

Spis treści

Wstęp	11
-------------	----

Część I

Zagadnienia ogólne

1. Jakie akty prawne regulują kwestię ochrony danych osobowych w Polsce?	13
2. Czy każdy podmiot, zarówno publiczny, jak i prywatny, jest zobowiązany do przestrzegania przepisów o ochronie danych osobowych?	14
3. Czym są dane osobowe?	14
4. Czy adres poczty elektronicznej jest daną osobową?	15
5. Co to są wrażliwe dane osobowe?	15
6. Co to są dane biometryczne?	16
7. Czym jest przetwarzanie danych osobowych?	16
8. Kiedy można przetwarzać dane osobowe?	16
9. Jakie warunki należy spełnić, by móc przetwarzać dane osobowe zgodnie z prawem?	17
10. Czym jest prawnie uzasadniony interes administratora danych osobowych?	18
11. Czy można pozyskiwać dane osobowe z powszechnie dostępnych źródeł bez zgody? ..	19
12. Kim jest administrator danych osobowych (ADO)?	19
13. Kto jest administratorem danych osobowych w spółce prawa handlowego?	20
14. Kto jest administratorem danych osobowych w szkole/zespole szkół?	20
15. Kto jest administratorem danych osobowych w urzędzie miasta/gminy?	20
16. Jakie obowiązki ma administrator danych osobowych?	21
17. Jakie prawa mają osoby, których dane osobowe są przetwarzane?	22
18. Czy osoba, której dane osobowe są przetwarzane, może zażądać, żebyśmy przestali je wykorzystywać?	22
19. Czy na żądanie osoby, której dane dotyczą, należy usunąć jej dane z bazy?	23
20. Jak długo można przetwarzać czyjeś dane osobowe?	24
21. Czy dane osobowe osób zmarłych podlegają ochronie?	24
22. Czy dane osobowe osób prowadzących działalność gospodarczą podlegają ochronie?	24

Część II

Zgłaszanie zbiorów danych osobowych do rejestracji

23. Kiedy mamy do czynienia ze zbiorem danych osobowych?	25
24. Czym jest doraźny zbiór danych osobowych?	25
25. Jakich zbiorów nie trzeba zgłaszać?	26
26. Kiedy powstaje obowiązek zgłoszenia?	26
27. Kto jest zwolniony z obowiązku zgłoszenia zbiorów danych osobowych do rejestracji GODO?	26
28. W jaki sposób zgłosić dane osobowe do rejestracji?	28
29. Czy zbiory danych osobowych trzeba przesłać do GODO?	28
30. Jak długo trwa rejestracja zbiorów danych?	28
31. Czy po zgłoszeniu zbioru GODO wydaje zaświadczenie?	29
32. Co grozi za niezgłoszenie zbioru danych do GODO?	29
33. Kiedy GODO może odmówić rejestracji zbioru danych osobowych?	30
34. Czy można korzystać z danych zawartych w zbiorze, którego rejestracji odmówił GODO?	30
35. Czy po odmowie rejestracji zbioru można złożyć wniosek o ponowne rozpatrzenie sprawy?	31
36. Czy administrator danych, który otrzymał decyzję o odmowie, a następnie usunął wady, które były przyczyną odmowy rejestracji, powinien złożyć wniosek o ponowne rozpatrzenie sprawy?	32
37. Czy można zignorować decyzję GODO w sprawie odmowy rejestracji zbioru?	32
38. Kiedy należy aktualizować zgłoszone zbiory danych osobowych?	32
39. Czy trzeba zgłosić usunięcie zbioru danych do GODO?	33

Część III

Administrator bezpieczeństwa informacji

40. Kim jest administrator bezpieczeństwa informacji (ABI)?	33
41. Kto może być administratorem bezpieczeństwa informacji?	34
42. Czy trzeba mieć ukończone szkolenie albo studia, żeby zostać ABI?	34
43. Czy administrator bezpieczeństwa informacji może pełnić funkcje niezwiązane z ochroną danych osobowych?	35
44. Czy każdy podmiot jest zobowiązany do wyznaczenia administratora bezpieczeństwa informacji?	35
45. Czy należy zgłosić administratora bezpieczeństwa informacji do rejestracji?	36
46. W jaki sposób należy dokonać zgłoszenia ABI?	36
47. Gdzie znajduje się rejestr administratorów bezpieczeństwa informacji?	37
48. Czy można powołać zastępców ABI?	37
49. Kto może być zastępcą ABI?	38
50. Jakie zadania ma administrator bezpieczeństwa informacji?	38
51. Czym jest plan sprawdzeń?	39
52. Jak powinno wyglądać sprawdzenie planowe?	39

53. Jak często trzeba wykonywać sprawdzenie planowe?	40
54. W jakich sytuacjach należy przeprowadzić sprawdzenie doraźne?	40
55. Czy należy przygotować sprawozdanie ze sprawdzeń?	40
56. Czy ABI musi szkolić pracowników z zasad ochrony danych osobowych?	41
57. Jak często powinno odbywać się takie szkolenie?	41
58. Na czym polega obowiązek nadzorowania tworzenia i aktualizowania dokumentacji ochrony danych osobowych?	42
59. Czy ABI upoważnia do przetwarzania danych osobowych i prowadzi ewidencję osób upoważnionych?	42
60. Co powinno się znaleźć w ewidencji osób upoważnionych do przetwarzania danych osobowych?	43
61. Czy ABI powinien prowadzić rejestr zbiorów danych osobowych?	43
62. Jak powinien wyglądać rejestr zbiorów danych osobowych prowadzony przez ABI?... 43	
63. Jak wygląda zgłaszanie zbiorów danych osobowych, gdy administrator danych nie powoła ABI?	44
64. Co się stanie, jeśli administrator danych nie zgłosi administratora bezpieczeństwa informacji do rejestracji GODO?	45
65. Czy jeśli ADO nie zgłosi ABI do GODO, sam prowadzi sprawdzenia?	45
66. Jeśli ABI nie jest powołany, ADO sam szkoli pracowników z ochrony danych?	46
67. Czy jeśli ABI nie jest powołany, ADO sam nadzoruje opracowanie i aktualizowanie dokumentacji?	46
68. Czy można odwołać administratora bezpieczeństwa informacji?	47
69. Czy jeśli między odwołaniem jednego a zgłoszeniem drugiego ABI do rejestracji wystąpi kilkumiesięczna przerwa, trzeba w tym czasie zgłaszać zbiory danych do rejestracji GODO?	47

Część IV

Administrator systemów informatycznych (ASI)

70. Kim jest administrator systemów informatycznych?	48
71. Czy powołanie ASI jest obowiązkowe?	48
72. Czy ASI może być jednocześnie ABI?	48
73. Jakie są zadania administratora systemów informatycznych?	49

Część V

Dokumentacja przetwarzania danych osobowych

74. Jaką dokumentację należy przygotować w ramach systemu ochrony danych osobowych?	50
75. Czy przed stworzeniem dokumentacji ochrony danych należy przeprowadzić analizę ryzyka?	50
76. Co to jest Polityka bezpieczeństwa przetwarzania danych osobowych?	51
77. Jakie informacje powinny się znaleźć w polityce bezpieczeństwa?	51
78. Co to jest Instrukcja zarządzania systemem informatycznym?	51

79. Co powinna zawierać instrukcja zarządzania?	52
80. Kto przygotowuje politykę bezpieczeństwa i instrukcję zarządzania?	52
81. Jak często należy aktualizować dokumentację przetwarzania danych osobowych?	53

Część VI

Zgoda na przetwarzanie danych osobowych

82. Czy zawsze trzeba mieć zgodę na przetwarzanie danych osobowych?	54
83. Czy zgoda musi zostać wyrażona w formie pisemnej?	54
84. Czy należy archiwizować zgody?	55
85. Jak powinna wyglądać prawidłowa klauzula zgody?	55
86. Czy na przetwarzanie danych wrażliwych potrzebna jest odrębna zgoda?	56

Część VII

Udostępnianie danych osobowych

87. Kiedy dochodzi do udostępnienia danych osobowych?	56
88. Czy osoba, której dane są udostępniane, musi wyrazić na to zgodę?	57
89. Co grozi za udostępnienie danych osobom nieupoważnionym?	57
90. Czym jest udostępnienie danych na wniosek?	57
91. Co grozi za nieudostępnienie danych podmiotowi składającemu wniosek, jeśli został on prawidłowo zgłoszony?	58

Część VIII

Powierzenie danych osobowych

92. Czym jest powierzenie danych osobowych?	58
93. Kiedy dochodzi do powierzenia danych osobowych?	59
94. Jakie warunki należy spełnić, by móc powierzyć dane osobowe?	59
95. Czym jest umowa o powierzeniu przetwarzania danych osobowych?	59
96. Czy osoba, której dane są powierzane, musi wyrazić na to zgodę?	60
97. Czym jest podpowierzenie danych osobowych?	60
98. Czy administrator danych osobowych, który przekazał dane procesorowi, musi wiedzieć o podpowierzeniu?	61
99. Kto jest odpowiedzialny za dane, które zostały powierzone lub podpowierzone?	62

Część IX

Przekazanie danych osobowych do państwa trzeciego

100. Jakie państwa należą do państw trzecich?	62
101. Kiedy dochodzi do przekazania danych do państwa trzeciego?	63
102. Jakie przepisy obowiązują przy przekazywaniu danych osobowych w ramach Unii Europejskiej?	63
103. Jakie są zasady przekazywania danych do państw trzecich?	64

104. Czy można przekazać dane osobowe do państwa trzeciego, mimo że nie zapewnia ono odpowiednich gwarancji ochrony danych osobowych?	64
105. Czym są standardowe klauzule umowne?	64
106. Jakie są podstawy prawne wykorzystania standardowych klauzul umownych?	65
107. Czy stosowanie standardowych klauzul umownych wymaga zgody GODO?	65
108. Czy zawsze można skorzystać ze standardowych klauzul umownych przy przekazaniu danych do państw trzecich?	66
109. Czy można zmieniać standardowe klauzule umowne?	66
110. Jaką formę powinny mieć standardowe klauzule umowne?	66
111. Kiedy nie trzeba stosować standardowych klauzul umownych?	67
112. Czym są wiążące reguły korporacyjne?	67
113. Jakie są podstawy prawne wiążących reguł korporacyjnych?	68
114. Czy GODO musi wyrazić zgodę na stosowanie wiążących reguł korporacyjnych? ..	68
115. W jaki sposób można przekazać dane osobowe do Stanów Zjednoczonych?	69
116. Kiedy może dojść do wstrzymania przekazania danych do państw trzecich?	69

Część X

Generalny Inspektor Ochrony Danych Osobowych (GODO)

117. Kim jest Generalny Inspektor Ochrony Danych Osobowych?	70
118. Czym zajmuje się Generalny Inspektor Danych Osobowych?	70
119. Jakie uprawnienia ma GODO?	71
120. Kiedy może dojść do kontroli?	71
121. Jak długo trwa kontrola GODO?	72
122. Jak wygląda kontrola GODO?	72
123. Czy kontrola GODO jest wcześniej zapowiadana?	73
124. Kto prowadzi kontrole?	73
125. Czy w czasie kontroli pracownicy mogą być przesłuchiwać przez inspektorów w charakterze świadków?	74
126. Czy z kontroli zostaje sporządzony protokół?	74
127. Czy administrator danych osobowych ma wgląd do tego protokołu?	74
128. Jakie kary może nakładać GODO?	75
129. Jakie są konsekwencje niewykonania decyzji GODO?	75
130. Kiedy GODO może zwrócić się do ABI o przeprowadzenie sprawdzenia?	76
131. Ile czasu ABI ma na przeprowadzenie takiego sprawdzenia?	76
132. Czy sprawdzenie dla GODO powinno przebiegać tak samo jak sprawdzenie planowe?	76
133. Czy ze sprawdzenia dla GODO trzeba przygotować sprawozdanie?	77
134. Czy sprawozdanie z takiego sprawdzenia trzeba przekazać do GODO?	78

Część XI

Odpowiedzialność

135. Co grozi za nieprzestrzeganie przepisów o ochronie danych osobowych?	78
---	----

136. Czy pracownik naruszający zasady ochrony danych osobowych może zostać ukarany?	79
137. Czy za naruszenia ochrony danych osobowych grozi odpowiedzialność karna?	80
138. Za jakie działania grozi odpowiedzialność karna?	80
139. Na czym polega odpowiedzialność cywilna za naruszenia ochrony danych?	82
140. Na czym polega odpowiedzialność administracyjna za naruszenia ochrony danych?	82

Część XII

Dane osobowe pracowników

141. Jakie dane osobowe pracowników można zbierać?	83
142. Czy należy zgłaszać do GODO zbiory z danymi osobowymi pracowników i kandydatów do pracy?	84
143. Czy pracownik musi wyrazić zgodę na przetwarzanie jego danych osobowych?	84
144. Czy można przekazać dane osobowe pracownika do komornika na jego wniosek?	85
145. Czy takie udostępnienie danych wymaga zgody pracownika?	85
146. Czy można zamieścić zdjęcie pracownika na stronie internetowej bez jego zgody? ..	86
147. Czy można sprawdzać pocztę elektroniczną pracownika?	86
148. Czy można sprawdzać, jakie połączenia telefoniczne wykonuje pracownik w czasie pracy?	87
149. Czy można stosować urządzenia szczytujące odciski linii papilarnych do mierzenia czasu pracy?	87
150. Czy pracownik musi przejść szkolenie z zakresu ochrony danych osobowych?	88
151. Co powinno zawierać szkolenie z ochrony danych osobowych?	89
152. Czy pracownik, który ma dostęp do danych osobowych, powinien być upoważniony do przetwarzania danych osobowych?	89
153. Czy pracownik powinien podpisać oświadczenie o zachowaniu poufności danych osobowych?	90
154. Czy należy upoważniać stażystów i praktykantów do przetwarzania danych osobowych?	90

Część XIII

Zabezpieczenia danych osobowych

155. Czym jest incydent ochrony danych osobowych?	90
156. Jak należy zachować się w przypadku wystąpienia incydentu ochrony danych osobowych?	91
157. Czy taki incydent należy zgłosić GODO?	91
158. Czy o incydencie należy poinformować osoby, których danych incydent dotyczy? ..	92
159. Co to jest polityka kluczy?	92
160. Co to jest zasada czystego biurka?	93

161. Czym są poziomy bezpieczeństwa danych osobowych?	93
162. Jakie fizyczne zabezpieczenia stosować do ochrony danych?	93
163. Na czym polega anonimizacja dokumentów?	94
164. Jak trwale usunąć dane osobowe?	95

Część XIV

Europejska reforma ochrony danych osobowych

165. Czym jest ogólne rozporządzenie o ochronie danych osobowych (rodo)?	95
166. Kiedy zacznie obowiązywać ten akt prawny?	95
167. Dlaczego rodo będzie obowiązywać dopiero w 2018 roku?	95
168. Czy trzeba już teraz przygotowywać się do obowiązywania rozporządzenia?	96
169. Czy rozporządzenie zmieni definicję danych osobowych?	96
170. Na czym będzie polegała pseudoanonimizacja danych osobowych?	96
171. Jak będzie wyglądała pozycja administratora bezpieczeństwa w rodo?	97
172. Czy powołanie inspektora ochrony danych będzie obowiązkowe?	97
173. Czy będzie możliwość powołania jednego inspektora np. dla całej grupy kapitałowej?	98
174. Czy rodo wprowadzi nowe obowiązki dla ABI?	98
175. Czy rodo wprowadzi nowe obowiązki dla ADO?	98
176. Czy rodo wprowadzi kary finansowe?	99
177. Czy rodo zmieni zasady przekazywania danych do państw trzecich?	99
178. Czy rodo zmieni przepisy dotyczące pozyskiwania zgód na przetwarzanie danych osobowych?	101
179. Jakie prawa rozporządzenie gwarantuje osobom, których dane są przetwarzane? ...	101
180. Na czym będzie polegało proaktywne podejście do ochrony danych osobowych? ...	102