

Spis treści

Wykaz skrótów	XI
Wykaz literatury	XV
O Autorach	XIX
Przedmowa	XXIII
Wprowadzenie	1
Rozdział I. Obowiązki informacyjne placówki medycznej względem pacjentów w praktyce (Michał Kibil, Ilona Kuźniecowa)	3
1. Obowiązek informacyjny	3
2. Sytuacje, w jakich należy poinformować o przetwarzaniu danych	4
3. Informacje, które należy przekazać	4
3.1. Uwagi ogólne	4
3.2. Pozyskanie danych od osoby, której dane dotyczą	5
3.3. Pozyskiwanie danych od innej osoby niż ta, której dane dotyczą	6
3.4. Aktualizacja informacji	7
4. Forma przekazania danych	7
5. Formułowanie treści informacji	8
6. Termin udzielenia informacji	9
6.1. Uwagi ogólne	9
6.2. Termin udzielenia informacji przy bezpośrednim pozyskaniu danych	9
6.3. Termin udzielenia informacji o uzyskaniu danych z innych źródeł	10
6.4. Termin udzielenia informacji o zmianie celu przetwarzania	10
7. Sytuacje, w których nie ma obowiązku przekazywania informacji	11
8. Przykładowe problemy występujące w służbie zdrowia związane z obowiązkiem informacyjnym	12
8.1. Brak informacji o stosowanym monitoringu	12
8.2. Traktowanie informacji przekazanych przez prawnego opiekuna jako informacji od osoby trzeciej	13
8.3. Niedostosowane klauzule informacyjne	13
8.4. Zbyt ogólna lub zbyt skomplikowana klauzula informacyjna	13

9. Wzór klauzuli informacyjnej dla placówki medycznej	13
Rozdział II. Dokumentowanie procesów przetwarzania danych osobowych (Paweł Litwiński)	19
1. Uwagi ogólne	19
2. Zasada rozliczalności danych osobowych a dokumentacja ochrony danych	21
3. Dokumentacja ochrony danych osobowych a przepisy RODO	22
4. Dokumentowanie czynności wymaganych przez przepisy RODO	23
5. Dokumentowanie czynności związanych z wykonywaniem obowiązków wynikających z RODO	25
6. Dokumentacja przetwarzania danych a <i>privacy by design</i>	28
7. Dokumentacja wynikająca z RODO	29
8. Wzory dokumentów	29
8.1. Wzór rejestru czynności przetwarzania	29
8.2. Wzór rejestru naruszeń ochrony danych	30
8.3. Wzór zgłoszenia naruszenia ochrony danych	31
Rozdział III. Ocena skutków dla ochrony danych w podmiocie medycznym (Maciej Gawroński)	33
1. Uwagi wstępne	33
2. Dane dotyczące zdrowia	33
3. Dane dotyczące zdrowia a dane medyczne, dokumentacja medyczna i dane objęte tajemnicą lekarską	34
4. Ryzyko przetwarzania danych dotyczących zdrowia	34
5. Ocena skutków dla ochrony danych – nowa instytucja ochrony danych osobowych	35
6. Duża skala przetwarzania danych dotyczących zdrowia	35
7. Sytuacje, w jakich należy przeprowadzić DPIA	36
8. Zakres DPIA	36
9. Elementy DPIA	37
10. Role w DPIA	40
11. Praktyczne porady	41
12. Wzór raportu z oceny skutków dla ochrony danych (DPIA) w służbie zdrowia ...	41
Rozdział IV. Analiza ryzyka w placówce medycznej (Robert Mołdach)	49
1. Rola metodyki przy ustanawianiu kontekstu	49
2. Metodologia PESTEL w analizie ryzyka płynącego z otoczenia biznesowego	50
2.1. PESTEL – krótkie wprowadzenie	50
2.2. Perspektywa polityczna	51
2.3. Perspektywa ekonomiczna	52
2.4. Perspektywa społeczna	53
2.5. Perspektywa technologiczna	54
2.6. Perspektywa prawna	55

3. Metodologia 7-S McKinsey'a w analizie ryzyka w perspektywie wewnętrznej	55
3.1. 7-S – krótkie wprowadzenie	55
3.2. Strategia	56
3.3. Struktura	57
3.4. Systemy	59
3.5. Personel	60
3.6. Kultura organizacyjna	62
3.7. Umiejętności	64
3.8. Wspólne (nadrzędne) wartości	65
4. Rekomendacja końcowa	67
Rozdział V. Wyznaczenie inspektora ochrony danych w placówce medycznej <i>(Monika Wieczorek)</i>	71
1. Zagadnienia wstępne	71
2. Obowiązek wyznaczenia inspektora ochrony danych	71
3. Wyznaczenie inspektora ochrony danych	73
4. Zadania inspektora ochrony danych	74
5. Status inspektora ochrony danych i jego pozycja w strukturze organizacji	76
6. Obowiązki administratora dotyczące inspektora ochrony danych	77
7. Odpowiedzialność inspektora ochrony danych	78
8. Sankcje administracyjne	79
9. Wzór umowy o świadczenie usług inspektora ochrony danych	80
Rozdział VI. Upoważnienie pracowników do przetwarzania danych osobowych <i>(Monika Wieczorek)</i>	85
1. Zagadnienia wstępne	85
2. Nadawanie upoważnień	86
3. Zróżnicowanie personelu	87
4. Forma i zakres upoważnienia	89
5. Sankcje administracyjne za naruszenie obowiązków	91
6. Wzór upoważnienia do przetwarzania danych osobowych	92
Rozdział VII. Kodeks postępowania dla sektora ochrony zdrowia a zasady prowadzenia dokumentacji medycznej <i>(Aneta Sieradzka, Dominika Tykwińska- Rutkowska)</i>	95
1. Instytucja kodeksów postępowania w świetle RODO	95
1.1. Uwagi ogólne	95
1.2. Pojęcie i cele sporządzania kodeksu postępowania	97
1.3. Przedmiot kodeksu postępowania	98
1.4. Procedura opracowania kodeksu postępowania	99
1.5. Znaczenie zobowiązania się administratorów i podmiotów przetwarzających dane do stosowania kodeksu postępowania	105
1.6. Monitorowanie przestrzegania kodeksu postępowania	106

2. Projekty kodeksu postępowania dla sektora ochrony zdrowia i problem dokumentacji medycznej	110
3. Podsumowanie	118
Rozdział VIII. Przechowywanie i zabezpieczenie dokumentacji medycznej a ochrona danych osobowych (Kajetan Wojsyk)	121
1. Uwagi ogólne	121
2. Prawne określenie dokumentacji medycznej	122
3. Elektroniczna dokumentacja medyczna	123
4. Praktyczne stosowanie dokumentacji medycznej	135
5. Problemy niespójności dokumentacji medycznej	136
6. Podsumowanie	137
Rozdział IX. Naruszenia ochrony danych osobowych oraz obowiązki notyfikacyjne administratora danych osobowych (Michał Miłośz)	139
1. Uwagi ogólne	139
2. Naruszenie ochrony danych osobowych	141
3. Obowiązek zgłoszenia naruszenia ochrony danych osobowych organowi nadzorcemu	146
4. Obowiązek zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych	154
5. Obowiązek dokumentowania naruszeń ochrony danych osobowych	159
6. Wzory dokumentów	161
6.1. Wzór instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych	161
6.2. Wzór zawiadomienia o naruszeniu ochrony danych osobowych osoby, której dane dotyczą	166
6.3. Wzór rejestru naruszeń ochrony danych osobowych	168
Rozdział X. Pozycja ustrojowa Prezesa UODO. Postępowania i administracyjne kary pieniężne (Izabela Oleksy-Piesik)	173
1. Prezes UODO jako następcą prawny Generalnego Inspektora Ochrony Danych Osobowych	173
2. Prezes UODO jako niezależny organ nadzorczy w rozumieniu przepisów RODO i jego pozycja prawnoustrojowa	176
3. Zadania Prezesa UODO i środki ich realizacji	181
4. Rola Prezesa UODO w postępowaniach szczególnych	188
4.1. Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych i środki stosowane przez Prezesa UODO w tym postępowaniu ..	188
4.2. Prezes UODO w postępowaniach związanych z dochodzeniem roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych na drodze postępowania cywilnego	189
4.3. Postępowanie kontrolne i środki stosowane przez Prezesa UODO w tym postępowaniu	192
5. Postępowanie przed Prezesem UODO	192

5.1. Odpowiedzialność z tytułu naruszenia przepisów o ochronie danych osobowych. Prawo wniesienia skargi do Prezesa UODO	192
5.2. Zasady postępowań prowadzonych przez Prezesa UODO	194
6. Administracyjne kary pieniężne	197
6.1. Pojęcie administracyjnej kary pieniężnej	197
6.2. Przepisy regulujące kwestie związane z nakładaniem administracyjnych kar pieniężnych	198
6.3. Dyrektywy wymiaru administracyjnych kar pieniężnych	199
6.4. Rodzaje i wysokość administracyjnych kar pieniężnych	201
6.5. Postępowanie w sprawie nałożenia administracyjnej kary pieniężnej	204
7. Praktyczne schematy	207
7.1. Środki ochrony prawnej przysługujące osobie, której dane dotyczą	207
7.2. Dochodzenie roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych przed Prezesem UODO	208
7.3. Konsekwencje prawne wydania decyzji administracyjnej przez Prezesa UODO dla toczącego się postępowania sądowego	209
7.4. Dochodzenie roszczeń z tytułu naruszenia przepisów RODO	209
7.5. Udział Prezesa UODO w postępowaniu sądowym w sprawie o naruszenie przepisów RODO	210
8. Wzory	211
8.1. Wzór skargi do Prezesa UODO	211
8.2. Wzór skargi do wojewódzkiego sądu administracyjnego na decyzję Prezesa UODO	212