

# Spis treści

Wykaz skrótów .....	XV
Wykaz literatury .....	XIX
Wprowadzenie .....	XXI
<b>Komentarz do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560) .....</b>	<b>1</b>
<b>Rozdział 1. Przepisy ogólne .....</b>	<b>3</b>
<b>Art. 1. [Zakres przedmiotowy ustawy i wyłączenia podmiotowe] (J. Dysarz) .....</b>	<b>3</b>
I. Implementacja dyrektywy NIS .....	4
II. Zakres obowiązywania ustawy .....	5
III. Wyłączenia ustawowe .....	5
<b>Art. 2. [Słowniczek] (J. Dysarz) .....</b>	<b>6</b>
I. Uwagi ogólne .....	8
II. Cyberbezpieczeństwo .....	8
III. System teleinformatyczny a system informacyjny .....	10
IV. Incydent, rodzaje incydentów .....	11
V. Obsługa incydentu, zarządzanie incydemem .....	13
VI. Wokół ryzyka: ryzyko, szacowanie ryzyka zarządzanie ryzykiem, zagrożenie cyberbezpieczeństwa, podatność .....	14
VII. Zespoły CSIRT .....	14
VIII. Usługa kluczowa, usługa cyfrowa .....	14
<b>Art. 3. [Cel krajowego systemu cyberbezpieczeństwa] (J. Dysarz) .....</b>	<b>17</b>
<b>Art. 4. [Zakres podmiotowy] (W. Wąsowicz) .....</b>	<b>18</b>
I. Krajowy system cyberbezpieczeństwa .....	19
II. Podmioty publiczne w krajowym systemie cyberbezpieczeństwa .....	20
III. Szczególne uprawnienia podmiotów krajowego systemu cyberbezpieczeństwa .....	21
<b>Rozdział 2. Identyfikacja i rejestracja operatorów usług kluczowych .....</b>	<b>23</b>
<b>Art. 5. [Decyzja o uznaniu podmiotu za operatora usługi kluczowej] (W. Wąsowicz) .....</b>	<b>23</b>
I. Definicja operatora usługi kluczowej .....	24
II. Postępowanie w przedmiocie uznania za operatora usługi kluczowej .....	24

III. Działalność na terytorium Rzeczypospolitej Polskiej .....	25
IV. Sektory podstawowe dla cyberbezpieczeństwa .....	26
V. Świadczenie „usługi kluczowej” .....	26
VI. Decyzja o uznaniu za operatora usługi kluczowej .....	27
VII. Procedura odwoławcza .....	28
<b>Art. 6. [Upoważnienie ustawowe] (W. Wąsowicz)</b> .....	30
<b>Art. 7. [Wykaz operatorów usług kluczowych] (W. Wąsowicz)</b> .....	31
<b>Rozdział 3. Obowiązki operatorów usług kluczowych</b> .....	35
<b>Art. 8. [Obowiązek wdrożenia systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej]</b> <i>(A. Besiekierska)</i> .....	37
I. Pojęcie systemu zarządzania bezpieczeństwem w systemie informacyjnym .....	38
II. Właściwości systemu zarządzania bezpieczeństwem w systemie informacyjnym .....	39
A. Systematyczne szacowanie ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem (art. 8 pkt 1 CyberbezpU) .....	39
B. Wdrożenie środków technicznych i organizacyjnych (art. 8 pkt 2 CyberbezpU) ...	41
C. Zbieranie informacji o zagrożeniach i podatnościach (art. 8 pkt 3 CyberbezpU) ....	47
D. Zarządzanie incydentami (art. 8 pkt 4 CyberbezpU) .....	49
E. Stosowanie środków zapobiegających i ograniczających wpływ incydentów (art. 8 pkt 5 CyberbezpU) .....	50
F. Stosowanie odpowiednich środków łączności (art. 8 pkt 6 CyberbezpU) .....	51
III. Wzorce dla systemu zarządzania bezpieczeństwem w systemie informacyjnym .....	53
IV. System zarządzania bezpieczeństwem w systemie informacyjnym a wymogi RODO .....	54
<b>Art. 9. [Obowiązek wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa; obowiązek zapewnienia użytkownikowi usługi kluczowej dostępu do wiedzy w zakresie zagrożeń cyberbezpieczeństwa] (A. Besiekierska)</b> .....	55
I. Obowiązek wyznaczenia osoby kontaktowej .....	56
II. Obowiązek zapewnienia dostępu do wiedzy .....	56
III. Obowiązek informacyjny .....	58
<b>Art. 10. [Obowiązek opracowania, wdrożenia i aktualizacji dokumentacji cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej] (A. Besiekierska)</b> .....	58
I. Charakter dokumentacji .....	59
II. Nadzór nad dokumentacją .....	59
III. Okres przechowania dokumentacji .....	60
IV. Dokumentacja właścicieli infrastruktury krytycznej .....	60
V. Dokumentacja zgodnie z DokCyberSysInfR .....	60
<b>Art. 11. [Obowiązek obsługi incydentów, zgłaszania incydentów poważnych i współdziałania przy obsłudze incydentu poważnego i incydentu krytycznego] (A. Besiekierska)</b> .....	64

I. Uwagi ogólne .....	65
II. Obsługa incydentu .....	66
III. Zgłaszanie incydentu .....	69
<b>Art. 12. [Zgłoszenie incydentu poważnego] (A. Besiekierska) .....</b>	<b>70</b>
I. Zakres zgłoszenia incydentu poważnego .....	71
II. Tajemnica prawnie chroniona .....	71
III. Obsługa incydentów w CyberbezpU a obsługa incydentów w RODO .....	73
<b>Art. 13. [Informacje przekazywane do właściwego CSIRT] (A. Besiekierska) .....</b>	<b>73</b>
I. Informacje fakultatywne .....	74
II. Forma przekazywania informacji .....	74
III. Tajemnice prawnie chronione .....	74
<b>Art. 14. [Powołanie wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo lub zawarcie umowy z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa] (A. Besiekierska) .....</b>	<b>74</b>
I. Uwagi ogólne .....	75
II. Wymogi organizacyjne wobec wewnętrznych struktur odpowiedzialnych oraz podmiotów świadczących usługi z zakresu cyberbezpieczeństwa .....	76
A. Warunki organizacyjne i techniczne .....	76
B. Odpowiednie pomieszczenia .....	76
C. Odpowiednie zabezpieczenia .....	77
III. Współpraca z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa .....	78
<b>Art. 15. [Audyty bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej] (A. Besiekierska) .....</b>	<b>79</b>
I. Uwagi ogólne .....	81
II. Podmioty uprawnione do przeprowadzenia audytu .....	82
III. Obowiązek zachowania poufności przez audytora .....	83
IV. Sprawozdanie z audytu .....	84
<b>Art. 16. [Terminy realizacji obowiązków przez operatora usługi kluczowej] (A. Besiekierska) .....</b>	<b>84</b>
I. Uwagi ogólne .....	85
II. Termin trzech miesięcy .....	85
III. Termin sześciu miesięcy .....	86
IV. Termin roku .....	86
<b>Rozdział 4. Obowiązki dostawców usług cyfrowych .....</b>	<b>87</b>
<b>Art. 17. [Status i obowiązki dostawcy usługi cyfrowej] (A. Besiekierska) .....</b>	<b>88</b>
I. Definicja dostawy usługi cyfrowej .....	89
II. Obowiązek podjęcia właściwych i proporcjonalnych środków technicznych i organizacyjnych .....	90
III. Obowiązek wyznaczenia przedstawiciela dla podmiotów nieposiadających siedziby w UE .....	94

<b>Art. 18. [Obowiązki w zakresie wykrywania, rejestrowania, analizowania oraz klasyfikowania incydentów] (A. Besiekierska)</b> .....	95
I. Uwagi ogólne .....	96
II. Obsługa incydentu .....	96
III. Zgłoszenie incydentu .....	98
<b>Art. 19. [Zgłoszenie incydentu istotnego] (A. Besiekierska)</b> .....	99
I. Zakres zgłoszenia incydentu istotnego .....	100
II. Tajemnice prawnie chronione w zgłoszeniu .....	100
<b>Art. 20. [Informacje przekazywane do właściwego CSIRT] (A. Besiekierska)</b> .....	100
I. Informacje fakultatywne przekazywane do właściwego zespołu CSIRT .....	101
II. Forma przekazywania informacji .....	101
<b>Rozdział 5. Obowiązki podmiotów publicznych</b> .....	103
<b>Art. 21. [Obowiązek wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa] (A. Besiekierska)</b> .....	104
I. Definicja podmiotu publicznego .....	104
II. Obowiązek wyznaczenia osoby odpowiedzialnej za utrzymanie kontaktu .....	106
<b>Art. 22. [Obowiązki w zakresie zgłaszania i obsługi incydentu w podmiocie publicznym] (A. Besiekierska)</b> .....	106
I. Uwagi ogólne .....	107
II. Zarządzanie incydemem w podmiocie publicznym .....	107
III. Zgłaszanie incydentu w podmiocie publicznym do zespołu CSIRT .....	107
IV. Dostęp do informacji .....	107
V. Przekazywanie informacji o osobie .....	108
<b>Art. 23. [Zgłoszenie incydentu w podmiocie publicznym] (A. Besiekierska)</b> .....	108
I. Zakres zgłoszenia incydentu w podmiocie publicznym .....	109
II. Tajemnice prawnie chronione w zgłoszeniu .....	109
<b>Art. 24. [Zgłoszenie fakultatywne] (A. Besiekierska)</b> .....	110
<b>Art. 25. [Przepisy stosowane do podmiotu publicznego uznanego za operatora usługi kluczowej] (A. Besiekierska)</b> .....	110
<b>Rozdział 6. Zadania CSIRT MON, CSIRT NASK i CSIRT GOV</b> .....	113
<b>Art. 26. [Zadania zespołów CSIRT, podział właściwości rzeczowej, dodatkowe uprawnienia] (J. Dysarz)</b> .....	113
I. Rola Zespołu CSIRT w Krajowym Systemie Cyberbezpieczeństwa .....	117
II. Zadania zespołów CSIRT .....	118
III. Główne elementy procedur postępowania w przypadku incydentu .....	119
IV. Szczegółowe zadania CSIRT MON .....	119
V. Szczegółowe zadania zespołu CSIRT NASK .....	120
VI. Szczegółowe zadania CSIRT GOV .....	121

VII. Przekazywanie informacji między zespołami CSIRT .....	121
VIII. Finansowanie działalności zespołów CSIRT .....	122
IX. Powierzenie zadań .....	122
<b>Art. 27. [Wyłączenie CSIRT GOV i CSIRT MON w przypadku incydentów o charakterze terrorystycznym – cywilnym i wojskowym] (J. Dysarz) .....</b>	<b>122</b>
<b>Art. 28. [Przekazywanie informacji o incydencie poważnym] (J. Dysarz) .....</b>	<b>123</b>
<b>Art. 29. [Przekazywanie informacji o incydencie istotnym] (J. Dysarz) .....</b>	<b>124</b>
<b>Art. 30. [Dobrowolne zgłaszanie incydentów] (J. Dysarz) .....</b>	<b>125</b>
<b>Art. 31. [Sposób dokonywania zgłoszeń i informowanie o nim] (J. Dysarz) .....</b>	<b>127</b>
<b>Art. 32. [Specjalne uprawnienia techniczne] (J. Dysarz) .....</b>	<b>128</b>
<b>Art. 33. [Rekomendacje stosowania sprzętu i oprogramowania] (J. Dysarz) .....</b>	<b>129</b>
<b>Art. 34. [Współpraca z organami ścigania i organem właściwym do spraw ochrony danych osobowych] (J. Dysarz) .....</b>	<b>131</b>
<b>Art. 35. [Wymiana informacji na temat incydentu krytycznego] (J. Dysarz) .....</b>	<b>133</b>
<b>Art. 36. [Koordynacja obsługi incydentu krytycznego] (J. Dysarz) .....</b>	<b>134</b>
<b>Rozdział 7. Zasady udostępniania informacji i przetwarzania danych osobowych .....</b>	<b>137</b>
<b>Art. 37. [Publikacja informacji o incydentach] (A. Besiekierska) .....</b>	<b>137</b>
I. Brak zastosowania DostInfPubU .....	138
II. Udostępnienie informacji o incydentach poważnych i istotnych .....	138
<b>Art. 38. [Negatywne przesłanki udostępniania informacji przetwarzanych na podstawie ustawy] (A. Besiekierska) .....</b>	<b>139</b>
<b>Art. 39. [Dane przetwarzane na podstawie ustawy] (A. Besiekierska) .....</b>	<b>139</b>
I. Upoważnienie do przetwarzania danych osobowych .....	141
II. Obowiązki związane z przetwarzaniem danych osobowych .....	142
<b>Art. 40. [Przetwarzanie danych stanowiących tajemnice prawnie chronione] (A. Besiekierska) .....</b>	<b>144</b>
<b>Rozdział 8. Organy właściwe do spraw cyberbezpieczeństwa .....</b>	<b>147</b>
<b>Art. 41. [Organy właściwe do spraw cyberbezpieczeństwa dla wybranych sektorów gospodarki] (J. Dysarz) .....</b>	<b>147</b>
<b>Art. 42. [Zadania organów właściwych] (J. Dysarz) .....</b>	<b>149</b>
I. Uwagi ogólne .....	150
II. Zadania związane z wyznaczaniem operatorów .....	151
III. Zadania związane z nadzorem .....	151
IV. Inne zadania i uprawnienia .....	151
V. Możliwość powierzenia .....	151

<b>Art. 43. [Wstępna ocena spełnienia wymogów]</b> ( <i>J. Dysarz</i> ) .....	152
<b>Art. 44. [Sektorowe zespoły do spraw cyberbezpieczeństwa]</b> ( <i>J. Dysarz</i> ) .....	153
I. Powoływanie sektorowych zespołów cyberbezpieczeństwa .....	154
II. Zadania sektorowych zespołów cyberbezpieczeństwa .....	154
<b>Rozdział 9. Zadania ministra właściwego do spraw informatyzacji</b> .....	157
<b>Art. 45. [Zadania ministra]</b> ( <i>I. Szulc</i> ) .....	157
I. Zakres odpowiedzialności ministra .....	158
A. Monitorowanie wdrażania Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej .....	158
B. Współpraca z sektorem prywatnym w celu zapewnienia cyberbezpieczeństwa ....	159
C. Roczne sprawozdania dotyczące incydentów poważnych i incydentów istotnych .....	159
D. Działania informacyjne dotyczące dobrych praktyk, programów edukacyjnych, kampanii i szkoleń .....	160
E. Gromadzenie informacji o incydentach poważnych .....	161
F. Udostępnianie informacji i dobrych praktyk uzyskanych z Grupy Współpracy .....	161
II. Rola Grupy Współpracy .....	162
<b>Art. 46. [Obowiązek zapewnienia rozwoju lub utrzymania systemu teleinformatycznego wspierającego współpracę w ramach krajowego systemu cyberbezpieczeństwa]</b> ( <i>I. Szulc</i> ) .....	163
I. System teleinformatyczny .....	163
II. Porozumienie jako podstawa korzystania z systemu teleinformatycznego .....	164
<b>Art. 47. [Delegowanie realizacji zadań na jednostki podległe lub nadzorowane przez ministra]</b> ( <i>I. Szulc</i> ) .....	164
I. Rodzaj zadań powierzonych do realizacji .....	165
II. Podmioty podległe Ministrowi Cyfryzacji lub przez niego nadzorowane .....	165
III. Zasady powierzenia i finansowania zadań .....	165
<b>Art. 48. [Zadania Pojedynczego Punktu Kontaktowego]</b> ( <i>I. Szulc</i> ) .....	165
I. Prowadzenie Pojedynczego Punktu Kontaktowego do spraw cyberbezpieczeństwa ..	166
II. Zadania Pojedynczego Punktu Kontaktowego do spraw cyberbezpieczeństwa .....	167
A. Przekazywanie i odbieranie zgłoszeń incydentu poważnego i istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej .....	167
B. Zadania w zakresie koordynacji współpracy w dziedzinie cyberbezpieczeństwa na forum Unii Europejskiej .....	168
<b>Art. 49. [Dane przekazywane przez Pojedynczy Punkt Kontaktowy Grupie Współpracy]</b> ( <i>I. Szulc</i> ) .....	168
I. Informacje przekazywane do Grupy Współpracy .....	169
II. Informacje pochodzące z Grupy Współpracy przekazywane podmiotom krajowym .....	170

<b>Art. 50. [Dane przekazywane przez Pojedynczy Punkt Kontaktowy Komisji Europejskiej] (I. Szulc)</b> .....	170
I. Obowiązki informacyjne wobec Komisji Europejskiej dotyczące organów właściwych do spraw cyberbezpieczeństwa, Pojedynczego Punktu Kontaktowego i CSIRT .....	171
II. Obowiązek przekazywania Komisji Europejskiej informacji umożliwiających ocenę wdrażania dyrektywy NIS .....	171
<b>Rozdział 10. Zadania Ministra Obrony Narodowej</b> .....	173
I. Uwagi ogólne .....	173
II. Wojska Obrony Cyberprzestrzeni .....	175
III. Pełnomocnik Ministra Obrony Narodowej do spraw utworzenia wojsk obrony cyberprzestrzeni .....	175
IV. Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej .....	176
<b>Art. 51. [Zadania ministra] (I. Szulc)</b> .....	176
I. Zadania MON .....	177
II. Pełnomocnik Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni .....	178
<b>Art. 52. [Zadania Narodowego Punktu Kontaktowego do współpracy z Organizacją Traktatu] (I. Szulc)</b> .....	178
I. Zadania Narodowego Punktu Kontaktowego do współpracy z Organizacją Traktatu Północnoatlantyckiego .....	179
II. Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni .....	180
<b>Rozdział 11. Nadzór i kontrola operatorów usług kluczowych, dostawców usług cyfrowych i podmiotów świadczących usługi w zakresie cyberbezpieczeństwa</b> .....	181
<b>Art. 53. [Organy nadzoru] (W. Wąsowicz)</b> .....	181
<b>Art. 54. [Odesłanie do ustawy – Prawo przedsiębiorców] (W. Wąsowicz)</b> .....	182
<b>Art. 55. [Uprawnienia osoby kontrolującej] (W. Wąsowicz)</b> .....	184
I. Podstawowe warunki prowadzenia kontroli .....	184
II. Kontrola a tajemnice prawnie chronione .....	185
III. Gromadzenie dowodów w toku kontroli .....	186
<b>Art. 56. [Obowiązki podmiotu kontrolowanego] (W. Wąsowicz)</b> .....	186
I. Podstawowe obowiązki podmiotów kontrolowanych .....	187
II. Instytucja sprzeciwu .....	187
<b>Art. 57. [Postępowanie dowodowe] (W. Wąsowicz)</b> .....	188
<b>Art. 58. [Protokół kontroli] (W. Wąsowicz)</b> .....	189
<b>Art. 59. [Zalecenia pokontrolne] (W. Wąsowicz)</b> .....	191
<b>Rozdział 12. Pełnomocnik i Kolegium</b> .....	193
<b>Art. 60. [Realizacja polityki rządu w zakresie zapewnienia cyberbezpieczeństwa przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa] (I. Szulc)</b> .....	194

<b>Art. 61. [Powołanie i odwołanie Pełnomocnika; podległość Radzie Ministrów]</b> <i>(I. Szulc)</i> .....	194
<b>Art. 62. [Zadania Pełnomocnika]</b> <i>(I. Szulc)</i> .....	195
I. Zadania Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa .....	196
II. Zadania Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa realizowane z właściwymi ministrami .....	197
<b>Art. 63. [Roczne sprawozdanie Pełnomocnika; przedstawianie wniosków i rekomendacji]</b> <i>(I. Szulc)</i> .....	198
I. Sprawozdanie z działalności Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa .....	199
II. Wnioski i rekomendacje przekazywane Radzie Ministrów .....	199
<b>Art. 64. [Status Kolegium do Spraw Cyberbezpieczeństwa]</b> <i>(I. Szulc)</i> .....	199
I. Charakter Kolegium do Spraw Cyberbezpieczeństwa .....	200
II. Rola Kolegium do Spraw Cyberbezpieczeństwa .....	200
<b>Art. 65. [Zadania Kolegium]</b> <i>(I. Szulc)</i> .....	200
I. Działania opiniowane przez Kolegium do Spraw Cyberbezpieczeństwa .....	201
II. Rekomendacje dla Rady Ministrów .....	202
<b>Art. 66. [Skład Kolegium; Przewodniczący i Sekretarz Kolegium; szczegółowy zakres działania i tryb pracy Kolegium]</b> <i>(I. Szulc)</i> .....	202
I. Skład Kolegium do Spraw Cyberbezpieczeństwa .....	203
II. Organizacja pracy Kolegium do Spraw Cyberbezpieczeństwa .....	204
<b>Art. 67. [Wytyczne Prezesa Rady Ministrów wydawane na podstawie rekomendacji Kolegium]</b> <i>(I. Szulc)</i> .....	205
I. Wydawanie wiążących wytycznych dotyczących zapewnienia cyberbezpieczeństwa na poziomie krajowym oraz funkcjonowania krajowego systemu cyberbezpieczeństwa oraz żądanie informacji i opinii .....	206
II. Wiążące wytyczne w zakresie obsługi incydentów krytycznych .....	206
<b>Rozdział 13. Strategia</b> .....	209
<b>Art. 68. [Przyjęcie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej]</b> <i>(I. Szulc)</i> .....	211
I. Przyjęcie Strategii w drodze uchwały Rady Ministrów .....	211
II. Procedowanie projektu uchwały Rady Ministrów .....	212
<b>Art. 69. [Treść Strategii]</b> <i>(I. Szulc)</i> .....	212
I. Zakres Strategii .....	213
II. Podmioty obowiązane do realizacji Strategii .....	214
III. Czas obowiązywania Strategii .....	215
<b>Art. 70. [Opracowanie projektu Strategii]</b> <i>(I. Szulc)</i> .....	215
I. Podmioty zaangażowane w opracowanie Strategii .....	216



II. Udział przedstawiciela Prezydenta Rzeczypospolitej Polskiej w opracowaniu Strategii .....	216
III. Pomoc ENISA przy opracowywaniu Strategii .....	217
<b>Art. 71. [Przegląd Strategii] (I. Szulc) .....</b>	<b>217</b>
<b>Art. 72. [Przekazanie Strategii Komisji Europejskiej] (I. Szulc) .....</b>	<b>218</b>
<b>Rozdział 14. Przepisy o karach pieniężnych .....</b>	<b>219</b>
<b>Art. 73. [Katalog kar pieniężnych] (W. Wąsowicz) .....</b>	<b>219</b>
I. Uwagi ogólne – instytucja kar administracyjnych .....	220
II. Ogólne uregulowania administracyjnych kar pieniężnych .....	221
III. Administracyjne kary pieniężne w Cyberbezpieczeństwie .....	222
IV. Wymierzanie kar pieniężnych według Cyberbezpieczeństwa .....	223
V. Przedawnienie karalności i wykonania kary .....	224
VI. Procedura odwoławcza .....	225
<b>Art. 74. [Nałożenie kary pieniężnej; wpływy z kar pieniężnych jako dochód budżetu państwa] (W. Wąsowicz) .....</b>	<b>226</b>
<b>Art. 75. [Niedochowanie należytej staranności przez kierownika operatora usługi kluczowej] (W. Wąsowicz) .....</b>	<b>226</b>
<b>Art. 76. [Inne przyczyny nałożenia kary] (W. Wąsowicz) .....</b>	<b>228</b>
<b>Rozdział 15. Zmiany w przepisach, przepisy przejściowe, dostosowujące i końcowe ...</b>	<b>229</b>
<b>Art. 77. [Zmiany w ustawie o systemie oświaty] (W. Wąsowicz) .....</b>	<b>229</b>
<b>Art. 78. [Zmiany w ustawie o działach administracji rządowej] (I. Szulc) .....</b>	<b>230</b>
<b>Art. 79. [Zmiany w ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu] (I. Szulc) .....</b>	<b>231</b>
I. Uprawnienie dla ABW do wdrażania, prowadzenia i koordynowania funkcjonowania systemu wczesnego ostrzegania o zagrożeniach występujących w sieci Internet .....	232
II. System ARAKIS-GOV .....	233
III. Obowiązek przystąpienia do systemu wczesnego ostrzegania o zagrożeniach występujących w sieci Internet .....	234
IV. Warunki i tryb wdrażania systemu wczesnego ostrzegania o zagrożeniach w sieci Internet .....	235
V. Koszty wdrożenia systemu wczesnego ostrzegania o zagrożeniach w sieci Internet .....	237
<b>Art. 80. [Zmiany w ustawie – Prawo zamówień publicznych] (W. Wąsowicz) .....</b>	<b>237</b>
<b>Art. 81. [Zmiany w ustawie – Prawo telekomunikacyjne] (A. Besiekierska) .....</b>	<b>238</b>
<b>Art. 82. [Zmiany w ustawie o zarządzaniu kryzysowym] (I. Szulc) .....</b>	<b>240</b>

I. Koordynacja przygotowania Raportu o zagrożeniach bezpieczeństwa narodowego w części dotyczącej zagrożeń cyberbezpieczeństwa .....	240
II. Uwzględnianie w planach ochrony infrastruktury krytycznej dokumentacji dotyczącej cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych .....	242
III. Udział Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa w posiedzeniach Rządowego Zespołu Zarządzania Kryzysowego .....	242
IV. Obsługa Zespołu do spraw Incydentów Krytycznych przez Rządowe Centrum Bezpieczeństwa .....	243
<b>Art. 83. [Raport o zagrożeniach bezpieczeństwa narodowego] (I. Szulc) .....</b>	<b>243</b>
<b>Art. 84. [Termin powołania Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa] (I. Szulc) .....</b>	<b>244</b>
<b>Art. 85. [Informacje o właściwych organach oraz o zakresie zadań CSIRT przekazywane Komisji Europejskiej] (I. Szulc) .....</b>	<b>244</b>
<b>Art. 86. [Termin wydania decyzji o uznaniu za operatora usługi kluczowej] (W. Wąsowicz) .....</b>	<b>245</b>
<b>Art. 87. [Sprawozdanie podsumowujące przekazywane Grupie Współpracy] (I. Szulc) .....</b>	<b>245</b>
<b>Art. 88. [Termin i zakres przekazania Komisji Europejskiej] (W. Wąsowicz) .....</b>	<b>246</b>
<b>Art. 89. [Termin uruchomienia systemu teleinformatycznego] (I. Szulc) .....</b>	<b>247</b>
<b>Art. 90. [Termin przyjęcia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej] (I. Szulc) .....</b>	<b>247</b>
I. Termin przyjęcia Strategii .....	247
II. Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 .....	247
<b>Art. 91. [Opracowanie pierwszego rocznego planu wdrożenia systemu wczesnego ostrzegania o zagrożeniach występujących w sieci Internet] (I. Szulc) .....</b>	<b>248</b>
<b>Art. 92. [Utrzymanie w mocy przepisów wykonawczych] (A. Besiekierska) .....</b>	<b>249</b>
<b>Art. 93. [Reguła wydatkowa] (J. Dysarz) .....</b>	<b>251</b>
I. Podstawa prawna sporządzania reguł wydatkowych .....	256
II. Wydatki wynikające z CyberbezpU .....	256
III. Mechanizmy korygujące .....	257
<b>Art. 94. [Wejście w życie] (W. Wąsowicz) .....</b>	<b>257</b>