2026 r. poz. 252), która wchodzi w życie 3.04.2026 r.

[11] Art. 2 pkt 8 w brzmieniu ustawy z dnia 23.01.2026 r. (Dz.U. z 2026 r. poz. 252), która wchodzi w życie 3.04.2026 r.

[12] Art. 2 pkt 8a dodany ustawą z dnia 23.01.2026 r. (Dz.U. z 2026 r. poz. 252), która wchodzi w życie 3.04.2026 r.

[13] Art. 2 pkt 9 uchylony ustawą z dnia 23.01.2026 r. (Dz.U. z 2026 r. poz. 252), która wchodzi w życie 3.04.2026 r.

[14] Art. 2 pkt 10a dodany ustawą z dnia 23.01.2026 r. (Dz.U. z 2026 r. poz. 252), która wchodzi w życie 3.04.2026 r.

szym i nauce (Dz.U. z 2024 r. poz. 1571, z późn. zm.), w zakresie, w jakim prowadzi ją z wykorzystaniem systemów informacyjnych;

11)[15] **podatność – właściwości produktu ICT lub usługi ICT, które mogą być wykorzystane przez cyberzagrożenie;**

11a)[16] **podmiot finansowy – podmiot, o którym mowa w art. 2 ust. 1 lit. a–t rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniającego rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.Urz. UE L 333 z 27.12.2022, str. 1, z późn. zm.), zwanego dalej „rozporządzeniem 2022/2554";**

11b)[16] **podmiot publiczny – podmiot wskazany w załączniku nr 1 lub 2 do ustawy w sektorze podmioty publiczne;**

11c)[16] **podmiot krytyczny – podmiot krytyczny w rozumieniu art. 2 pkt 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylającej dyrektywę Rady 2008/114/WE (Dz.Urz. UE L 333 z 27.12.2022, str. 164), zwanej dalej „dyrektywą 2022/2557";**

11d)[16] **podmiot świadczący usługi rejestracji nazw domen – rejestratora lub agenta działającego w imieniu rejestratorów, w tym dostawcę lub odsprzedawcę usług w zakresie prywatnej rejestracji lub pośrednictwa w rejestracji;**

11e)[16] **potencjalne zdarzenie dla cyberbezpieczeństwa – zdarzenie, które mogło mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych, które jednak nie wystąpiło lub któremu udało się zapobiec;**

11f)[16] **poważne cyberzagrożenie – cyberzagrożenie, które przez swoje właściwości techniczne może mieć poważny wpływ na bezpieczeństwo systemów informacyjnych lub użytkowników tych systemów przez wywołanie poważnej szkody materialnej lub niematerialnej;**

11g)[16] **projekt – przedsięwzięcie realizowane w ramach programu, o którym mowa w art. 45a ust. 1, na podstawie umowy o dofinansowanie, zawieranej między beneficjentem a podmiotem udzielającym pomocy;**

11h)[16] **poważny incydent związany z ICT – poważny incydent związany z technologiami informacyjno–komunikacyjnymi w rozumieniu art. 3 pkt 10 rozporządzenia 2022/2554;**

11i)[16] **przedsiębiorca komunikacji elektronicznej – przedsiębiorcę komunikacji elektronicznej w rozumieniu art. 2 pkt 39 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz.U. poz. 1221 oraz z 2025 r. poz. 637 i 820);**

---

[15] Art. 2 pkt 11 w brzmieniu ustawy z dnia 23.01.2026 r. (Dz.U. z 2026 r. poz. 252), która wchodzi w życie 3.04.2026 r.

[16] Art. 2 pkt 11a–11n dodane ustawą z dnia 23.01.2026 r. (Dz.U. z 2026 r. poz. 252), która wchodzi w życie 3.04.2026 r.

11j)[16] **przedsiębiorca telekomunikacyjny – przedsiębiorcę telekomunikacyjnego w rozumieniu art. 2 pkt 40 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej;**

11k)[16] **proces ICT – proces ICT w rozumieniu art. 2 pkt 14 rozporządzenia 2019/881;**

11l)[16] **produkt ICT – produkt ICT w rozumieniu art. 2 pkt 12 rozporządzenia 2019/881;**

11m)[16] **usługa ICT – usługę ICT w rozumieniu art. 2 pkt 13 rozporządzenia 2019/881;**

11n)[16] **rejestr nazw domen najwyższego poziomu (TLD) – podmiot, któremu powierzono konkretną domenę najwyższego poziomu (TLD) i który odpowiada za zarządzanie nią, w tym za rejestrację nazw domen w ramach TLD oraz za jej techniczne funkcjonowanie, w tym za obsługę jej serwerów nazw, utrzymanie jej baz danych oraz dystrybucję plików strefowych TLD we wszystkich serwerach nazw, bez względu na to, czy którekolwiek z tych działań jest wykonywane przez sam podmiot czy zlecane na zewnątrz, ale z wyłączeniem sytuacji, w których rejestr wykorzystuje nazwy TLD wyłącznie do własnego użytku;**

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

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

14)[17] **system informacyjny:**

a) 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 2025 r. poz. 1703 oraz z 2026 r. poz. 160), lub

b) urządzenie lub grupę połączonych urządzeń i oprogramowania zaprogramowanych w celu przetwarzania danych

– wraz z danymi przetwarzanymi w postaci elektronicznej;

14a)[18] **właściwy organ w rozumieniu rozporządzenia 2022/2554 – Komisję Nadzoru Finansowego w zakresie nadzoru przewidzianego rozporządzeniem 2022/2554;**

15)[19] **(*uchylony*)**

16)[19] **(*uchylony*)**

17)[19] **(*uchylony*)**

[17] Art. 2 pkt 14 w brzmieniu ustawy z dnia 23.01.2026 r. (Dz.U. z 2026 r. poz. 252), która wchodzi w życie 3.04.2026 r.

[18] Art. 2 pkt 14a dodany ustawą z dnia 23.01.2026 r. (Dz.U. z 2026 r. poz. 252), która wchodzi w życie 3.04.2026 r.

[19] Art. 2 pkt 15–17 uchylone ustawą z dnia 23.01.2026 r. (Dz.U. z 2026 r. poz. 252), która wchodzi w życie 3.04.2026 r.

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.

Spis treści

1. **Metoda językowa i wyrażenia profesjonalne.** Artykuł 2 stanowi tzw. słowniczek ustawowy zawierający legalne definicje pojęć występujących w przepisach CyberbezpU. Odgrywa on rolę porządkującą i interpretacyjną. Definicje legalne formułujące normy prawne są niezwykle silnymi dyrektywami wykładni. O normatywnym znaczeniu definicji ustawowych świadczą ustalone przez prawodawcę zasady ich redagowania. Zgodnie z § 8 ust. 1 oraz ust. 2 TechPrawodR w ustawie należy posługiwać się poprawnymi wyrażeniami językowymi (określeniami) w ich podstawowym i powszechnie przyjętym znaczeniu, jednocześnie należy unikać posługiwania się określeniami specjalistycznymi, o ile ich użycie nie jest powodowane zapewnieniem należytej precyzji tekstu. Słownik wyrażeń użytych w ustawie zawsze ma charakter objaśniający i interpretacyjny. Wynika to z faktu, iż kluczową metodą wykładni prawa jest przecież wykładnia językowa, stanowiąca klucz do interpretacji tekstu prawnego. Zgodnie z zasadą *clara non sunt interpretanda* – nie ma potrzeby sięgania po inne, pozajęzykowe metody wykładni. W takim wypadku wykładnia pozajęzykowa może jedynie dodatkowo potwierdzać, a więc wzmacniać, wyniki wykładni językowej wykładnią systemową czy funkcjonalną (*G. Wierczyński*, Redagowanie i ogłaszanie aktów normatywnych, 2016). Ponieważ pierwszeństwo wykładni językowej jest zasadą, w przypadku braku ustawowej definicji danego określenia organy stosujące prawo przyjmują, że określenie to zostało użyte przez prawodawcę zgodnie z jego poprawnym, podstawowym i powszechnie przyjętym znaczeniem (*G. Wierczyński*, Redagowanie i ogłaszanie aktów normatywnych, 2009, s. 731). Zdaniem *G. Wierczyńskiego* te zasady są konsekwencją jednej z najważniejszych zasad techniki prawodawczej – zasady komunikatywności. Prawodawca, który zamierza wyrazić normy prawne w sposób komunikatywny i adekwatnie do swoich intencji, musi wyrażać je zgodnie z zasadami: języka oraz wykładni, którymi posługują się odbiorcy kodowanych przez niego informacji. Jakiekolwiek odstępstwo od tych zasad naraża go na niebezpieczeństwo, że te informacje będą odczytywane niezgodnie z jego intencjami (*G. Wierczyński*, Redagowanie i ogłaszanie aktów normatywnych, 2016). Obowiązek posługiwania się wyrażeniami poprawnymi wynika nie tylko ze wskazanego powyżej § 8 TechPrawodR, ale przede wszystkim z obowiązku ochrony języka polskiego, który nałożono na wszystkie organy władzy publicznej oraz instytucje i organizacje uczestniczące w życiu publicznym. W zakresie używanych wyrażeń należy więc dbać o to, by te wyrażenia były używane jedynie w takim znaczeniu i w takich formach, które są przewidziane w słownikach języka polskiego. Powołując się na tę zasadę, sądy odwołują się do słowników języka polskiego, ustalając znaczenie danych wyrażeń. Poszczególne wyrażenia powinny być używane w aktach normatywnych w ich podstawowym znaczeniu. Za podstawowe należy uznać takie znaczenie, które wśród wszystkich znaczeń danego wyrażenia wysuwa się na pierwszy plan, a więc np. w słowniku języka polskiego w części zawierającej wyjaśnienie danego wyrażenia to właśnie znaczenie jest jednym z pierwszych. Jeśli dany zwrot składa się z kilku wyrazów, a definicja tej grupy wyrazów jako całości (zwrotu) znajduje się w słowniku, to właśnie w takim znaczeniu należy używać tego zwrotu. Znaczenie przenośne danego wyrażenia zazwyczaj nie jest jego znaczeniem podstawowym, dlatego raczej nie należy używać wyrażeń w ich przenośnym znaczeniu (zob. wyr. WSA we Wrocławiu z 27.7.2010 r., II SA/Wr 287/10, Legalis). W tym sensie „podstawowość" oznacza **1**

również dosłowność danego znaczenia. Możliwe jest jednak posłużenie się określeniami nieostrymi, jeżeli zachodzi potrzeba zapewnienia elastyczności tekstu aktu normatywnego (§ 155 ust. 1 TechPrawodR). Stosownie do § 147 ust. 2 załącznika do wspomnianego rozporządzenia, jeżeli zachodzi konieczność odstąpienia od zasady wyrażonej w ust. 1, to wyraźnie podaje się inne znaczenie danego określenia i ustala się jego zakres odniesienia [zob. *R. Hauser*, *W. Piątek*, w: *R. Hauser*, *M. Wierzbowski* (red.), Postępowanie egzekucyjne w administracji, komentarz do art. 1a; 13 oraz § 146 ust. 1 załącznika do TechPrawodR].

Niezrozumiałość treści tekstu aktu prawnego może być konsekwencją użycia tzw. profesjonalizmów (określenia specjalistyczne używane jedynie przez członków danej grupy zawodowej), które dopuszcza się, pod warunkiem że nie mają one zrozumiałych odpowiedników (zob. § 8 ust. 2 pkt 1 i 2 TechPrawodR), ale również wtedy, gdy takie odpowiedniki istnieją, ale nie zapewniają potrzebnej precyzji wypowiedzi.

2 2. **CSIRT MON, CSIRT NASK, CSIRT GOV.** Z uwagi na różnice w krajowych strukturach zarządzania państwa członkowskie zostały upoważnione do wyznaczenia właściwych organów krajowych (więcej niż jeden), odpowiedzialnych za wykonywanie zadań związanych z bezpieczeństwem sieci i systemów informatycznych operatorów usług kluczowych i dostawców usług cyfrowych. Ponadto w celu ułatwienia współpracy i komunikacji transgranicznej każde państwo członkowskie zostało zobowiązane do wyznaczenia jednego krajowego punktu kontaktowego odpowiedzialnego za koordynację kwestii związanych z bezpieczeństwem sieci i systemów informatycznych oraz współpracę transgraniczną na poziomie Unii. Dyrektywa NIS dała zatem państwom dowolność w zakresie powoływania liczby CSIRT, z zastrzeżeniem że operatorzy usług kluczowych i dostawcy usług cyfrowych będą mieli wyznaczony CSIRT, do którego będą raportować. Pojęcie CSIRT użyte w art. 2 pkt 1–3 CyberbezpU pochodzi od angielskiej nazwy *Computer Security Incident Response Team*, występującej w treści dyrektywy NIS, której odpowiednikiem w języku polskim jest określenie „Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego". Ustawodawca wyodrębnił trzy typy CSIRT działające na poziomie krajowym. Podział wynika z podziału zadań pomiędzy Szefem ABW (CSIRT GOV), MON (CSIRT MON) oraz Dyrektorem Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (CSIRT NASK). Realizując postanowienia dyrektywy NIS nakazujące utworzenie zespołów CSIRT, nie powołano do życia nowych podmiotów, ale wykorzystano już istniejące na poziomie krajowym, nakładając na nie przewidziane w dyrektywie obowiązki. CSIRT GOV – Rządowy Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający od stycznia 2008 r. w ramach ABW. Jego zadaniem jest koordynacja obsługi incydentów zgłaszanych przez podmioty wskazane w art. 26 ust. 7 CyberbezpU. Ponadto odpowiada za rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych wchodzących w skład infrastruktury krytycznej. Działający w ramach Systemu Reagowania na Incydenty Komputerowe Resortu Obrony Narodowej (SRnIK RON) CSIRT MON odpowiada za koordynację procesów zapobiegania, wykrywania i reagowania na incydenty komputerowe w systemach i sieciach teleinformatycznych

resortu obrony narodowej. CSIRT MON koordynuje obsługę incydentów zgłaszanych przez podmioty podległe MON lub przez niego nadzorowane, w tym podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne wchodzą w skład infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z 26.4.2007 r. o zarządzaniu kryzysowym (t.j. Dz.U. z 2023 r. poz. 122), oraz przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym. Naukowa i Akademicka Sieć Komputerowa jest istniejącym od 1993 r. państwowym instytutem badawczym prowadzącym działalność naukową, Krajowy Rejestr Domen .pl i dostarczającym zaawansowane usługi teleinformatyczne. W jego ramach od 1996 r. działa CERT POLSKA, koordynujący – obecnie jako CSIRT NASK – obsługę incydentów naruszających bezpieczeństwo sieci „sferze cywilnej", mających miejsce w sieciach publicznych, czyli zgłaszane przez pozostałe podmioty (tj. niekwalifikujące się do grup wskazanych wyżej), w tym m.in. operatorów usług kluczowych (oczywiście tych niebędących operatorami infrastruktury krytycznej), dostawców usług cyfrowych, samorządu terytorialnego. Naukowa i Akademicka Sieć Komputerowa działa na podstawie ustawy z 30.4.2010 r. o instytutach badawczych. CSIRT NASK stanowi kontynuację CERT Polska, który powstał w 1996 r., będąc pierwszym w Polsce zespołem reagowania na incydenty. W zasadzie CSIRT NASK obejmuje swoją właściwością wszystkie incydenty zgłaszane przez podmioty, które nie są we właściwości CSIRT GOV i CSIRT MON (bez względu na kategorię zgłaszającego podmiotu – właściwe w przypadku incydentów o charakterze terrorystycznym, a w przypadku incydentów związanych z obronnością właściwy jest CSIRT MON). Nazywany jest tzw. CERT-em ostatniej szansy (*CERT of last resort*), gdyż każdy obywatel (w zasadzie szerzej – każda osoba fizyczna i każda jednostka organizacyjna) może zgłosić do niego incydent. Ponadto – w przypadku kiedy jakiś podmiot nie jest w stanie uzyskać bezpośredniego kontaktu lub oczekiwanej pomocy od podmiotu, który jest zaangażowany w incydent bezpośrednio – zgłaszający przekazuje zapytanie właśnie do CSIRT „ostatniej szansy" (*C. Banasiński*, *W. Nowak*, Europejski i krajowy, s. 161–162). CSIRT MON, CSIRT NASK lub CSIRT GOV, w przypadku otrzymania zgłoszenia incydentu spoza jego właściwości, przekazuje je niezwłocznie do właściwego CSIRT wraz z otrzymanymi informacjami. Instytucje te 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 (art. 26 ust. 1 CyberbezpU). CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT sektorowe współpracują ze sobą, z organami właściwymi do spraw cyberbezpieczeństwa, ministrem właściwym do spraw informatyzacji, CSIRT sektorowymi oraz Pełnomocnikiem, zapewniając spójny i kompletny system zarządzania ryzykiem na poziomie krajowym, realizując zadania na rzecz przeciwdziałania cyberzagrożeniom o charakterze ponadsektorowym i transgranicznym, a także zapewniając koordynację obsługi zgłoszonych incydentów. Ponadto CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowe oraz podmioty świadczące usługi z zakresu cyberbezpieczeństwa współpracują z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji

ich ustawowych zadań (art. 34 ust. 1 CyberbezpU), a koordynując obsługę incydentu, który doprowadził do naruszenia ochrony danych osobowych, współpracują z organem właściwym do spraw ochrony danych osobowych (art. 34 ust. 2 CyberbezpU). CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowe oraz dostawcy usług zarządzanych z zakresu cyberbezpieczeństwa współpracują z Prezesem Urzędu Lotnictwa Cywilnego, Prezesem UKE oraz KNF oraz z NBP w zakresie wymiany informacji o incydentach, podatnościach i cyberzagrożeniach, które mają wpływ na systemy płatności. Ustawa o krajowym systemie cyberbezpieczeństwa przewiduje szczególne zadania dla poszczególnych CSIRT uwzględniające ich specyfikę. Zespoły CSIRT stanowią poziom techniczny koordynacji obsługi incydentów oraz wskazują na przyjęcie przez polskiego ustawodawcę zdekoncentrowanego systemu w zakresie funkcjonowania CSIRT. W celu uniknięcia sporów kompetencyjnych ustawodawca określił właściwość zespołów reagowania na incydenty komputerowe. Zadania CSIRT uwzględniają przypisane poszczególnym CSIRT zakresy odpowiedzialności na potrzeby zarządzania cyberbezpieczeństwem państwa oraz zawierają katalogi obsługiwanych podmiotów tworzących krajowy system cyberbezpieczeństwa. Zakres kompetencyjny ma charakter przedmiotowo-podmiotowy. Koordynacja incydentów jest podstawowym zadaniem zespołów CSIRT. Jest ona konieczna dla prawidłowego wykonywania zadań, w szczególności kiedy incydent ma charakter ponadsektorowy. Ustawodawca zobowiązał zespoły CSIRT do przestrzegania swojej właściwości. Jeżeli CSIRT MON, CSIRT NASK lub CSIRT GOV otrzyma zgłoszenie incydentu od podmiotu, w stosunku do którego nie ma przypisanej właściwości do koordynacji, przekazuje niezwłocznie to zgłoszenie do właściwego CSIRT wraz z otrzymanymi informacjami. O przekazaniu zgłoszenia powinien także zostać poinformowany dokonujący zgłoszenia z uwagi na ciążące na nim obowiązki. W CyberbezpU została także przewidziana możliwość zawarcia przez CSIRT porozumień, w ramach których może dojść do modyfikacji ogólnej właściwości poszczególnych CSIRT. Podmioty te mogą także w drodze porozumienia powierzyć sobie wzajemnie wykonywanie zadań w stosunku do niektórych rodzajów podmiotów. W przypadku zawarcia takiego porozumienia CSIRT informuje o tym podmiot, w stosunku do którego nastąpiła zmiana podporządkowania. Komunikat powinien zawierać w szczególności: strony porozumienia; listę podmiotów, w stosunku do których następuje zmiana CSIRT; termin, od którego porozumienie obowiązuje; obowiązek poinformowania przez CSIRT podmiotów, których dotyczy porozumienie o jego zawarciu; adres strony internetowej, na której zostanie opublikowany tekst porozumienia. Ustawodawca polski nałożył na zespoły CSIRT MON, CSIRT NASK i CSIRT GOV obowiązek poinformowania innych państw członkowskich UE o incydentach, które na nie oddziałują. Obowiązek ten odnosi się do incydentów poważnych, zgłoszonych przez operatorów usług kluczowych. Przekazania informacji dokonuje się za pośrednictwem Pojedynczego Punktu Kontaktowego. Pojedynczy Punkt Kontaktowy służy komunikacji w ramach współpracy w UE. Wymiana informacji pomiędzy państwami członkowskimi UE służy realizacji celów dyrektywy NIS2 w zakresie osiągnięcia wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w UE. Przyjęcie przez polskiego ustawodawcę kilku podmiotów odpowiedzialnych za wykonywanie zadań związanych z bezpieczeństwem sieci i systemów informatycznych operatorów usług kluczowych

i dostawców usług cyfrowych – trzy CSIRT poziomu Krajowego: CSIRT MON, CSIRT NASK i CSIRT GOV – skutkowało obowiązkiem utworzenia zespołu, który będzie koordynował działania podejmowane przez CSIRT MON, CSIRT NASK, CSIRT GOV oraz Rządowe Centrum Bezpieczeństwa. CSIRT MON, CSIRT NASK i CSIRT GOV przekazują sobie wzajemnie informacje o incydencie krytycznym lub incydencie w cyberbezpieczeństwie na dużą skalę oraz informują o nim Rządowe Centrum Bezpieczeństwa, właściwy CSIRT sektorowy oraz ministra właściwego do spraw zagranicznych. W komentowanym artykule ustawodawca powołał Zespół do spraw Incydentów Krytycznych, w ramach którego następuje koordynacja działań CSIRT oraz wymiana informacji w przypadku zaistnienia incydentu krytycznego. Do wspólnych zadań CSIRT należy szacowanie ryzyka związanego z ujawnionym zagrożeniem cyberbezpieczeństwa oraz zaistniałymi incydentami, w tym prowadzenie dynamicznej analizy ryzyka. Analiza incydentu to jeden z najważniejszych etapów postępowania w przypadku wystąpienia incydentu. Jej odpowiednie przeprowadzenie może i powinno służyć wyciąganiu wniosków i uszczelnianiu systemów. Postępowanie w trakcie tego etapu powinno obejmować zabezpieczenie dowodów, przygotowanie dokumentacji zdarzenia, na podstawie której będzie następować późniejsza oraz ich faktyczna analiza. CSIRT zostały zobowiązane do przekazywania informacji dotyczących incydentów i ryzyk podmiotom krajowego systemu cyberbezpieczeństwa oraz wydawania komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. W przypadku incydentów o charakterze ponadsektorowym ustawodawca nakazał przekazanie do właściwego CSIRT informacji technicznych dotyczących incydentu, którego koordynacja obsługi wymaga współpracy CSIRT. W uzasadnionych przypadkach CSIRT zostały zobowiązane do przeprowadzenia 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.

3. **CSIRT sektorowy.** Dyrektywa NIS2 przewiduje harmonizację minimalną, tym samym nie uniemożliwia państwom członkowskim przyjęcia lub utrzymania przepisów zapewniających wyższy poziom cyberbezpieczeństwa, pod warunkiem że takie przepisy są spójne z obowiązkami państw członkowskich ustanowionymi w prawie Unii (art. 4). Państwa członkowskie mogą więc ustanowić dodatkowe wymagania i zasady. Dyrektywa NIS2 określa m.in. obowiązki państw członkowskich dotyczące przyjęcia krajowych strategii cyberbezpieczeństwa oraz wyznaczenia lub powołania właściwych organów, organów ds. zarządzania kryzysowego w cyberbezpieczeństwie, pojedynczych punktów kontaktowych ds. cyberbezpieczeństwa (Pojedyncze Punkty Kontaktowe) oraz zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) (art. 1 ust. 2 dyrektywy NIS2). Zgodnie z definicją jest to Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, działający na poziomie sektora lub podsektora, ustanowiony przez organ właściwy do spraw cyberbezpieczeństwa dla danego sek- **3**