ABI – teraźniejszość i przyszłość

Wersja 1.2

PROINFOSEC@ODORADCA.PL

14 grudzień 2011

Autor: Jarosław Żabówka

Autor:
Praktyk, z wieloletnim doświadczeniem w tworzeniu i wdrażaniu polityki bezpieczeństwa danych osobowych w administracji publicznej i przedsiębiorstwach prywatnych.
Administrator bezpieczeństwa informacji, audytor normy ISO 27001 i manager systemów informatycznych.
Popularyzator zagadnień ochrony danych osobowych, aktywnie uczestniczący w budowaniu polskiej społeczności administratorów bezpieczeństwa informacji. Współorganizator „Internetowych Spotkań ABI".

ABI

Badania pokazują, że nasze społeczeństwo jest coraz bardziej świadome swoich praw wynikających z ustawy o ochronie danych osobowych. Świadomość ta zwykle koncentruje się wokół kilku pojęć. „Zgoda na przetwarzanie danych osobowych", „GIODO", „ABI" – są najczęściej używanymi słowami-kluczami, z którymi ludzie kojarzą ochronę danych. W praktyce, niejednokrotnie przedsiębiorcy ograniczają się jedynie do wyznaczenia Administratora Bezpieczeństwa Informacji, traktując to jako dopełnienie swoich obowiązków oraz jako przerzucenie ewentualnej odpowiedzialności na inną osobę.

Ale kim zgodnie z ustawą jest ABI? Jakie zadania pełni w praktyce? Jakie zmiany w tym zakresie są niezbędne? W założeniu tent tekst miał odpowiadać na te pytania oraz pokrótce zebrać opinie pojawiające się w toczonych ostatnio na różnych forach dyskusjach o przyszłości tej profesji. W międzyczasie pojawiły się „przecieki" o planowanych zmianach w europejskim prawie ochrony danych, w tym dotyczących pozycji i zadań ABI. Ponieważ zmiany te w dużym stopniu wydają się wychodzić naprzeciw oczekiwaniom środowiska (w każdym razie, ja uważam je za interesujące), postanowiłem nie zmieniać istotnie tego tekstu, a jedynie dodać fragment mówiący o planowanych zmianach.

TERAŹNIEJSZOŚĆ

KIM JEST OFICJALNIE

DYREKTYWA

Europejskie prawo ochrony danych osobowych opiera się na 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.

Dyrektywa wprowadza pojęcie Urzędnika do spraw ochrony danych, któremu w ustawie o ochronie danych osobowych odpowiada Administrator bezpieczeństwa informacji. Od razu należy jednak zwrócić uwagę na kilka szczegółów. Angielska wersja Dyrektywy, mówi o „data protection official" (DPO) czemu w polskim tłumaczeniu odpowiada „Urzędnik odpowiedzialny za ochronę danych". Jednak w art. 18 tłumaczenia pojawia się „Urzędnik do spraw ochrony danych". Czy jest to celowe rozróżnienie? Tym bardziej, że w wersji angielskiej też pojawia się drobna różnica. Mamy tutaj „personal data protection official".

Jednak nieco więcej zamieszania może wyniknąć z rozporządzenia Nr 45/2001 Parlamentu Europejskiego I Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych. Rozporządzenie mówi o „Data Protection Officer", co zostało przetłumaczone jako „inspektor ochrony danych". Powrócę do tego tematu na końcu tekstu.

Co Dyrektywa mówi o DPO:

- Musi mieć on 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.

USTAWA

W polskiej ustawie ABI pojawia się w wyniku nowelizacji z 2004 roku. Nie będę tutaj rozważał sytuacji sprzed tej nowelizacji. Zgodnie z art. 36 ustawy o ochronie danych osobowych, administrator bezpieczeństwa musi być wyznaczony przez administratora danych osobowych, chyba, że ADO sam będzie wykonywał jego czynności. Zgodnie z ustawą, ABI nadzoruje przestrzeganie środków technicznych i organizacyjnych przetwarzania danych osobowych przyjętych u administratora danych. Zapis ten możemy uznać za bardzo ogólny i w rzeczywistości zakres zadań realizowanych przez ABI bywa bardzo różny. Warto zwrócić uwagę, że w innych państwach europejskich, wymogi co do zadań i kwalifikacji ABI (DPO), zostały niejednokrotnie bardziej szczegółowo określone.

Z obowiązku powołania ABI (lub samodzielnego pełnienia jego zadań) zwolnieni są administratorzy pełniący działalność dziennikarską, literacką lub artystyczną.

„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 może, ale nie musi być pracownikiem administratora danych. Należy jednak zwrócić uwagę, że powinien być konkretną osobą fizyczną, wyznaczoną przez ADO. 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. Zwykle postuluje się tutaj, że nie powinien on być pracownikiem pionu IT, podlegającego zwykle szczególnej uwadze ABI. Ze względów dowodowych, wyznaczenie ABI powinno mieć formę pisemną.

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.

Istnieją podzielone opinie, co do tego, czy ADO może wyznaczyć kilku ABI. Ja skłaniałbym się do tego, że jest dopuszczalne, a w wielu organizacjach nawet wskazane.

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.*

KIM JEST W RZECZYWISTOŚCI

W rzeczywistości zakres zadań realizowanych przez ABI bywa bardzo szeroki. Chciałbym jednak zwrócić uwagę na jeszcze jeden aspekt jego roli – bardzo często, ochrona danych osobowych bywa utożsamiana z powołaniem ABI (obok zgłoszenia zbioru i zgody na przetwarzanie danych), szkoda, że często administratorem bezpieczeństwa informacji staje się osoba przypadkowa, niezdająca sobie sprawy ze spoczywających na niej obowiązków i co gorsza, z grożącej jej odpowiedzialności. Na szczęście wydaje się, że możemy obserwować stałą poprawę tej sytuacji.

Zbyt często jednak, moim zdaniem, ABI znajduje się w sytuacji konfliktu interesów. Bardzo trudno jest pełnić tę rolę będąc jednocześnie kierownikiem, lub co gorsza, pracownikiem działu IT. Wyobraźmy sobie takiego ABI-ego, przychodzącego do swojego szefa:

> *-(ABI/Informatyk) Szefie, musimy w naszych systemach wdrożyć mechanizm pozwalający użytkownikom na zmianę haseł.*
> *-(Kierownik IT) Zgadzam się całkowicie. Jesteś informatykiem, zrób to.*
> *-Ale tego się nie da zrobić narzędziami które mamy…*
> *-To, po co do mnie przychodzisz?!*

Niejednokrotnie też, ABI jest autorem procedur, których funkcjonowanie musi później nadzorować. Czy jest w stanie dobrze i wiarygodnie to robić?

Rola administratora bezpieczeństwa ma wiele twarzy:

- 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.

Zwykle ABI musi łączyć wszystkie lub większość z tych funkcji. Przykładowe zakresy obowiązków administratora bezpieczeństwa informacji, które możemy znaleźć w literaturze, liczą nieraz po kilka stron. Czy to źle? Myślę, że nie można w ten sposób powiedzieć. Każda organizacja jest inna, a i każdy ABI ma nieco inne predyspozycje i doświadczenie. Moim zdaniem, że dopóki nie obniża to bezpieczeństwa przetwarzanych danych, taka różnorodność może być korzystna. Na szczęście ABI przestał już być utożsamiany z informatykiem.

ABI nie powinien jednak zapominać, że działa na rzecz administratora danych i powinien stanowić

jego prawą rękę w rozwiązywaniu problemów ochrony danych.

W Internecie można znaleźć mnóstwo przykładowych zakresów czynności ABI. Ważne żeby nie traktować żadnego z nich jako obowiązującego wzoru. Obowiązująca ustawa nakłada na administratora bezpieczeństwa konkretne obowiązki, nie oznacza to jednak, że konkretny zakres czynności nie może być dostosowany do potrzeb konkretnej organizacji. Czy ABI powinien prowadzić szkolenia? Bardzo dobrze, jeżeli to robi i taka jest potrzeba w konkretnej organizacji. Jeżeli jednak ograniczy się do nadzoru, czy pracownicy posiadają wymaganą wiedzę, a szkolenia będzie prowadzić wyspecjalizowana, zatrudniająca trenerów firma zewnętrzna, to również będzie dobre rozwiązanie.

ABI, zwykle jest osobą, która koordynuje działania związane z ochroną danych osobowych odpowiada za kontakty z GIODO, wspiera pracowników i kierownictwo. I taka rola bardzo mi się podoba. Oby w jak największej ilości organizacji, zarząd rozumiał obowiązki ochrony danych i postrzegał administratorów bezpieczeństwa informacji jako wsparcie w rozwiązywaniu związanych z tym problemów.

JAKIE KWALIFIKACJE SĄ NIEZBĘDNE WSPÓŁCZESNEMU ABI-EMU?

Z powyższych rozważań wynika, że ABI powinien posiadać bardzo szerokie kwalifikacje. Z pewnością powinien dobrze orientować się w zagadnieniach prawa przetwarzania danych osobowych. Powinien posiadać również wiedzę informatyczną, w przeciwnym wypadku może być świetnym specjalistą od zagadnień ochrony danych osobowych, ale we współczesnych organizacjach, trudno będzie mu prawidłowo realizować nakładany przez ustawę obowiązek nadzoru.

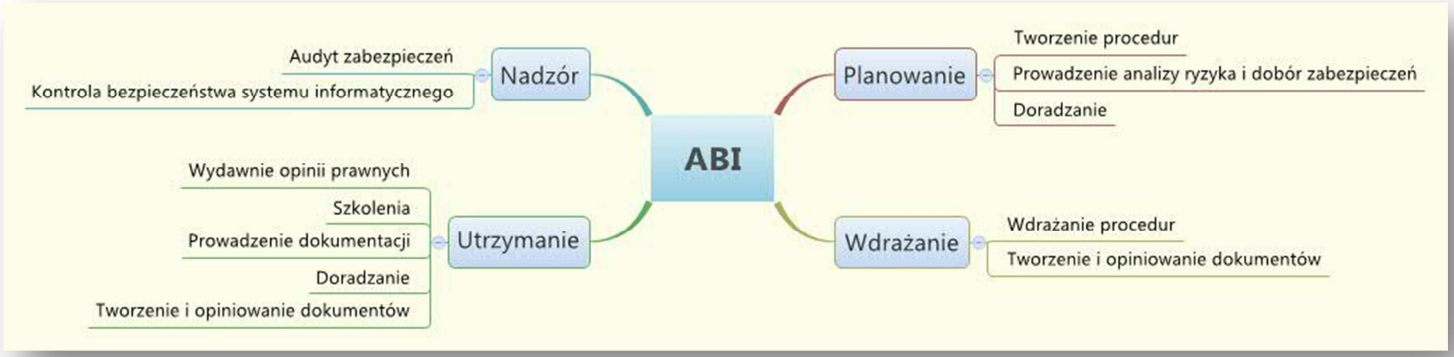
Z pewnością nie powinna być to osoba przypadkowa. Umiejętność współpracy i skutecznego prowadzenia nadzoru wydaje się kluczowa. Musi posiadać umiejętność podejmowania decyzji i być gotowym na ponoszenie ich konsekwencji.

ODPOWIEDZIALNOŚĆ

Pełnienie roli administratora bezpieczeństwa informacji wiąże się z dużą odpowiedzialnością. O możliwości odpowiedzialności karnej już wspominałem. Oczywiście, w wyniku zaniedbania swoich obowiązków, ABI może ponieść również konsekwencje służbowe.

Administrator bezpieczeństwa informacji, powinien mieć zawsze świadomość konsekwencji swoich decyzji. Czasami, mogą się one wiązać się ze sporymi kosztami dla pracodawcy. I mam tu na myśli, nie tylko ewentualne odszkodowania, ale np. prowadzone przez niektóre organizacje akcje rozsyłania do tysięcy swoich klientów druków zgody na przetwarzanie danych osobowych, w sytuacjach, gdy taka zgoda w ogóle nie była potrzebna…

„SYSTEMATYKA”



PRZYSZŁOŚĆ

JAKI ABI JEST NAM POTRZEBNY

Coraz bardziej widoczna stała się potrzeba uregulowania zadań i pozycji administratora bezpieczeństwa informacji w organizacjach. Na różnych forach przetoczyła się dyskusja i pojawiły się różne, czasami bardzo sprzeczne propozycje uregulowań. Jako o jednym z najbardziej spójnych rozwiązań, wypada wspomnieć o propozycji Stowarzyszenia ABI. Można się z nimi zapoznać na stronie stowarzyszenia.

Wydaje się, że bardziej szczegółowe określenie zadań ABI w ustawie jest wskazane. Nie powinno to jednak oznaczać, że wpisujemy poszczególne czynności, jak prowadzenie szkoleń, czy rejestru pomieszczeń. Zapisy ustawowe powinny stanowić dla administratora bezpieczeństwa informacji narzędzie pozwalające mu skutecznie realizować podstawowy obowiązek, którym jest nadzór nad stosowaniem szeroko rozumianych zabezpieczeń, ale również udział w ich tworzeniu i wdrażaniu. Najważniejsze wydaje się zapewnienie skutecznych mechanizmów gwarantujących administratorowi bezpieczeństwa informacji niezależność w podejmowanych decyzjach. Mechanizmy te nie powinny jednocześnie nakładać dużych obowiązków na administratorów danych.

Rozmawiając o roli nowego ABI, zbyt często, moim zdaniem, koncentrujemy się na dużych organizacjach. Rzecz w tym, że duże organizacje zwykle zagadnienia ochrony danych mają uporządkowane. Nawet, jeżeli powodują one ogromne problemy, to w skali dużego podmiotu, są one rozwiązywalne. Inaczej wygląda sprawa małych organizacji. Niewielki zakład, nawet jeżeli przetwarza jedynie dane pracowników, staje często przed problemami, które w jego skali są nierozwiązywalne. Inny przykład mogą stanowić szkoły – sytuacja jest tutaj katastrofalna, a dane niejednokrotnie bardzo wrażliwe (stan zdrowia, rozwój psychiczny, współpraca z innymi podmiotami, np. ośrodkami pomocy społecznej). Wprowadzenie nowych uregulowań, nie spowoduje automatycznego uzdrowienia sytuacji. Konieczne wydaje się niezbędne wypracowanie rozwiązań możliwych do wdrożenia przez takie podmioty.

Pojawiają się również propozycje, by znieść obowiązek rejestrowania zbiorów danych i w zamian powierzyć administratorom bezpieczeństwa informacji obowiązek prowadzenia rejestru takich zbiorów. Co prawda głównym celem tej zmiany wydaje się odciążenie urzędu, spowoduje to jednak również zmniejszenie ilości pracy wykonywanej przez administratorów bezpieczeństwa informacji. Przecież rejestr zbiorów i tak muszą oni prowadzić. Może warto jednak pomyśleć o jakimś wzmocnieniu pozycji ABI. Wielu administratorów danych utożsamia rejestrację zbiorów z ochroną danych osobowych. Oby nie doszło tu do sytuacji, w której ABI usłyszy od prezesa – „ty mi tu głowy nie zawracaj, przecież tą całą ochronę danych już znieśli".

Planując zmiany w zakresie przepisów dotyczących ABI, wyróżnić możemy podstawowe obszary:

- Zadania ABI
- Uprawnienia ABI
- Umocowanie ABI w strukturze organizacyjnej

KWALIFIKACJE. ZAWÓD REGULOWANY? CERTYFIKATY?

Z pewnością warto zagwarantować posiadanie przez administratora bezpieczeństwa informacji odpowiednich kwalifikacji. Wydaje się jednak, że wpisanie do ustawy obowiązku posiadania wykształcenia prawniczego lub informatycznego może spowodować więcej szkody niż korzyści. Być może dobrym rozwiązaniem jest prosty zapis mówiący o tym żeby ABI musiał posiadać odpowiednie kwalifikacje w stosunku do konkretnego zakresu realizowanych zadań.

Z pewnością, bardzo ważne jest posiadanie przez ABI odpowiednich cech osobistych. Jakiekolwiek próby odgórnej regulacji, może spowodować, że do zawodu dostaną się osoby nie posiadające odpowiednich predyspozycji.

Kuszącym pomysłem wydaje się początkowo utworzenie nowego zawodu regulowanego. ABI musi zdać egzamin kwalifikujący, uzyskać akceptację GIODO, posiadać odpowiednie certyfikaty zawodowe… Po głębszej analizie, okazuje się jednak, że takie rozwiązanie nie tylko nie ma szansy bycia przyjętym (bo kto się odważy powiedzieć, że w imię ochrony danych osobowych, przedsiębiorcy będą musieli ponosić nowe, wysokie koszty, które w rezultacie przeniosą się na społeczeństwo), ale prawdopodobnie doprowadziłoby do obniżenia poziomu zabezpieczenia danych. Musielibyśmy się liczyć z ukrywaniem faktu przetwarzania danych, z opanowaniem rynku przez pojedyncze podmioty i w konsekwencji dyktowaniem cen i poziomu realizacji usług.

Wydaje się jednak, że posiadanie pewnych uprawnień, np. certyfikatów zawodowych mogłoby być premiowane, np. możliwością prowadzenia rejestru zbiorów danych osobowych i braku konieczności ich zgłaszania GIODO.

Możliwe wydaje się również przyjęcie rozwiązania, zgodnie z którym, w określonych odstępach czasu ABI przesyła GIODO sprawozdanie z prowadzonych kontroli. Z takiego obowiązku mogliby być zwolnieni administratorzy bezpieczeństwa posiadający odpowiednie certyfikaty (zakres wymieniony w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych z dnia 10 września 2010 r. wydaje się dobrym przykładem).

ODPOWIEDZIALNOŚĆ?

Uważam, że uszczegółowienie obowiązków ABI, zapewnienie mu swego rodzaju nienaruszalności, powinno wiązać się również z większą odpowiedzialnością. Chcemy mieć gwarancję, że ABI będzie korzystał ze zwiększenia swoich obowiązków w sposób prawidłowy. Nie koniecznie musi to być odpowiedzialność karna. Podobałaby mi się możliwość ponoszenia odpowiedzialności służbowej, np. jeżeli ABI nie dopełni swoich obowiązków i zostanie to stwierdzone przez GIODO.

ABI – CZŁOWIEK GIODO, CZY ADO?

Do tej pory, administrator bezpieczeństwa informacji działał na rzecz administratora danych. Nadzorował, doradzał, ale zawsze występował po stronie administratora danych. W proponowanych rozwiązaniach, ABI zaczyna pełnić rolę przedstawiciela GIODO w organizacji. Z jednej strony nie chcemy tworzyć nowego zawodu regulowanego, nie chcemy istotnie podnosić kosztów administratora danych, z drugiej jednak strony planujemy wprowadzić obowiązek wyznaczania osoby, która będzie po części pełniła rolę urzędnika biura GIODO. Nie twierdzę że ABI nie powinien mieć pewnych obowiązków, do których spełnienia będzie zobowiązany, nawet gdy ADO będzie miał inne zdanie. Uważam, że danie ABI takich możliwości jest mocno wskazane. W połączeniu z zagwarantowaniem pewnej niezależności i podniesieniem ewentualnej odpowiedzialności, może to dać bardzo dobre efekty. Konieczne jest jednak bardzo dobre wyważenie roli ABI, a jednocześnie podejmowane działania muszą w minimalny sposób nakładać nowe obciążenia na organizacje.

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.

PODSTAWOWE ZNACZENIE MA 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 kontrolowaniu 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.
- 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 kontrolera o ich obowiązkach oraz dokumentuje te działania.
- Monitoruje wdrażanie i stosowanie polityki, w tym prowadzenie szkoleń, audytów i przypisywanie obowiązków.
- Monitoruje wdrażanie i stosowanie rozporządzenia.
- Zapewnia prowadzenie wymaganej rozporządzeniem dokumentacji.
- 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 100 tyś. – 1 mln. Euro lub 5% światowego obrotu przedsiębiorstwa.

PKT 62 PREAMBUŁY

DPO może, ale nie musi być pracownikiem ADO. Swoje zadania wykonuje niezależnie.

SPRÓBUJMY PRZEWIDZIEĆ PRZYSZŁOŚĆ

W najbliższym czasie możemy się spodziewać nowej wersji rozporządzenia MSWiA z 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służą ce do przetwarzania danych osobowych, a być może również ustawy o ochronie danych osobowych. Generalny Inspektor wydaje się zdeterminowany by przeprowadzić te zmiany, zresztą nie ma innego

wyjścia – rozporządzenie w obecnej postaci nie nadaje się do stosowania.

Następnie możemy spodziewać się zastąpienia Dyrektywy i Ustawy przez rozporządzenie UE. Ucieczki nie ma – prawo ochrony danych osobowych musi zostać zmienione albo przestanie funkcjonować.

Jaka będzie po tych zmianach rola Administratorów Bezpieczeństwa Informacji? Starajmy się na to wpłynąć już teraz.

profesjonalna
ochrona informacji

proInfoSec
Jarosław Żabówka

Rozwiązania dla Twojej firmy