

Konrad Gałaj-Emiliańczyk

**Wdrożenie RODO
w małych i średnich organizacjach
Praktyczny poradnik
(z suplementem elektronicznym)**



ODDK Spółka z ograniczoną odpowiedzialnością Spółka komandytowa
Gdańsk 2018

Spis treści

Wstęp	7
Rozdział 1	
Obecny stan prawny a przyszły stan prawny	11
1.1. System ochrony danych regulowany przepisami prawa	12
1.2. System ochrony danych regulowany wewnątrznie	15
1.3. Co się zmienia, a co pozostaje takie samo	17
1.4. Nowy model ochrony danych osobowych – opinie ekspertów	20
Rozdział 2	
Od czego zacząć, czyli co jest, a co powinno być	25
2.1. Weryfikacja zgodności działań organizacji z UODO – krok po kroku	26
2.2. Weryfikacja zgodności działań organizacji z RODO – krok po kroku	29
2.3. Tworzenie harmonogramu dostosowania do RODO	31
2.4. Planowanie dostosowania do RODO w czasie	32
Rozdział 3	
Proces przetwarzania danych osobowych, czyli klucz do zgodności z RODO	35
3.1. Identyfikacja procesów przetwarzania danych osobowych	36
3.2. Klasyfikacja danych osobowych w procesach ich przetwarzania i DPIA	38
3.3. Identyfikacja zasobów niezbędnych do bezpiecznego działania procesów	43
3.4. Identyfikacja zagrożeń w procesach przetwarzania danych	46
3.5. Identyfikacja podatności w procesach przetwarzania danych	48
Rozdział 4	
Analiza ryzyka – proste metody	51
4.1. Wybór metody oceny ryzyka	51
4.2. Jakościowa metoda analizy ryzyka	52
4.3. Ilościowa metoda analizy ryzyka	56
4.4. Mieszana metoda analizy ryzyka	60
4.5. Klasyfikacja zidentyfikowanych ryzyk	63
Rozdział 5	
Plan postępowania z ryzykiem i monitorowanie ryzyka	65
5.1. Sposoby zarządzania ryzykiem – praktyczne podejście	67
5.2. Akceptacja ryzyka i ryzyka szczytkowe	70
5.3. Harmonogram działań zarządzania ryzykiem	71
5.4. Planowanie dostosowania zabezpieczeń w czasie	71
5.5. Analizy ryzyka na etapie projektowania produktu lub usługi	73

Rozdział 6	
Dostosowanie zabezpieczeń – fizycznych, organizacyjnych i informatycznych . . .	77
6.1. Zabezpieczenia fizyczne obszaru przetwarzania	77
6.2. Zabezpieczenia infrastruktury informatycznej	80
6.3. Zabezpieczenia programowe i konfiguracyjne	81
6.4. Zabezpieczenia organizacyjne	84
6.5. Zabezpieczenia urządzeń mobilnych i nośników danych	86
Rozdział 7	
Dostosowanie procesów przetwarzania danych osobowych	89
7.1. Przygotowanie wdrożenia zmian w funkcjonujących procesach	89
7.2. Zapewnienie podstaw prawnych przetwarzania danych	91
7.3. Spełnienie obowiązku informacyjnego	92
7.4. Wdrożenie umów powierzenia z procesorami danych osobowych	94
7.5. Przygotowanie lub dostosowanie Polityki bezpieczeństwa zgodnej z RODO	96
7.6. Definicje oraz podstawa prawna regulacji	98
7.7. Zakres podmiotowy i przedmiotowy regulacji	98
7.8. Opis zastosowanych zabezpieczeń fizycznych	99
7.9. Opis zastosowanych zabezpieczeń organizacyjnych	100
7.10. Opis zastosowanych zabezpieczeń informatycznych	112
7.11. Rejestr czynności przetwarzania	113
7.12. Funkcja IOD i kontakty z organem nadzorczym	114
7.13. Przepisy końcowe i podsumowanie	116
7.14. Doskonalenie projektowanego systemu ochrony danych osobowych	116
Rozdział 8	
Przejęcie z systemu UODO na system RODO – 25 maja 2018 r.	119
8.1. Uruchomienie systemu RODO – komunikacja wewnętrzna i zewnętrzna	120
8.2. Funkcjonowanie IOD w organizacji	121
8.3. Komunikacja z organem nadzorczym	123
Rozdział 9	
Podsumowanie	125
9.1. Największe problemy przy wdrożeniu	126
9.2. Prawa osób, których dane dotyczą, a ich świadomość	127
9.3. Podsumowanie zmian – spojrzenie praktyczne	128
Bibliografia	131
Spis rysunków	133
Spis tabel	134