

Spis treści

Wykaz skrótów	XIX
Wprowadzenie	XXV
Rozdział I. Historia kształtowania się prawa do ochrony danych osobowych	1
1. Pojęcie prywatności	1
2. Pojęcie ochrony danych osobowych	2
3. Dane osobowe jako tajemnica	3
4. Regulacje dotyczące ochrony danych i prywatności	3
4.1. Powszechna deklaracja praw człowieka	5
4.2. Konwencja o ochronie praw człowieka i podstawowych wolności	5
4.3. Ustawa o ochronie danych osobowych w Hesji	5
4.4. Rezolucja 22 i 29	6
4.5. Wytoczne OECD	6
4.6. Konwencja Nr 108	6
4.7. Dyrektywa 95/46/WE	7
4.8. Konstytucja RP	9
4.9. Ustawa o ochronie danych osobowych z 1997 r.	10
4.10. Kodeks cywilny	12
4.11. Karta praw podstawowych Unii Europejskiej	12
4.12. Ogólne rozporządzenie o ochronie danych	13
4.13. Ustawa o ochronie danych osobowych z 2018 r.	16
Rozdział II. Obecne przepisy o ochronie danych osobowych	17
1. Zasady implementacji prawa unijnego	17
2. Przepisy RODO	18
2.1. Główne założenia RODO	18
2.2. Zasięg terytorialny RODO	20
2.3. Zakres stosowania RODO	21
2.4. Podstawowe zasady przetwarzania danych osobowych	23

2.4.1. Zgodność z prawem, rzetelność i przejrzystość przetwarzania danych	23
2.4.2. Ograniczenie celu zbierania i przetwarzania danych	23
2.4.3. Minimalizacja danych	24
2.4.4. Prawidłowość danych	24
2.4.5. Ograniczenie przechowywania danych	24
2.4.6. Integralność i poufność przetwarzania danych	25
2.4.7. Rozliczalność	25
2.5. Przesłanki legalności przetwarzania danych osobowych zwykłych	26
2.6. Zgoda na przetwarzanie danych osobowych	26
2.7. Prawa podmiotu danych	27
2.8. Wbudowana ochrona danych	30
2.9. Zaufani partnerzy w biznesie	30
2.10. Inspektor ochrony danych – administrator bezpieczeństwa informacji	31
2.11. Ocena skutków dla ochrony danych	32
2.12. Zabezpieczenie danych	33
2.13. Zgłaszanie naruszeń ochrony danych	33
2.14. Rejestr czynności przetwarzania	33
2.15. Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych	34
2.16. Kary za naruszenie przepisów RODO	34
3. Przepisy ustawy o ochronie danych osobowych	35
3.1. Organ nadzoru – Prezes Urzędu Ochrony Danych Osobowych	36
3.2. Wystąpienia organu nadzoru	37
3.3. Pomocne materiały publikowane przez organ nadzoru	37
3.4. Postępowanie przed organem nadzorczym	38
3.5. Obowiązek powołania inspektora ochrony danych	38
3.6. Odpowiedzialność administracyjna i karna	38
4. Wpływ przepisów o ochronie danych osobowych na działalność przedsiębiorstwa	39
Rozdział III. Najważniejsze definicje w przepisach o ochronie danych osobowych ...	43
1. Zagadnienia wstępne	43
2. Terminy zawarte w RODO	44
2.1. Dane osobowe	44
2.2. Dane szczególnych kategorii – dane wrażliwe	48
2.3. Dane zwykłe	49
2.4. Dane biometryczne	49
2.5. Uwierzytelnienie	50
2.6. Osoba dorosła i dziecko	50
2.7. Prawa i wolności osób	50

2.8. Główna działalność	52
2.9. Przetwarzanie danych	52
2.10. Duża skala przetwarzania	54
2.11. Zbieranie danych	55
2.12. Uzasadniony (prawnie) interes	56
2.13. Odbiorca danych	57
2.14. Strona trzecia	57
2.15. Zbiór danych osobowych	58
2.16. Przesłanki legalności	58
2.17. Upoważnienie do przetwarzania danych osobowych	59
2.18. Administrator danych osobowych	59
2.19. Współadministrator	60
2.20. Firma	60
2.21. Zgoda	60
2.22. Państwo trzecie	61
2.23. Przetwarzający (procesor)	61
2.24. Powierzenie przetwarzania danych	62
2.25. Pseudonimizacja	62
2.26. Anonimizacja	63
2.27. Ograniczenie przetwarzania	63
2.28. Ocena skutków dla ochrony danych	64
2.29. Profilowanie	64
2.30. Naruszenie ochrony danych osobowych	65
2.31. Inspektor ochrony danych	65
2.32. Grupa Robocza Art. 29 – Europejska Rada Ochrony Danych	66
3. Pozostałe przydatne terminy	68
3.1. Organy i podmioty publiczne	68
3.2. Generalny Inspektor Ochrony Danych Osobowych – Prezes Urzędu Ochrony Danych Osobowych	68
3.3. Polityka bezpieczeństwa informacji/polityka ochrony danych	69
3.4. Interes publiczny	70
3.5. Informacje i dane	70
3.6. Oświadczenie woli	72
3.7. Upublicznienie danych	72
3.8. Europejski Obszar Gospodarczy	72
3.9. Tajemnica prawnie chroniona	73
Rozdział IV. Najczęściej spotykane rodzaje danych osobowych	75
1. Zagadnienia wstępne	75
2. Dane osobowe zwykłe	79
2.1. Imię i nazwisko	79

2.2. Dane kontaktowe	81
2.2.1. Adres i kod pocztowy, dzielnica miasta	82
2.2.2. Numer telefonu	83
2.2.3. Adres e-mail	85
2.2.4. Identyfikatory w komunikatorach internetowych	87
2.3. Geolokalizacja i monitorowanie położenia	88
2.4. Numer dokumentu	91
2.5. Numer PESEL	91
2.6. Oznaczenia licencji na wykonywanie zawodu	94
2.7. Numer IP	95
2.8. Adres strony internetowej	99
2.9. Login i nick	99
2.10. Numer rejestracyjny samochodu, VIN	100
2.11. Numer rachunku bankowego	101
2.12. Dane osoby fizycznej prowadzącej działalność gospodarczą	102
2.13. Numer NIP	103
2.14. Numer REGON	103
2.15. Numer karty płatniczej	104
2.16. Wizerunek, zdjęcie, nagranie wideo, monitoring	104
2.17. Tożsamość osoby	105
2.18. Profil	105
2.19. Kody paskowe, 2D, 3D	106
2.20. Notatki na dokumentach	106
2.21. Rozmiar odzieży i obuwia	107
3. Dane osobowe szczególnych kategorii	107
3.1. Dane biometryczne	108
3.2. Dane o stanie zdrowia	109
3.3. Dane osób nieżyjących i nieurodzonych	111
3.3.1. Osoby zmarłe	111
3.3.2. Dane dziecka jeszcze nieurodzonego	112
4. Przykładowe sytuacje, w których informacje stają się danymi osobowymi i odwrotnie	112
5. Procedura rozpoznawania danych osobowych	113
5.1. Identyfikacja osoby	114
5.2. Możliwość zidentyfikowania	114
5.3. Dane dotyczące osoby	114
5.4. Cel przetwarzania – wpływanie na decyzje	114
Rozdział V. System ochrony danych w kilkunastu krokach	117
1. Zagadnienia wstępne	117
2. Identyfikacja procesów biznesowych i danych osobowych	117

3. Karty procesów przetwarzania	118
4. Przesłanki legalności danych (w tym zgody)	119
5. Obowiązki informacyjne	119
6. Minimalizacja danych	119
7. Retencja danych	120
8. Prawa osób, których dane dotyczą	121
9. Umowy powierzenia przetwarzania	121
10. Transfery do państw trzecich	121
11. Ocena skutków dla ochrony danych	122
12. Bezpieczeństwo danych osobowych	122
13. Postępowanie w przypadku naruszenia ochrony danych osobowych	123
14. Budowanie świadomości	123
15. Nadzór nad systemem	124
Rozdział VI. Zbieranie i gromadzenie danych osobowych	125
1. Czynności wstępne	125
2. Zbieranie danych	125
3. Spełnienie przesłanki legalności przetwarzania danych	126
4. Adekwatność danych do celów przetwarzania	127
5. Obowiązek informacyjny	130
6. Odnotowywanie daty i okoliczności zebrania danych	131
7. Zbieranie danych dzieci i od dzieci	132
8. Aktualność danych	134
Rozdział VII. Przetwarzanie danych osobowych przez różne działy firmy	137
1. Zagadnienia wstępne	137
2. Dział personalny	137
2.1. Przetwarzanie danych w związku z zatrudnieniem	139
2.1.1. Zatrudnienie na podstawie umowy cywilnoprawnej	140
2.1.2. Samozatrudnienie	141
2.2. Przetwarzanie danych w związku z rekrutacją	141
2.2.1. Head hunterzy	142
2.2.2. Rekrutacje ukryte (ślepe)	142
2.2.3. Zaświadczenie o niekaralności, badania wariografem	143
2.2.4. Sprawdzanie kandydatów w serwisach internetowych	144
2.2.5. Listy referencyjne, <i>background screening</i>	145
2.2.6. Testy psychometryczne	146
2.2.7. Czarne listy kandydatów do pracy	146
2.3. Wypożyczanie pracowników	146
2.3.1. Pracownik tymczasowy	146
2.3.2. Pracownik wypożyczony od innego pracodawcy	147

2.4. Udostępnianie danych pracowników	147
2.4.1. Obowiązek noszenia identyfikatorów	147
2.4.2. Dane pracowników na firmowej stronie internetowej	148
2.4.3. Udostępnianie komornikowi danych pracowników	150
2.4.4. Kupowanie pracownikom biletów, rezerwowanie hotelu	151
2.4.5. Przekazywanie danych zakładom świadczącym prywatną opiekę medyczną	151
2.4.6. Ujawnianie informacji o wynagrodzeniu	151
2.5. Wymiana informacji między pracownikami	152
2.6. Okresowa ocena pracownika	152
2.7. Wypadki przy pracy	153
2.8. Wnioski urlopowe	153
2.9. Zwalnianie i wręczanie wypowiedzenia	154
2.10. Monitorowanie pracowników	154
2.10.1. Monitoring wizyjny	155
2.10.2. Monitoring poczty elektronicznej i analiza korzystania z Internetu ..	157
2.10.2.1. Blokowanie dostępu do Internetu	158
2.10.2.2. Wypowiedzi pracowników w Internecie	159
2.10.3. Monitoring korespondencji	159
2.10.4. Monitoring telefonów służbowych	159
2.10.5. Nawigacja GPS w samochodzie	160
2.10.6. Kamera w samochodzie	161
2.10.7. Kontrola czasu pracy	162
2.10.8. Monitorowanie w celu bezpieczeństwa	163
3. Dział administracji	163
3.1. Korespondencja pocztowa	163
3.1.1. Usługi pocztowe	163
3.1.2. Adresowanie przesyłek	164
3.1.3. Rozpowszechnianie korespondencji	165
3.2. Kontrola dostępu do pomieszczeń	165
3.3. Służby ochrony, zapobieganie oszustwom	166
3.4. Serwis sprząający	169
3.5. Tablice informacyjne na budowie	169
4. Dział marketingu	170
4.1. Promowanie własnych i cudzych produktów	170
4.2. Lista Robinsonów	172
4.3. Kupno bazy danych klientów	172
4.4. Fanpage na Facebooku	173
4.5. Konkursy i loterie, programy lojalnościowe	174
4.6. Publikowanie list klientów	175

4.7. Wysyłanie życzeń świątecznych do klientów	175
4.8. Druki bezadresowe	175
4.9. Zbieranie danych z Internetu i z książek telefonicznych	175
4.10. Automaty dzwoniące	176
4.11. Telemarketing	176
4.12. Kontakt z użyciem komunikatorów	177
4.13. Przetwarzanie w systemach CRM, hurtowniach danych i Big Data	178
4.14. Mailing elektroniczny	179
4.15. Publikowanie zdjęć i nagrań wideo	180
4.16. Dane z wizytówek, dane współpracowników	181
5. Dział sprzedaży	181
5.1. Używanie wideo do weryfikacji tożsamości klientów	181
5.2. Sprzedaż jako umowa	182
5.3. Zgoda na przetwarzanie danych jako zapłata	183
5.4. Sklep internetowy	184
5.5. Usługi hotelowe	185
5.6. Zatrzymywanie dokumentów jako zastawu	186
5.7. Sieć sprzedawców – sprzedaż przez agentów ubezpieczeniowych	186
5.8. <i>Cross-selling</i> i <i>up-selling</i>	187
5.9. Wystawianie faktur i rachunków	188
6. Dział obsługi klienta	189
6.1. Identyfikacja klienta	189
6.2. Przyjmowanie sprzeciwów, skarg, odwołań dotyczących zgody oraz zgłoszeń naruszenia ochrony danych osobowych	190
6.3. Udostępnianie lub przenoszenie danych	190
6.4. Obsługa klienta za pośrednictwem strony internetowej	191
6.5. Korespondencja e-mailowa z klientem	191
6.6. Telefoniczne centrum obsługi klienta	192
6.7. Stanowisko obsługi klienta, wywoływanie klienta w obecności innych osób	193
6.8. Ocena wykonywanych usług	195
7. Dział finansów i księgowości	195
7.1. Wykonywanie przelewów i e-przelewów	196
7.2. Prowadzenie księgowości przez biuro	197
7.3. Udostępnianie danych urzędом skarbowym	197
7.4. Podatek VAT od czynności dotyczących danych osobowych	197
8. Dział windykacji i obsługi długów	198
8.1. Miękka windykacja, rejestr dłużników	199
8.2. Sprzedaż długu – cesja wierzytelności	200
9. Dział informatyki	201
9.1. Firmowa strona internetowa – zbieranie danych przez Internet	202

9.2. Hosting i outsourcing witryny	203
9.3. Przetwarzanie w chmurze	204
9.4. Zabezpieczenie witryny i innych usług internetowych	205
9.5. Pliki <i>cookies</i>	206
9.6. Aplikacje mobilne dla klientów	208
9.7. Środowiska testowe i deweloperskie	210
Rozdział VIII. Nadawanie uprawnień do przetwarzania danych osobowych	213
1. Zagadnienia wstępne	213
2. Upoważnienie do przetwarzania danych osobowych	213
2.1. Upoważnienie w formie pisemnej	214
2.2. Wzór upoważnienia	215
3. Oświadczenia o ochronie danych osobowych	216
4. Szkolenia z ochrony danych osobowych	217
5. Uprawnienia w systemach informatycznych	218
5.1. Model RBAC	219
5.2. Poziom dostępu	219
Rozdział IX. Dane osobowe w grupach przedsiębiorstw	221
1. Zagadnienia wstępne	221
2. Korzyści dla grup przedsiębiorstw wynikające z wprowadzenia RODO	223
3. Powody wymiany informacji w grupach przedsiębiorstw	225
4. Synergia w grupach kapitałowych	226
5. Uzyskiwanie odpowiednich zgód na marketing w grupie przedsiębiorstw	227
6. Agregowanie danych w grupach kapitałowych	228
7. Sprzedaż, połączenie i podział spółek	229
Rozdział X. Formuły zgody na przetwarzanie danych osobowych	233
1. Zagadnienia wstępne	233
2. Zgoda w dawnych i obecnych przepisach o ochronie danych osobowych	234
3. Zakres stosowania zgody	235
4. Warunki wyrażenia zgody	236
5. Zgody zbierane przez Internet	240
6. Zgody wyrażane przez dzieci	240
7. Zgoda na marketing	242
8. Zgoda na kontakt telefoniczny	245
9. Zgoda na nagranie wideo lub na fotografowanie	246
10. Zgoda na nagrywanie rozmów	246
11. Zgoda na rekrutację	248
12. Odwołanie zgody	249
13. Multizgody	249
14. Przykładowe formuły zgody	251

Rozdział XI. Identyfikacja i ocena ryzyka	269
1. Zagadnienia wstępne	269
2. Znaczenie terminu „ryzyko” i teoretyczne podstawy zarządzania ryzykiem	270
3. Etapy zarządzania ryzykiem	272
3.1. Identyfikacja ryzyka	272
3.2. Analiza ryzyka	275
3.3. Ocena ryzyka	276
3.4. Sterowanie ryzykiem	277
3.5. Monitorowanie ryzyka	278
4. Ryzyko z perspektywy ochrony danych osobowych	279
4.1. Szacowanie ryzyka	279
4.2. Projektowanie przetwarzania	283
4.3. Ryzyko związane z podmiotami przetwarzającymi	283
4.4. Ryzyko związane z przyjęciem przetwarzania	284
5. Normy ISO dotyczące zarządzania ryzykiem	284
5.1. Norma ISO 29134	284
5.2. Norma ISO 31000	285
5.3. Norma ISO 27005	286
Rozdział XII. Ocena skutków dla ochrony danych	287
1. Zagadnienia wstępne	287
2. Definicja oceny skutków dla ochrony danych	288
3. Przeprowadzanie oceny skutków dla ochrony danych	292
3.1. Wysoki poziom ryzyka	292
3.2. Operacje znajdujące się w wykazie organu nadzoru	294
3.3. Operacje wynikające z art. 35 ust. 3 RODO	296
3.3.1. Profilowanie	296
3.3.2. Dane wrażliwe przetwarzane na dużą skalę	296
3.3.3. Monitorowanie na dużą skalę miejsc publicznych	297
4. Przypadki, w których ocena skutków dla ochrony danych nie jest wymagana	297
5. Dokumentowanie oceny skutków dla ochrony danych	298
5.1. Opis operacji przetwarzania i ich ocena	298
5.2. Ocena ryzyka i środków zaradczych	300
6. Narzędzia do wykonywania oceny skutków dla ochrony danych	301
7. Konsultacje z inspektorem ochrony danych	302
8. Uprzednie konsultacje z organem	303
9. Monitorowanie ocen skutków dla ochrony danych	306
Rozdział XIII. Projektowanie nowego procesu przetwarzania danych osobowych	309
1. Zagadnienia wstępne	309
2. Etapy projektowania nowego procesu przetwarzania danych	310

2.1. Określenie celów przetwarzania danych osobowych	311
2.2. Przeprowadzenie oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych	316
2.3. Zapewnienie środków zmniejszających ryzyko	317
2.3.1. Ochrona na etapie projektowania oraz ochrona domyślna	317
2.3.2. Pseudonimizacja danych	320
2.3.3. Szyfrowanie danych	323
2.4. Zadbanie o jakość danych	324
2.5. Realizacja praw osób, których dane dotyczą	325
2.5.1. Prawo dostępu	326
2.5.2. Prawo do przenoszenia danych	327
2.6. Zmiany w systemach informatycznych	328
3. Dokumentowanie procesu przetwarzania	330
4. Standardy ISO w świetle RODO	331
4.1. Normy serii 27000	333
4.1.1. Norma ISO 27000	333
4.1.2. Norma ISO 27001	333
4.1.3. Norma ISO 27002	335
4.1.4. Norma ISO 27005	335
4.1.5. Norma ISO 27018	335
4.2. Normy serii 29000	336
4.2.1. Norma ISO 29100	336
4.2.2. Norma ISO 29101	337
4.2.3. Norma ISO 29134	338
4.2.4. Norma ISO 29151	338
4.2.5. Norma ISO 29190	338
4.3. Norma ISO 31000	338
Rozdział XIV. Powierzenie zleceniobiorcom przetwarzania danych osobowych	341
1. Zagadnienia wstępne	341
2. Przetwarzanie danych w imieniu administratora – typowe sytuacje	342
3. Kryteria, jakie muszą spełniać podmioty przetwarzające	343
3.1. Podmioty certyfikowane	344
3.2. Ocena ryzyka związanego z powierzeniem przetwarzania danych	345
4. Zawarcie umowy między podmiotami	346
4.1. Umowa powierzenia	348
4.2. Rodzaje danych, które można powierzyć do przetwarzania	350
5. Obowiązki zleceniodawcy	351
6. Obowiązki zleceniobiorcy	354
7. Powierzenie przetwarzania przedsiębiorcy zagranicznemu	355
8. Ograniczenia przy dalszym powierzeniu danych osobowych	356

9. Zmiana celu przetwarzania danych osobowych przez procesora	357
10. Przykładowe zapisy umowy powierzenia	358
Rozdział XV. Inspektor ochrony danych	363
1. Zagadnienia wstępne	363
2. Wyznaczenie inspektora ochrony danych	363
2.1. Organy i podmioty publiczne zobowiązane do wyznaczenia inspektora ochrony danych	365
2.2. Obowiązek wyznaczenia inspektora ochrony danych ze względu na systematyczne monitorowanie osób	365
2.3. Obowiązek wyznaczenia inspektora ochrony danych ze względu na przetwarzanie na dużą skalę szczególnych kategorii danych	366
2.4. Wyznaczanie inspektora ochrony danych pomimo braku takiego obowiązku	367
2.5. Organizacje spoza Unii Europejskiej a obowiązek wyznaczenia inspektora ochrony danych	367
3. Forma zatrudnienia inspektora ochrony danych	368
3.1. Jeden inspektor ochrony danych dla kilku organizacji	368
3.2. Kilku inspektorów ochrony danych w jednej organizacji	369
3.3. Inspektor ochrony danych z zewnątrz	369
4. Kryteria, jakie musi spełniać inspektor ochrony danych	371
5. Zadania inspektora ochrony danych	374
5.1. Informowanie stron o przepisach o ochronie danych osobowych	377
5.2. Doradzanie przy ocenie skutków dla ochrony danych	377
5.3. Współpraca z organem nadzorczym	378
5.4. Prowadzenie rejestru czynności przetwarzania danych osobowych	379
5.5. Monitorowanie przestrzegania przepisów	380
5.6. Zadania okresowe i planowanie	381
5.7. Prowadzenie rejestru odchyleń	382
6. Rola i odpowiedzialność inspektora ochrony danych w organizacji	383
7. Kontakt z inspektorem ochrony danych	385
8. Zgłaszanie inspektora ochrony danych do rejestracji	388
9. Administrowanie bezpieczeństwem	390
Rozdział XVI. Naruszenia bezpieczeństwa danych osobowych	395
1. Zagadnienia wstępne	395
2. Wymagania dotyczące zgłaszania naruszenia ochrony danych osobowych	396
3. Sytuacje, w których nie trzeba zgłaszać naruszenia ochrony danych osobowych	397
4. Zasady postępowania z incydentami w ustawie o krajowym systemie cyberbezpieczeństwa	399
5. Zasady postępowania z incydentami w ustawie – Prawo telekomunikacyjne	400
6. Proces zarządzania incydentami	400
6.1. Plan postępowania z incydentami	402

6.2. Wykrywanie i raportowanie incydentów	403
6.2.1. Odpowiednie środki organizacyjne	403
6.2.2. Rozwiązania techniczne wykrywające naruszenia	404
6.2.2.1. Systemy SIEM	404
6.2.2.2. Systemy IDS/IPS	405
6.2.2.3. Systemy NAC	406
6.2.2.4. Oprogramowanie antywirusowe	406
6.2.2.5. Skanowanie podatności	406
6.3. Ocena skutków naruszenia ochrony danych osobowych	406
6.4. Karta naruszenia ochrony danych osobowych	408
6.5. Zgłaszanie naruszenia do organu nadzorczego	409
6.6. Zgłaszanie naruszenia przez podmiot przetwarzający	412
6.7. Zawiadamianie osób, których dane dotyczą, o naruszeniu	412
6.8. Lekcje na przyszłość	414
7. Komunikacja z mediami w sprawie naruszenia bezpieczeństwa informacji	415
8. Zgłaszanie popełnienia przestępstwa	416
9. Postępowanie, gdy incydent przerodzi się w katastrofę	417
Rozdział XVII. Transfer danych osobowych poza kraj	419
1. Zagadnienia wstępne	419
2. Przekazywanie danych osobowych na obszarze Unii Europejskiej	420
3. Przekazywanie danych osobowych na obszarze Europejskiego Obszaru Gospodarczego	420
4. Przekazywanie danych osobowych do państw trzecich	421
4.1. Gwarancje ochrony	422
4.2. Program Tarcza Prywatności UE–USA	423
4.3. Mechanizmy przekazywania danych osobowych bez zgody organu	424
4.3.1. Standardowe klauzule umowne	424
4.3.2. Wiążące reguły korporacyjne	425
4.4. Wyjątki w szczególnych sytuacjach	427
4.5. Informowanie o przekazywaniu danych osobowych do państwa trzeciego .	429
Rozdział XVIII. Usuwanie danych osobowych	431
1. Zagadnienia wstępne	431
2. Prawo do usunięcia danych osobowych	432
3. Ograniczenie przetwarzania danych osobowych	433
3.1. Ograniczenie przetwarzania, gdy wygaśnie cel przetwarzania danych	434
3.2. Metody pozwalające ograniczyć przetwarzanie danych	435
4. Czas przetwarzania danych osobowych	436
4.1. Przetwarzanie danych ze względu na realizację umowy	436
4.2. Przetwarzanie danych ze względu na świadczenie usług drogą elektroniczną	438

4.3. Przetwarzanie danych pracowniczych	439
4.4. Przetwarzanie danych na podstawie wyrażonej zgody	440
4.5. Przetwarzanie danych a likwidacja przedsiębiorstwa	440
5. Proces usuwania danych osobowych	440
5.1. Całkowite usunięcie danych	442
5.1.1. Niszczenie dokumentów w formie papierowej	442
5.1.2. Usunięcie danych z systemu informatycznego	444
5.1.3. Fizyczne niszczenie nośników danych	446
5.1.4. Usunięcie danych z zapasowych kopii danych	446
5.1.5. Usunięcie danych z baz danych i aplikacji	447
5.2. Modyfikacja danych	447
Rozdział XIX. Ochrona i zabezpieczenie danych osobowych	453
1. Zagadnienia wstępne	453
2. Polityki ochrony danych	453
3. Dokumentacja przetwarzania danych	455
4. Bezpieczeństwo danych osobowych	456
5. Zabezpieczenia organizacyjne	457
5.1. Wstęp na obszar przetwarzania danych	458
5.1.1. Obsługa klientów i interesantów	458
5.1.2. Zabezpieczenie serwerowni	458
5.1.3. Oznaczanie obszarów przetwarzania	459
5.2. Zasada czystego biurka i ekranu	459
5.3. Wyrzucanie dokumentów do kosza	460
5.4. Praca poza firmą	460
5.5. Program budowania świadomości	461
6. Zabezpieczenia systemów informatycznych	462
6.1. Kontrola dostępu	463
6.2. Zasady tworzenia haseł	464
6.3. Zabezpieczenia komputera	465
6.3.1. Ochrona przed złośliwym oprogramowaniem	465
6.3.2. Szyfrowanie całego dysku	466
6.3.3. Samodzielne instalowanie programów	466
6.3.4. Poprawki bezpieczeństwa, aktualizacje	467
6.4. Zapasowe kopie danych	467
6.5. Pozbywanie się sprzętu	468
6.6. Szyfrowanie transmisji danych	468
Rozdział XX. Kontrola przestrzegania przepisów o ochronie danych osobowych	469
1. Zagadnienia wstępne	469
2. Uprawnienie do kontroli	469

3. Rodzaje kontroli	470
4. Zawiadomienie o kontroli	471
5. Przygotowanie do kontroli	472
6. Przebieg kontroli	473
6.1. Prawa i obowiązki kontrolera	474
6.2. Obowiązki przedsiębiorcy	476
7. Protokół kontroli	476
8. Uprawnienia w razie stwierdzenia nieprawidłowości	477
9. Miejsce przygotowane dla kontrolera	478
10. Utrudnianie kontroli	478
Rozdział XXI. Kary za przetwarzanie danych osobowych niezgodnie z przepisami ...	481
1. Zagadnienia wstępne	481
2. Zasada <i>ne bis in idem</i>	482
3. Zakres odpowiedzialności	483
3.1. Odpowiedzialność przedsiębiorcy – administratora danych	483
3.2. Odpowiedzialność podmiotu przetwarzającego	483
3.3. Odpowiedzialność pracowników	483
3.4. Odpowiedzialność osób wykonujących pracę na podstawie umowy cywilnoprawnej	484
3.5. Odpowiedzialność osób samozatrudnionych	485
3.6. Odpowiedzialność inspektora ochrony danych	485
4. Wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych	485
5. Postępowanie administracyjne	486
5.1. Kary administracyjne	487
5.1.1. Kary nakładane na sektor publiczny	487
5.1.2. Kary nakładane na pozostałe podmioty	488
5.2. Wymierzanie kary administracyjnej	490
5.2.1. Umyślność naruszenia	491
5.2.2. Działania minimalizujące szkodę	491
5.2.3. Łączenie naruszeń	492
5.3. Pozostałe kary z RODO	492
5.4. Pozostałe kary z ustawy o ochronie danych osobowych	493
5.4.1. Nielegalne przetwarzanie danych	493
5.4.2. Udaremnianie lub utrudnianie kontroli	494
5.4.3. Niestawienie się na żądanie organu	495
5.4.4. Postanowienie o ograniczeniu zakresu przetwarzania danych	496
6. Postępowanie cywilne	496