

Spis treści

O autorach	XXI
Wykaz skrótów	XXV

Część I. Ochrona danych osobowych – zagadnienia ogólne z uwzględnieniem rozporządzenia unijnego

Rozdział I. Zastosowanie przepisów o ochronie danych osobowych w jednostkach sektora publicznego (Piotr Kowalik, Dariusz Wociór)	3
1. Wstęp	3
2. Ustawa o ochronie danych osobowych a rozporządzenie unijne	3
3. Dane osobowe	5
3.1. Zagadnienia ogólne	5
3.2. Dane osobowe zwykle i szczególnie chronione (wrażliwe, sensytywne)	6
3.3. Dane osobowe szczególnej kategorii w ogólnym rozporządzeniu unijnym ..	6
3.4. Dane osobowe pogrupowane według rodzaju informacji	7
4. Ogólne zasady ochrony danych osobowych	7
4.1. Przetwarzanie danych osobowych	7
4.2. Zbieg ustawy o ochronie danych osobowych z innymi przepisami	8
5. Podmioty zobowiązane do stosowania ustawy o ochronie danych osobowych	8
5.1. Podmioty publiczne	9
5.1.1. Organy państwowe	9
5.1.2. Organy samorządu terytorialnego	9
5.1.3. Państwowe i komunalne jednostki organizacyjne	10
5.2. Podmioty prywatne	10
6. Administrator danych	11
7. Obowiązki administratora danych	11
8. Wyłączenia stosowania ustawy o ochronie danych osobowych	12
9. Kodyfikacje europejskie	12
9.1. Zakres podmiotowy i przedmiotowy ogólnego rozporządzenia unijnego	12
9.2. Pojęcie osoby, której dane dotyczą w ogólnym rozporządzeniu unijnym	13

9.3. Warunki przetwarzania szczególnych kategorii danych osobowych w ogólnym rozporządzeniu unijnym	14
9.4. Dane biometryczne w ogólnym rozporządzeniu unijnym	15
9.5. Współadministratorzy w kodyfikacji europejskiej	15
9.6. Przedstawiciele administratorów niemających siedziby w UE w kodyfikacji europejskiej	16

Rozdział II. Szczególne przypadki uznania informacji za dane osobowe (Piotr Kowalik, Bogusław Nowakowski)	19
---	----

1. Wstęp	19
2. Adres poczty elektronicznej	19
3. Wątpliwości wokół adresu IP	20
4. Numer VIN pojazdu	21

Rozdział III. Administratorzy danych osobowych w jednostkach samorządu terytorialnego (Piotr Kowalik, Bogusław Nowakowski)	23
---	----

1. Ustalenie podmiotu uznanego za administratora danych	23
2. Marszałek województwa – administrator danych lekarzy uprawnionych do przeprowadzania badań lekarskich osób ubiegających się o kierowanie pojazdami	24
3. Starosta jako administrator danych instruktorów nauki jazdy	25

Rozdział IV. Administrator danych osobowych w sektorze publicznym po zmianach wprowadzonych ustawą o pomocy państwa w wychowywaniu dzieci (dr Paweł Litwiński)	27
--	----

1. Ustawowa definicja administratora danych osobowych	27
1.1. Definicja pojęcia administratora danych osobowych	27
1.2. Administrator danych osobowych a podmiot przetwarzający dane na zlecenie	28
2. Administrator danych osobowych w sektorze publicznym	29
2.1. Wskazanie w przepisach podmiotu pełniącego funkcję ADO w stosunku do konkretnych zbiorów	29
2.2. Przetwarzanie danych osobowych w celu wykonywania określonych prawem zadań	30
3. Zmiany wprowadzone ustawą o pomocy państwa w wychowywaniu dzieci	30
3.1. Dwa typy administratorów danych osobowych	31
3.2. Pojęcie interesu publicznego	33
3.3. Wymiana danych między organami władzy publicznej	33

Rozdział V. Powierzenie przetwarzania danych osobowych (dr Jowita Sobczak, Dariusz Wociór)	35
--	----

1. Wstęp	35
2. Podmioty powierzające i przetwarzające dane i ich obowiązki	35
2.1. Podmiot przetwarzający dane	35
2.2. Obowiązki podmiotu, któremu powierzono dane	36
2.3. Zleceniobiorca mający siedzibę za granicą	36

2.4. Procedura zwrotu danych	36
2.5. Powierzenie danych – przypadki szczególne	37
2.6. Podpowierzenie przetwarzania danych	39
3. Podmiot przetwarzający i powierzenie danych do przetwarzania w ogólnym rozporządzeniu unijnym	41
4. Umowa o powierzenie do przetwarzania danych osobowych	42

Rozdział VI. Powierzenie przetwarzania danych osobowych w sektorze publicznym po zmianach wprowadzonych ustawą o pomocy państwa w wychowywaniu dzieci (Paweł Barta)

47

1. Instytucja powierzenia przetwarzania danych osobowych w sektorze publicznym w dotychczasowych przepisach ustawy o ochronie danych osobowych	47
2. Zmiany w zakresie powierzenia wprowadzone ustawą o pomocy państwa w wychowywaniu dzieci	48
3. Wyłączenie z art. 31 ust. 2a ustawy o ochronie danych osobowych w świetle prawa europejskiego	48
4. Skutki wyłączenia z art. 31 ust. 2a ustawy o ochronie danych osobowych	49
4.1. Skutki wyłączenia dla kontroli GIODO	49
4.2. Skutki wyłączenia dla zastosowania środków zabezpieczenia danych	49
4.3. Inne konsekwencje wprowadzenia wyłączenia	50
5. Wyłączenie z art. 31 ust. 2a ustawy o ochronie danych osobowych a cel ustawy o pomocy państwa w wychowywaniu dzieci	51
6. Przekazanie danych a wyłączenie z art. 31 ust. 2a ustawy o ochronie danych osobowych	51
7. Podpowierzenie a wyłączenie z art. 31 ust. 2a ustawy o ochronie danych osobowych	52

Rozdział VII. Zgłaszanie zbiorów danych osobowych do rejestracji do GIODO

(Piotr Kowalik, Dariusz Wociór)

53

1. Zbiór danych osobowych – definicja, zasady tworzenia	53
1.1. Zagadnienia ogólne	53
1.2. Zbiory danych rozproszone lub podzielone funkcjonalnie	54
1.3. Tworzenie zbiorów danych	56
1.4. Zbiór danych a system informatyczny służący do przetwarzania danych (baza danych)	56
2. Zgłaszanie zbiorów danych osobowych do Generalnego Inspektora Ochrony Danych Osobowych	57
2.1. Zagadnienia ogólne	57
2.2. Prawa i obowiązki administratora	58
2.3. Zaświadczenie o zarejestrowaniu zbioru danych	58
2.4. Proces rejestracji zbioru danych	59
3. Zwolnienia z obowiązku zgłoszenia zbioru danych do rejestracji	59
3.1. Zwolnienia przedmiotowe	59
3.2. Zwolnienie podmiotowe	60

3.2.1. Rejestr zbiorów danych osobowych przetwarzanych przez administratora danych	61
4. Odmowa rejestracji zbioru danych	61
4.1. Kodyfikacja europejska	62
5. Przykłady zbiorów danych prowadzonych w sektorze publicznym	62
5.1. Wykazy radnych	62
5.2. Rejestr korespondencji	63
5.3. Ewidencja czytelników bibliotek	64
5.3.1. Jedna biblioteka dla kilku szkół	64
5.3.2. System biblioteczno-informacyjny uczelni	64
5.4. Newsletter	65
5.5. Zbiory zawierające informacje o osobach fizycznych występujących w obrocie gospodarczym	65
5.5.1. Zagadnienia ogólne	65
5.5.2. Centralna Ewidencja i Informacja o Działalności Gospodarczej	66
5.5.3. Pozyskanie danych dostępnych w przestrzeni publicznej	66
5.5.4. Rejestry Krajowego Rejestru Sądowego	67
6. Rejestrowanie kategorii czynności przetwarzania danych osobowych przez administratora na podstawie ogólnego rozporządzenia unijnego	67
Rozdział VIII. Zabezpieczenie danych osobowych (Piotr Kowalik, Bogusław Nowakowski, Dariusz Wociór)	71
1. Wstęp	71
2. Środki organizacyjne	71
2.1. Wymagania dotyczące środków organizacyjnych	71
2.2. Dokumentacja opisująca sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych	72
2.3. Upoważnienie do przetwarzania danych	73
3. Środki techniczne	73
3.1. Wymagania dotyczące środków technicznych	73
3.2. Poziomy bezpieczeństwa	74
4. Regulacje europejskie	75
5. Zgłoszenie naruszenia ochrony danych i ocena skutków na podstawie rozporządzenia unijnego	75
5.1. Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorcemu	75
5.2. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych	76
Rozdział IX. Administrator bezpieczeństwa informacji (Piotr Kowalik, Dariusz Wociór)	79
1. Rola ABI	79
2. Powołanie i status ABI	79

3. Wymogi wobec ABI	81
3.1. Wymogi prawne	81
3.2. Wymogi organizacyjne	81
3.2.1. Wymóg bezpośredniej podległości ABI	82
3.2.2. Wymóg zapewnienia odpowiednich środków niezbędnych do niezależnego wykonywania zadań	82
3.2.3. Wymóg odrębności ABI w strukturze organizacyjnej	82
3.2.4. Wymogi dotyczące możliwości łączenia funkcji ABI z realizacją innych obowiązków	83
3.2.5. Łączenie funkcji ABI i ASI	83
3.2.6. Łączenie funkcji ABI w kilku jednostkach sektora publicznego	83
3.2.7. Zgłoszenie ABI do rejestru do GIODO	84
3.3. Forma zatrudnienia administratora bezpieczeństwa informacji	84
3.3.1. Administrator bezpieczeństwa informacji zewnętrzny lub w niepełnym wymiarze godzin	84
4. Zadania ABI	85
4.1. Delegowanie uprawnień ABI	85
5. Zapewnianie przestrzegania przepisów o ochronie danych osobowych przez ABI	86
5.1. Sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych	87
5.1.1. Plan sprawdzeń	87
5.1.2. Czynności sprawdzające	88
5.1.3. Sprawozdanie	89
5.2. Nadzorowanie opracowania i aktualizowania dokumentacji	90
5.3. Zapewnienie zapoznania osób upoważnionych z przepisami	91
5.4. Aktywność ABI w kontekście zabezpieczenia danych osobowych	92
6. Rejestr zbiorów danych przetwarzanych przez administratora danych	95
6.1. Wpisanie zbioru danych do rejestru, jego aktualizacja i wykreślenie	95
7. Kodyfikacja europejska	97
7.1. Inspektor ochrony danych	97
7.2. Zadania inspektora ochrony danych	98
8. Wzory dokumentów	99
8.1. Zarządzenie w sprawie powołania administratora bezpieczeństwa informacji	99
8.2. Upoważnienie do przetwarzania danych osobowych	102
8.3. Powołanie ABI	103
8.4. Sprawozdanie ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ich ochronie	103

Rozdział X. Wykonywanie sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (Maciej Byczkowski)	107
--	-----

1. Wymagania ustawowe dotyczące wykonywania sprawdzeń zgodności przetwarzania danych z przepisami	107
1.1. Obowiązki administratora danych związane z wykonywaniem sprawdzeń	107
1.2. Analiza zagrożeń dla przetwarzania danych	108
1.3. Audyt zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przed 1.1.2015 r.	108
1.4. Rodzaje sprawdzeń	109
1.5. Tryb i sposób realizacji sprawdzeń	109
1.6. Zasady przeprowadzania sprawdzeń, gdy nie został powołany administrator bezpieczeństwa informacji	109
1.7. Kontrola przetwarzania danych osobowych w razie zawarcia umowy powierzenia	110
2. Wykonywanie sprawdzeń planowych przez administratora bezpieczeństwa informacji	110
2.1. Etapy wykonywania sprawdzeń planowych	110
2.2. Przygotowanie planu sprawdzenia	110
2.2.1. Termin przygotowania planu sprawdzenia	110
2.2.2. Częstotliwość wykonywania sprawdzeń	111
2.2.3. Wyszczególnienie najważniejszych elementów planu sprawdzeń	111
2.2.4. Pierwszy plan sprawdzeń ABI	113
2.3. Przeprowadzanie sprawdzenia	114
2.4. Wzór formularza wywiadu do sprawdzenia	115
2.5. Sporządzanie sprawozdania ze sprawdzenia	116
3. Wykonywanie sprawdzeń doraźnych przez administratora bezpieczeństwa informacji w razie naruszenia ochrony danych osobowych	117
3.1. Wymagania przepisów dotyczące wykonywania sprawdzeń doraźnych przez administratora bezpieczeństwa informacji	117
3.2. Postępowanie w razie naruszenia ochrony danych osobowych	118
3.2.1. Instrukcja postępowania w razie naruszenia ochrony danych osobowych	118
3.2.2. Naruszenie szczegółowych zasad przetwarzania danych osobowych	120
3.2.3. Konieczność aktualizacji dokumentacji przetwarzania danych w zakresie wykonywania sprawdzeń doraźnych	121
3.3. Wykonywanie sprawdzeń doraźnych w praktyce	122
3.4. Prowadzenie przez administratora bezpieczeństwa informacji rejestru incydentów	123
4. Wykonywanie sprawdzeń zgodności przetwarzania danych osobowych z przepisami w razie niepowołania administratora bezpieczeństwa informacji ...	124
4.1. Konieczność przeprowadzania sprawdzeń przez administratora danych	124
4.2. Podział czynności w zakresie sprawdzeń	125
4.3. Częstotliwość przeprowadzania sprawdzeń	125
4.4. Lista kontrola w zakresie przedmiotu sprawdzenia	126
4.5. Etapy planu sprawdzenia	126

4.6. Dokument podsumowujący wykonane sprawdzenie	127
5. Wykonywanie sprawdzeń zgodności przetwarzania danych osobowych z przepisami po wejściu w życie przepisów ogólnego rozporządzenia unijnego ..	128
5.1. Zadania inspektora ochrony danych w zakresie monitorowania przestrzegania przepisów o ochronie danych	128
5.2. Kodeksy postępowania	128
5.3. Przygotowanie do pełnienia nowej funkcji inspektora ochrony danych w zakresie monitorowania ochrony danych	129

Rozdział XI. Polityka bezpieczeństwa informacji (Anna Jędruszczak, Piotr Kowalik, Dariusz Wociór)	131
1. Bezpieczeństwo informacji	131
1.1. Przesłanki stworzenia polityki bezpieczeństwa informacji	131
1.1.1. Zakres informacji zawartych w polityce bezpieczeństwa informacji .	131
1.1.2. Podstawowe zasady bezpieczeństwa zawarte w polityce bezpieczeństwa informacji	133
1.2. Polityka bezpieczeństwa (danych osobowych)	134
1.3. Obowiązkowe elementy polityki bezpieczeństwa informacji (danych osobowych)	135
1.3.1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe	135
1.3.2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	136
1.3.3. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	137
1.3.4. Sposób przepływu danych między poszczególnymi systemami	137
1.3.5. Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych	138
2. Środki bezpieczeństwa stosowane w jednostce	140
2.1. Środki bezpieczeństwa na poziomie podstawowym	140
2.2. Środki bezpieczeństwa na poziomie podwyższonym	141
2.3. Środki bezpieczeństwa na poziomie wysokim	141
3. Ocena skutków pod kątem ochrony danych z użyciem nowych technologii w ogólnym rozporządzeniu unijnym	143
4. Wzory dokumentów dotyczących polityki bezpieczeństwa informacji	145
4.1. Zarządzenie w sprawie ochrony danych osobowych	145
4.2. Polityka bezpieczeństwa informacji	146
4.3. Załączniki do Polityki Bezpieczeństwa Informacji	159
4.3.1. Wykaz pomieszczeń	159
4.3.2. Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe	159
4.3.3. Wykaz zasobów danych osobowych i systemów ich przetwarzania ..	161

4.3.4. Oświadczenie dotyczące zgody na przetwarzanie danych osobowych	162
4.3.5. Informacja o przetwarzaniu danych osobowych w trakcie procesu rekrutacyjnego	163
4.3.6. Wniosek o udostępnienie danych osobowych	163
4.3.7. Upoważnienie do obsługi systemu informatycznego	165
4.3.8. Ewidencja osób upoważnionych do przetwarzania danych osobowych	166
4.3.9. Porozumienie w sprawie wykorzystania oddanego do dyspozycji sprzętu informatycznego, oprogramowania oraz zasobów sieci informatycznej	166
4.3.10. Oświadczenie o zachowaniu w tajemnicy danych osobowych	168
4.3.11. Umowa powierzenia przetwarzania danych osobowych	169
4.3.12. Raport z naruszenia bezpieczeństwa zasad ochrony danych osobowych	172
Rozdział XII. Instrukcja zarządzania systemem informatycznym (Adam Gałach)	175
1. Elementy instrukcji zarządzania systemem informatycznym	175
2. Wzory dokumentów	177
2.1. Instrukcja zarządzania systemem informatycznym	177
2.2. Załączniki do instrukcji zarządzania systemem informatycznym	183
2.2.1. Wniosek o nadanie/cofnięcie uprawnień do przetwarzania danych osobowych	183
2.2.2. Upoważnienie do wykonywania czynności związanych z przetwarzaniem danych osobowych	183
2.2.3. Ewidencja osób upoważnionych do przetwarzania danych osobowych	184
Rozdział XIII. Kodeksy postępowania i mechanizmy certyfikacji (Dariusz Wociór)	187
1. Wstęp	187
2. Kodeksy postępowania a podmioty publiczne	188
3. Monitorowanie zatwierdzonych kodeksów postępowania	189
4. Certyfikacja	190
5. Zadania podmiotu certyfikującego	191
Rozdział XIV. Uprawnienia informacyjne i kontrolne osoby, której dane dotyczą (Bogusław Nowakowski, Piotr Kowalik, Dariusz Wociór)	193
1. Obowiązek informacyjny	193
1.1. Pozyskiwanie danych bezpośrednio od osoby, której dane dotyczą	193
1.2. Pozyskiwanie danych z innych źródeł niż bezpośrednio od osoby, której dane dotyczą	194
2. Uprawnienia kontrolne	195
3. Wniosek osoby, której dane dotyczą	197
4. Dbłość o poprawność danych osobowych	198
5. Kodyfikacja europejska	198

5.1. Prawa osoby, której dane dotyczą, a obowiązki administratora danych	199
5.2. Informacje podawane w przypadku zbierania danych	200
5.3. Prawo dostępu przysługujące osobie, której dane dotyczą	202
5.4. Prawo do poprawienia danych	202
5.5. Prawo do bycia zapomnianym	202
5.6. Prawo do ograniczenia przetwarzania	203
5.7. Obowiązek powiadomienia o sprostowaniu danych, ich usunięciu lub ograniczeniu przetwarzania	204
5.8. Prawo do przenoszenia danych	204
5.9. Prawo do sprzeciwu	204
5.10. Prawo do sprzeciwu a dane osobowe przetwarzane do celów marketingu, historycznych, statystycznych lub naukowych	204
5.11. Nowe obowiązki administratora wobec osób, których dotyczą dane, w ogólnym rozporządzeniu unijnym	205
5.12. Strategie ochrony danych <i>privacy by design</i> i <i>privacy by default</i>	205

Rozdział XV. Ochrona danych osób pełniących funkcje publiczne (Piotr Kowalik, Bogusław Nowakowski, Barbara Pietrzak)	207
---	------------

1. Dane radnego	207
1.1. Dane radnego a informacja publiczna	207
1.2. Zakres ingerencji w prywatność osób pełniących funkcje publiczne	208
1.3. Przypadki ograniczenia prawa do informacji publicznej	209
1.4. Oświadczenia majątkowe radnych	209
2. Dane reprezentantów gminy w radach nadzorczych spółek prawa handlowego .	210
3. Dane osobowe osób wchodzących w skład organów jednostki pomocniczej w gminie	211
4. Wynagrodzenie dyrektorów samorządowych jednostek organizacyjnych posiadających osobowość prawną	212
5. Odmowa udostępnienia informacji publicznej	212
5.1. Warunki ograniczenia dostępu oraz procedura odwoławcza od odmowy ...	212
5.2. Wzór decyzji o odmowie udostępnienia informacji publicznej ze względu na prywatność osoby fizycznej	213
5.3. Objasnienia do wzoru decyzji o odmowie udostępnienia informacji publicznej ze względu na prywatność osoby fizycznej	216
5.3.1. Elementy decyzji	216
5.3.2. Forma decyzji	216
5.3.3. Wniosek pisemny	216
5.3.4. Etapy postępowania z wnioskiem	216
5.3.5. Zgoda osoby fizycznej na udostępnienie informacji	217
5.3.6. Elementy uzasadnienia decyzji	217

Rozdział XVI. Przetwarzanie danych osobowych pracowników (Kamila Kędzierska, Piotr Kowalik, Dariusz Wociór)	219
--	------------

1. Dane, których może żądać pracodawca od pracownika	219
--	-----

2. Zakres prowadzenia dokumentacji osobowej pracownika	220
2.1. Dokumenty, których pracodawca ma prawo żądać od pracownika	220
2.2. Dodatkowe dokumenty	222
2.3. Akta osobowe pracownika	222
2.3.1. Kwestionariusz osobowy	222
2.3.2. Zakres akt osobowych	223
2.4. Listy obecności pracowników	225
3. Przetwarzanie danych osobowych pracownika po ustaniu stosunku pracy	226
4. Udostępnienie danych osobowych pracownika do badań profilaktycznych	226
5. Przetwarzanie danych osobowych w kontekście zatrudnienia – rozporządzenie unijne	227
Rozdział XVII. Dane osobowe w rekrutacjach (Miroslaw Gumularz)	229
1. Wstęp	229
2. Dane, których może żądać pracodawca od osoby ubiegającej się o zatrudnienie .	230
2.1. Katalog informacji	230
2.2. Szerszy zakres danych osobowych – jeżeli to wynika z przepisów szczególnych	230
2.3. Dane, których pracodawca może żądać już od osoby zatrudnionej	231
2.4. Katalog dokumentów, jakich pracodawca może żądać na etapie rekrutacji .	231
2.5. Zbieranie zgód od kandydatów do pracy	231
3. Dodatkowe dane	231
4. Przyszłe rekrutacje	233
5. Wykorzystanie danych osobowych kandydatów w celach marketingowych	234
6. Wykorzystanie danych po zakończonej rekrutacji	234
7. Testy psychologiczne	234
8. Rejestracja zbiorów danych kandydatów do pracy	235
9. Modele rekrutacji – rekrutacje zewnętrzne	236
9.1. Pracodawca zleca zewnętrznemu podmiotowi przeprowadzenie na jego rzecz rekrutacji	236
9.2. Pracodawca pozyskuje dane osobowe kandydatów z zewnętrznej bazy kandydatów	237
10. Obowiązek informacyjny i rekrutacje ukryte	237
11. Prowadzenie rekrutacji po wejściu w życie ogólnego rozporządzenia unijnego ..	238
Rozdział XVIII. Uprawnienia organu do spraw ochrony danych osobowych (Bogusław Nowakowski, Piotr Kowalik, Dariusz Wociór)	241
1. Organ ochrony danych osobowych	241
1.1. Wygaśnięcie kadencji GODO	241
1.2. Wymagania wobec osoby pełniącej funkcję GODO	242
2. Zadania GODO	243
2.1. Wystąpienia GODO	243
3. Postępowania administracyjne prowadzone przez GODO	244

3.1. Przebieg postępowania	244
3.2. Środek zaskarżenia od decyzji GODO	245
4. Generalny Inspektor Ochrony Danych Osobowych a przepisy karne ustawy	246
4.1. Nielegalne przetwarzanie danych w zbiorze danych	246
4.2. Udostępnienie danych osobie nieupoważnionej	247
4.3. Nieumyślne naruszenie obowiązku zabezpieczenia danych	247
4.4. Niezgłoszenie danych do rejestru	248
4.5. Nieinformowanie o przysługujących prawach	248
4.6. Udaremnienie wykonania czynności kontrolnej	248
5. Organ nadzorczy w kodyfikacji europejskiej	249
6. Koncepcja <i>one stop shop</i> w kodyfikacji europejskiej	249
Rozdział XIX. Postępowanie kontrolne GODO (Bogusław Nowakowski, Piotr Kowalik, Dariusz Wociór)	251
1. Czynności kontrolne	251
2. Upoważnienie do kontroli	252
3. Miejsce i czas kontroli	255
4. Ustalenia w trakcie kontroli	255
5. Protokół z czynności kontrolnych	257
6. Zakończenie postępowania kontrolnego	258
7. Wyłączenia uprawnień kontrolnych GODO	259
Rozdział XX. Środki ochrony prawnej, odpowiedzialność prawna i sankcje w rozporządzeniu unijnym (Dariusz Wociór)	261
1. Prawo wniesienia skargi do organu nadzorczego	261
2. Prawo do skutecznego sądowego środka ochrony prawnej przeciwko organowi nadzorcemu	261
3. Reprezentowanie osób, których dane dotyczą	262
4. Zawieszenie postępowania	262
5. Prawo do odszkodowania i odpowiedzialność prawna	263
6. Kary pieniężne	264
7. Wysokość kar pieniężnych	265
8. Dodatkowe kary	266
Rozdział XXI. Odpowiedzi na pytania	267
1. Rodzaje odpowiedzialności za niewłaściwe przetwarzanie danych osobowych ...	267
2. Gońcy a upoważnienie do przetwarzania danych osobowych	269
3. Zakres przedmiotowy kontroli przetwarzania danych przez osobę, której dane dotyczą	270
4. Przesłanki odmowy udzielenia informacji o danych osobowych osobie, której dane dotyczą	272
5. Zakres ciężącego na administratorze danych osobowych obowiązku uzupełniania i sprostowania danych osobowych	273
6. Podległość administratora bezpieczeństwa informacji	274

7. Dane dłużników a obowiązek zawierania umów o powierzenie przetwarzania danych	275
8. Deklaracje śmieciowe zbiorem danych?	276
9. Nagrywanie rozmów w urzędzie	278
10. Łączenie funkcji administratora bezpieczeństwa informacji i administratora systemu informatycznego	279
11. Zasady przekazywania danych osobowych do państwa trzeciego	280
12. Usuwanie danych osobowych z dysku twardego	283
13. Administrator systemu informatycznego zastępcą administratora bezpieczeństwa informacji	284
14. Usuwanie danych z nośników magnetycznych	286

Część II. Ochrona danych osobowych z uwzględnieniem specyfiki poszczególnych rodzajów podmiotów

Rozdział I. Ochrona danych osobowych w jednostkach oświatowych (dr Adam Balicki, Kamila Kędzierska, Bogusław Nowakowski, Piotr Wieczorek)	289
1. Stosowanie ustawy o ochronie danych osobowych w oświacie	289
1.1. Akty prawne uszczegóławiające zapisy ustawy o ochronie danych osobowych	289
1.2. Zasady postępowania przy przetwarzaniu danych osobowych	290
1.3. Określenie administratora danych osobowych oraz administratora bezpieczeństwa informacji w jednostkach oświatowych	291
1.4. Obowiązki dyrektora w związku z ochroną danych osobowych	292
1.5. Specyfika danych osobowych jednostek oświatowych	292
1.6. Rodzaje dokumentacji, w których przetwarzane są dane osobowe	293
1.7. Dane osobowe słuchaczy	294
1.8. Dane uczniów, którym udzielana jest pomoc psychologiczno-pedagogiczna	295
1.9. Dane identyfikacyjne i dane rodzinowe	297
2. Przekazywanie danych do baz danych systemu informacji oświatowej	297
3. Przypadki szczególne	299
3.1. Rejestr uczniów realizujących obowiązek szkolny w innej szkole	299
3.2. Sposób przekazywania danych osobowych podmiotom zewnętrznym	301
3.3. Dzienniki i e-dzienniki	303
3.4. Zebrania klasowe	310
3.5. Publikacja danych	313
3.6. Klasówka z imieniem i nazwiskiem ucznia oraz numerem klasy	314
3.7. Wycieczka szkolna z udziałem uczniów z innej szkoły	314
3.8. Instalacja kamer wizyjnych – monitoring	315
3.9. Wizerunek dziecka	317
3.10. Przekazanie danych osobowych ucznia do sądu rodzinnego	318
3.11. Dokumentacja szkolna związana z przetwarzaniem danych osobowych	319

3.12. Kontrole Generalnego Inspektora Danych Osobowych w szkołach i placówkach oświatowych	319
Rozdział II. Ochrona danych osobowych w ramach pomocy społecznej	
(dr Adam Balicki (6–7), Kamila Kędzierska (1–5))	321
1. Dane osobowe w pomocy społecznej	321
2. Przepisy o ochronie danych osobowych a ustawa o pomocy społecznej	322
3. Zakres przetwarzania danych w pomocy społecznej	323
3.1. Informacje o sytuacji osobistej, rodzinnej, dochodowej i majątkowej	324
3.2. Dokumentacja osób przebywających w placówkach zapewniających opiekę	326
4. Dane szczególnie wrażliwe	327
5. Ochrona danych a audyt	327
6. Pozyskanie informacji przez miejski ośrodek pomocy społecznej o pobieranym stypendium	329
7. Przetwarzanie danych osobowych a wywiad środowiskowy	330
Rozdział III. Ochrona danych osobowych w instytucjach kultury	
(Kamila Kędzierska)	333
1. Wstęp	333
2. Biblioteki	334
2.1. Zakres danych możliwych do gromadzenia	334
2.2. System MAK+ a ochrona danych osobowych	335
2.2.1. Administrator danych osobowych czytelników oraz pracowników bibliotek	335
2.2.2. Zgoda czytelnika na przetwarzanie danych osobowych	335
2.3. Windykacja opłat	336
3. Systemy rezerwacji i zakupu biletów instytucji kultury a ochrona danych osobowych	337
4. Ośrodki badań i dokumentacji	337
Część III. Ochrona danych osobowych w różnych obszarach działalności	
Rozdział I. Rachunkowość a ochrona danych osobowych (Dariusz Wociór)	341
1. Wstęp	341
2. Przechowywanie dokumentacji	342
3. Nośniki magnetyczne	342
4. Miejsce i sposób gromadzenia	343
5. Okres przechowywania	343
5.1. Okresy przechowywania zawarte w ustawie o rachunkowości	343
5.2. Okresy przechowywania zawarte w ustawie – Ordynacja podatkowa	345
5.3. Okresy przechowywania zawarte w ustawie o systemie ubezpieczeń społecznych	345
6. Udostępnianie danych	346
7. Zakończenie działalności a dane osobowe	346

7.1. Działalność gospodarcza w zakresie przechowywania dokumentacji osobowej i płacowej pracodawców o czasowym okresie przechowywania ..	347
7.1.1. Wpis do rejestru przechowawców akt osobowych i płacowych	347
7.1.2. Warunki wykonywania działalności w zakresie przechowywania dokumentacji osobowej i płacowej pracodawców	348
7.2. Postępowanie z dokumentacją osobową i płacową w przypadku likwidacji lub upadłości pracodawcy	348
7.2.1. Przejęcie dokumentacji przez archiwum państwowe	349
7.2.2. Zadania likwidatora lub syndyka w zakresie dokumentacji	349
7.2.3. Zadania archiwum państwowego	349
7.2.4. Procedura nadania decyzji nakazującej złożenie dokumentacji na odpłatne przechowywanie	349
8. Generalny Inspektor Ochrony Danych Osobowych oraz ABL a dostęp do dokumentacji księgowej	350
Rozdział II. Windykacja należności jednostek samorządu terytorialnego a ochrona danych osobowych i prawa do prywatności dłużników (Miroslaw Gumularz, Karol Kozieł)	351
1. Stosowanie ustawy o ochronie danych osobowych przez jednostki samorządu terytorialnego	351
2. Podstawa prawna przetwarzania danych osobowych dłużników jednostek samorządu terytorialnego	352
2.1. Przetwarzanie danych osobowych dłużników w celach związanych z windykacją	353
2.2. Klauzula usprawiedliwionego celu	353
3. Ujawnianie danych dłużników	354
Rozdział III. Bezpieczeństwo administracji publicznej w cyberprzestrzeni (dr Agnieszka Stępień)	357
1. Upowszechnienie e-administracji	357
2. Charakterystyka cyberprzestrzeni	358
3. Zagrożenia związane z funkcjonowaniem administracji publicznej w cyberprzestrzeni	358
4. Raporty Najwyższej Izby Kontroli	360
5. Poprawa bezpieczeństwa administracji publicznej w cyberprzestrzeni	361
Rozdział IV. Bezpieczeństwo danych osobowych w jednostkach publicznych świadczących e-usługi (Maciej Jurczyk)	363
1. Wstęp	363
2. Pojęcie e-usługi	363
3. Ochrona danych w e-usługach	365
4. Warunki przetwarzania danych osobowych przez e-usługodawcę	365
5. Obowiązek informacyjny	366
6. Umowa powierzenia danych podmiotowi trzeciemu	366
7. Regulamin świadczenia usług drogą elektroniczną	367

8. Mechanizmy kontroli dostępu do danych	369
9. Kryptografia danych przesyłanych w sieci publicznej	371
10. Bezpieczeństwo kanału komunikacyjnego	371
11. Audyt i testy bezpieczeństwa	372

Rozdział V. Przetwarzanie danych osobowych w chmurze obliczeniowej

<i>(dr Jowita Sobczak)</i>	375
1. Wstęp	375
2. Umowa o świadczenie usług przetwarzania danych w chmurze obliczeniowej ...	376
3. Elementy umowy powierzenia	376
3.1. Konieczność określenia celu i zakresy przetwarzania danych w chmurze ...	376
3.2. Zapisy zobowiązujące procesora do prawidłowego przetwarzania powierzonych danych	377
3.3. Dodatkowe elementy	377
4. Podpowierzenie danych osobowych	377
5. Środki zabezpieczające dane w chmurze	378
6. Okres przechowywania danych w chmurze	378
7. Miejsce przetwarzania danych i miejsce prawa właściwego	379
8. Kodeks postępowania w zakresie ochrony danych dla dostawców usług w chmurze	380