KANCELARIA
SENATU

BIURO LEGISLACYJNE

Warszawa, 27 stycznia 2026 r.

Opinia do ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw

(druk nr 609)

I. Cel i przedmiot ustawy

Opiniowana ustawa ma na celu wdrożenie dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), zwanej dalej „dyrektywą NIS 2".

Dyrektywa NIS 2 zastąpiła dotychczasowy podział na operatorów usług kluczowych i dostawców usług cyfrowych określony w dyrektywie 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, zwanej dalej „dyrektywą NIS 1", wprowadzając podział na podmioty kluczowe i podmioty ważne. Ponadto rozszerzono katalog sektorów objętych dyrektywą. Dyrektywa NIS 2 nakłada również szereg obowiązków na podmioty kluczowe i podmioty ważne. Jako podstawowy obowiązek należy wskazać stosowanie odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców tych usług lub na inne usługi bądź minimalizowania takiego wpływu.

ul. Wiejska 6/8, 00-902 Warszawa, tel. 22 694 93 38, e-mail: Iwona.Kozera@senat.gov.pl

Jak podkreślono w uzasadnieniu do projektu ustawy (druk sejmowy nr 1955), zmiany wprowadzone przez dyrektywę NIS 2 oraz pojawiające się nowe cyberzagrożenia powodują konieczność wprowadzenia stosownych zmian w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Jest to podstawowy akt dotyczący cyberbezpieczeństwa w Polsce, który wdrożył dyrektywę NIS 1. Celem nowelizacji jest uspójnienie krajowego systemu cyberbezpieczeństwa z rozwiązaniami przyjętymi na poziomie Unii Europejskiej.

Nowelizacja polega w szczególności na:

1) rozszerzeniu katalogu podmiotów krajowego systemu cyberbezpieczeństwa o nowe sektory gospodarki tj. zarządzania technologią informacyjno-komunikacyjną (ICT), przestrzeni kosmicznej, poczty, produkcji, w tym produkcji i dystrybucji chemikaliów, żywności oraz gospodarowania ściekami;
2) nałożeniu obowiązków z zakresu środków zarządzania ryzykiem na podmioty kluczowe oraz podmioty ważne w cyberbezpieczeństwie, dotyczących stosowania odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych służących zarządzaniu ryzykiem dla bezpieczeństwa sieci i systemów informatycznych;
3) uregulowaniu zasad odpowiedzialności kierownika podmiotu kluczowego lub podmiotu ważnego za realizację zadań z zakresu cyberbezpieczeństwa – kierownik takiego podmiotu będzie odpowiedzialny za realizację zadań przez dany podmiot, a w przypadku niewywiązania się z obowiązków na kierownika będą mogły być nałożone kary; kierownik będzie również obowiązany do odbycia stosownego szkolenia z zakresu cyberbezpieczeństwa;
4) wprowadzeniu możliwości zgłaszania incydentów przez podmioty kluczowe i podmioty ważne, za pomocą systemu teleinformatycznego ministra właściwego do spraw informatyzacji, zwanego dalej „ministrem”, do właściwych zespołów CSIRT sektorowych i CSIRT poziomu krajowego;
5) utworzeniu zespołów CSIRT sektorowych w poszczególnych sektorach gospodarki, które będą wspierać podmioty kluczowe i podmioty ważne w obsłudze incydentów cyberbezpieczeństwa;
6) wzmocnieniu kompetencji nadzorczych organów właściwych do spraw cyberbezpieczeństwa; wzmocnienie kompetencji obejmuje umożliwienie wydawania ostrzeżeń, wyznaczania urzędnika monitorującego wykonywanie obowiązków przez dany podmiot kluczowy, nakazywania przeprowadzenia oceny bezpieczeństwa systemu informacyjnego lub audytu bezpieczeństwa;

7) wprowadzeniu kar pieniężnych za niewykonanie obowiązków ustawowych przez podmioty kluczowe lub podmioty ważne, m.in. za niewdrożenie systemu zarządzania bezpieczeństwem informacji czy niezarejestrowanie się w wykazie podmiotów kluczowych i podmiotów ważnych;
8) wprowadzeniu Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę;
9) rozszerzeniu kompetencji ministra – organ ten będzie mógł dokonać, w drodze decyzji, prawnej identyfikacji dostawcy wysokiego ryzyka, będzie mógł też wydać polecenie zabezpieczające ze wskazaniem zachowania, które ograniczy skutki trwającego incydentu krytycznego;
10) wzmocnieniu pozycji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa poprzez:
    a) zapewnienie możliwości żądania od organów administracji rządowej informacji niezbędnych do wykonywania jego zadań;
    b) przyznanie uprawnienia do zlecania wykonania badań niezbędnych do realizacji zadań;
    c) wprowadzenie możliwości dokonywania zakupu oprogramowania z zakresu cyberbezpieczeństwa dla uczestników posiedzeń Połączonego Centrum Operacyjnego Cyberbezpieczeństwa;
    d) utrzymanie w mocy rekomendacji mających na celu wzmocnienie poziomu cyberbezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa, jak i uprawnienia do ich wydawania;
11) rozszerzeniu kompetencji zespołów CSIRT poziomu krajowego, w tym CSIRT NASK, co jest związane ze zwiększoną liczbą podmiotów kluczowych i podmiotów ważnych, którym CSIRT NASK będzie udzielał wsparcia w reagowaniu na incydenty;
12) rozwijaniu kompetencji ministra w zakresie edukacji cyberbezpieczeństwa – przewiduje się środki na prowadzenie kampanii edukacyjnych i programów z zakresu cyberbezpieczeństwa.

Nowelizacja ma ponadto na celu podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym.

W ustawie nałożono obowiązki na podmioty kluczowe i podmioty ważne zgodne z wykazem tych podmiotów wskazanym w załączniku nr 1 i 2 do dyrektywy NIS 2. Podmioty te będą obowiązane do dokonania samorejestracji w wykazie podmiotów kluczowych lub

podmiotów ważnych, co umożliwi ich identyfikację, zapewni ich aktywne wsparcie przez zespoły CSIRT sektorowe i zespoły CSIRT poziomu krajowego oraz ułatwi wykonywanie czynności nadzorczych przez organy właściwe do spraw cyberbezpieczeństwa. Zmiana ta zapewni także przekazywanie danych o liczbie tych podmiotów do Komisji Europejskiej oraz Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa.

Podmioty kluczowe i podmioty ważne będą obowiązane do wdrożenia systemu zarządzania bezpieczeństwem informacji w procesach służących świadczeniu usług przez te podmioty. Podmioty kluczowe obowiązane będą przeprowadzać audyty bezpieczeństwa co trzy lata. Możliwe będzie także zlecenie przeprowadzenia audytu doraźnego.

Zmiany dotyczące zgłaszania incydentów poważnych polegają w szczególności na wprowadzeniu dwuetapowego zgłaszania incydentu. W pierwszej kolejności podmiot kluczowy lub podmiot ważny będzie zgłaszał do CSIRT sektorowego wczesne ostrzeżenie o incydencie poważnym (w ciągu 24 godzin od momentu wykrycia). Kolejnym krokiem będzie zgłoszenie incydentu poważnego (w ciągu 72 godzin od momentu wykrycia). Zgłoszenie wczesnego ostrzeżenia będzie mogło zawierać wniosek o wskazanie wytycznych dotyczących możliwych do wdrożenia środków ograniczających skutki incydentu poważnego lub o wsparcie techniczne przy obsłudze incydentu. CSIRT sektorowy zobowiązany będzie do udzielenia wsparcia zgodnie z treścią wniosku w ciągu 24 godzin. W trakcie obsługi incydentu poważnego podmiot zgłaszający incydent, na wniosek CSIRT sektorowego, przekaże sprawozdanie okresowe z obsługi tego incydentu. Natomiast sprawozdanie końcowe przekazywane będzie nie później niż w terminie miesiąca od dnia zgłoszenia incydentu.

Progi uznania incydentu za incydent poważny zostaną określone przez Radę Ministrów, w drodze rozporządzenia. Zgłoszenie incydentu będzie dokonywane za pośrednictwem systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. System ten ma być głównym środkiem komunikacji pomiędzy podmiotami krajowego systemu cyberbezpieczeństwa.

Krajowy Plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę będzie nowym dokumentem strategicznym przyjmowanym w drodze uchwały Rady Ministrów. Dokument ten będzie określał zasady postępowania w przypadku wystąpienia takiego incydentu oraz zasady współpracy między organami realizującymi zadania z zakresu cyberbezpieczeństwa a organami właściwymi do spraw zarządzania kryzysowego.

Minister, w drodze postępowania administracyjnego, będzie mógł uznać dostawcę produktów ICT, usług ICT lub procesów ICT za dostawcę wysokiego ryzyka. Sprzęt takiego dostawcy będzie musiał być wycofany z systemów podmiotów kluczowych lub podmiotów ważnych, a nowy sprzęt tego dostawcy nie będzie mógł być wprowadzany do użytku.

Ponadto minister będzie mógł wydać, w drodze decyzji administracyjnej, polecenie zabezpieczające w przypadku wystąpienia incydentu krytycznego. Zawarte w nim będzie wskazanie określonego zachowania, które będzie miało na celu zmniejszenie skutków incydentu lub zapobieżenie jego rozprzestrzenianiu się, do wdrożenia, którego będzie obowiązany podmiot objęty procedurą.

Określone zostały również sposoby nadzoru, które w głównej mierze sprowadzają się do prowadzenia kontroli oraz nakładania kar pieniężnych na podmioty kluczowe i podmioty ważne. Organy właściwe do spraw cyberbezpieczeństwa będą w szczególności mogły wydawać ostrzeżenia, nakazy i decyzje administracyjne nakazujące podjęcie albo zaniechanie określonego działania. Organy te zostaną również wyposażone w środki, które znajdą zastosowanie w sytuacji, w której podmiot kluczowy lub podmiot ważny nie wykona w terminie postanowień określonych w ostrzeżeniu, nakazie czy decyzji. Wprowadza się również katalog kryteriów, które organ właściwy do spraw cyberbezpieczeństwa będzie musiał przeanalizować w celu podjęcia działań nadzorczych i egzekwowania przepisów, w tym także nakładania kar pieniężnych.

Minister właściwy do spraw energii będzie organem właściwym w rozumieniu rozporządzenia delegowanego Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniającego rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej.

Poza ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa nowela zmienia następujące akty prawne: ustawę z dnia 8 marca 1990 r. o samorządzie gminnym, ustawę z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej, ustawę z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej, ustawę z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym, ustawę z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa, ustawę z dnia 5 czerwca 1998 r. o samorządzie województwa, ustawę z dnia 5 czerwca 1998 r. o samorządzie powiatowym, ustawę z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych, ustawę z dnia 24 maja 2000 r. o Krajowym Rejestrze

Karnym, ustawę z dnia 21 grudnia 2000 r. o dozorze technicznym, ustawę z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, ustawę z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym, ustawę z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, ustawę z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych, ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych, ustawę z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa, ustawę z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej, ustawę z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej oraz ustawę z dnia 12 lipca 2024 r. – Przepisy wprowadzające ustawę – Prawo komunikacji elektronicznej.

W ustawie zamieszczono przepisy przejściowe i dostosowujące, w których uregulowano wpływ nowelizacji na stosunki powstałe pod działaniem ustaw dotychczasowych oraz sprawy związane z dostosowaniem do znowelizowanych ustaw jej adresatów, w tym organów i instytucji. Ponadto sformułowano regułę wydatkową określającą maksymalne limity wydatków budżetu państwa dla poszczególnych części budżetowych, będących skutkiem finansowym wejścia w życie nowelizacji.

Ustawa wejdzie w życie po upływie miesiąca od dnia ogłoszenia.

II. Przebieg prac legislacyjnych

Sejm uchwalił ustawę na 50. posiedzeniu w dniu 23 stycznia 2026 r. Projekt ustawy został wniesiony do Sejmu przez Radę Ministrów w dniu 7 listopada 2025 r. Pierwsze czytanie projektu ustawy odbyło się na 46. i 47. posiedzeniu Sejmu w dniach 4 i 5 grudnia 2025 r. Projekt ustawy został skierowany do Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii. Komisja, po rozpatrzeniu projektu ustawy na posiedzeniach w dniach 17 grudnia 2025 r. oraz 8 i 9 stycznia 2026 r., wniosła o jego uchwalenie w brzmieniu zawartym w sprawozdaniu (druk sejmowy nr 2139). Na etapie prac w komisji wprowadzono do projektu liczne zmiany mające charakter doprecyzowujący, uściślający i techniczno-legislacyjny. Zmiany te nie zmieniły meritum rozwiązań zaproponowanych w projekcie.

Podczas drugiego czytania projektu ustawy, które odbyło się na 50. posiedzeniu Sejmu w dniu 21 stycznia 2026 r., zgłoszono wniosek o odrzucenie projektu ustawy oraz 17 poprawek

(druk sejmowy nr 2139-A). Wniosek o odrzucenie projektu ustawy nie uzyskał poparcia Sejmu. Natomiast część zgłoszonych poprawek takie poparcie uzyskała.

Za uchwaleniem projektu ustawy opowiedziało się 407 posłów, 10 było przeciw, zaś 17 posłów wstrzymało się od głosowania.

III. Uwagi

Ze względu na ograniczony czas na sporządzenie opinii w sprawie ustawy oraz szczegółowy i specjalistyczny charakter tego aktu prawnego, przedstawiona opinia nie stanowi pełnej i wszechstronnej analizy wszystkich techniczno-legislacyjnych i merytorycznych aspektów nowelizacji.

1) Zgodnie z § 84 Zasad techniki prawodawczej, jeżeli zmiany wprowadzane w ustawie miałyby być liczne albo miałyby naruszać konstrukcję lub spójność ustawy albo gdy ustawa była już poprzednio wielokrotnie nowelizowana, opracowuje się projekt nowej ustawy. Biorąc pod uwagę szeroki i wieloaspektowy zakres zmian wprowadzanych nowelą do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, obejmujący w szczególności modyfikację zakresu przedmiotowego i podmiotowego, istotne zmodyfikowanie katalogu definicji określeń ustawowych, wprowadzenie nowych mechanizmów nadzorczych, rozszerzenie kompetencji organów administracji publicznej i modyfikację relacji pomiędzy kluczowymi instytucjami systemu cyberbezpieczeństwa, prowadzący w istocie do zmiany modelu regulacyjnego, właściwym rozwiązaniem byłoby przygotowanie projektu nowej ustawy w miejsce nowelizacji.

2) art. 1 pkt 4 lit. c, art. 2 pkt 4f – definicja wymaga doprecyzowania poprzez wskazanie konkretnego przepisu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, który odnosi się do określenia „świadczenie usługi drogą elektroniczną”. Dodatkowo należy usunąć zbędny wyraz.

   Propozycja poprawki:

w art. 1 w pkt 4 w lit. c, w pkt 4f:

a) skreśla się wyraz „świadczoną”,

b) wyraz „przepisów” zastępuje się wyrazami „art. 2 pkt 4”;

3) art. 1 pkt 14 (art. 7j ust. 2), art. 1 pkt 64 (art. 53e ust. 16), art. 1 pkt 66 (art. 56 ust. 3), art. 2 pkt 1 lit. b (art. 10a pkt 3), art. 7 pkt 1 lit. b (art. 8c pkt 3) i art. 8 pkt 1 lit. b (art. 6a pkt 3) – w wymienionych przepisach sformułowano odesłanie do „odrębnych przepisów" albo „odrębnych ustaw". Takie blankietowe odesłanie nie spełnia standardów określonych w § 156 Zasad techniki prawodawczej oraz jest niezgodne z dobrą praktyką legislacyjną[1)]. W przepisach należy unikać posługiwania się wyrażeniem „przepisy odrębne", ponieważ jest to niewłaściwa metoda konstruowania odesłań. Nie informuje bowiem precyzyjnie adresata aktu, które normy ma w danej sytuacji zastosować. Należałoby zatem wskazać konkretne akty prawne, do których się odsyła albo zrezygnować z odesłania w tych przypadkach, w których nie ma ono wartości normatywnej. Sformułowanie propozycji poprawek wymagać będzie ustalenia do jakich przepisów należałoby odesłać.

4) art. 1 pkt 19 lit. a tiret czwarte (art. 11 ust. 1 pkt 4c), art. 1 pkt 21 (art. 12b ust. 2), art. 1 pkt 26 (art. 16c ust. 3), art. 1 pkt 28 lit. d (art. 26 ust. 2b), art. 1 pkt 76 (art. 67c ust. 2), art. 24 ust. 2 pkt 1 – w wymienionych przepisach należałoby uporządkować terminologię w zakresie stosowania sformułowań „w terminie" i „w ciągu". Ustawodawca co do zasady konsekwentnie posługuje się sformułowaniem „w terminie" w odniesieniu do dni, miesięcy i lat oraz określeniem „w ciągu" w odniesieniu do upływu określonej liczby godzin.

Ponadto w art. 24 ust. 2 pkt 1 użyto sformułowania „w ciągu" w innym znaczeniu niż w pozostałych przepisach. W tym przypadku „w ciągu" jest synonimem określenia „w okresie". Mając na uwadze § 10 Zasad techniki prawodawczej niżej proponuje się stosowną korektę terminologiczną.

Dodatkowo warto zwrócić uwagę, że w art. 16c w ust. 3 (art. 1 pkt 26 noweli) wskazano, że rejestry nazw domen najwyższego poziomu (TLD) oraz podmioty świadczące usługi rejestracji nazw domen udzielają odpowiedzi nie później niż w terminie **72 godzin od dnia** otrzymania żądania udostępnienia danych. W związku z tym przepisem może powstać wątpliwość w jaki sposób należy liczyć upływ 72 godzin. Wydaje się, że w przepisie należałoby wskazać, że 72 godziny powinny być liczone **od momentu** otrzymania żądania udostępnienia danych, a nie od **dnia** jego otrzymania.

---

1) Dobra praktyka legislacyjna nr 20; https://rcl.gov.pl/wp-content/uploads/2020/11/artykul_20.pdf

Ewentualnie można by przesądzić, że dane należy przekazać w terminie 3 dni od dnia otrzymania żądania.

Propozycja poprawek:

w art. 1:

a) w pkt 19 w lit. a w tiret czwartym, w pkt 4c,

b) w pkt 21, w art. 12b w ust. 2,

c) w pkt 28 w lit. d, w ust. 2b,

d) w pkt 76, w art. 67c w ust. 2

– wyrazy „w ciągu” zastępuje się wyrazami „w terminie”;

w art. 1 w pkt 26, w art. 16c w ust. 3 wyrazy „w terminie” zastępuje się wyrazami „w ciągu” oraz skreśla się wyraz „dnia”;

albo

w art. 1 w pkt 26, w art. 16c w ust. 3 wyrazy „72 godzin” zastępuje się wyrazami „3 dni”;

w art. 24 w ust. 1 w pkt 1 wyrazy „w ciągu” zastępuje się wyrazami „w okresie”;

5) art. 1 pkt 26, art. 16h pkt 1 – przepis ten powinien być skorelowany terminologicznie z art. 11 ust. 1 pkt 4–4c. Zgodnie z art. 11 ust. 1 wczesne ostrzeżenie o incydencie poważnym oraz incydent poważny są zgłaszane, natomiast sprawozdania są przekazywane, a nie zgłaszane.

Propozycja poprawki:

w art. 1 w pkt 26, w art. 16h w pkt 1 wyrazy „zgłoszenie incydentu poważnego, sprawozdanie” zastępuje się wyrazami „incydent poważny oraz przekazuje sprawozdanie”;

6) art. 1 pkt 33, art. 31 ust. 1 i 3 – należy uporządkować zakres odesłań w nowelizowanym art. 31 ust. 1 z uwagi na to, że art. 11 mówi o przekazywaniu zgłoszeń, zaś art. 13

o przekazywaniu informacji. Przepis odsyłający sugeruje, że o zgłoszeniach stanowi art. 13, a o przekazywaniu informacji art. 11.

Dodatkowo nieprecyzyjne jest również odesłanie w nowelizowanym art. 31 ust. 3. Wynika z niego, że w art. 13 jest mowa jest o zgłoszeniu. Zakresu odesłania nie da się w tym przypadku pogodzić z treścią przepisu, do którego się odsyła.

Poza tym w nowelizowanym art. 31 ust. 1 mówi się o przekazywaniu zgłoszeń, zaś w ust. 3 tego artykułu o dokonywaniu zgłoszeń. Różnica terminologiczna stanowi naruszenie § 10 Zasad techniki prawodawczej, zgodnie z którym do oznaczenia jednakowych pojęć używa się jednakowych określeń.

Propozycja poprawki:

w art. 1 w pkt 33, w art. 31:

a) w ust. 1 wyrazy „przekazywania informacji i zgłoszeń, o których mowa w art. 11 i w art. 13” zastępuje się wyrazami „dokonywania zgłoszeń, o których mowa w art. 11, i przekazywania informacji, o których mowa w art. 13”,

b) w ust. 3 „odpowiednio w art. 11, art. 13 i art. 30 ust. 1,” zastępuje się wyrazami „w art. 11, i art. 30 ust. 1, oraz przekazywania informacji, o których mowa w art. 13,”;

7) art. 1 pkt 39, art. 36b ust. 8 – należy usunąć zbędne wyrazy.

Propozycja poprawki:

w art. 1 w pkt 39, w art. 36b w ust. 8 skreśla się wyrazy „w związku z § 1”;

8) art. 1 pkt 42 – celem przepisu jest zastąpienie wyrażenia „sektorowy zespół cyberbezpieczeństwa” wyrażeniem „CSIRT sektorowy”. W art. 44 w ust. 3 zmieniane wyrażenie jest dwukrotnie zapisane wielką literą i dlatego jego modyfikacja powinna być dokonana odrębnym przepisie zmieniającym.

Ponadto kierując się dyrektywą § 10 Zasad techniki prawodawczej, zgodnie z którą do oznaczenia jednakowych pojęć używa się jednakowych określeń, należy w całej ustawie posługiwać się wyłącznie określeniem – „CSIRT sektorowy”. Co więcej, wprowadzenie skrótu oznacza – co do zasady – konieczność posługiwania się nim konsekwentnie w obrębie całego aktu.

Jednocześnie w art. 46 doprecyzowania wymaga przywołana podstawa prawna powołania przekształcanych sektorowych zespołów cyberbezpieczeństwa.

Propozycja poprawek:

w art. 1:

a) w pkt 42 skreśla się wyrazy „w art. 44 w ust. 3 w zdaniu pierwszym i drugim,”,

b) w pkt 48 po lit. c dodaje się lit. ca w brzmieniu:

„ca) w ust. 3 w zdaniu pierwszym i drugim wyrazy „Sektorowy zespół cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowy”,

c) w pkt 88 w lit. b, w art. 11 w pkt 4 wyrazy „sektorowego zespołu cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowego”,

d) w art. 46 po wyrazach „art. 44 ustawy zmienianej w art. 1” dodaje się wyrazy „ , w brzmieniu dotychczasowym,”;

9) art. 1 pkt 46 lit. a tiret pierwsze, art. 42 ust. 1 pkt 3 – zmieniany art. 42 ust. 1 pkt 3 zawiera odesłanie do art. 71 ust. 1. Przepis, do którego następuje odesłanie, po pierwsze nie odnosi się do decyzji o uznaniu podmiotu za podmiot kluczowy lub podmiot ważny, a po drugie nie istnieje. Przepis art. 71 w nowym brzmieniu jest bowiem bezustępowy. Odesłanie jest zbędne również z uwagi na to, że nie ma ono żadnej wartości normatywnej.

Propozycja poprawki:

w art. 1 w pkt 46 w lit. a w tiret pierwszym, w pkt 3 skreśla się wyrazy „ , o której mowa w art. 71 ust. 1”;

10) art. 1 pkt 49, art. 44e w ust. 1 i 2 – wskazane przepisy odnosząc się do zawarcia porozumienia powinien odsyłać do art. 44b ust. 4. Odsyła on natomiast do art. 44b ust. 3, który dotyczy ogłaszania komunikatu, w przypadku gdy powierzenie zadań odbywa się w drodze decyzji.

Propozycja poprawki:

w art. 1 w pkt 49, w art. 44e w ust. 1 we wprowadzeniu do wyliczenia i w ust. 2 wyrazy „art. 44b ust. 3” zastępuje się wyrazami „art. 44b ust. 4”;

11) art. 1 pkt 53 lit. a titet drugie, art. 46 ust. 1 pkt 7 – dodawany przepis powinien zawierać odesłanie do art. 55 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, a nie do jej art. 44, który przesądza, że przepisy ustawy dotyczące odpowiedzialności karnej Prezesa Urzędu Ochrony Danych Osobowych stosuje się odpowiednio do odpowiedzialności za wykroczenia. Natomiast art. 55 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych stanowi, że Prezes Urzędu Ochrony Danych Osobowych może prowadzić system teleinformatyczny umożliwiający administratorom dokonywanie zgłoszenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 rozporządzenia 2016/679.

Propozycja poprawki:

w art. 1 w pkt 53 w lit. a w tiret drugim, w pkt 7 wyrazy „art. 44” zastępuje się wyrazami „art. 5”;

12) art. 1 pkt 77, art. 69 ust. 2 pkt 6 i 9 – opiniowana ustawa w art. 1 pkt 16 (zmieniany art. 8 ust. 1 lit. j) i w dodawanym załączniku nr 4 posługuje się pojęciem „cyberhigieny”, natomiast w art. 1 pkt 77 (zmieniany art. 69 ust. 1 pkt 6 i 9) posługuje się pojęciem „higieny cyfrowej”. Mając na uwadze § 10 ZTP statuujący zasadę konsekwencji terminologicznej (do oznaczenia jednakowych pojęć używa się jednakowych określeń) ustawodawca powinien używać w przepisach ustawy tylko jednego z tych określeń. W związku z tym rekomendowane jest przyjęcie poniższej poprawki. Ponadto należy podkreślić, że pojęcia „cyberhigiena” oraz „higiena cyfrowa” nie zostały zdefiniowane. Mając na uwadze § 146 ust. 1 pkt 2 i 3 Zasad techniki prawodawczej, które stanowią, że definicję danego określenia formułuje się w przypadku, gdy określenie to jest nieostre i wymagane jest ograniczenie tej nieostrości, oraz gdy określenie to nie jest powszechnie zrozumiałe, należałoby rozważyć sformułowanie definicji pojęcia „cyberhigieny”. Sformułowanie definicji „cyberhigieny” jest możliwe w oparciu o przepisy dyrektywy (UE) 2022/2555, posługującej się pojęciem „polityka cyberhigieny”. Sformułowanie ewentualnej poprawki w tym zakresie będzie możliwe po uzyskaniu wyjaśnień wnioskodawcy opiniowanej ustawy.

Propozycja poprawki:

w art. art. 1 w pkt 77, w art. 69 w ust. 2 w pkt 6 i 9 wyrazy „higieny cyfrowej” zastępuję się

wyrazem „cyberhigieny”;

13) art. 1 pkt 64, art. 53a – zgodnie z art. 53a ust. 2 zakres nadzoru na podmiotami kluczowymi, sposób jego przeprowadzania oraz kryteria oceny zostaną określone w metodykach nadzoru. Należy zauważyć, że elementy metodyk nadzoru w praktyce będą bezpośrednio wpływać na sytuację prawną podmiotów nadzorowanych**,** determinując zakres ich obowiązków, sposób weryfikacji ich realizacji oraz przesłanki negatywnej oceny w ramach nadzoru. Tym samym metodyki nadzoru nie będą miały wyłącznie charakteru wewnętrznego, organizacyjnego, lecz będą stanowić w istocie instrument konkretyzujący normy ustawowe, którego stosowanie może prowadzić do określonych konsekwencji prawnych po stronie podmiotów kluczowych i ważnych. W przypadku stworzenia metodyki nadzoru organy właściwe do spraw cyberbezpieczeństwa będą zobowiązane do jej stosowania oraz do okresowej oceny jej skuteczności, a następnie do dokonywania zmian w tej metodyce (art. 53a ust. 3 i 4). Oznacza to, że metodyka nadzoru stanie się trwałym elementem systemu prawa, a jej treść *de facto* będzie wyznaczać standardy zachowania wymagane od podmiotów nadzorowanych. Mając powyższe na uwadze, należy wskazać, że w sytuacji, gdy ustawodawca dopuszcza ustanawianie instrumentu, który w sposób wiążący wpływa na wykonywanie obowiązków ustawowych przez podmioty spoza administracji publicznej, instrument ten powinien stanowić przedmiot regulacji w przepisach powszechnie obowiązujących. Wynika to z obowiązującego w Rzeczypospolitej Polskiej systemu źródeł prawa art. 87 Konstytucji oraz z art. 92 ust. 1 Konstytucji, zgodnie z którym ustawy są wykonywane przez rozporządzenia. Pozostawienie organom administracji swobody w kształtowaniu metodyk nadzoru w formie aktów niebędących źródłami powszechnie obowiązującego prawa może prowadzić do naruszenia zasady demokratycznego państwa prawa (art. 2 Konstytucji), w szczególności zasady pewności prawa oraz zaufania obywateli do państwa i stanowionego przez nie prawa. W związku z powyższym zasadne jest przyjęcie rozwiązania, zgodnie z którym metodyki nadzoru byłyby określane w drodze rozporządzenia. Sformułowanie poprawki zawierającej upoważnienie ustawowe do wydania rozporządzenia będzie możliwe po wskazaniu przez wnioskodawcę organu właściwego do wydania rozporządzenia i wytycznych.

14) art. 1 pkt 64, art. 53d ust. 1 pkt 1 – stanowi, że urzędnik monitorujący w zakresie nadzorowania wykonywania przez podmiot kluczowych obowiązków, jest uprawniony między innymi do swobodnego wstępu i poruszania się po terenie podmiotu kluczowego. Biorąc pod uwagę, że celem przepisu jest umożliwienie urzędnikowi monitorującemu nadzorowanie wykonywania przez podmiot kluczowy obowiązków określonych w ustawie należy uznać, że urzędnik ten powinien mieć dostęp i możliwość poruszania się nie tylko po terenie, ale po wszystkich nieruchomościach podmiotu kluczowego, w tym po budynkach. Zgodnie z definicją słownikową za „teren" uznaje się wyłącznie „obszar ziemi"/„grunt". Natomiast zgodnie z art. 46 § 1 ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny, nieruchomościami są zarówno grunty (tereny) jak i budynki trwale z gruntem związane lub części takich budynków. W związku z powyższym rekomendowane jest przyjęcie poprawki mającej na celu umożliwienie wejścia oraz swobodnego poruszania się urzędnika monitorującego po wszystkich nieruchomościach podmiotu kluczowego.

Propozycja poprawki:

w art. 1 w pkt 64, w art. 53d w ust. 1 w pkt 1 wyraz „terenie" zastępuję się wyrazem „nieruchomościach";

~~15) *art. 1 pkt 64, art. 53e ust. 7 – przepis wskazuje 7-dniowy termin na rozpatrzenie wniosku podmiotu kluczowego o uchylenie decyzji o zastosowaniu środków wskazanych w art. 53 ust. 9, które mogą być stosowane* ***nie dłużej niż przez 14 dni od dnia doręczenia decyzji****. Biorąc pod uwagę, że przedmiotowa decyzja może obowiązywać przez okres nie dłuższy niż 14 dni, wątpliwości budzi 7-dniowy termin na rozpatrzenie wniosku o jej uchylenie.* ***Mimo tego, że podmiot kluczowy usunie naruszenia lub zaprzestanie dokonywania naruszeń po 7 dniach od wydania decyzji i złoży wniosek o uchylenie decyzji, decyzja ta będzie mogła obowiązywać do końca okresu na który została wydana****. Taka konstrukcja przepisu może naruszać wywodzącą się z demokratycznego państwa prawnego zasadę zaufania obywateli do państwa poprzez kreowanie uprawnień pozornych. Zgodnie z orzecznictwem Trybunału Konstytucyjnego ustawodawca nie może tworzyć konstrukcji normatywnych, które są niewykonalne, stanowią złudzenie prawa*~~

~~*i w konsekwencji dają jedynie pozór ochrony interesów jednostki.*~~[2)] ~~*W związku z tym rekomendowana jest poprawka eliminująca pozorność przyjętego rozwiązania.*~~

~~***Propozycja poprawki:***~~

~~*w art. 1 w pkt 64, w art. 53e w ust. 7 wyrazy „w terminie 7 dni od dnia” zastępuję się wyrazami „następnego dnia po dniu”;*~~

1~~5~~6) art. 16, art. 104 – przepis art. 104 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, w dotychczasowym brzmieniu, wyrażał zasadę, że środki z administracyjnej kary pieniężnej stanowią dochód budżetu państwa. Jest to norma powtórzona za art. 11 pkt 12 ustawy o finansach publicznych, mówiącym: „Dochodami podatkowymi i niepodatkowymi budżetu państwa są grzywny, mandaty i inne kary pieniężne, o ile odrębne ustawy nie stanowią inaczej”. Niniejsza ustawa wprowadza wyjątek od tej zasady, zawarty w ust. 2, że środki z kary, ale jedynie takiej, która została nałożona za naruszenie wskazanych w nim enumeratywnie przepisów rozporządzenia 2016/679 stanowią dochód w 50% budżetu państwa, a w 50% Funduszu Cyberbezpieczeństwa. Zgodnie z § 23 ust. 3 Zasad techniki prawodawczej „(…) przepis formułujący wyjątki lub uściślenia zamieszcza się bezpośrednio po danym przepisie szczegółowym”, tak jak to ma miejsce w analizowanym przypadku. Nie ulega wątpliwości, że nowelizowany art. 104 ust. 2 stanowi *lex specialis* (w tym wypadku wyjątek) w stosunku do ogólnej zasady wyrażonej w ust. 1. Sformułowanie „z uwzględnieniem ust. 2” należy zatem uznać za zbędne i legislacyjnie wadliwe.

Poza tym należy stwierdzić, że w analizowanym przepisie określenia „z uwzględnieniem” użyto w znaczeniu „z wyjątkiem”. Odesłanie jest w związku z tym nieprecyzyjne i niezgodne z intencją prawodawcy.

Analizując nowelizowany art. 104 ust. 1 i zastosowane w nim odesłanie, należy mieć także na względzie ustalenia międzyinstytucjonalne oraz poglądy doktryny,[3)] zgodnie z którymi:

[2)] ~~Wyrok Trybunału Konstytucyjnego z 8 stycznia 2013 r., sygn. akt K 18/10.~~

[3)] Zob.:

1) rekomendacje nr 25 i 26 [w:] Rekomendacje dla legislatorów dotyczące wybranych zagadnień legislacyjnych, zaakceptowane przez kierownictwo Rządowego Centrum Legislacji, Biura Legislacyjnego Kancelarii Sejmu oraz Biura Legislacyjnego Kancelarii Senatu, po szkoleniu „Ujednolicanie praktyki legislacyjnej rządowych i parlamentarnych służb legislacyjnych” – Jachranka, wrzesień/październik 2011r. Źródło: http://bip.ksap.gov.pl/pliki/ORikU_ba_260_6_2019/zalacznik_do_wyjasnien.pdf.

a) w przypadku gdy przepis formułujący wyjątek albo uściślenie od któregoś z elementów przepisu szczegółowego nie zostanie (z jakiegoś powodu) zamieszczony bezpośrednio po danym przepisie szczegółowym (§ 23 ust. 3 Zasad techniki prawodawczej), a jest to konieczne do wyrażenia intencji prawodawcy w sposób zrozumiały dla adresatów norm, określa się relację pomiędzy przepisami (wskazuje się wyraźnie przepis, w którym sformułowano wyjątek albo uszczegółowienie),

b) w przypadku konieczności wskazania, że wyjątek od któregoś z elementów przepisu szczegółowego sformułowano **w przepisie szczegółowym innym niż przepis zamieszczony bezpośrednio po danym przepisie szczegółowym**, używa się zwrotu „z wyjątkiem określonym w art. …”,

c) w przypadku konieczności wskazania, że uściślenie któregoś z elementów przepisu szczegółowego sformułowano **w przepisie szczegółowym innym niż przepis zamieszczony bezpośrednio po danym przepisie szczegółowym**, używa się zwrotu „z uwzględnieniem art. …”,

Propozycja poprawki:

w art. 16, w art. 104 w ust. 1 skreśla się wyrazy „, z uwzględnieniem ust. 2”;

1~~7~~6) art. 32 – zgodnie z tym przepisem dotychczasowe przepisy wykonawcze wydane na podstawie art. 11 ust. 4 i art. 66 ust. 9 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, zachowają moc do dnia wejścia w życie nowych przepisów wykonawczych wydanych na podstawie wymienionych przepisów w nowym brzmieniu, nie dłużej niż przez 12 miesięcy od dnia wejścia w życie nowelizacji **i będą mogły być zmieniane na podstawie tych przepisów**.

Z § 34 Zasad techniki prawodawczej wynika, że nie nowelizuje się aktu wykonawczego zachowanego czasowo w mocy przez nową ustawę, chyba że ustawa ta wyraźnie przewiduje taką możliwość. W związku z tym, że podstawą obowiązywania aktu wykonawczego czasowo utrzymanego w mocy jest przepis przejściowy, który

---

2) M. Kłodawski [w:] Określanie relacji między przepisami prawnymi za pomocą zwrotu „z zastrzeżeniem” i zwrotów podobnych z perspektywy teorii i praktyki tworzenia prawa [w:] Doskonalenie i standaryzacja procesu legislacyjnego – dobre praktyki opracowane w ramach projektu LEGIS, Wydawnictwo KSAP, Warszawa 2019 r., s. 479.

utrzymał akt w mocy, oraz mając na uwadze, że przepis upoważniający do zmiany rozporządzenia powinien być (tak jak każdy przepis upoważniający) zgodny z art. 92 ust. 1 Konstytucji (powinien wskazywać organ wydający, zakres spraw przekazanych do uregulowania oraz wytyczne), za nieprawidłową należy uznać technikę zastosowaną w art. 32 opiniowanej ustawy.

Przepis ten nie określa precyzyjnie granic kompetencji prawotwórczej w zakresie nowelizowania dotychczasowych rozporządzeń. Prawidłowość przepisu można zapewnić poprzez odesłanie wprost do przepisów upoważniających, które należy wziąć pod uwagę szukając odpowiedzi na pytania, kto ma kompetencję prawotwórczą, co można uregulować w rozporządzeniu (zakres spraw) i jak ukształtować jego treść (wytyczne). Wskazane byłoby zatem przeredagowanie przepisu przejściowego.

Należałoby również określić, czy ustawodawca ma na myśli przepisy upoważaniające w dotychczasowym brzmieniu, czy też w brzmieniu nadanym nowelizacją.

Propozycja poprawki:

w art. 32 w części wspólnej wyliczenia wyrazy „na podstawie tych przepisów” zastępuje się wyrazami „w granicach określonych w art. 11 ust. 4 i art. 66 ust. 9 ustawy zmienianej w art. 1, w brzmieniu dotychczasowym”;

albo

w art. 32 w części wspólnej wyliczenia wyrazy „na podstawie tych przepisów” zastępuje się wyrazami „w granicach określonych w art. 11 ust. 4 i art. 66 ust. 9 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą”;

178) art. 33 ust. 3 zawiera wprowadzające w błąd sformułowanie, z którego wynika, że w art. 34 ust. 3 pkt 1 opiniowanej ustawy określony został harmonogram złożenia wniosków o wpis do wykazu, podczas gdy przepis ten stanowi jedynie ustawowe upoważnienie do ogłoszenia komunikatu określającego taki harmonogram.

Propozycja poprawki:

w art. 33 w ust. 3 wyrazy „art. 34 ust. 3 pkt 1” zastępuje się wyrazami „komunikacie, o którym mowa w art. 34 ust. 3”;

189) art. 44 ust. 1 i 2 – przepisy te w obecnym brzmieniu skutkują luką prawną, w wyniku której przepisy nie będą wskazywały adresata zgłoszeń incydentów poważnych pomiędzy „dniem wydania komunikatu” (ust. 1) a „dniem opublikowania komunikatu” (ust. 2). Zakładając racjonalność językową ustawodawcy, dzień wydania komunikatu i dzień opublikowania komunikatu oznaczając co innego. Gdyby oznaczały to samo ustawodawca użyłby w ust. 1 i 2 tego samego określenia (§ 10 Zasad techniki prawodawczej).

Propozycja poprawki:

w art. 44 w ust. 1 wyrazy „wydania” zastępuje się wyrazami „opublikowania”;

2019) propozycje poprawek redakcyjnych:

w art. 1 w pkt 16, w art. 8 w ust. 1 w pkt 5 w lit. d wyrazy „z uwzględnieniem konieczność” zastępuje się wyrazami „z uwzględnieniem konieczności”;

w art. 1 w pkt 64, w art. 53e w ust. 1 we wprowadzeniu do wyliczenia wyrazy „uprawnienie, o którym” zastępuję się wyrazami „uprawnienia, o których”;

w art. 1 w pkt 88 w lit. b, w ust. 11 we wprowadzeniu do wyliczenia wyraz „nadany” zastępuję się wyrazami „na dany”.

Iwona Kozera-Rytel – Główny legislator
Danuta Drypa – Główny legislator
Łukasz Makarski – Główny legislator
Adam Oleksy – Ekspert

Jakub Zabielski – Główny legislator

~~*Główny legislator*~~