

SPIS TREŚCI

Wykaz skrótów	15
Wstęp do III wydania	19
Wstęp do II wydania	21
Wstęp do I wydania	25

Część I **Zagadnienia wstępne**

Rozdział 1

Podstawowe pojęcia	31
1.1. Pojęcie danych osobowych	31
1.1.1. Informacje a dane	31
1.1.2. Osobowy charakter informacji	34
1.1.3. Identyfikowalność osoby	37
1.2. Pojęcie danych medycznych	39
1.3. Inne kluczowe definicje	41

Część II **Ogólne standardy ochrony danych medycznych na podstawie norm prawa konstytucyjnego, międzynarodowego i europejskiego**

Rozdział 2

Konstytucyjne prawo do ochrony danych medycznych	49
---	-----------

Rozdział 3

Prawo do ochrony danych medycznych jako prawo człowieka	
w świetle uniwersalnych i europejskich standardów praw człowieka	58
3.1. Obowiązkiwanie MPPOiP i EKPC w polskim systemie prawnym	58

3.2. Ochrona danych medycznych w świetle uniwersalnych standardów praw człowieka	59
3.3. Ochrona danych medycznych w ramach systemu Rady Europy	61
3.3.1. Ochrona danych medycznych na podstawie EKPC	61
3.3.2. Ochrona danych medycznych na podstawie orzecznictwa strasburskiego	64
3.3.2.1. Obowiązek wprowadzenia zabezpieczeń instytucjonalnych	65
3.3.2.2. Dostęp do danych medycznych podmiotu danych	66
3.3.2.3. Przetwarzanie danych medycznych	67
3.3.2.4. Ochrona danych medycznych w kontekście tajemnicy lekarskiej	69
3.3.2.5. Dopuszczalność ograniczenia ochrony danych medycznych	70
3.4. Instytucjonalne zabezpieczenia uniwersalnego i europejskiego standardu praw człowieka	73
3.4.1. Gwarancje formalne ochrony danych medycznych w ramach ONZ (MPPOiP)	74
3.4.2. Gwarancje formalne ochrony danych medycznych w ramach Rady Europy (EKPC)	75
 Rozdział 4	
Ochrona danych medycznych zgodnie z konwencją nr 108 Rady Europy	78
4.1. Zakres stosowania konwencji	78
4.2. Zasady przetwarzania danych medycznych	80
4.3. Prawa podmiotu danych	80
4.4. Obowiązki podmiotu przetwarzającego dane medyczne	81
4.5. Ponadgraniczny obrót danymi medycznymi	82
4.6. Procedury ochronne wynikające z konwencji nr 108	82
 Rozdział 5	
Ogólne standardy ochrony danych medycznych w prawie	
Unii Europejskiej	86
5.1. Źródła prawa Unii Europejskiej obejmujące ochronę danych osobowych	86
5.1.1. Traktaty	89
5.1.2. Karta Praw Podstawowych	89
5.1.3. Dyrektywy	91
5.1.4. Rozporządzenia	92
5.2. Instytucjonalne zabezpieczenia unijnego standardu ochrony danych medycznych	93
5.3. Orzecznictwo TSUE w sprawie danych medycznych	96
5.3.1. Zakres danych osobowych chronionych	96

5.3.2. Sposób przetwarzania danych osobowych	97
5.3.3. Prawo do bycia zapomnianym	99
5.3.4. Transgraniczne przetwarzanie danych osobowych	99

Rozdział 6

Ochrona danych medycznych według zalecanych standardów praw

człowieka	101
6.1. Ochrona danych medycznych według rekomendacji Komitetu Ministrów Rady Europy R(97)5	101
6.1.1. Zakres stosowania rekomendacji	102
6.1.2. Zasady przetwarzania danych medycznych	103
6.1.3. Prawa podmiotu danych i obowiązki podmiotu przetwarzającego dane medyczne	104
6.1.4. Ponadgraniczny obrót danymi medycznymi	107
6.1.5. Ochrona danych medycznych używanych do badań naukowych	107
6.2. Ochrona danych medycznych według wytycznych ONZ	108
6.2.1. Ochrona danych medycznych według rezolucji 45/95 Zgromadzenia Ogólnego ONZ – Wytyczne w sprawie uregulowania kartotek skomputeryzowanych danych osobistych	108
6.2.2. Ochrona danych medycznych według rezolucji 34/169 Zgromadzenia Ogólnego ONZ – Kodeks postępowania funkcjonariuszy porządku prawnego	110
6.3. Ochrona danych medycznych według wytycznych OECD	111

Część III

Ochrona danych medycznych według RODO, polskiej ustawy o ochronie danych osobowych i innych ustaw

Rozdział 7

Przetwarzanie i ochrona danych medycznych według RODO	117
7.1. Zakres zastosowania RODO	117
7.1.1. Obowiązywanie RODO	117
7.1.2. Przedmiot regulacji	119
7.1.2.1. Identyfikowalna osoba fizyczna. Usługi <i>e-health</i>	119
7.1.2.2. Dane przetwarzane w sposób zautomatyzowany oraz dane w zbiorach	120
7.1.2.3. Dane medyczne – domniemanie ochrony	121
7.1.3. Terytorialny zakres obowiązywania RODO	121
7.1.4. Wyłączenia	123
7.1.4.1. Czynności o charakterze prywatnym	123
7.1.4.2. Osoby zmarłe	124

7.1.4.3. Działalność nieobjęta prawem Unii	124
7.2. Zasady przetwarzania danych medycznych w RODO	126
7.2.1. Przedmiot ochrony. Wrażliwość danych	126
7.2.2. Zakaz przetwarzania danych wrażliwych. Ograniczenia zakazu	126
7.2.2.1. Zasada oraz wyjątki	126
7.2.2.2. Zastosowanie zakazu do danych medycznych	127
7.2.3. Dopuszczalność przetwarzania danych medycznych	128
7.2.3.1. Legalność przetwarzania. Legalność w ujęciu danych medycznych	129
7.2.3.2. Zgoda uprawnionego	130
7.2.3.2.1. Jednoznaczność oświadczenia o zgodzie	130
7.2.3.2.2. Ocena dobrowolności	131
7.2.3.2.3. Dodatkowe warunki zgody na przetwarzanie danych wrażliwych	133
7.2.3.2.4. Zgoda małoletniego	134
7.2.3.2.5. Praktyczne aspekty zgody na przetwarzanie danych medycznych	135
7.2.3.3. Wykonanie obowiązku prawnego lub realizacja uprawnienia	135
7.2.4. Zadanie realizowane w interesie publicznym	137
7.2.4.1. Interes publiczny <i>sensu largo</i>	137
7.2.4.2. Cele zdrowotne	138
7.2.4.3. Przetwarzanie danych medycznych w związku ze zdrowiem publicznym, jakością produktów i usług medycznych	141
7.2.4.4. Cele archiwalne, badawcze i statystyczne	141
7.2.5. Interes administratora	142
7.2.6. Dane upublicznione w sposób oczywisty	143
7.2.7. Pozostałe przesłanki dopuszczalności przetwarzania danych medycznych	143
7.2.7.1. Rzetelność	143
7.2.7.2. Przezrzystość i ograniczenie celu	144
7.2.7.3. Pozostałe zasady przetwarzania danych	145
7.3. Prawa podmiotu danych	146
7.3.1. Informacje i dostęp do danych	148
7.3.2. Sprostowanie, usuwanie, ograniczenie przetwarzania i przenoszenie danych	154
7.3.3. Sprzeciw i zautomatyzowane podejmowanie decyzji	160
7.3.4. Zasady ogólne	163
7.4. Obowiązki podmiotów przetwarzających dane medyczne	166
7.4.1. Generalna charakterystyka obowiązków administratora danych medycznych	166

7.4.2. Uwzględnienie ochrony w fazie projektowania oraz domyślna ochrona danych	170
7.4.3. Instytucja współadministracji danymi medycznymi	172
7.4.4. Obowiązek wyznaczenia przedstawiciela w Unii	174
7.4.5. Obowiązek powierzenia przetwarzania oraz instytucja podmiotu przetwarzającego dane medyczne	174
7.4.6. Upoważnienie administratora lub podmiotu przetwarzającego ...	178
7.4.7. Rejestrowanie czynności przetwarzania	180
7.4.8. Współpraca z organem nadzorczym	183
7.4.9. Bezpieczeństwo przetwarzania	183
7.4.10. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu	187
7.4.11. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych	189
7.4.12. Ocena skutków dla ochrony danych	190
7.4.13. Obowiązek konsultacji z organem nadzorczym	194
7.5. Ponadgraniczny obrót danymi medycznymi	195
7.5.1. Obrót danymi medycznymi pomiędzy państwami członkowskimi UE	196
7.5.2. Przekazywanie danych medycznych do państw trzecich	197
7.5.2.1. Decyzja stwierdzająca odpowiedni poziom ochrony (art. 45 RODO)	200
7.5.2.2. Zastrzeżenie odpowiednich zabezpieczeń (art. 46–47 RODO)	206
7.5.2.3. Wyjątki w szczególnych sytuacjach (art. 49 RODO)	210
7.5.2.4. Dane medyczne przekazywane do państw trzecich – wybrane aspekty	212
7.6. Instytucjonalne zabezpieczenia procesów przetwarzania danych medycznych	213
7.6.1. Uwagi wstępne	213
7.6.2. Organ nadzorczy	214
7.6.2.1. Właściwość organu nadzorczego	215
7.6.2.2. Ustanowienie organu nadzorczego	215
7.6.2.3. Niezależność organu nadzorczego	216
7.6.2.4. Zadania, obowiązki i uprawnienia	216
7.6.2.5. Zadania i obowiązki	217
7.6.2.6. Kompetencje	217
7.6.2.7. Obowiązek współpracy z organem nadzorczym	218
7.6.3. Inspektor ochrony danych	218
7.6.3.1. Jeden inspektor dla kilku podmiotów	219
7.6.3.2. Ustanowienie inspektora ochrony danych	219
7.6.3.3. Kwalifikacje do pełnienia funkcji inspektora ochrony danych	221

7.6.3.4. Zadania inspektora ochrony danych	222
7.6.3.5. Publikacja danych kontaktowych inspektora	223
7.6.3.6. Odpowiedzialność inspektora ochrony danych	223
7.6.4. Kodeksy postępowania, akredytacja i certyfikacja	223
7.6.4.1. Kodeksy postępowania	223
7.6.4.2. Przedmiot kodeksów	224
7.6.4.3. Opracowywanie kodeksów	224
7.6.4.4. Stosowanie kodeksów	225
7.6.4.5. Kodeks branży medycznej	225
7.6.4.6. Akredytacja	226
7.6.4.7. Certyfikacja	226
7.6.5. Ocena skutków dla ochrony danych i konsultacje	228
7.6.5.1. Konsultacje z organem nadzorczym	232
7.7. eHealth	234
7.7.1. Zarządzanie informacjami o zdrowiu	234
7.7.2. Technologie informacyjno-komunikacyjne w opiece zdrowotnej ...	237
7.7.3. Telemedycyna, telematyka i zdalna opieka medyczna	239
7.7.4. Rozwiązania IoT w eHealth	240
7.7.5. Neutralność technologiczna a standaryzacja eHealth	242
7.7.6. Wpływ inicjatyw pozalegislacyjnych na standaryzację eHealth ...	246
7.7.7. Zagrożenia cybernetyczne związane z rozwojem eHealth	249
7.7.8. Rola zasady neutralności technologicznej w eHealth a standaryzacja	252

Rozdział 8

Przetwarzanie danych medycznych według przepisów ustawy o ochronie

danych osobowych	254
8.1. Ochrona danych medycznych za pomocą innych przepisów polskiego prawa administracyjnego	254
8.1.1. Uwagi wstępne	254
8.1.2. Pojęcie pacjenta w przepisach ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta	255
8.1.3. Prawo do ochrony danych medycznych w przepisach ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta	259
8.1.3.1. Prawo do zachowania tajemnicy	259
8.1.3.2. Prawo do informacji	262
8.1.3.3. Prawo dostępu do dokumentacji medycznej	264
8.1.3.4. Uprawnienia Rzecznika Praw Pacjenta	269
8.1.4. Prawo do ochrony danych medycznych w przepisach wykonawczych do ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta	271
8.1.5. Prawo do ochrony danych medycznych w przepisach o ubezpieczeniu zdrowotnym	273

8.1.6. Prawo do ochrony danych medycznych w ustawie o systemie informacji w ochronie zdrowia	277
8.2. Prawo do ochrony danych medycznych w innych aktach normatywnych polskiego prawa administracyjnego	282

Rozdział 9

Odpowiedzialność za naruszenie przepisów o ochronie danych

medycznych	283
9.1. Odpowiedzialność administracyjna	283
9.1.1. Odpowiedzialność administracyjna jako instrument ochrony danych osobowych	283
9.1.2. Pojęcie oraz funkcje odpowiedzialności administracyjnej oraz sankcji administracyjnych na gruncie ochrony danych medycznych	285
9.1.3. Podmioty podlegające odpowiedzialności administracyjnej w związku z przetwarzaniem danych medycznych	286
9.1.3.1. Regulacja RODO	286
9.1.3.2. Regulacja ustawy o ochronie danych osobowych – problematyka NFZ i podmiotów publicznych prowadzących działalność leczniczą	287
9.1.4. Rodzaje sankcji administracyjnych	289
9.1.5. Kary pieniężne	290
9.1.5.1. Wprowadzenie kar pieniężnych jako materialnoprawnych sankcji administracyjnych	290
9.1.5.2. Wzajemne relacje pomiędzy przepisami RODO, k.p.a. oraz ustawy o ochronie danych osobowych w zakresie przepisów dotyczących kar pieniężnych	291
9.1.5.3. Autonomiczność kar pieniężnych	293
9.1.5.4. Podstawy nałożenia kary pieniężnej	293
9.1.5.5. Przesłanki decydujące o nałożeniu oraz wymiarze kary pieniężnej	295
9.1.5.6. Wysokość kar pieniężnych	297
9.1.6. Środki naprawcze stosowane przez organy nadzorcze	300
9.1.7. Postępowanie w przedmiocie naruszenia zasad przetwarzania danych medycznych	301
9.1.7.1. Regulacja RODO	301
9.1.7.2. Regulacja ustawy o ochronie danych osobowych – postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych	302
9.1.7.3. Proceduralna ochrona podmiotu w ramach postępowań dotyczących naruszenia przepisów o ochronie danych osobowych	306
9.1.8. Postępowanie kontrolne	307

9.2. Odpowiedzialność cywilnoprawna związana z naruszeniem norm nakazujących ochronę danych medycznych	309
9.2.1. Wprowadzenie	309
9.2.2. Cywilnoprawna ochrona danych medycznych według RODO ...	310
9.2.2.1. Wprowadzenie	310
9.2.2.2. Relacja cywilnoprawnych środków ochrony danych medycznych przewidziana w RODO do innych środków ochrony przewidzianych tym rozporządzeniem (relacja przepisów prawa prywatnego do przepisów prawa publicznego)	312
9.2.2.3. Pojęcie skutecznego środka ochrony (ang. <i>effective judicial remedy</i>)	315
9.2.2.4. Charakter konstrukcji przewidzianej w art. 82 RODO ...	319
9.2.2.5. Stosowanie art. 82 RODO w polskim systemie prawnym	320
9.2.2.6. Proceduralne aspekty dochodzenia roszczeń cywilnoprawnych przewidzianych w RODO przed sądem polskim	326
9.2.2.7. Zagadnienia kolizyjnoprawne w związku z dochodzeniem roszczeń cywilnoprawnych za naruszenie zasad ochrony danych medycznych na podstawie RODO	344
9.2.3. Ochrona danych medycznych za pomocą przepisów Kodeksu cywilnego	346
9.2.3.1. Wprowadzenie	346
9.2.3.2. Relacja przepisów Kodeksu cywilnego do RODO w sferze ochrony danych medycznych	348
9.2.3.3. Adekwatność reżimu ochrony dóbr osobistych dla cywilnoprawnej ochrony danych osobowych – uwagi wprowadzające i rys historyczny	351
9.2.3.4. Środki ochrony dóbr osobistych przewidziane w Kodeksie cywilnym w przypadku naruszenia reguł ochrony danych medycznych – możliwość samoistnej ochrony bez odesłania z art. 92 u.o.d.o.	358
9.2.4. Ochrona cywilnoprawna danych medycznych w ramach reżimu odpowiedzialności z umowy – wzmianka	360
9.2.5. Ochrona cywilnoprawna danych medycznych przewidziana w ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta	362
9.2.5.1. Wprowadzenie	362
9.2.5.2. Relacja art. 4 u.p.p. do regulacji ogólnej Kodeksu cywilnego	362
9.2.5.3. Znaczenie wyłączeń opisanych w art. 4 ust. 3 u.p.p. dla ochrony danych medycznych	364

9.2.6. Podsumowanie podrozdziału o cywilnoprawnej ochronie danych medycznych	365
--	-----

Rozdział 10

Ochrona danych medycznych na podstawie przepisów polskiego prawa

karnego	370
10.1. Wstęp – zmiany na podstawie RODO i dyrektywy 2016/680	370
10.2. Ochrona danych medycznych na podstawie przepisów prawa karnego materialnego	372
10.2.1. Ochrona danych medycznych według przepisów karnych zawartych w ustawie o ochronie danych osobowych	372
10.2.1.1. Niedopuszczalne i nieuprawnione przetwarzanie danych (art. 101 ust. 2)	373
10.2.1.2. Udaremnienie lub utrudnianie prowadzenia kontroli (art. 108)	376
10.2.2. Ochrona danych medycznych przepisami Kodeksu karnego ...	378
10.2.2.1. Ujawnienie lub wykorzystanie tajemnicy zawodowej, prywatnej i służbowej	378
10.2.2.2. Bezprawne uzyskanie informacji	380
10.2.2.3. Utrudnianie dostępu do bazy danych	382
10.3. Ochrona danych medycznych za pomocą przepisów postępowania karnego	382
10.3.1. Ochrona danych medycznych a art. 237 k.p.k.	383
10.3.2. Kontrola rozmów a owoce zatrutego drzewa	385

Rozdział 11

Tajemnica zawodowa osób zatrudnionych w służbie zdrowia	389
11.1. Tajemnica zawodowa elementem ochrony danych medycznych	389
11.2. Tajemnica lekarska	392
11.2.1. Ustawa o zawodach lekarza i lekarza dentysty	393
11.2.2. Wyjątki od obowiązku zachowania tajemnicy lekarskiej w ustawie o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi	396
11.2.2.1. Ustawa o ochronie zdrowia psychicznego	398
11.2.2.2. Ustawa o cmentarzach i chowaniu zmarłych	399
11.2.3. Obowiązek zachowania tajemnicy lekarskiej w związku z toczącym się postępowaniem	399
11.2.3.1. Tajemnica lekarska a postępowanie cywilne	399
11.2.3.2. Tajemnica lekarska w postępowaniu karnym	400
11.2.4. Tajemnica lekarska w Kodeksie etyki lekarskiej	403
11.3. Tajemnica pielęgniarki i położnej	404
11.4. Tajemnica aptekarska	405
11.5. Inne ustawy	406

11.6. Odpowiedzialność za naruszenie tajemnicy lekarskiej	407
11.6.1. Odpowiedzialność cywilna	407
11.6.2. Odpowiedzialność karna	408
11.6.3. Odpowiedzialność zawodowa pracowników służby zdrowia ...	408
Bibliografia	411
Wykaz najważniejszych orzeczeń	419
O Autorach	421