

Spis treści

Wykaz autorów	IX
Wykaz skrótów	XI
Wprowadzenie	XV
CZĘŚĆ 1. Ochrona danych osobowych	1
1. Zastosowanie ustawy o ochronie danych osobowych w jednostkach sektora publicznego	3
1.1. Ogólne zasady ochrony danych osobowych	3
1.2. Podmioty, wobec których stosuje się ustawę o ochronie danych osobowych	4
1.2.1. Organ państwa	5
1.2.2. Organy samorządu terytorialnego	5
1.2.3. Podmioty niepubliczne	6
1.2.4. Podmioty prywatne	6
1.3. Podmioty niepodlegające kontroli	7
2. Rejestracja zbiorów	9
2.1. Wymogi prawidłowego zgłoszenia	9
2.2. Administrator bezpieczeństwa informacji	10
2.3. Zabezpieczenie techniczne przetwarzanych danych osobowych	21
2.4. Wykazy radnych	21
2.5. Rejestr korespondencji	22
2.6. Ewidencja czytelników bibliotek	23
2.6.1. Jedna biblioteka dla kilku szkół	23
2.7. System biblioteczno-informacyjny uczelni	23
2.8. Newsletter	24
3. Przypadki szczególne uznania za dane osobowe	25
3.1. Identyfikacja osoby fizycznej	25
3.2. Adres poczty elektronicznej	26
3.3. Wątpliwości wokół adresu IP	27
4. Marszałek województwa jako administrator danych osobowych	29
5. Uprawnienia osoby, której dane dotyczą	33
5.1. Czego może zażądać osoba, której dane osobowe są przetwarzane	33
5.2. Wniosek osoby, której dane dotyczą	35
5.3. Obowiązek informacyjny urzędu miasta wobec petentów	37
6. Ochrona danych osobowych w oświacie	39
6.1. Stosowanie ustawy o ochronie danych osobowych w oświacie	39
6.2. Kiedy dochodzi do przetwarzania danych osobowych	40
6.3. Jakie dane wchodzą w zakres pojęcia danych osobowych	40

6.4. Podstawa prawna przetwarzania danych osobowych	41
6.5. Przekazywanie danych do baz danych systemu informacji oświatowej	42
6.6. Dane identyfikacyjne oraz dziedzinowe uczniów	45
6.7. Dane identyfikacyjne oraz dziedzinowe nauczycieli	50
6.8. Szczególne przypadki	54
6.8.1. Rejestr uczniów realizujących obowiązek szkolny w innej szkole	54
7. Ochrona danych urzędników	95
7.1. Dane radnego	95
7.2. Dane reprezentantów gminy w radach nadzorczych spółek prawa handlowego	98
7.3. Dane osobowe szefa jednostki pomocniczej	100
7.4. Nagrody roczne dyrektorów samorządowych jednostek organizacyjnych posiadających osobowość prawną	101
7.5. Odpisy akt stanu cywilnego	103
8. Ogólne zasady kontroli przetwarzania danych osobowych	105
8.1. Stosowanie ustawy o ochronie danych osobowych w ramach kontroli	105
8.2. Ograniczenia podmiotowe kontroli	106
8.3. Kwestie, na które zwraca uwagę inspektor ochrony danych osobowych	107
9. Postępowanie kontrolne	113
9.1. Termin i czas kontroli	113
9.2. Miejsce kontroli	113
9.3. Ustalenia w trakcie kontroli	114
9.4. Elementy kontroli urządzeń i systemów informatycznych	115
9.5. Polityka bezpieczeństwa	115
9.6. Upoważnienie do kontroli i legitymacja	116
9.7. Protokół z czynności kontrolnych	118
9.8. Sankcje prawne w postępowaniu kontrolnym	121
9.8.1. Uprawnienia inspektora w razie stwierdzenia naruszenia przepisów	121
9.9. Uprawnienia GODO w razie stwierdzenia naruszenia przepisów	123
9.10. Odpowiedzialność za nieprawidłowe udostępnienie	124
CZĘŚĆ 2. Ochrona informacji niejawnych	127
1. Ogólne zasady ochrony informacji niejawnych	129
1.1. Zakres obowiązywania ustawy o ochronie informacji niejawnych	130
1.2. Sprawowanie nadzoru nad ochroną informacji niejawnych oraz kontrola ochrony informacji niejawnych	131
1.3. Postępowania sprawdzające	132
2. Odpowiedzialność kierownika jednostki oraz pełnomocnika do spraw ochrony informacji niejawnych	135
2.1. Odpowiedzialność i obowiązki kierownika jednostki w związku z ochroną informacji niejawnych	135
2.2. Zadania pełnomocnika ds. ochrony informacji niejawnych	136
3. Klasyfikacja informacji niejawnych	139
3.1. Charakterystyka klasyfikacji informacji niejawnych	139
3.2. Tryb nadawania klauzuli tajności	140
4. Udostępnianie informacji niejawnych	143
4.1. Rękojmia zachowania tajemnicy	143
4.2. Bezwzględna ochrona informacji	143
4.3. Warunki dostępu do informacji niejawnych	144

4.4. Warunki dopuszczenia do pracy z dostępem do informacji o klauzuli „poufne” oraz „zastrzeżone”	144
5. Postępowanie sprawdzające	145
5.1. Charakterystyka postępowań sprawdzających	145
5.1.1. Postępowanie zwykle	145
5.1.2. Postępowanie poszerzone	147
5.2. Cel przeprowadzania postępowań sprawdzających	148
5.3. Termin zakończenia postępowań sprawdzających	149
5.4. Ankieta bezpieczeństwa osobowego	149
5.5. Zakończenie postępowania sprawdzającego	149
5.5.1. Wydanie poświadczenia bezpieczeństwa	150
5.5.2. Odmowa wydania poświadczenia bezpieczeństwa	150
5.5.3. Umorzenie postępowania sprawdzającego	151
5.6. Kontrolne postępowanie sprawdzające	151
5.7. Postępowanie odwoławcze i skargowe	152
6. Kancelarie tajne	155
6.1. Charakterystyka kancelarii tajnej	155
7. Środki bezpieczeństwa fizycznego	167
7.1. Charakterystyka środków bezpieczeństwa fizycznego	167
7.2. Bezpieczeństwo przemysłowe	168
7.3. Przechowywanie akt postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego	168
8. Wezwanie do wyjaśnienia zasadności zastrzeżenia informacji jako tajemnicy przedsiębiorstwa	171
8.1. Zasada jawności	171
8.2. Tajemnica przedsiębiorstwa	171
8.2.1. Warunki uznania informacji za tajemnicę przedsiębiorstwa	171
8.2.2. Charakter techniczny i wartość gospodarcza informacji	172
8.2.3. Ujawnienie do publicznej wiadomości	172
8.2.4. Zakres działań zmierzających do ochrony informacji poufnych	173
8.2.5. Termin na zastrzeżenie informacji jako tajemnicy przedsiębiorstwa	173
8.3. Forma wezwania	174
8.4. Obowiązek przeprowadzenia procedury wyjaśniającej	174
8.5. Adresaci wezwania	175
8.6. Treść wezwania	176
8.7. Wylączenie możliwości zastrzeżenia informacji	179
8.8. Odpowiedzi na pytania w zakresie tajemnicy przedsiębiorstwa	179
8.8.1. Wymogi formalne w zakresie oznaczania fragmentu oferty jako tajemnica przedsiębiorstwa	179
8.8.2. Nieudzielenie przez wykonawcę wyjaśnień na poparcie uznania informacji za tajemnicę przedsiębiorstwa	180
8.8.3. Wstrzymanie udostępnienia jawnych części ofert do chwili zakończenia badania zasadności utajnienia informacji	180
8.8.4. Zasada jawności dokumentacji przetargowej	181
8.9. Przykładowe orzeczenia dotyczące tajemnicy przedsiębiorstwa	182
8.9.1. Zakres informacji stanowiących tajemnicę przedsiębiorstwa w usługach sprzątnia	182
8.9.2. Informacje nieprawdziwe i tajemnica przedsiębiorstwa	184
8.9.3. Zakres możliwości zastrzeżenia tajemnicy przedsiębiorstwa	187

8.9.4. Formularz cenowy nie jest tajemnicą przedsiębiorstwa	187
8.9.5. Obowiązek zamawiającego zbadania zasadności zastrzeżenia tajemnicy przedsiębiorstwa	189
8.9.6. Termin na wniesienie odwołania na utajnione informacje	190
9. Polityka bezpieczeństwa informacji	195
9.1. Części składowe polityki bezpieczeństwa informacji	195
9.1.1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe	198
9.1.2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	199
9.1.3. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	200
9.1.4. Sposób przepływu danych pomiędzy poszczególnymi systemami	200
9.1.5. Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych	201
9.2. Elementy składowe polityki bezpieczeństwa informacji	203
9.2.1. Środki bezpieczeństwa na poziomie podstawowym	203
9.2.2. Środki bezpieczeństwa na poziomie podwyższonym	204
9.2.3. Środki bezpieczeństwa na poziomie wysokim	205
9.2.4. Założenia określania poziomu zagrożenia	206
9.3. Plan ochrony informacji niejawnych w jednostce samorządu terytorialnego	220
10. Odpowiedzialność za naruszenie przepisów o ochronie informacji niejawnych	233
10.1. Rodzaje przestępstw przeciwko ochronie informacji	233
10.2. Odpowiedzialność służbowa	238
10.3. Obowiązek szkolenia	241
11. Zasady postępowania w przypadku utraty lub ujawnienia informacji niejawnych	243
CZĘŚĆ 3. Ochrona systemów teleinformatycznych	247
1. Prawne i normatywne podstawy zabezpieczenia systemów teleinformatycznych w jednostkach finansów publicznych	249
2. Bezpieczeństwo infrastruktury informatycznej	253
2.1. Ochrona sieci teleinformatycznej	253
2.2. Bezpieczeństwo transmisji danych	256
2.3. Kontrola dostępu w systemach informatycznych	260
2.4. Monitorowanie i rozliczalność operacji w systemie informatycznym	263
2.5. Ochrona przed niepożądanym oprogramowaniem	265
2.6. Kopie zapasowe	268
2.7. Nośniki danych	270
2.8. Scentralizowane zarządzanie infrastrukturą informatyczną	272
2.9. Ciągłość działania infrastruktury informatycznej	272
3. Bezpieczeństwo aplikacji	275
3.1. Aplikacje przetwarzające dane osobowe	275
3.1.1. Mechanizmy bezpieczeństwa w aplikacjach	279
4. Usługi podpisu elektronicznego	285
5. Zarządzanie danymi elektronicznymi	289
6. Publikacja danych w Biuletynie Informacji Publicznej	295
7. Zabezpieczenie fizyczne i środowiskowe systemów informatycznych	297

8. Zarządzanie bezpieczeństwem	301
8.1. Idea systemu zarządzania bezpieczeństwem informacji	301
8.2. Organizacja zarządzania bezpieczeństwem informacji	302
8.3. Procesy związane z wdrożeniem, utrzymaniem i doskonaleniem systemu zarządzania bezpieczeństwem informacji	303
8.4. Zarządzanie ryzykiem informatycznym	304
8.5. Bezpieczeństwo osobowe i zarządzanie wiedzą	306
8.6. Zarządzanie aktywami informacyjnymi – inwentaryzacja i klasyfikacja	308
8.7. Zarządzanie dostępem do informacji	309
8.8. Zarządzanie rozwojem infrastruktury informatycznej	311
8.9. Zarządzanie incydentami i podatnościami	312
8.10. Zarządzanie ciągłością działania	313
8.11. Zapewnienie bezpieczeństwa we współpracy z podmiotami zewnętrznymi	314
9. Dokumentacja dla systemów informatycznych przetwarzających dane osobowe	317
10. Weryfikacja bezpieczeństwa infrastruktury informatycznej	321