

Spis treści

Wykaz skrótów.....	11
Rozdział 1. Wprowadzenie.....	15
1.1. Źródła prawa.....	17
1.2. Podstawowe pojęcia z zakresu ochrony danych osobowych.....	22
1.2.1. Dane osobowe.....	22
1.2.2. Dane wrażliwe.....	26
1.2.3. Dane jawne.....	27
1.2.4. Administrator danych.....	30
1.2.5. Procesor (podmiot przetwarzający).....	33
1.2.6. Administrator bezpieczeństwa informacji.....	34
1.2.7. Przetwarzanie danych.....	36
1.2.8. Zbiór danych.....	36
1.2.9. System informatyczny.....	39
1.3. Dobre praktyki w zakresie bezpieczeństwa danych.....	41
Rozdział 2. Osoby zaangażowane w zabezpieczanie danych osobowych i ich obowiązki.....	43
2.1. Administrator danych.....	45
2.1.1. Zapewnienie środków technicznych i organizacyjnych służących do ochrony przetwarzanych danych osobowych.....	47
2.1.2. Upoważnianie osób dopuszczonych do przetwarzania danych.....	48
2.1.3. Powoływanie i odwoływanie osób funkcyjnych.....	48
2.1.4. Wdrożenie dokumentacji opisującej sposób przetwarzania danych osobowych.....	49
2.1.5. Zapewnianie przestrzegania przepisów o ochronie danych osobowych.....	50
2.1.6. Przydzielenie obowiązków ADO innym osobom.....	51
2.2. Administrator bezpieczeństwa informacji i jego zastępcy.....	51
2.2.1. Niezbędne kompetencje i odrębność organizacyjna.....	52
2.2.2. Zgłoszenie do rejestru GIODO.....	54
2.2.3. Zakres zadań.....	55
2.2.4. Powołanie zastępcy lub zastępców ABI.....	68
2.2.5. Korzyści z powołania ABI.....	68
2.2.6. Odwołanie ABI.....	70
2.3. Administratorzy systemu informatycznego.....	70

2.4. Użytkownicy.....	72
2.5. Inne osoby.....	77
2.5.1. Bez powołania ABI.....	78
2.5.2. Wsparcie dla ABI.....	79
2.5.3. Wsparcie dla ASI.....	81
Rozdział 3. Zabezpieczenia organizacyjne.....	83
3.1. Polityka bezpieczeństwa (danych osobowych).....	85
3.1.1. Obszar przetwarzania danych osobowych.....	86
3.1.2. Wykaz zbiorów danych osobowych i programów stosowanych do ich przetwarzania.....	89
3.1.3. Opis struktury zbiorów danych.....	93
3.1.4. Sposób przepływu danych pomiędzy poszczególnymi systemami.....	97
3.1.5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.....	99
3.2. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.....	102
3.2.1. Procedury nadawania uprawnień.....	103
3.2.2. Metody i środki uwierzytelnienia.....	105
3.2.3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy.....	106
3.2.4. Procedury tworzenia kopii zapasowych.....	108
3.2.5. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji i kopii zapasowych.....	109
3.2.6. Sposób zabezpieczenia systemu informatycznego przed złośliwym oprogramowaniem.....	110
3.2.7. Sposób odnotowania w systemie informacji o udostępnieniu danych osobowych odbiorcom.....	111
3.2.8. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji.....	113
3.3. Upoważnienia do przetwarzania danych i ewidencja osób upoważnionych.....	114
3.3.1. Upoważnienia do przetwarzania danych.....	114
3.3.2. Ewidencja osób upoważnionych.....	117
3.4. Zgoda na przebywanie w miejscu przetwarzania danych.....	120
3.5. Zapisy dotyczące poufności danych osobowych.....	122
3.6. Organizacyjne zasady pracy (dobre praktyki).....	123
3.7. Inne procedury wpływające na bezpieczeństwo danych osobowych.....	125

3.7.1. Zasady udostępniania danych osobowych.....	126
3.7.2. Zasady powierzania przetwarzania danych osobowych.....	128
3.7.3. Procedury reagowania na incydenty.....	129
3.7.4. Procedura używania komputerów przenośnych.....	131
Rozdział 4. Zabezpieczenia fizyczne.....	133
4.1. Zasady ogólne.....	135
4.2. Przykłady adekwatnych zabezpieczeń fizycznych.....	137
4.2.1. Szacowanie ryzyka.....	138
4.2.2. Katalog zabezpieczeń fizycznych.....	138
4.2.3. Polityka czystego biurka i czystego ekranu.....	140
4.2.4. Przykłady stosowania adekwatnych zabezpieczeń.....	140
4.2.5. Przetwarzanie danych poza obszarem ich przetwarzania.....	141
4.3. Zabezpieczenia fizyczne przewidziane w normie ISO 27001 jako przykład dobrych praktyk.....	142
Rozdział 5. Zabezpieczenia techniczne (informatyczne).....	145
5.1. Minimalne wymogi wskazane w przepisach wykonawczych do ustawy o ochronie danych osobowych.....	147
5.1.1. Zasady ogólne.....	147
5.1.2. Środki techniczne przewidziane przez przepisy prawa.....	148
5.1.3. Uwierzytelnienie.....	151
5.1.4. Oprogramowanie antywirusowe.....	154
5.1.5. Szyfrowanie danych.....	155
5.1.6. Komunikacja i udostępnianie danych w chmurze obliczeniowej.....	156
5.1.7. Przydzielanie zróżnicowanych uprawnień.....	158
5.1.8. Kopie zapasowe.....	159
5.1.9. Monitorowanie zabezpieczeń.....	160
5.1.10. Obligatoryjne funkcjonalności systemu informatycznego.....	161
5.2. Zabezpieczenia techniczne (informatyczne) przewidziane w normie ISO 27001 jako przykład dobrych praktyk.....	162
5.3. Inne przepisy prawne odnoszące się do bezpieczeństwa infrastruktury IT.....	164
Rozdział 6. Zagrożenia dla bezpieczeństwa danych i najczęściej popełniane błędy.....	167
6.1. Typowe błędy użytkowników.....	169
6.1.1. Hasła.....	171

6.1.2.	Nośniki.....	173
6.1.3.	Praca na koncie z pełnymi uprawnieniami.....	174
6.1.4.	Niebezpieczne strony WWW.....	175
6.2.	Narzędzia programowe wykorzystywane do ataków na bezpieczeństwo informacji.....	175
6.2.1.	Wirusy.....	177
6.2.2.	Robaki.....	177
6.2.3.	Trojany (konie trojańskie).....	178
6.2.4.	Backdoor.....	178
6.2.5.	Rootkity.....	179
6.2.6.	Keyloggery.....	179
6.2.7.	Spyware.....	180
6.2.8.	Exploity.....	180
6.2.9.	Dialery.....	180
6.3.	Socjotechnika.....	181
6.3.1.	Socjotechnika werbalna.....	181
6.3.2.	Phishing.....	182
6.3.3.	Smishing.....	183
6.3.4.	Pharming.....	183
Rozdział 7.	Audyt bezpieczeństwa danych osobowych.....	185
7.1.	Wymogi prawne.....	187
7.1.1.	Pojęcie audytu.....	187
7.1.2.	Sprawdzenia przeprowadzane przez ABI.....	188
7.1.3.	Sposób prowadzenia sprawdzeń.....	190
7.1.4.	Sprawozdanie ze sprawdzenia.....	191
7.1.5.	Nadzór nad dokumentacją ochrony danych osobowych.....	192
7.2.	Przygotowanie audytu bezpieczeństwa danych osobowych.....	194
7.2.1.	Cel audytu.....	194
7.2.2.	Planowanie audytu.....	195
7.2.3.	Opisywanie niezgodności w raporcie z audytu.....	196
7.2.4.	Listy kontrolne.....	198
7.3.	Zakres podmiotowy i przedmiotowy audytu bezpieczeństwa danych osobowych.....	199
7.3.1.	Zakres podmiotowy.....	199
7.3.2.	Zakres przedmiotowy.....	200
7.4.	Dobre praktyki audytowe przewidziane w normie ISO 19011.....	203

Rozdział 8. Odpowiedzialność z tytułu naruszenia obowiązków dotyczących zabezpieczenia danych osobowych	207
8.1. Odpowiedzialność administracyjna	209
8.2. Odpowiedzialność karna	211
8.3. Odpowiedzialność cywilnoprawna	212
8.4. Odpowiedzialność wynikająca z prawa pracy	213
Wzory dokumentów	215
Wybrane akty prawne	247
Bibliografia	305
Indeks	309