

Konrad Gałąj-Emiliańczyk

Inspektor ochrony danych

**Kompetencje, obowiązki i odpowiedzialność.
Poradnik praktyka z wzorami dokumentów**

(z suplementem elektronicznym)



ODDK Spółka z ograniczoną odpowiedzialnością Sp.k.
Gdańsk 2018

Spis treści

Wstęp	11
Rozdział 1.	
Rys historyczny nadzoru nad ochroną danych osobowych	13
Lata 1995–2011	15
Lata 2011–2015	17
Lata 2015–2018	19
Obecnie	21
Rozdział 2.	
System ochrony danych osobowych	25
Zaplanowanie systemu ochrony danych	27
Audyt zgodności systemu ochrony danych	34
Modyfikacja systemu ochrony danych.....	36
Rozdział 3.	
Warunki pełnienia funkcji IOD – zewnętrzne	39
Wiedza fachowa IOD.....	40
Rozdział 4.	
Warunki organizacyjne pełnienia funkcji IOD – wewnętrzne	43
Status inspektora ochrony danych.....	44
Wsparcie i niezbędne zasoby IOD	45
Zasoby niezbędne do utrzymania fachowej wiedzy inspektora ochrony danych (IOD)	47
Inne obowiązki inspektora ochrony danych (IOD) a brak konfliktu interesów	50
Rozdział 5.	
Wybór IOD – pracownik, freelancer, outsourcing	53
IOD jako pracownik administratora danych	54
IOD jako samodzielny specjalista zewnętrzny.....	58
IOD jako firma outsourcingowa.....	60
Rozdział 6. Powołanie do pełnienia funkcji IOD	65
Wybór osoby do pełnienia funkcji IOD	65
Wybór zespołu wdrażającego.....	67
Powołanie IOD	69

Rozdział 7. Zawiadomienie o powołaniu IOD.....	73
Przygotowanie zawiadomienia.....	74
Kontakt do inspektora ochrony danych (IOD)	75
Rozdział 8.	
Pełnienie nadzoru – od czego zacząć?	77
Specyfika branży i sektora organizacji	78
Rozmiar i złożoność organizacji	79
Liczba osób przetwarzających dane osobowe.....	80
Struktura najwyższego kierownictwa organizacji	80
Zadania inspektora ochrony danych (IOD).....	81
Szacowanie ryzyka – nowy obowiązek inspektora ochrony danych (IOD)	85
Rozdział 9.	
Przygotowanie planu audytu – krok po kroku	89
Częstotliwość audytów	93
Terminy audytów	95
Zakres audytu	96
Metodyka audytów.....	98
Rozdział 10.	
Przygotowanie narzędzi do pełnienia nadzoru	101
Przygotowanie harmonogramu audytu	101
Przygotowanie list kontrolnych – wywiad osobowy.....	102
Przygotowanie list kontrolnych – wizja lokalna	105
Przygotowanie list kontrolnych – dokumentacja	107
Przygotowanie list kontrolnych – systemy informatyczne	109
Przygotowanie list kontrolnych dla podmiotów zewnętrznych	113
Rozdział 11.	
Audyt początkowy systemu ochrony danych.....	115
Informowanie o audycie	116
Pouczanie i instruowanie osób	117
Typowe problemy przy sprawdzeniu początkowym	118
Rozdział 12.	
Raport z audytu w praktyce.....	121
Zgodności i niezgodności	123
Potencjalne ryzyka	124
Możliwości doskonalenia	125
Rekomendacje w zakresie dostosowania.....	126
Rozdział 13.	
Przygotowanie dokumentacji ochrony danych osobowych	129
Propozycja dokumentacji ochrony danych osobowych	130
Modyfikacje i akceptacja zespołu wdrożeniowego	132

Akceptacja najwyższego kierownictwa.....	133
Przydzielenie osób do procesów – wdrożenie	134
Rozdział 14.	
Zapoznanie osób upoważnionych	137
Wybór metody zapoznania osób upoważnionych	137
Ocena skuteczności zapoznania.....	141
Zaplanowanie okresowej aktualizacji wiedzy	141
Rozdział 15.	
Rejestr czynności przetwarzania a IOD	143
Identyfikacja i kategoryzacja procesów przetwarzania danych osobowych.....	143
Przygotowanie rejestru czynności przetwarzania.....	147
Udostępnienie rejestru czynności przetwarzania.....	148
Rozdział 16.	
Rekomendacje IOD w zakresie dostosowania	149
Alternatywność rekomendacji.....	150
Ocena wpływu rekomendacji na procesy w organizacji.....	151
Terminy realizacji rekomendacji	152
Wskazanie osób odpowiedzialnych za wdrożenie zmian.....	153
Opinie Grupy roboczej art. 29 ds. ochrony danych osobowych / ERODO.....	153
Rozdział 17.	
Codzienna praca IOD – studium przypadku	155
Opiniowanie procesów – pytania zespołu wdrożeniowego	155
Opiniowanie procesów – pytania osób upoważnionych.....	156
Opiniowanie i negocjowanie umów powierzenia przetwarzania danych osobowych	158
Nadzór nad podmiotami zewnętrznymi	159
Zgody na przetwarzanie danych osobowych.....	160
Spełnienie obowiązku informacyjnego	160
Zarządzanie incydentami	161
Raporty z incydentów	162
Wnioski o realizację praw osób, których dane dotyczą.....	163
Rozdział 18.	
Praktyczne porównanie ABI i IOD	165
Fakultatywność powołania ABI a obowiązek powołania IOD.....	165
Dane kontaktowe IOD w obowiązku informacyjnym	166
Dane IOD w rejestrze czynności przetwarzania danych osobowych...	167
Obowiązkowe konsultacje administratora danych z IOD.....	167
Jeden IOD w grupie administratorów danych	168

Podsumowanie i zakończenie	169
Bibliografia.....	171
Przepisy prawa.....	171
Orzecznictwo	172
Strony internetowe	172
Publikacje	173