

# **Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz**

Przejdź do produktu na [ksiegarnia.beck.pl](https://ksiegarnia.beck.pl)

## Spis treści

Autorzy . . . . .	XIII
Od Redaktorów . . . . .	XIX
Wykaz literatury . . . . .	XXI
Wykaz skrótów . . . . .	XXXI

### **Ustawa o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r. (Dz.U. z 2018 r. poz. 1560)**

<b>Tekst jednolity z dnia 29 grudnia 2025 r. (Dz.U. z 2026 r. poz. 20) . . . . .</b>	<b>1</b>
--	----------

<b>Rozdział 1. Przepisy ogólne . . . . .</b>	<b>1</b>
Art. 1. Zakres przedmiotowy . . . . .	1
Art. 2. Objaśnienie pojęć . . . . .	4
Art. 2a. Pojęcie usługi . . . . .	65
Art. 3. Cel regulacji . . . . .	68
Art. 3a. Wykrywanie źródła lub dokonywanie analizy aktywności . . . . .	70
Art. 4. Zakres podmiotowy . . . . .	72

<b>Rozdział 2. Identyfikacja i rejestracja podmiotów kluczowych lub podmiotów ważnych . . . . .</b>	<b>82</b>
Art. 5. Podmiot kluczowy . . . . .	82
Art. 5a. Zakres obowiązków . . . . .	92
Art. 6. ( <i>uchylony</i> ) . . . . .	95
Art. 7. Wykaz . . . . .	95
Art. 7a. Uzupełnianie danych . . . . .	103
Art. 7b. Zawiadomienie o wpisie do wykazu, wezwanie . . . . .	104
Art. 7c. Wniosek o wpis do wykazu . . . . .	105
Art. 7d. Wpis do wykazu . . . . .	108
Art. 7e. Aktualizacja danych . . . . .	110
Art. 7f. Wykreślenie podmiotu z wykazu . . . . .	110
Art. 7g. Udostępnianie danych . . . . .	111
Art. 7h. Informacja o uznaniu podmiotu kluczowego lub podmiotu ważnego za podmiot krytyczny . . . . .	113
Art. 7i. Aktualizacja danych . . . . .	113
Art. 7j. Wpis podmiotu do wykazu . . . . .	114
Art. 7k. Czynności sprawdzające . . . . .	115
Art. 7l. Uznanie za podmiot kluczowy lub podmiot ważny . . . . .	116
Art. 7m. Uznanie . . . . .	118

<b>Rozdział 3. Obowiązki podmiotów kluczowych lub podmiotów ważnych</b>	120
Art. 8. System zarządzania bezpieczeństwem informacji w systemie informacyjnym	120
Art. 8a. Upoważnienie ustawowe	153
Art. 8b. Stosowanie środków zarządzania ryzykiem	154
Art. 8c. Zakres odpowiedzialności	156
Art. 8d. Zakres zadań kierownika podmiotu kluczowego	158
Art. 8e. Szkolenie	159
Art. 8f. Wymagania	160
Art. 8g. Udostępnienie informacji dotyczących działalności	161
Art. 8h. Wymiana informacji, ostrzeżeń i zaleceń	163
Art. 8i. Wyłączenie zastosowania przepisów	167
Art. 8j. Uprawnienia służb specjalnych	169
Art. 9. Obowiązek wyznaczenia	170
Art. 10. Dokumentacja	173
Art. 11. Uznanie incydentu za poważny	178
Art. 12. Wczesne ostrzeżenie	193
Art. 12a. Sprawozdanie końcowe	197
Art. 12b. Sprawozdania	197
Art. 12c. Zastosowanie przepisów	198
Art. 13. Informacje	199
Art. 14. Realizacja zadań	201
Art. 15. Audyt bezpieczeństwa systemu informacyjnego	202
Art. 16. Termin realizacji obowiązków określonych w ustawie	208
Art. 16a. ( <i>uchylony</i> )	209
<b>Rozdział 3a. Obowiązki rejestrów nazw domen najwyższego poziomu oraz zadania i obowiązki podmiotów świadczących usługi rejestracji nazw domen</b>	209
Art. 16b. Baza danych dotycząca rejestracji nazw domen	209
Art. 16c. Udostępnianie danych	221
<b>Rozdział 3b. Wspólne wykonywanie obowiązków z zakresu cyberbezpieczeństwa przez podmioty publiczne</b>	225
Art. 16d. Realizacja obowiązków	225
Art. 16e. Jednostka odpowiedzialna za realizację obowiązków	226
Art. 16f. Współpraca	229
Art. 16g. Terminy na przekazanie informacji o incydentach	230
Art. 16h. Zakres zadań jednostki wyznaczonej	231
<b>Rozdziały 4–5. (<i>uchylone</i>)</b>	232
Art. 17–25. ( <i>uchylone</i> )	232
<b>Rozdział 6. Zadania CSIRT MON, CSIRT NASK i CSIRT GOV</b>	233
Art. 26. Zadania poszczególnych CSIRT	233
Art. 26a. Zgłoszenie podatności	258
Art. 26b. Udostępnienie listy	261

Art. 26c. Usługa online	262
Art. 26d. Wymagania	264
Art. 27. Właściwość CSIRT GOV i CSIRT MON	266
Art. 28. Informowanie innych państw członkowskich UE o zgłoszeniu incydentu poważnego	269
Art. 29. ( <i>uchylony</i> )	271
Art. 30. Zgłaszanie incydentów do CSIRT NASK	271
Art. 31. Alternatywne kanały zgłoszeń	273
Art. 32. Obsługa incydentu	274
Art. 33. Badanie produktu ICT lub usługi ICT	276
Art. 34. Współpraca z organami i służbami	281
Art. 35. Wzajemne przekazywanie informacji	283
Art. 35a. Wsparcie CSIRT koordynującego obsługę incydentu	286
Art. 36. Zespół ds. Incydentów Krytycznych	286
<b>Rozdział 6a. Ocena bezpieczeństwa</b>	289
Art. 36a. Ocena bezpieczeństwa	289
Art. 36b. Przeprowadzenie oceny	295
Art. 36c. Wykryta podatność	313
Art. 36d. Delegacja ustawowa	313
<b>Rozdział 7. Zasady udostępniania informacji i przetwarzania danych osobowych</b>	315
Art. 37. Ochrona informacji i danych osobowych	315
Art. 38. Informacje nieudostępniane	321
Art. 39. Przetwarzanie danych pozyskanych w związku z incydentami i zagrożeniami cyberbezpieczeństwa	325
Art. 40. Przetwarzanie informacji stanowiących tajemnice prawnie chronione	333
Art. 40a. Ocena wzajemna	336
<b>Rozdział 8. Organy właściwe do spraw cyberbezpieczeństwa</b>	338
Art. 41. Organy właściwe	338
Art. 41a. Organy właściwe do spraw cyberbezpieczeństwa w sektorze podmiotów publicznych	343
Art. 42. Zakres zadań	347
Art. 43. Wystąpienie o udzielenie informacji	355
Art. 44. CSIRT sektorowy	356
Art. 44a. Powierzenie realizacji zadań CSIRT sektorowego	362
Art. 44b. Powierzenie realizacji zadań CSIRT sektorowego przez ministra kierującego kilkoma działami administracji rządowej	364
Art. 44c. Powierzenie CSIRT poziomu krajowego realizacji zadań CSIRT sektorowego	367
Art. 44d. Finansowanie CSIRT sektorowego	368
Art. 44e. Obowiązki informacyjne dotyczące porozumień	370
Art. 44f. Sprawozdanie z funkcjonowania CSIRT sektorowego	372

<b>Rozdział 9. Zadania ministra właściwego do spraw informatyzacji</b>	373
Art. 45. Zadania ministra	373
Art. 45a. Wsparcie finansowe	379
Art. 45b. Podmiot odpowiedzialny	382
Art. 45c. Wybór projektów	383
Art. 46. Obowiązek zapewnienia rozwoju	384
Art. 46a. Zasady korzystania ze środków komunikacji elektronicznej	388
Art. 46b. Zawiadomienie o możliwości odebrania pisma	390
Art. 47. Delegowanie realizacji zadań na jednostki podległe lub nadzorowane przez ministra	392
Art. 48. Zadania Pojedynczego Punktu Kontaktowego	393
Art. 49. Dane przekazywane przez Pojedynczy Punkt Kontaktowy Grupy Współpracy	395
Art. 50. Dane przekazywane przez Pojedynczy Punkt Kontaktowy KE	400
<b>Rozdział 10. Zadania Ministra Obrony Narodowej</b>	401
Art. 51. Zadania ministra	401
Art. 52. Zadania Narodowego Punktu Kontaktowego do współpracy z Organizacją Traktatu	410
<b>Rozdział 10a. Zadania ministra właściwego do spraw energii</b>	417
Art. 52a. Właściwy organ	417
Art. 52b. Kontrole podmiotów zidentyfikowanych jako podmioty o krytycznym wpływie	418
<b>Rozdział 10b. Zadania ministra właściwego do spraw zagranicznych</b>	419
Art. 52c. Działalność dyplomatyczna	419
Art. 52d. Informacja	419
<b>Rozdział 10c. Organy odpowiedzialne za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę</b>	421
Art. 52e. Organ odpowiedzialny za zarządzanie incydentami i zarządzanie kryzysowe	421
Art. 52f. Podmiot odpowiedzialny	425
Art. 52g. Podmiot odpowiedzialny	426
Art. 52h. Koordynacja działań organów państwa zgodnie z Krajowym planem	426
<b>Rozdział 11. Nadzór i kontrola podmiotów kluczowych lub podmiotów ważnych</b>	427
Art. 53. Nadzór nad podmiotami kluczowymi i podmiotami ważnymi	427
Art. 53a. Metodyki nadzoru	438
Art. 53b. Hierarchia priorytetów w sprawowaniu nadzoru	439
Art. 53c. Obowiązek przekazania danych niezbędnych do wykonywania nadzoru	440
Art. 53d. Uprawnienia urzędnika monitorującego	442
Art. 53e. Elementy składowe decyzji; postępowanie w zakresie wydania decyzji	443

Art. 53f. Wspólne wykonywanie nadzoru . . . . .	446
Art. 54. Przepisy szczególne dotyczące wykonywania kontroli . . . . .	447
Art. 55. Uprawnienia osoby kontrolującej . . . . .	449
Art. 56. Obowiązki podmiotu kontrolowanego . . . . .	450
Art. 57. Postępowanie dowodowe . . . . .	452
Art. 58. Protokół kontroli . . . . .	453
Art. 59. Zalecenia pokontrolne . . . . .	456
Art. 59a. Podejrzenie naruszenia ochrony danych osobowych . . . . .	458
Art. 59b. Europejska współpraca administracyjna w ramach cyberbezpieczeństwa . . . . .	460
Art. 59c. Kontrola doraźna . . . . .	463
<b>Rozdział 12. Pełnomocnik i Kolegium . . . . .</b>	<b>465</b>
Art. 60. Pełnomocnik Rządu do Sprawy Cyberbezpieczeństwa . . . . .	465
Art. 61. Organ powołujący . . . . .	467
Art. 62. Zakres zadań Pełnomocnika . . . . .	468
Art. 62a. Połączone Centrum Operacyjne Cyberbezpieczeństwa . . . . .	475
Art. 63. Sprawozdanie, wnioski i rekomendacje . . . . .	479
Art. 64. Kolegium, forma organizacyjna . . . . .	480
Art. 65. Zakres zadań Kolegium . . . . .	481
Art. 65a. Zlecenie analiz . . . . .	485
Art. 66. Skład Kolegium . . . . .	486
Art. 67. Wytyczne dotyczące zapewnienia cyberbezpieczeństwa . . . . .	492
<b>Rozdział 12a. Szczególne działania na rzecz zapewnienia cyberbezpieczeństwa na poziomie krajowym . . . . .</b>	<b>495</b>
Art. 67a. Rekomendacje Pełnomocnika . . . . .	495
Art. 67b. Postępowanie w sprawie uznania za dostawcę wysokiego ryzyka . . . . .	497
Art. 67c. Wycofanie sprzętu lub oprogramowania . . . . .	504
Art. 67d. Wniosek . . . . .	507
Art. 67e. Skarga na decyzję . . . . .	510
Art. 67f. Obowiązek publikacyjny . . . . .	511
Art. 67g. Polecenie zabezpieczające . . . . .	512
Art. 67h. Obowiązek przekazania informacji . . . . .	520
Art. 67i. Skarga na polecenie zabezpieczające . . . . .	521
Art. 67j. Wyłączenie zastosowania przepisów . . . . .	522
Art. 67k. Nadzór i kontrola wykonywania obowiązków . . . . .	523
Art. 67l. Powierzenie realizacji wybranych zadań . . . . .	525
<b>Rozdział 13. Strategia . . . . .</b>	<b>527</b>
Art. 68. Przyjęcie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej . . . . .	527
Art. 69. Zakres Strategii . . . . .	532
Art. 70. Opracowanie projektu Strategii . . . . .	542
Art. 70a. Monitorowanie realizacji Strategii . . . . .	544
Art. 71. Okresowe przeglądy Strategii . . . . .	547
Art. 72. Przekazanie Strategii KE . . . . .	548

## Spis treści

<b>Rozdział 13a. Krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę</b> .....	549
Art. 72a. Krajowy plan .....	549
Art. 72b. Zakres .....	551
Art. 72c. Przekazywanie informacji o bieżącym stanie realizacji zadań wynikających z Krajowego planu .....	553
Art. 72d. Projekt Krajowego planu .....	554
Art. 72e. Aktualizacja planu .....	556
Art. 72f. Przekazywanie informacji .....	556
<b>Rozdział 14. Przepisy o karach pieniężnych</b> .....	557
Art. 73. Działania lub zaniechania podlegające karze pieniężnej; wysokość kary pieniężnej .....	557
Art. 73a. Nałożenie kary pieniężnej na kierownika podmiotu kluczowego lub podmiotu ważnego .....	568
Art. 73b. Nałożenie kary pieniężnej na inne podmioty .....	570
Art. 73c. Nałożenie kary pieniężnej na podmiot finansowy niebędący podmiotem kluczowym lub podmiotem ważnym .....	572
Art. 74. Procedura nałożenia kary pieniężnej; wpływy z kar pieniężnych jako przychód Funduszu Cyberbezpieczeństwa .....	574
Art. 75–76. ( <i>uchylone</i> ) .....	578
Art. 76a. Kryteria uwzględniane przy ustalaniu wysokości kary pieniężnej; uiszczenie kary pieniężnej .....	578
Art. 76b. Okresowa kara pieniężna .....	583
Art. 76c. Pouczenie w przypadku nałożenia kary pieniężnej przez Prezesa UODO .....	583
Art. 76d. Procedura nałożenia kary pieniężnej z wykorzystaniem pism generowanych automatycznie. Odesłanie do KPA .....	585
Art. 76e. Uzupełniające stosowanie przepisów KPA .....	586
<b>Rozdział 15. Zmiany w przepisach, przepisy przejściowe, dostosowujące i końcowe</b> .....	586
Art. 77–82. ( <i>pominięte</i> ) .....	586
Art. 83. Raport o zagrożeniach bezpieczeństwa narodowego .....	586
Art. 84. Powołanie Pełnomocnika .....	588
Art. 85. Zakres informacji przekazanych KE .....	588
Art. 86. Wydanie decyzji o uznaniu za operatora usługi kluczowej .....	589
Art. 87. Przekazanie sprawozdania podsumowującego .....	590
Art. 88. Przekazanie informacji KE .....	590
Art. 89. Uruchomienie systemu teleinformatycznego .....	591
Art. 90. Przyjęcie strategii .....	592
Art. 91. Roczny plan wdrożenia .....	592
Art. 92. Derogacja przepisów wykonawczych .....	593
Art. 93. Limit wydatków z budżetu państwa .....	594
Art. 94. Wejście w życie .....	601

## Spis treści

Odnośnik nr 1 .....	601
Odnośnik nr 2 .....	602
Załącznik nr 1 .....	602
Załącznik nr 2 .....	615
Załącznik nr 3 .....	619
Załącznik nr 4 .....	620

**Przejdź do księgarni →**

**ksiegarnia.beck.pl**