

Bezpieczeństwo danych osobowych. Podejście oparte na ryzyku

Dowiedz się więcej na www.ksiegarnia.beck.pl

Spis treści

Wykaz skrótów	XI
Wykaz literatury	XV
Wprowadzenie	XXIII
Rozdział I. Przepisy i normy dotyczące ochrony danych osobowych	1
1. Wymagania nałożone przez RODO	1
1.1. Ochrona praw i wolności osób fizycznych	1
1.2. Zabezpieczenie danych	2
1.3. Monitorowanie i wykrywanie naruszeń	5
1.4. Stosowanie zabezpieczeń przez podmiot przetwarzający	6
1.4.1. Powierzenie przetwarzania danych	6
1.4.2. Zaufani dostawcy i zleceniobiorcy	6
1.4.3. Podpowierzenie przetwarzania danych	7
1.5. Środki minimalizujące ryzyko: szyfrowanie, pseudonimizacja i anonimizacja	8
1.6. Środki i polityki bezpieczeństwa	9
1.7. Rejestr czynności przetwarzania	10
1.8. Ocena skutków dla ochrony danych	11
1.9. Nadzór nad bezpieczeństwem danych	13
2. Wymagania wynikające z Kodeksu pracy	14
2.1. Monitoring w miejscu pracy	15
2.2. Upoważnienia do przetwarzania danych	15
3. Wymagania zawarte w przepisach branżowych	16
3.1. Przepisy dotyczące instytucji finansowych	16
3.2. Przepisy dotyczące operatorów usług kluczowych i dostawców usług cyfrowych	16
3.3. Przepisy dotyczące podmiotów stosujących ustawę o rachunkowości	18
3.4. Przepisy dotyczące organów unijnych	19
4. Odpowiedzialność za naruszenie przepisów o ochronie danych osobowych	21
4.1. Osoby odpowiedzialne za przetwarzanie danych osobowych	21

4.1.1. Administrator danych (przedsiębiorca, organizacja)	21
4.1.2. Podmiot przetwarzający (procesor)	21
4.1.3. Pracownicy	22
4.1.4. Osoby zatrudnione na podstawie umowy cywilnoprawnej	23
4.1.5. Osoby samozatrudnione	23
4.1.6. Inspektor ochrony danych	23
4.1.7. Administrator systemu informatycznego	23
4.2. Obowiązek zachowania informacji w poufności	24
4.3. Kary za naruszenie przepisów o ochronie danych osobowych	25
5. Uznane normy i standardy	29
5.1. Normy ISO	29
5.1.1. Standardy ISO jako narzędzia ułatwiające zarządzanie bezpieczeństwem danych osobowych zgodnie z RODO	29
5.1.2. ISO 29100 „Ramy prywatności”	30
5.1.3. ISO 29134 „Wytyczne dotyczące oceny skutków dla prywatności” ...	33
5.1.4. ISO 29151 „Praktyczne zasady ochrony danych osobowych”	33
5.1.5. ISO 27000 „System zarządzania bezpieczeństwem informacji – informacje ogólne i słownik pojęć”	34
5.1.6. ISO 27001 „System zarządzania bezpieczeństwem informacji – wymagania”	35
5.1.7. ISO 27002 „Praktyczne zasady zarządzania bezpieczeństwem informacji”	36
5.1.8. ISO 27005 „Zarządzanie ryzykiem w bezpieczeństwie informacji” ...	36
5.1.9. ISO 22301 „Zarządzanie ciągłością działania”	36
5.1.10. ISO 31000 „Zarządzanie ryzykiem – zasady i wytyczne”	37
5.2. Standardy NIST	37
5.2.1. SP 800-12 Rev. 1 „ <i>An Introduction to Information Security</i> ”	38
5.2.2. SP 800-53 Rev. 4 „ <i>Security and Privacy Controls for Federal Information Systems and Organizations</i> ”	39
5.2.3. SP 800-122 „ <i>Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)</i> ”	41
5.2.4. SP 800-30 rev. 1 „ <i>Guide for Conducting Risk Assessments</i> ”	42
5.2.5. NISTIR 7621 Rev. 1 „ <i>Small Business Information Security: The Fundamentals</i> ”	43
5.3. Wytyczne NCSC	45
5.4. CIS Controls v7.1	47
5.5. CIS Benchmarks	49
5.6. Wytyczne i rekomendacje Komisji Nadzoru Finansowego	50

Rozdział II. Ochrona informacji w społeczeństwie informacyjnym – rozważania teoretyczne	53
1. Społeczeństwo informacyjne i gospodarka oparta na wiedzy	53

2. Dane, informacje i wiedza	57
2.1. Informacje a dane – różnice definicyjne	57
2.2. Specyficzne cechy informacji	59
2.3. Wiedza i mądrość	60
3. Komunikacja	61
4. Tajemnica	62
4.1. Asymetria informacyjna	62
4.2. Cechy tajemnicy	63
4.3. Ochrona informacji	64
5. Bezpieczeństwo i cyberbezpieczeństwo	66
6. Zagrożenia	68
6.1. Złodzieje informacji	68
6.2. Źródła, przykłady i skutki zagrożeń	69
6.3. Użytkownik jako zagrożenie	72
Rozdział III. Podstawowe zabezpieczenia	75
1. Minimalne wymagania dotyczące zabezpieczeń	75
2. Zabezpieczenia fizyczne	77
2.1. Środki ochrony fizycznej	77
2.2. Wstęp na obszar przetwarzania	77
2.3. Ochrona urządzeń przed uszkodzeniem	79
2.4. Zabezpieczenia stosowane w podróży	80
2.5. Fizyczne niszczenie dokumentów i innych nośników informacji	81
3. Zabezpieczenia techniczne	83
3.1. Zapora sieciowa i zapora ogniowa	83
3.2. Sieć komputerowa	85
3.3. Dostęp do danych w systemie informatycznym	90
3.3.1. Identyfikacja osoby w systemie informatycznym	90
3.3.2. Zabezpieczenie urządzeń i aplikacji hasłem	91
3.3.3. Tworzenie i zapisywanie haseł	93
3.3.4. Uwierzytelnianie wieloskładnikowe	96
3.3.5. Stosowanie wygaszacza ekranu	99
3.4. Zabezpieczenia komputerów	100
3.4.1. Instalowanie programów	100
3.4.2. Licencjonowane oprogramowanie	103
3.4.3. Uprzywilejowany dostęp	104
3.4.4. Zabezpieczanie danych na dysku	105
3.4.5. Aktualizacje	105
3.4.6. Pozbywanie się sprzętu	108
3.5. Przesyłanie plików	110
3.6. Przeglądanie zasobów Internetu	114

3.7. Bezpieczna poczta elektroniczna	115
3.8. Tworzenie kopii danych	115
3.9. Domeny internetowe	118
4. Zabezpieczenia aplikacji i stron internetowych	119
5. Zabezpieczenia organizacyjne	120
Rozdział IV. Zarządzanie ryzykiem	123
1. Bezpieczeństwo a zarządzanie ryzykiem	123
2. Pojęcie ryzyka	124
3. Proces zarządzania ryzykiem	125
4. Etapy zarządzania ryzykiem	128
4.1. Identyfikacja ryzyka	128
4.2. Analiza ryzyka	130
4.3. Ocena ryzyka	133
4.3.1. Sterowanie ryzykiem	134
4.3.2. Monitorowanie ryzyka	135
5. Ryzyko z perspektywy ochrony danych osobowych	136
5.1. Zarządzanie ryzykiem zgodnie z RODO	136
5.2. Podejście do ochrony danych osobowych oparte na ryzyku	139
5.3. Ryzyko związane z podmiotami przetwarzającymi	142
5.3.1. Wybór wiarygodnego podmiotu przetwarzającego	142
5.3.2. Zabezpieczenie danych osobowych przez podmiot przetwarzający ..	144
5.4. Ryzyko związane z przetwarzaniem danych osobowych w państwach trzecich	145
5.5. Proces zarządzania ryzykiem a ocena skutków dla ochrony danych	146
6. Metody pomocne w zarządzaniu ryzykiem	148
6.1. Metoda SWIFT („co, jeśli”)	149
6.2. Analiza przyczynowo-skutkowa (CEA)	150
6.3. Matryca skutek/prawdopodobieństwo (macierz ryzyka)	151
6.4. Analizy: przyczyn i konsekwencji (CCA), drzewa błędów i drzewa zdarzeń ..	152
6.5. Macierz Haddona	153
6.6. Listy kontrolne	154
Rozdział V. Poziomy ryzyka i zabezpieczeń w praktyce	157
1. Analiza ryzyka dla procesu wysyłki newslettera	157
2. Poziomy ryzyka	161
2.1. Poziomy graniczne ryzyka	161
2.2. Skala skutków naruszenia ochrony danych	164
3. Poziomy zabezpieczeń	169
3.1. Wybór poziomu zabezpieczeń	169
3.2. Ocena podstawowych zabezpieczeń dla przykładowego procesu	170

Rozdział VI. Zarządzanie dostępami i polityki haseł	181
1. Posiadanie dostępu do danych osobowych a zezwolenie na ich przetwarzanie ...	181
2. Proces logowania do systemu informatycznego	182
3. Ogólne zasady zarządzania uprawnieniami dostępu	185
3.1. Identyfikatory użytkowników systemu	185
3.2. Minimalizacja dostępu	189
3.3. Dostęp bazujący na rolach	189
3.4. Przegląd kont	190
3.5. Wykaz systemów i przyznanych dostępu	190
3.6. Active Directory	191
4. Polityki haseł	192
4.1. Budowa hasła a czas jego łamania	192
4.2. Numer PIN	193
4.3. Hasła maskowane i hasła jednorazowe	195
4.4. Procedura resetowania haseł domyślnych	196
4.5. Hasła w aplikacjach szytych na miarę	197
4.6. Transmisja haseł	199
4.7. Alternatywy dla haseł	200
5. Pewność uwierzytelnienia	201
Rozdział VII. Aktualizacje (poprawki) bezpieczeństwa	205
1. Cyfrowa higiena bezpieczeństwa	205
2. Wykaz zasobów wykorzystywanych do przetwarzania danych osobowych	206
3. Instalowanie aktualizacji	207
Rozdział VIII. Dokumentacja i polityki bezpieczeństwa danych osobowych	209
1. Znaczenie terminu „polityka bezpieczeństwa” w kontekście ochrony danych osobowych	209
2. Dokumentacja na gruncie RODO	210
3. Kodeksy postępowania	210
4. Plan postępowania z naruszeniami	211
5. Rozwiązania techniczne wykrywające naruszenia	212
5.1. <i>Security information and event management (SIEM)</i>	212
5.2. <i>Intrusion detection systems (IDS) oraz intrusion prevention system (IPS)</i>	214
5.3. <i>Network access control (NAC)</i>	214
5.4. Oprogramowanie antywirusowe	215
5.5. Skanowanie podatności	215
6. Plany zachowania ciągłości działania	215
Rozdział IX. Budowanie świadomości bezpieczeństwa	217
1. Świadomość zagrożeń a podatność użytkownika na ataki	217

2. Program budowania świadomości bezpieczeństwa	218
3. Socjotechnika	220
Rozdział X. Zarządzanie bezpieczeństwem	223
1. Bezpieczeństwo jako stan i jako proces	223
2. Projektowanie systemu zabezpieczeń	225
2.1. Obrona wielowarstwowa	225
2.2. Bezpieczeństwo przez zaciemnianie	226
2.3. Klasyfikacja informacji	227
2.3.1. Poziomy klasyfikacji informacji	227
2.3.2. Praktyczna klasyfikacja informacji	227
3. Nadzór nad zabezpieczeniami	229

[Przejdź do księgarni →](#)



ksiegarnia.beck.pl