

SPIS TREŚCI

Wykaz skrótów	15
Słowo wstępne	17

Rozdział 1

Zagadnienia wprowadzające, zakres zastosowania

i podstawowe pojęcia	19
1.1. Zagadnienia ogólne	19
1.2. Zakres zastosowania	22
1.2.1. Zakres przedmiotowy	22
1.2.2. Zakres terytorialny	26
1.3. Najważniejsze pojęcia	27
1.3.1. Dane osobowe	28
1.3.1.1. Wszelkiego rodzaju informacje	29
1.3.1.2. Informacje dotyczące osoby fizycznej	31
1.3.1.3. Informacje pozwalające na zidentyfikowanie osoby fizycznej	31
1.3.1.4. Osoba fizyczna	33
1.3.1.5. Dane zwykle i szczególne kategorie danych	33
1.3.2. Przetwarzanie	34
1.3.3. Profilowanie	35
1.3.4. Administrator	36
1.3.5. Podmiot przetwarzający	37
1.3.6. Odbiorca	38
1.3.7. Osoba, której dane dotyczą (podmiot danych)	38
1.3.8. Przedsiębiorca i grupa przedsiębiorców	40
1.3.9. Usługa społeczeństwa informacyjnego	42
1.3.10. Podejście oparte na ryzyku	46

1.3.11. Naruszenie ochrony danych osobowych	47
1.3.12. Organ nadzorczy	48
1.3.13. Klauzule kompetencyjne dla państw członkowskich	48

Rozdział 2

Zasady przetwarzania danych osobowych	50
2.1. Zagadnienia ogólne	50
2.2. Zasada legalności i rzetelności	51
2.3. Zasada przejrzystości	52
2.4. Zasada ograniczenia celu	56
2.5. Zasada prawidłowości	59
2.6. Zasada minimalizacji danych	60
2.7. Zasada ograniczenia przechowywania	61
2.8. Zasada integralności i poufności	63
2.9. Zasada rozliczalności	64

Rozdział 3

Przesłanki legalizacyjne przetwarzania danych osobowych	67
3.1. Zagadnienia ogólne	67
3.2. Zgoda	71
3.2.1. Dobrowolność zgody	71
3.2.2. Konkretność zgody	73
3.2.3. Świadomość zgody	74
3.2.4. Jednoznaczność zgody	75
3.2.5. Rozliczalność zgody	78
3.2.6. Wyraźność zgody	78
3.2.7. Forma zgody	79
3.2.8. Dodatkowe wymogi dotyczące pisemnej zgody	80
3.2.9. Wycofanie zgody	82
3.2.10. Zgoda dziecka	83
3.2.11. Zgody dotychczasowe	86
3.3. Niezbędność do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy	88
3.3.1. Wykonanie umowy	89
3.3.2. Działania przed zawarciem umowy	91

3.4. Niezbędność do wypełnienia obowiązku prawnego ciążącego na administratorze	92
3.4.1. Obowiązek prawny	93
3.4.2. Niezbędność	94
3.5. Niezbędność do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi	94
3.6. Niezbędność do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej	97
3.7. Niezbędność do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią	98
3.8. Przetwarzanie szczególnych kategorii danych osobowych	102
3.8.1. Szczególne kategorie danych	102
3.8.2. Szczególne kategorie danych w handlu elektronicznym	104
3.8.3. Przesłanki legalizacyjne szczególnych kategorii danych	107
3.8.4. Przesłanki legalizacyjne szczególnych kategorii danych – wybrane zagadnienia	109
3.8.4.1. Zgoda na przetwarzanie danych osobowych szczególnych kategorii	109
3.8.4.2. Żywotny interes	110
3.8.4.3. Upublicznienie danych	110
3.8.4.4. Interes publiczny	111
3.8.4.5. Przetwarzanie wrażliwych danych osobowych w celach medycznych i związanych z ochroną zdrowia	113

Rozdział 4

Prawa podmiotów danych	115
4.1. Zagadnienia ogólne	115
4.2. Prawa informacyjne	118
4.3. Prawo dostępu do danych	126
4.4. Prawo do usunięcia danych („prawo do bycia zapomnianym”)	130

4.4.1. Zasady korzystania z prawa do usunięcia danych	130
4.4.2. Wyłączenia od prawa do usunięcia danych oraz prawa do bycia zapomnianym	132
4.4.3. Prawo do bycia zapomnianym a wolność wypowiedzi	133
4.5. Prawo do przenoszenia danych	133
4.6. Prawo do niepodlegania profilowaniu	138
4.6.1. Pojęcie profilowania	138
4.6.2. Zautomatyzowane podejmowanie decyzji	139
4.6.3. Warunki dopuszczalności	141
4.6.4. Gwarancje związane z profilowaniem	142
4.7. Ograniczenie przetwarzania	142
4.7.1. Pojęcie	142
4.7.2. Okoliczności, w jakich można żądać ograniczenia przetwarzania	144
4.7.2.1. Zakwestionowanie prawidłowości danych	145
4.7.2.2. Sprzeciw podmiotu danych wobec usunięcia danych mimo niezgodności przetwarzania danych z prawem	145
4.7.2.3. Zbędność danych osobowych do celów przetwarzania przez administratora i jednocześnie występowanie potrzeby dostępu do danych osoby, której one dotyczą, w celu ustalenia, dochodzenia lub obrony roszczeń	146
4.7.2.4. Wniesienie sprzeciwu przez osobę, której dane dotyczą	146
4.7.3. Sposób wykonania obowiązku przez administratora	147
4.7.3.1. Techniczny aspekt ograniczenia przetwarzania	147
4.7.3.2. Formalny aspekt ograniczenia przetwarzania	148
4.7.3.3. Wyjątki	148
4.7.4. Uprawniony do żądania ograniczenia przetwarzania danych osobowych i zakres żądania	149

4.7.5. Okres oznaczenia danych w celu ograniczenia ich przetwarzania	150
4.7.6. Dalsze obowiązki administratora związane z ograniczeniem przetwarzania	152
4.7.7. Odpowiedzialność administratora	153

Rozdział 5

Nowe obowiązki administratorów	154
5.1. Zagadnienia ogólne	154
5.2. Ogólny obowiązek zapewnienia zgodności przetwarzania z rozporządzeniem 2016/679	158
5.2.1. Ryzyko jako element wyznaczający standard ochrony	159
5.2.2. Zapewnienie zgodności przetwarzania z RODO jako element oceniany przez pryzmat konsekwencji dla podmiotu danych	160
5.3. Ochrona danych w fazie projektowania i domyślna ochrona danych	162
5.3.1. Ochrona danych w fazie projektowania – pojęcie	162
5.3.2. Podstawowe zasady ochrony danych w fazie projektowania	166
5.3.2.1. Podejście proaktywne, a nie reaktywne, zaradcze, a nie naprawcze	166
5.3.2.2. Domyślna ochrona danych	168
5.3.2.3. Prywatność włączona w projekt	170
5.3.2.4. Pełna funkcjonalność rozumiana jako osiągnięcie sumy dodatniej, a nie sumy zerowej	171
5.3.2.5. Ochrona prywatności od początku do końca cyklu życia informacji	173
5.3.2.6. Transparentność i przejrzystość	174
5.3.2.7. Poszanowanie dla prywatności użytkowników	175
5.3.3. Zasada <i>privacy by design</i> – prywatność wpisana w projekt rozwiązania	176
5.3.4. Realizacja zasady <i>privacy by default</i>	177

5.3.5. Okres stosowania zasady	177
5.3.6. Czynniki wpływające na decyzje administratora w zakresie zastosowania odpowiednich środków ochrony danych osobowych	178
5.3.6.1. Stan wiedzy technicznej	178
5.3.6.2. Koszt wdrożenia	179
5.3.6.3. Charakter, zakres, kontekst i cele przetwarzania	179
5.3.6.4. Ryzyko naruszenia praw i wolności osób fizycznych	180
5.3.7. Odpowiednie środki techniczne i organizacyjne	182
5.3.8. Cele realizowane przez zasadę <i>privacy by default</i>	184
5.3.9. Obowiązek dokumentacyjny	185
5.3.10. Odpowiedzialność administratora (procesora)	185
5.4. Dokumentacja przetwarzania	187
5.4.1. Rejestr czynności przetwarzania	190
5.4.1.1. Zakres danych w rejestrze	190
5.4.1.2. Forma rejestru	192
5.4.1.3. Podmioty zobowiązane do prowadzenia rejestru	192
5.4.1.4. Przykładowy rejestr czynności przetwarzania	193
5.4.2. Rejestr kategorii czynności przetwarzania	195
5.4.3. Polityki ochrony danych	196
5.4.4. Dokumentacja naruszeń ochrony danych i zgłoszenie naruszenia	199
5.4.4.1. Dokumentacja wszelkich naruszeń ochrony danych	199
5.4.4.2. Dokumentacja zgłoszeń naruszeń ochrony danych organowi nadzorcemu	200
5.4.4.3. Dokumentacja zgłoszeń naruszeń ochrony danych podmiotowi danych	201
5.4.5. Dokumentacja oceny skutków dla ochrony danych	202
5.4.6. Dokumentacja uprzednich konsultacji	203
5.4.7. Dokumentacja transferów danych do państw trzecich	203

5.5. Bezpieczeństwo przetwarzania	204
5.5.1. Zasada proporcjonalności	205
5.5.2. Środki techniczne i organizacyjne zapewniające odpowiedni poziom ochrony	206
5.5.3. Obowiązek aktualizacji zabezpieczeń	208
5.5.4. Parametry oceny środków bezpieczeństwa	209
5.5.5. Dokumentacja środków bezpieczeństwa	210
5.6. Ocena skutków dla ochrony danych	211
5.6.1. Przesłanki prowadzenia oceny skutków dla ochrony danych	212
5.6.2. Elementy oceny skutków dla ochrony danych	213
5.6.3. Gromadzenie informacji niezbędnych do dokonania oceny skutków dla ochrony danych	215
5.6.4. Uprzedni charakter oceny	216
5.6.5. Konsultacje z osobami, których dane dotyczą, lub ich przedstawicielami	217
5.7. Uprzednie konsultacje	218
5.7.1. Przesłanki prowadzenia uprzednich konsultacji	218
5.7.2. Rezultat uprzednich konsultacji	218
5.7.3. Zakres informacji przekazywanych w ramach uprzednich konsultacji	220
5.8. Zgłoszenia naruszeń	221
5.8.1. Zgłaszanie naruszenia organowi nadzorcemu	221
5.8.2. Zawiadamianie podmiotów danych o naruszeniach ochrony danych osobowych	223

Rozdział 6

Powierzenie przetwarzania i współadministrowanie	226
6.1. Powierzenie przetwarzania	226
6.1.1. Zagadnienia ogólne	226
6.1.2. Wybór podmiotu przetwarzającego	229
6.1.3. Podstawy powierzenia	231
6.1.4. Forma umowy powierzenia	232
6.1.5. Zakres przedmiotowy umowy powierzenia	233
6.1.6. Obowiązki procesora	235
6.1.7. Łańcuch powierzeń – warunki korzystania z usług podwykonawców	238

6.1.8. Odpowiedzialność podmiotu przetwarzającego za naruszenie ochrony danych	241
6.1.9. Powierzenie danych do państw trzecich	242
6.1.10. Umowy powierzenia zawarte na podstawie przepisów ustawy o ochronie danych osobowych	243
6.2. Współadministrowanie	244
6.2.1. Zagadnienia ogólne	244
6.2.2. Pojęcie współadministratora	244
6.2.3. Uzgodnienia i ich udostępnianie	246
6.2.4. Zapewnienie realizacji praw osób, których dane dotyczą	247

Rozdział 7

Przekazywanie danych do państw trzecich i organizacji

międzynarodowych	249
7.1. Zagadnienia ogólne	249
7.2. Podstawy przekazywania	251
7.2.1. Przekazywanie na podstawie decyzji stwierdzającej odpowiedni poziom ochrony	253
7.2.2. Przekazywanie z zastrzeżeniem odpowiednich zabezpieczeń	256
7.2.3. Przekazywanie w szczególnych sytuacjach	258

Rozdział 8

Inspektor ochrony danych osobowych	261
8.1. Zagadnienia ogólne	261
8.2. Obowiązek wyznaczenia IOD	262
8.2.1. Podmiot publiczny	263
8.2.2. Podmioty wskazane w art. 37 ust. 1 lit. b, c RODO	264
8.3. Wyznaczenie IOD	266
8.4. Wspólny IOD	267
8.5. Status IOD	268
8.6. Zadania IOD	271
8.6.1. Informowanie oraz doradztwo	271
8.6.2. Nadzór	272
8.6.3. Komunikacja	273

Rozdział 9

Kodeksy postępowania i certyfikacja	275
9.1. Kodeksy postępowania	275
9.1.1. Charakter kodeksów postępowania	276
9.1.2. Zakres przedmiotowy kodeksów postępowania	276
9.1.3. Weryfikacja i zatwierdzanie kodeksów postępowania	278
9.2. Monitorowanie zatwierdzonych kodeksów postępowania	279
9.2.1. Warunki uzyskania akredytacji	280
9.2.2. Uprawnienia podmiotu akredytowanego	281
9.3. Certyfikacja	281
9.3.1. Charakter certyfikacji i korzyści płynące z certyfikacji	282
9.3.2. Proces certyfikacji	283
9.4. Podmioty certyfikujące	284
9.4.1. Zasady udzielania akredytacji dla podmiotów certyfikujących	284
9.4.2. Sposób udzielania akredytacji i czas jej trwania	285

Rozdział 10

Organ nadzorczy i postępowanie kontrolne	287
10.1. Organ nadzorczy	287
10.1.1. Zagadnienia ogólne	287
10.1.2. Właściwość miejscowa organu nadzorczego	288
10.1.3. Kompetencje organu nadzorczego	289
10.1.4. Uprawnienia organu nadzorczego	291
10.2. Postępowanie kontrolne	292
10.2.1. Zagadnienia ogólne	292
10.2.2. Pojęcie kontroli	293
10.2.3. Procedura kontrolna	294

Rozdział 11

Środki ochrony prawnej, odpowiedzialność i sankcje	304
11.1. Uprawnienia organu nadzorczego	304
11.1.1. Uprawnienia naprawcze organu nadzorczego	304
11.1.2. Administracyjne kary pieniężne	305

11.1.2.1. Naruszenia podlegające administracyjnym karom pieniężnym	306
11.1.2.2. Podmioty podlegające administracyjnym karom pieniężnym	308
11.1.2.3. Wysokość i kumulacja sankcji	308
11.1.2.4. Kryteria wymiaru administracyjnych kar pieniężnych	309
11.2. Uprawnienia podmiotu danych	311
11.2.1. Prawo do wniesienia skargi do organu nadzorczego ..	311
11.2.1.1. Podmioty uprawnione do wniesienia skargi i podstawy do jej wniesienia	311
11.2.1.2. Właściwość miejscowa organu nadzorczego	311
11.2.1.3. Przebieg postępowania	312
11.2.2. Prawo do odszkodowania	313
11.2.2.1. Podmioty zobowiązane do uiszczenia odszkodowania	313
11.2.2.2. Przesłanki odpowiedzialności odszkodowawczej	315
11.2.2.3. Charakter i wymiar odszkodowania	316
11.2.2.4. Właściwość miejscowa sądu	317
11.3. Inne sankcje	317
11.3.1. Sankcje karne	318
11.3.2. Sankcje dyscyplinarne	318
Bibliografia	319
O autorach	331