Administrator Bezpieczeństwa informacji

- teraźniejszość i przyszłość

Jarosław Żabówka
proinfosec@odoradca.pl

Plan prezentacji

- Dyrektywa i ustawa
- Praktyka
- Oczekiwania
- Propozycje Komisji Europejskiej

Teraźniejszość: Dyrektywa

- Dyrektywie 95/46/WE Parlamentu Europejskiego I Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, wprowadza pojęcie **„Data protection official”**, co w naszej ustawie zostało zaimplementowane jako „Administrator bezpieczeństwa informacji”.

DPO

- Musi mieć możliwość wykonywania swoich obowiązków w sposób niezależny od Administratora danych (pkt 49 preambuły).
- Współpracuje z GIODO przed przetworzeniem danych (pkt 54 preambuły).
- Odpowiada za zapewnienie stosowania przepisów krajowych przyjętych na mocy Dyrektywy (art. 18 pkt 2).
- Odpowiada za prowadzenie rejestru operacji przetwarzania danych (art. 18 pkt 2).
- W wypadku powołania DPO, administrator może zostać zwolniony z obowiązku zawiadamiania o przetwarzaniu danych (u nas – rejestracji zbiorów).
- Współpracuje z GIODO w trakcie kontroli wstępnych.

DPO – problemy z tłumaczeniem

Wersja angielska

- Data protection official
- Art. 18: personal data protection official

Wersja polska

- Urzędnik odpowiedzialny za ochronę danych
- Art. 18: Urzędnik do spraw ochrony danych

Rozporządzenie Nr 45/2001 Parlamentu Europejskiego I Rady z dnia 18 grudnia 2000r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych:

- Data Protection Officer
- Inspektor ochrony danych

Spojrzenie w przyszłość

- Czy ABI stanie się IOD?

Teraźniejszość: Ustawa

- W polskiej ustawie ABI pojawia się w wyniku nowelizacji z 2004 roku.
- administrator bezpieczeństwa musi być wyznaczony przez administratora danych osobowych, chyba, że ADO sam będzie wykonywał jego czynności.
- Z obowiązku powołania ABI (lub samodzielnego pełnienia jego zadań) zwolnieni są administratorzy pełniący działalność dziennikarską, literacką lub artystyczną.

Zadania ABI

- ABI nadzoruje przestrzeganie środków technicznych i organizacyjnych przetwarzania danych osobowych przyjętych u administratora danych.
- W innych państwach europejskich, wymogi co do zadań i kwalifikacji ABI (DPO), zostały niejednokrotnie bardziej szczegółowo określone.
- „Nadzór” oznacza, że ABI powinien mieć możliwość ingerencji, wydawania poleceń, itd. w sytuacji gdy zasady przetwarzania danych nie są przestrzegane lub w celu zapewnienia zgodnego z tymi zasadami przetwarzania danych.

ABI

- ABI może, ale nie musi być pracownikiem administratora danych.
- Powinien być konkretną osobą fizyczną, wyznaczoną przez ADO.
- Wyznaczenie ABI powinno mieć formę pisemną.
- Czy ADO może wyznaczyć kilku ABI?

ABI – konflikt interesów

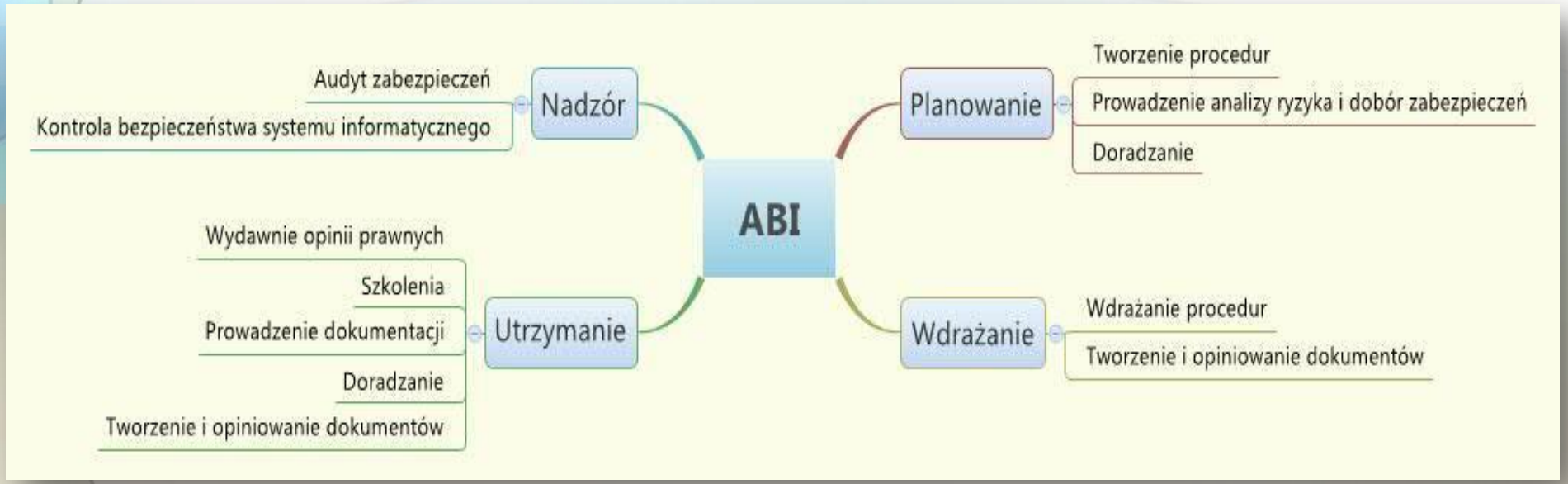
- Mimo, że nie jest to określone wprost, ABI powinien być w taki sposób umocowany w strukturze organizacji, by móc w sposób prawidłowy realizować swoje zadania, kontaktować się z kierownictwem działów i w sposób niezależny nadzorować przetwarzanie w nich danych.
- Nic nie stoi na przeszkodzie, żeby pełnił jednocześnie inne funkcje. Nie powinny one jednak powodować powstania konfliktu interesu, który mógłby utrudnić administratorowi bezpieczeństwa informacji realizowanie jego zadań.

ABI - odpowiedzialność

- Przyjmuje się, że niewłaściwe realizowanie obowiązków przez ABI, jako osobę zobowiązaną do ochrony danych osobowych może podlegać karze zgodnie z art.51 ustawy.
  - *Art. 51.*

  1. *Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*
  2. *Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*

Teraźniejszość: Praktyka



Przykładowe role ABI

- Prawnik – tworzy umowy powierzenia, upoważnienia, itd.
- Pracownik biurowy – prowadzi szereg rejestrów.
- Audytor bezpieczeństwa.
- Specjalista od analizy ryzyka.
- Twórca polityki bezpieczeństwa.
- Informatyk - administrator bezpieczeństwa systemu.
- Trener.

- Czy ABI musi posiadać umiejętności we wszystkich powyższych dziedzinach?

- ABI działa na rzecz administratora danych i powinien stanowić jego prawą rękę w rozwiązywaniu problemów ochrony danych.

ABI - cechy

- Umiejętność podejmowania decyzji i ponoszenia ich konsekwencji
- Umiejętność rozwiązywania problemów
- Umiejętność pracy w zespole
- Zdolności myślenia analitycznego
- Zmysł obserwacji
- …

ABI – konflikt interesów

- ABI – kierownik lub pracownik działu IT
- ABI – autor polityki bezpieczeństwa
- ABI – pracownik przetwarzający dane

Przykładowy zakres zadań

Zakres zadań ABI w MSZ:

- wdrożenie oraz uaktualnianie dokumentacji, o którym mowa w § 3 ust. 1 oraz § 4 rozporządzenia (…)
- nadzór nad ochroną danych osobowych (…)
- informowanie (…) o przypadkach naruszenia(…)
- koordynacja i nadzór nad procesem opisu zbioru danych osobowych (…)
- zgłaszanie nowych zbiorów oraz zmian dotyczących zarejestrowanych zbiorów (…)
- prowadzenie ewidencji zbiorów(…)
- prowadzenie rejestru zdarzeń (…)

Oczekiwania

- Coraz większa potrzeba szczegółowych uregulowań w obszarach:
  - Zadania ABI
  - Uprawnienia ABI
  - Umocowanie ABI w strukturze organizacyjnej
- Najważniejsze wydaje się zapewnienie skutecznych mechanizmów gwarantujących ABI niezależność w podejmowanych decyzjach. Mechanizmy te nie mogą nakładać dodatkowych obciążeń na administratorów danych.

Postulaty

- Ustawa nie powinna określać szczegółowych czynności ABI.
- Ustawa powinna stanowić dla ABI narzędzie pozwalające mu skutecznie realizować podstawowy obowiązek, którym pozostaje nadzór nad stosowaniem szeroko rozumianych zabezpieczeń, ale również udział w ich tworzeniu i wdrażaniu.
- Proponowane rozwiązania muszą być dostosowane zarówno do dużych jak i bardzo małych podmiotów.
- Nie możemy tworzyć kolejnego zawodu regulowanego.

Propozycje

- Planuje się rezygnację z obowiązku rejestracji zbiorów danych i zobowiązanie ABI do prowadzenia takiego rejestru.
  - Rozwiązanie korzystne dla Urzędu i dla ADO
  - ABI i tak powinien prowadzić taki rejestr
  - Być może jednak ABI powinien posiadać odpowiedni mechanizm gwarantujący mu możliwość realizacji tego zadania?
- Możliwe wydaje się rozwiązanie w którym, w określonych odstępach czasu, ABI przesyła GIODO sprawozdanie z prowadzonych kontroli. Z takiego obowiązku mogliby być zwolnieni administratorzy bezpieczeństwa posiadający odpowiednie certyfikaty.

ABI – CZŁOWIEK GIODO, CZY ADO?

- Do tej pory, administrator bezpieczeństwa informacji działał na rzecz administratora danych. W proponowanych rozwiązaniach, ABI zaczyna pełnić rolę przedstawiciela GIODO w organizacji.
- Konieczne jest bardzo dobre wyważenie roli ABI.
- Podejmowane działania muszą w minimalny sposób nakładać nowe obciążenia na organizacje.

Przyszłość: Projekt rozporządzenia

- Przygotowany przez Komisję Europejską projekt rozporządzenia *(General Data Protection Regulation)*, które być może zastąpi wkrótce naszą krajową, ustawę o ochronie danych osobowych, bardzo szeroko traktuje zadania i prawa ABI, który staje się tutaj „Data protection officer".
- Omówmy pokrótce proponowany rozwiązania.

Rozdział 4 – Data protection officer. Art. 32 – Wyznaczenie DPO

- DPO musi być wyznaczony przez ADO lub procesora *(również art. 19 ust. 2. pkt (e))*:
  - Będącego instytucją publiczną
  - Zatrudniającego powyżej 250 pracowników
  - Podstawowa działalność ADO lub procesora polega na regularnym i systematycznym monitorowaniu osób
- Inne podmioty mogą wyznaczyć DPO.
- DPO powinien posiadać adekwatną wiedzę i powinna być ona dostosowana do przetwarzanych danych.
- ADO i procesor powinni zapewnić, że DPO wykonując swoje zadania nie będzie narażony na konflikty interesów.

Rozdział 4 – Data protection officer. Art. 32 – Wyznaczenie DPO

- ADO lub procesor wyznacza DPO na dwuletnią kadencję, która może być następnie przedłużona. W czasie swojego urzędowania, DPO może być zwolniony, jedynie, jeżeli nie spełnia wymagań koniecznych do pełnienia swoich obowiązków.
- DPO może być zatrudniony przez ADO lub procesora, lub wykonywać swoje zadania w oparciu o umowę o świadczenie usług.
- Dane DPO powinny być przekazane GIODO, podane do publicznej wiadomości oraz udostępnione osobom, których dane są przetwarzane *(również w art. 12 ust. 1. pkt (a))*. Osoby te muszą mieć możliwość kontaktu z DPO w wypadku incydentów i w celu skorzystania z praw nadanych przez rozporządzenie.

Art. 33 – DPO w strukturze organizacyjnej

- ADO lub procesor zapewnia, że DPO jest zaangażowany we wszystkie zagadnienia związane z ochroną danych.
- DPO wykonuje swoje zadania niezależnie i podlega bezpośrednio dyrekcji.
- ADO lub procesor wspierają DPO w realizacji zadań oraz zapewniają niezbędne zasoby.

Art. 34 –Zadania DPO

- Rozporządzenie określa jedynie minimalne zadania DPO.
- Informuje ADO i procesora o ich obowiązkach oraz dokumentuje te działania.
- Monitoruje wdrażanie i stosowanie polityki, w tym prowadzenie szkoleń, audytów.
- Monitoruje wdrażanie i stosowanie rozporządzenia.
- Zapewnia prowadzenie wymaganej rozporządzeniem dokumentacji.

Art. 34 –Zadania DPO

- Monitoruje skuteczność oceny skutków przetwarzania danych.
- Monitoruje odpowiedzi na żądania GIODO *(supervisory authority)* oraz współpracuje z GIODO w zakresie własnych kompetencji.
- Stanowi osobę kontaktową dla GIODO.

- W części przepisów komisja ma prawo wprowadzać dodatkowe wymagania.

Art. 79 – odpowiedzialność administracyjna

- W wypadku niewyznaczenia DPO lub umyślnego lub nieumyślnego niespełnienia wymagań określonych w art. 32, 33 lub 34, GIODO powinien nałożyć w karę w wysokości 100tyś.- 1mln. Euro lub 5% światowego obrotu przedsiębiorstwa.

Bardzo dziękujemy za uwagę i zapraszamy do dyskusji.