

Konrad Gałąj-Emiliańczyk

Administrator bezpieczeństwa informacji /Inspektor ochrony danych

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

(z suplementem elektronicznym)



ODDK Spółka z ograniczoną odpowiedzialnością Sp.k.
Gdańsk 2017

Niniejszy poradnik opisuje od strony praktycznej pełnienie funkcji administratora bezpieczeństwa informacji (ABI) w systemie ochrony danych osobowych. Celem opracowania jest przede wszystkim pomoc osobom obejmującym funkcje ABI, a mającym niewielkie doświadczenie w zakresie bezpieczeństwa informacji. Przystępnie opisano wybór osoby mającej objąć tę funkcję, niezbędne kompetencje oraz uprawnienia i obowiązki, jakie osoba ta posiada w ramach nadzoru prowadzonego nad systemem ochrony danych osobowych. Opracowanie przedstawia ewolucję funkcji ABI od początku jej istnienia do kolejnego etapu modyfikacji, jakim jest powoływanie inspektora ochrony danych (IOD). Szczególnie użytecznym elementem poradnika jest opis najczęściej występujących problemów, z którymi styka się ABI w trakcie pełnienia swojej funkcji, a także propozycje alternatywnych rozwiązań tych problemów.

Spis treści

Wstęp	11
Rozdział 1.	
Rys historyczny nadzoru nad ochroną danych osobowych.....	13
Lata 1995–2011	15
Obecnie	19
Od ABI do inspektora ochrony danych (IOD).....	21
Rozdział 2.	
System ochrony danych osobowych.....	25
Zaplanowanie systemu ochrony danych	28
Sprawdzenie systemu ochrony danych	36
Modyfikacja systemu ochrony danych.....	40
Rozdział 3.	
Warunki prawne pełnienia funkcji ABI – zewnętrzne	43
Pełna zdolność do czynności prawnych i pełnia praw publicznych	45
Odpowiednia wiedza w zakresie ochrony danych osobowych.....	46
Brak karalności za przestępstwo umyślne	47
Rozdział 4.	
Warunki organizacyjne pełnienia funkcji ABI – wewnętrzne.....	49
Bezpośrednia podległość pod administratora danych.....	50
Środki i odrębność organizacyjna ABI.....	51
Obowiązek włączania inspektora ochrony danych (IOD) w procesy	52
Zasoby niezbędne do utrzymania fachowej wiedzy inspektora ochrony danych (IOD)	54
Inne obowiązki inspektora ochrony danych (IOD) a brak konfliktu interesów	56
Rozdział 5.	
Wybór ABI – pracownik, freelancer, outsourcing	59
ABI jako pracownik administratora danych	60
ABI jako samodzielny specjalista zewnętrzny	64
ABI jako firma outsourcingowa	66
Rozdział 6. Powołanie do pełnienia funkcji ABI	69
Wybór osoby do pełnienia funkcji ABI	69
Wybór zespołu wdrażającego.....	71
Powołanie ABI.....	73

Rozdział 7. Zgłoszenie ABI do rejestru GIODO	75
Przygotowanie wniosku zgłoszeniowego	76
Kontakt do ABI, inspektora ochrony danych (IOD).....	78
Skutki zgłoszenia ABI do rejestru prowadzonego przez GIODO	80
Rozdział 8. Pełnienie nadzoru – od czego zacząć?	81
Specyfika branży i sektora organizacji	82
Rozmiar i złożoność organizacji	83
Liczba osób przetwarzających dane osobowe.....	84
Struktura najwyższego kierownictwa organizacji	85
Zadania inspektora ochrony danych (IOD).....	86
Szacowanie ryzyka – nowy obowiązek inspektora ochrony danych (IOD).....	90
Rozdział 9.	
Przygotowanie planu sprawdzeń – krok po kroku.....	93
Częstotliwość sprawdzeń.....	97
Terminy sprawdzeń	99
Zakres sprawdzeń	101
Metodyka sprawdzeń	103
Rozdział 10.	
Przygotowanie narzędzi do pełnienia nadzoru	105
Przygotowanie harmonogramu sprawdzeń.....	105
Przygotowanie list kontrolnych – wywiad osobowy.....	106
Przygotowanie list kontrolnych – wizja lokalna	110
Przygotowanie list kontrolnych – dokumentacja	112
Przygotowanie list kontrolnych – systemy informatyczne	115
Przygotowanie list kontrolnych dla podmiotów zewnętrznych.....	119
Rozdział 11.	
Sprawdzenie początkowe systemu ochrony danych.....	121
Informowanie o sprawdzeniu.....	122
Pouczanie i instruowanie osób	124
Typowe problemy przy sprawdzeniu początkowym	124
Rozdział 12. Sprawozdanie ze sprawdzenia w praktyce.....	127
Zgodności i niezgodności	128
Potencjalne ryzyka	130
Możliwości doskonalenia	131
Rekomendacje w zakresie dostosowania.....	132
Rozdział 13.	
Przygotowanie dokumentacji ochrony danych osobowych	135
Propozycja dokumentacji ochrony danych osobowych	137
Modyfikacje i akceptacja zespołu wdrożeniowego	139

Akceptacja najwyższego kierownictwa.....	140
Przydzielenie osób do procesów – wdrożenie	141
Rozdział 14. Zapoznanie osób upoważnionych	143
Wybór metody zapoznania osób upoważnionych	143
Ocena skuteczności zapoznania	147
Zaplanowanie okresowej aktualizacji wiedzy	147
Rozdział 15. Rejestr zbiorów prowadzony przez ABI	149
Identyfikacja i kategoryzacja zbiorów danych osobowych.....	150
Przygotowanie rejestru zbiorów danych osobowych.....	153
Udostępnienie rejestru zbiorów danych osobowych.....	155
Aktualizacja rejestru zbiorów danych osobowych	159
Rozdział 16.	
Rekomendacje ABI w zakresie dostosowania	161
Alternatywność rekomendacji	163
Ocena wpływu rekomendacji na procesy w organizacji.....	164
Terminy realizacji rekomendacji	164
Wskazanie osób odpowiedzialnych za wdrożenie zmian.....	165
Opinie ERODO i rekomendacje inspektora ochrony danych (IOD)	166
Rozdział 17.	
Codzienna praca ABI – studium przypadku	167
Opiniowanie procesów – pytania zespołu wdrożeniowego	167
Opiniowanie procesów – pytania osób upoważnionych.....	168
Opiniowanie i negocjowanie umów powierzenia przetwarzania danych osobowych	170
Nadzór nad podmiotami zewnętrznymi	171
Zgody na przetwarzanie danych osobowych.....	172
Spełnienie obowiązku informacyjnego	172
Zarządzanie incydentami	173
Sprawozdania ze sprawdzeń doraźnych.....	174
Sprawdzenia na żądanie GIODO.....	175
Rozdział 18.	
Praktyczne porównanie ABI i inspektora ochrony danych (IOD).....	177
Fakultatywność powołania ABI a obowiązek powołania IOD	177
Dane kontaktowe IOD w obowiązku informacyjnym	178
Dane IOD w rejestrze czynności przetwarzania danych osobowych...	179
Obowiązkowe konsultacje administratora danych z IOD.....	179
Jeden IOD w grupie administratorów danych	180
Podsumowanie i zakończenie	181
Bibliografia.....	183
Przepisy prawa	183

Orzecznictwo	184
Strony internetowe	184
Publikacje	185