ACTA UNIVERSITATIS WRATISLAVIENSIS
No 3661
PRZEGLĄD PRAWA I ADMINISTRACJI C/2
WROCŁAW 2015

KRZYSZTOF WYGODA
Uniwersytet Wrocławski

POWOŁYWANIE ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI JAKO ZASADA BEZPIECZNEGO PRZETWARZANIA DANYCH NA GRUNCIE USTAWY O OCHRONIE DANYCH OSOBOWYCH

1. ZAGADNIENIA WSTĘPNE

Nowelizacja ustawy o ochronie danych osobowych[1] (dalej u.o.d.o.), zmieniająca dotychczasową regulację prawną m.in. w zakresie zniesienia art. 36 ust. 3, spowodowała, iż wielu administratorów danych (dalej ADO) zaczęło zastanawiać się, czy nowe rozwiązania legislacyjne podtrzymują *status quo* w zakresie obowiązku powołania administratora bezpieczeństwa informacji (dalej ABI), czy też prowadzą do jego zmiany idącej w kierunku większej swobody w podejmowaniu decyzji o powołaniu tego bez wątpienia kluczowego w procesie bezpiecznego przetwarzania danych osobowych pomiotu. Pojawiające się wzmianki dotyczące tej kwestii (m.in. na stronie GIODO), sprowadzają się jedynie do dość lakonicznych stwierdzeń niewskazujących uzasadnienia przyjętego stanowiska[2].

Biorąc pod uwagę znaczenie problemu, warto się zastanowić, czy nowy materiał normatywny daje możliwość pogłębienia interpretacji, która oprócz art. 36a ust. 1 u.o.d.o. uwzględniać będzie również inne elementy nowego stanu prawnego, co być może pozwoli na nieco pełniejszą ocenę roli ADO w procesie kreacji ABI, w kontekście związania tego pierwszego podmiotu przesłankami przesądzającymi o potrzebie powołania takiej osoby.

Prowadzona analiza wymagać będzie oceny znowelizowanych przepisów w kilku aspektach, począwszy od nowej pozycji i zakresu zadań przypisanych ABI z uwzględnieniem tych, których przejęcie następowałoby w przypadku stwierdzenia braku przesłanek jego powołania, przez dokładne wskazanie nowej pod-

[1] Zmiany do u.o.d.o. wprowadzone zostały w art. 9 ustawy z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej opublikowanej 27 listopada 2014 (Dz.U. 2014, poz. 1662), a ich wejście w życie nastąpiło 1 stycznia 2015.

[2] Por. wypowiedź „Zgodnie z art. 36a ust. 1 u.o.d.o. powołanie ABI jest uprawnieniem, a nie obowiązkiem administratora danych. W przypadku niepowołania ABI, jego zadania wykonuje sam administrator danych (art. 36b u.o.d.o.)", http://www.giodo.gov.pl/1520224/id_art/8344/j/pl/.

stawy normatywnej powoływania ABI, a na próbie oceny rzeczywistego zakresu swobody powołania tego podmiotu skończywszy. Niezbędne wydaje się również przybliżenie zagadnień związanych z zakresem związania ADO obowiązkiem powołania ABI w ujęciu sprzed nowelizacji — stanowi bowiem podstawę do snucia porównań z obecnym stanem normatywnym.

Powołanie ABI rodzi oczywiście też wiele innych problemów, wynikających choćby z jego formy, trybu, terminów, obowiązku oceny spełniania przez kandydata warunków ustawowych itd., które bez wątpienia również zasługują na analizę, ich omówienie nie może jednak zostać ujęte w tym z konieczności krótkim opracowaniu.

2. POZYCJA I ROLA ABI W PROCESACH PRZETWARZANIA DANYCH

Wyznaczenie ustawowego zakresu obowiązków ABI[3] powoduje istotną zmianę statusu tego organu wewnętrznego podmiotów przetwarzających dane osobowe. Staje się on „typowym" organem nadzoru wewnętrznego (ew. organem koordynująco-nadzorczym) w zakresie zapewniania przestrzegania przepisów o ochronie danych osobowych, funkcjonującym w oparciu o pewną autonomię (umocowaną w normach prawnych) z możliwością zlecenia określonych działań mieszczących się w zakresie jego kompetencji wynikających z u.o.d.o. i aktów wykonawczych. Ma też pewne poboczne zadania administracyjne (prowadzenie jawnego rejestru zbiorów danych przetwarzanych przez ADO), niestanowiące jednak obszaru działania, który może wpływać w sposób istotny na bezpieczeństwo procesów przetwarzania danych. Pełna analiza zadań ABI zasługuje na odrębne omówienie, które będzie jednak możliwe dopiero po ukazaniu się wszystkich aktów wykonawczych — niemniej na potrzeby wynikające z tematu omawianego zagadnienia, istniejące obecnie normy pozwalać będą na dokonanie niezbędnych ustaleń co do charakteru i podstawowego zakresu obowiązków tego organu.

Sama decyzja o powołaniu ABI (nie przesadzając w tym miejscu o jej ewentualnym obligatoryjnym charakterze) musi być bowiem postrzegana jako świadome działanie ADO, zmierzające do przeniesienia części kompetencji związanych z zapewnieniem przestrzegania przepisów u.o.d.o. na osobę, która posiadając „[...] odpowiednią wiedzę w zakresie ochrony danych osobowych..."[4], dawać będzie gwarancję realnego, a nie czysto formalnego, przestrzegania zasad ochrony danych osobowych. W przypadku jego niepowołania administrator danych, obok innych swoich obowiąz-

[3] W chwili pisania opracowania nie wydano jeszcze wszystkich aktów wykonawczych pozwalających na pełną analizę normatywnego zakresu obowiązków ABI, w tym kluczowego w tej materii rozporządzenia w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych. Niemniej istniejący (już czwarty — z 27.04.2015 r.) projekt owej regulacji daje chyba ostateczny obraz wszystkich zadań, jakie stawia się przed tym organem.

[4] Art. 36a ust. 5 pkt 2 u.o.d.o.

ków, wykonywać musi[5] również te wynikające z art. 36a ust. 2 pkt 1 u.o.d.o., przy czym, biorąc pod uwagę dość często występujący w praktyce niski, a nawet znikomy, stan jego wiedzy z zakresu ochrony danych, nie będzie mógł zakładać, że zadania te wykonuje prawidłowo. Poza oczywistymi, w tym wypadku, skutkami w postaci naruszania praw osób, których dane są przetwarzane, może dojść również do konieczności ponoszenia odpowiedzialności karnej obejmującej praktycznie całość rozdz. 8 u.o.d.o. (przejmując obowiązki ABI, administrator ma bowiem możliwość naruszenia wszystkich jego norm), a w relatywnie bliskiej przyszłości również finansowej[6].

3. OBOWIĄZKI ABI W KONTEKŚCIE ICH PRZEJĘCIA PRZEZ ADO

Biorąc pod uwagę rozwiązania ustawowe, do zadań ABI przewidzianych w art. 36a ust. 2 u.o.d.o. należy:

„1) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

[5] „Art. 36b. W przypadku niepowołania administratora bezpieczeństwa informacji zadania określone w art. 36a ust. 2 pkt 1, z wyłączeniem obowiązku sporządzania sprawozdania, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, wykonuje administrator danych", u.o.d.o.

[6] Należy bowiem brać pod uwagę, że od kilku lat UE prowadzi dość intensywne prace legislacyjne w zakresie zastąpienia dyrektywy 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 (Dz.Urz. WE L 281 z 23.11.1995, s. 31, z późn. zm.; Dz.Urz. UE, polskie wydanie specjalne, rozdz. 13, t. 15, s. 355, z późn. zm.) i ustanowienia nowego standardu ochrony danych osobowych, jakim stać się ma rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych). Kierując się prognozą zaprezentowaną przez W. Wiewiórowskiego, byłego GIODO, a obecnego zastępcy europejskiego inspektora ochrony danych „wszystko wskazuje na to, że do końca roku 2015 nastąpi przyjęcie samego tekstu rozporządzenia. Zostanie on wiosną przyszłego roku opublikowany w Dz.Urz. UE i w ciągu dwóch lat w całości wejdzie w życie" (cała wypowiedź dostępna na: www.youtube.com/watch?v=Tqqk2VAwoZg), można zakładać, iż w 2017 r. zaczną obowiązywać normy dotyczące odpowiedzialności odszkodowawczej (art. 77) i możliwe będzie nałożenie sankcji finansowych za uchybienie przepisom rozporządzenia (art. 79). Nie przesądzając o ich ostatecznym kształcie, można wskazać, iż w trakcie prac legislacyjnych generalnie zakładano, że w ramach odszkodowania osoba, która poniesie szkodę, w tym niepieniężną, w wyniku niezgodnej z prawem operacji przetwarzania danych lub działania niezgodnego z przepisami ustanowionymi w rozporządzeniu, będzie miała prawo do dochodzenia odszkodowania od administratora lub podmiotu przetwarzającego dane. Jeśli przetwarzaniem danych zajmować się będzie więcej niż jeden administrator lub podmiot przetwarzający, wówczas będą oni odpowiadać solidarnie za całą szkodę. Z kolei przewidywana, w ramach nadzoru, odpowiedzialność podmiotów, które nie wywiązują się z zobowiązań określonych w rozporządzeniu, obliguje organ nadzorczy (w Polsce GIODO) do nałożenia sankcji administracyjnych, również kumulatywnie obejmujących m.in. karę grzywny w wysokości 100 mln EUR lub 5% rocznego światowego obrotu, w przypadku przedsiębiorstw (wg propozycji Parlamentu UE) — przy czym w trakcie prac przewidywano istnienie sporej ilości wyjątków dających możliwość nałożenia jej w niższej wysokości.

a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,

b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych,

c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

2) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2–4a i 7". W przypadku przejęcia tych obowiązków przez ADO należy zaznaczyć, że poza brakiem obowiązku przygotowywania sprawozdań (art. 36b u.o.d.o.) nie będzie też konieczne podejmowanie zadań wynikających z art. 36 ust. 2 pkt 2. Co dość jednoznacznie zdaje się wynikać z art. 43 ust. 1a u.o.d.o.[7], wiążącego istnienie tego jawnego rejestru zbiorów (prowadzonego przez ABI) ze zgłoszeniem do prowadzonego przez GIODO rejestru ABI faktu powołania konkretnej osoby do pełnienia owej funkcji (zgodnie z art. 46b u.o.d.o.[8]), przy czym dotyczy to tych, których powołanie miało miejsce po 1 stycznia 2015 r.

W kontekście analizy wskazanych wyżej przepisów brak nawiązania w art. 36b u.o.d.o. do kwestii realizacji obowiązku wynikającego z art. 36a ust. 2 pkt 2 wydaje się celowym zabiegiem ustawodawcy. Wykładnia funkcjonalna (zastosowana w zakresie niewynikającym wprost z literalnego brzmienia przepisów) oparta została na założeniu, że obowiązek prowadzenia jawnego rejestru spoczywa osobiście na ABI, a od faktycznego przeprowadzenia procedury powołania i zgłoszenia go do rejestru GIODO uzależniona została możliwość korzystania ze zwolnienia z obowiązku rejestracji zbiorów, o którym mowa w art. 43 ust. 1a u.o.d.o. Co prowadzi do wniosku, że w sytuacji braku powołania ABI nie istnieją też przesłanki do korzystania ze wspomnianego zwolnienia ani też nie występuje obowiązek prowadzenia wewnętrznego jawnego rejestru zbiorów przez ADO. W przypadku innej interpretacji dochodziłoby do powielania praktycznie całości informacji dotyczącej zarejestrowanych przez GIODO zbiorów w rejestrze wewnętrznym. Takie dublowanie się źródeł informacji, choć samo w sobie wykonalne, wydaje się poniekąd sprzeczne z *ratio legis* wyrażonym choćby w tytule ustawy o ułatwieniu wykonywania działalności gospodarczej, na podstawie której wprowadzono nowelizację u.o.d.o., gdyż poza nałożeniem dodatkowego

[7] „Art. 431a. Obowiązkowi rejestracji zbiorów danych osobowych, z wyjątkiem zbiorów zawierających dane, o których mowa w art. 27 ust. 1, nie podlega administrator danych, który powołał administratora bezpieczeństwa informacji i zgłosił go Generalnemu Inspektorowi do rejestracji, z zastrzeżeniem art. 46e ust. 2".

[8] „Art. 46b. 1. Administrator danych jest obowiązany zgłosić do rejestracji Generalnemu Inspektorowi powołanie i odwołanie administratora bezpieczeństwa informacji w terminie 30 dni od dnia jego powołania lub odwołania", u.o.d.o.

obowiązku na podmioty prowadzące działalność gospodarczą, będące ADO, nie prowadziłoby to do żadnych ułatwień związanych z jej wykonywaniem — *vide* brak możliwości korzystania ze zwolnienia dotyczącego zgłaszania zbiorów w rejestrze GIODO.

Jeśli nawet przyjmować będziemy, że ADO nie będzie musiał tworzyć sprawozdań i prowadzić rejestru zbiorów, pozostanie mu jednak zmierzyć się z następującymi zagadnieniami:

— Sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych — co jeśli nawet nie zaowocuje przygotowaniem sprawozdania, obejmować będzie wszystkie wcześniejsze etapy działań wykonywane z założenia przez ABI. Nie wchodząc głęboko w kwestie regulowane rozporządzeniami wykonawczymi, można przyjąć, również w kontekście tego, co obejmuje sprawozdanie, że ADO miałby obowiązek prowadzenia kontroli (sprawdzeń) planowych i doraźnych, gromadzenia i tworzenia materiałów dokumentujących dokonywane czynności w ramach tzw. sprawdzenia, przy czym sprawdzenia planowe powinny uwzględniać założenie, że zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych powinny być objęte sprawdzeniem co najmniej raz na pięć lat. Z kolei sprawdzenie doraźne powinno być przeprowadzane niezwłocznie po powzięciu wiadomości przez ADO o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia.

— Nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2 u.o.d.o. (m.in. polityki bezpieczeństwa, instrukcji zarządzania systemem informatycznym, upoważnieniami i ewidencją osób upoważnionych, umowami powierzającymi przetwarzanie danych osobowych itd.) oraz przestrzegania zasad w niej określonych; w ramach owego nadzoru ADO winien dokonywać weryfikacji: opracowania i kompletności dokumentacji przetwarzania danych; zgodności dokumentacji przetwarzania danych z obowiązującymi przepisami prawa; stanu faktycznego w zakresie przetwarzania danych osobowych; zgodności ze stanem faktycznym przewidzianych w dokumentacji przetwarzania danych środków technicznych i organizacyjnych służących przeciwdziałaniu zagrożeniom dla ochrony danych osobowych; przestrzegania zasad i obowiązków określonych w dokumentacji przetwarzania danych. W przypadku wykrycia podczas weryfikacji nieprawidłowości, np.: nieopracowania, nieaktualności lub braków w dokumentacji, ADO zobligowany będzie do podjęcia działań niezbędnych w celu doprowadzenia jej do wymaganego stanu, w szczególności powinien wdrożyć projekty dokumentów usuwające stan niezgodności. Ponadto ABI, a zatem i ADO, poucza lub instruuje osobę nieprzestrzegającą zasad określonych w dokumentacji przetwarzania danych o prawidłowym sposobie ich realizacji, przy czym pouczenia lub instrukcje mają być zawarte w odrębnym dokumencie skierowanym do osoby nieprzestrzegającej zasad określonych w dokumentacji przetwarzania danych.

— Zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych; można przyjąć, iż chodzi o stworzenie systemu szkoleń w zakresie ochrony danych, stanowiącego element procesu nadawania upoważnień (w przypadku gdy ADO, z uwagi na brak pracowników itp., nie nadaje upoważnień, nie będzie musiał podejmować żadnych czynności).

Nawet ten mocno skrócony, nieoddający pełnej gamy działań szczegółowych[9], wykaz dodatkowych obowiązków, jakie spoczywać będą na ADO w przypadku niepowołania ABI (pomijając już kwestie zwiększonego zakresu odpowiedzialności), pozwala na uznanie, iż należy dokładnie rozważyć, czy ADO jest w stanie realizować przejmowane zadania. Można przyjąć, że sytuacja taka nader często generować będzie trudności, których przezwyciężenie będzie mogło nastąpić jedynie w wyniku powołania osoby przygotowanej merytorycznie do pełnienia obowiązków ABI i jej dobrej współpracy z ADO.

4. ZWIĄZANIE ADO OBOWIĄZKIEM POWOŁYWANIA ABI — KONTEKST HISTORYCZNY

Zarysowanie problematyki zadań nadzorczych, jakie wiązałyby się z niepowoływaniem ABI, prowadzi ponownie do głównego zagadnienia, jakim jest problem obligatoryjności lub jej braku, związania zasadą powoływania tego organu wewnętrznego w związku z obowiązkiem bezpiecznego przetwarzania danych osobowych. Przechodząc do próby omówienia tego problemu, nie można pominąć oficjalnego stanowiska wyrażanego w imieniu ministra administracji i cyfryzacji, ujawnionego choćby w OSR dołączonej do projektu rozporządzenia „w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji”[10],

[9] Podane obowiązki wynikają z analizy u.o.d.o. i aktów wykonawczych. Szczegółowy zakres zadań spoczywających na barkach ABI w zakresie czynności zapewniających przestrzeganie przepisów u.o.d.o. wynikać będzie z rozporządzenia Ministra Administracji i Cyfryzacji w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji, którego projekt z dnia 27.04.2015 r. dostępny był w chwili zakończenia prac nad opracowaniem pod adresem: http://legislacja.rcl.gov.pl/docs//519/268582/268620/dokument161739.pdf.

[10] Całość dostępna pod adresem: http://legislacja.rcl.gov.pl/projekt/268582/katalog/268610#268610 — tu warto wskazać, że w pkt 4 oceny skutków regulacji zauważa się: „powołanie administratora bezpieczeństwa informacji jest dobrowolne — nie można na tym etapie określić precyzyjnie, ile jednostek się na to zdecyduje. Jako górną granicę szacunków przyjęliśmy 3000 podmiotów potencjalnie zainteresowanych powołaniem ABI”, podobną wymowę ma pkt 6: „powołanie ABI jest dobrowolne. Instytucje sektora publicznego, które się na to zdecydują, potencjalnie mogą liczyć się z większą ilością obowiązków związanych ze sprawdzaniem zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Obowiązki te obejmują wykonywanie (co najmniej raz w roku) okre-

w której stanowczo podkreśla się nie tylko dobrowolność powoływania ABI, ale również bardzo minimalistycznie szacuje się liczbę podmiotów, które zdecydują się na taki krok, na ok. 3000. Biorąc pod uwagę, że stwierdzenie to nie odnosi się do skutków prawnych wywoływanych samym rozporządzeniem, lecz wypływa z oceny zmian, jakie wprowadzono do u.o.d.o., analizę należy rozpocząć od wskazania poprzedniego stanu prawnego i choćby zarysu jego doktrynalno-jurydycznej interpretacji.

Uchylony przez ostatnią nowelizację art. 36 ust. 3 u.o.d.o. stanowił, że „Administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1, chyba że sam wykonuje te czynności". Zarówno dwa wcześniejsze ustępy art. 36, jak i art. 7 pkt 4 u.o.d.o., definiujący pojęcie administratora danych, obowiązują w dalszym ciągu, warto więc przyglądając się prezentowanemu niżej stanowisku, brać pod uwagę jego przynajmniej częściową aktualność.

Na tle istniejącego przed 1 stycznia 2015 stanu prawnego zarysowuje się wyraźna tendencja do traktowania normy dotyczącej powoływania ABI jako regulacji o dualnym charakterze, a dobrowolność lub obligatoryjność tego procesu uzależniana była od rzeczywistej formy organizacyjnej, w jakiej funkcjonował ABI. Jednoosobowe wypełnianie obowiązków ADO wiązano generalnie ze swobodą podejmowania decyzji o powołaniu ABI, podmioty złożone działały zaś w warunkach obligatoryjności podjęcia decyzji o powołaniu osoby fizycznej do pełnienia tej funkcji.

Autorzy najobszerniejszego komentarza[11] nie zajęli w tej kwestii jednoznacznego stanowiska. Podnosili wprawdzie, że „obowiązek, jaki w wyniku nowelizacji z 2004 r. zawarty został w komentowanym przepisie, dotyczy wyznaczenia osoby, której zadaniem jest nadzorowanie przestrzegania zasad ochrony danych. Osoba taka — [...] ABI — powinna być przez administratora wyznaczona, chyba że administrator sam wykonuje czynności nadzorcze (np. gdy osoba fizyczna samodzielnie przetwarza dane, będąc ich administratorem)". Podając jednak ogólną regułę pozwalającą na ominięcie wskazywanego obowiązku, nie poddali jej szerszej analizie. Wskazany przykład zastosowania takiego wyjątku nie budził kontrowersji, co wobec braku wyraźnie określonej grupy administratorów objętych obowiązkiem powołania ABI nie pozwalało określić rzeczywistego znaczenia komentowanej normy.

---

sowego sprawdzenia zgodności z przetwarzania danych osobowych z przepisami o ochronie danych osobowych przez ABI oraz dokonanie dodatkowego sprawdzenia na wniosek GIODO", również pkt 7 stanowi *de facto* powtórzenie pkt 6 z ciekawym wątkiem pobocznym „jednocześnie rozszerzenie katalogu obowiązków ABI, a także wprowadzenie szerokiego zakresu niezależności ABI od swoich przełożonych może skutkować rozwojem firm wyspecjalizowanych w świadczeniu usług ABI".

[11] Zob. szerzej J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz* (wyd. 4), Kraków 2007, s. 600–613.

Zdecydowanie jednoznacznie wypowiedział się w tej kwestii A. Drozd, który zauważając występowanie wątpliwości, „czy administrator danych będący jednostką organizacyjną może wykonywać obowiązki ABI", odpowiada: mimo że u.o.d.o. „nie stanowi o tym wyraźnie, to należy przyjąć, że ABI powinien być osobą fizyczną, a w konsekwencji administrator danych może przejąć jego obowiązki tylko wtedy, gdy jest osobą fizyczną"[12]. Autor ten zakłada więc brak jakichkolwiek elementów pośrednich pomiędzy stanem: ADO będący osobą fizyczną (istnieje możliwość przejęcia zadań ABI) a ADO niebędący osobą fizyczną (wykluczenie przejmowania zadań ABI do samodzielnej realizacji).

Podobny pogląd prezentują również P. Barta i P. Litwiński, wskazując, że „choć brak stosownego uzasadnienia zmiany komentowanego przepisu, które umożliwia administratorowi danych samodzielne wykonywanie funkcji ABI (ustawa z 22 stycznia 2004 r. o zmianie ustawy o ochronie danych osobowych), zdaniem autorów przepis ten ma umożliwić wykonywanie obowiązków administratora bezpieczeństwa informacji samodzielnie przez administratorów danych będących osobami fizycznymi prowadzącymi działalność gospodarczą. Jednocześnie wydaje się, że ze względu na konstrukcję osób prawnych administrator danych osobowych, będący osobą prawną, ze swej istoty nie może korzystać z komentowanej instytucji i samodzielnie wykonywać obowiązków administratora bezpieczeństwa informacji. Podkreślić należy, że administrator danych osobowych, który nie wyznaczył administratora bezpieczeństwa informacji, nie może twierdzić, iż z mocy prawa wykonuje w takim przypadku obowiązki ABI samodzielnie. W tym zakresie komentowany przepis nie wprowadza żadnych domniemań, tak więc również samodzielne wykonywanie obowiązków administratora bezpieczeństwa informacji powinno zostać odnotowane w treści dokumentacji danych osobowych"[13].

Zarówno GIODO, jak i sady administracyjne skłaniały się ku poglądom prezentowanym przez A. Drozda oraz P. Bartę i P. Litwińskiego. W ostatnim głośnym wyroku NSA z 21 lutego 2014 r., związanym z obowiązkiem powołania ABI przez Google, wprost powoływano się na przytoczone wyżej poglądy, zauważając jednocześnie, że „zakres podmiotowy administratora danych osobowych obejmujący osoby prawne, jednostki organizacyjne niemające osobowości prawnej wyznacza dopuszczalność odstąpienia od obowiązku wyznaczenia administratora bezpieczeństwa informacji. Wymaga to odkodowania z regulacji prawnej obowiązującego systemu prawa, zgodnie z regułą wykładni niedopuszczalności wykładni przepisu prawa w oderwaniu od kontekstu regulacji przyjętej w ustawie, regulacji przyjętej w systemie prawa. Z pełnej regulacji przyjętej w kodeksie cywilnym wynika, że obowiązującą regułą jest, że osoby prawne i jednostki organizacyjne

[12] A. Drozd, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warszawa 2005, s. 252.

[13] P. Bata, P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2013, s. 356.

niemające osobowości prawnej działają przez swoje organy, jeżeli innych reguł nie przyjmuje ustawa szczególna. Taką regulacją szczególną jest art. 36 ust. 3 ustawy o ochronie danych osobowych, z której wynika, że jeżeli administratorem danych jest jednostka organizacyjna mająca osobowość prawną, jak i niemająca osobowości prawnej, obowiązana jest wyznaczyć administratora bezpieczeństwa informacji”[14].

Reasumując powyższe stanowiska, można przyjąć, iż przed 1 stycznia 2015 r. obowiązywała zasada wyrażona w uzasadnieniu do wcześniejszego wyroku w sprawie Google: „art. 36 ust. 3 ustawy o ochronie danych osobowych nakłada na administratora danych obowiązek wyznaczenia (»wyznacza«) administratora bezpieczeństwa informacji w każdym przypadku, jeśli zadań administratora bezpieczeństwa informacji administrator danych nie wykonuje sam lub nie może wykonywać ich samodzielnie [...], nie powinno budzić wątpliwości, że w każdej sytuacji, w której struktura organizacyjna administratora danych jest wieloosobowa, powinien on w ramach tej struktury wyznaczyć osobę fizyczną odpowiedzialną za wykonywanie czynności nadzorczych, powierzając jej obowiązki administratora bezpieczeństwa informacji, i to niezależnie od tego, czy administrator danych jest organem, jednostką organizacyjną, podmiotem czy osobą prawną”[15].

5. PODSTAWA NORMATYWNA POWOŁYWANIA ABI PO NOWELIZACJI

Jak już kilkakrotnie wspomniano, nowelizacja u.o.d.o. doprowadziła jednak do uchylenia omawianej normy. Nie zmieniono przy tym ani definicji administratora danych, ani zakresu obowiązków ADO wynikającego z art. 36 ust. 1 i 2 u.o.d.o., obowiązuje również w pełnym zakresie zasada wyrażona w jej art. 26

[14] Wyrok NSA z 21.02.2014 r. I OSK 2445/12.

[15] Wyrok WSA w Warszawie z 5.07.2012 r., II SA/Wa 630/12. Podnoszono w nim jeszcze jeden istotny argument dotyczący tak rozumianego zakresu obowiązku powołania ABI: „Wychodząc z reguł wykładni celowościowej, warto zwrócić uwagę, że ustawodawca, tworząc podstawy bezpieczeństwa w procesie przetwarzania danych osobowych (art. 36 – art. 39 ww. ustawy), swą uwagę koncentruje na odpowiedzialności i możliwości jej egzekwowania, zwłaszcza w wymiarze prawnokarnym (rozdział 8 ustawy), co w przypadku podmiotów o wieloosobowej strukturze organizacyjnej jest szczególnie ważne [...]. To z tego względu prawodawca zdecydował o takim właśnie brzmieniu art. 36 ust. 3 ustawy, wprowadzając obowiązek, by osobą odpowiedzialną za nadzór i bezpieczeństwo przetwarzania danych osobowych w podmiotach o wieloosobowej strukturze organizacyjnej była konkretnie wskazana osoba fizyczna. Jedynie bowiem w przypadku administratorów danych będących osobami fizycznymi, którzy samodzielnie (osobiście) administrują proces przetwarzania danych, ustawa nie nakłada obowiązku wyznaczenia administratora bezpieczeństwa informacji, gdyż tylko w takiej sytuacji administrator danych jednocześnie dzierży uprawnienia i obowiązki administratora bezpieczeństwa informacji, co pozwala na ustalenie jego odpowiedzialności i w konsekwencji na zastosowanie sankcji karnych, gdyby — prowadząc swą działalność — naruszył przepisy o ochronie danych osobowych”.

nakazująca ADO zachowanie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą.

Ustawodawca nie pozostawił jednak kwestii powoływania ABI przypadkowi — włączył bowiem do tekstu u.o.d.o. art. 36b stanowiący, że „W przypadku niepowołania administratora bezpieczeństwa informacji zadania określone w art. 36a ust. 2 pkt 1, z wyłączeniem obowiązku sporządzania sprawozdania, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, wykonuje administrator danych", która wespół z art. 36a ust. 1. „Administrator danych może powołać administratora bezpieczeństwa informacji". Te dwa przepisy tworzą nową podstawę normatywną, której analiza będzie próbą udzielenia odpowiedzi na pytanie: czy istotnie mamy do czynienia z w pełni swobodną decyzją ADO o powołaniu ABI, czy też będzie ona miała, podobnie jak we wcześniejszym stanie prawnym, dualny charakter.

Na początku warto odnieść się do faktu, iż ustawodawca zdecydował się jednak na uchylenie art. 36 ust. 3 u.o.d.o., co samo w sobie stanowi przesłankę do przyjęcia tezy, iż zamierzał na nowo uregulować to zagadnienie (choć niekoniecznie dążyć musiał do odmiennego ukształtowania reguł rządzących powoływaniem ABI). Biorąc pod uwagę szeroki zakres zmiany przepisów dotyczących pozycji tego podmiotu można stać na stanowisku, iż usunięcie jednego ustępu z art. 36 i wprowadzenie do ustawy rozbudowanych regulacji art. 36a, 36b i 36c miało raczej, czy może przede wszystkim, charakter porządkujący — nie chciano pozostawiać jednego (ale jakże istotnego) elementu określającego status ABI poza artykułami bezpośrednio poświęconymi tej właśnie funkcji. Artykuł 36a u.o.d.o. kilkakrotnie nawiązuje do relacji pomiędzy ABI a ADO (poza ust. 1 ma to miejsce w ust. 4, 6, 7 i 8), zatem zupełnie naturalny wydaje się fakt, iż otwiera go właśnie przepis wyznaczający podstawową zasadę umożliwiającą zadzierzgnięcie tej relacji.

Jako uzupełnienie obrazu tych powiązań warto też wskazać wymieniony ust. 7[16], w którym wyraźnie ustawodawca rozgranicza dwie modelowe grupy ADO powołujące ABI.

W pierwszej pojawiają się jednostki organizacyjne, w przypadku których ABI ma podlegać bezpośrednio kierownikowi takiej jednostki.

W drugiej wyraźnie nawiązuje się do istniejącej możliwości powoływania ABI również wtedy, gdy ADO jest osobą fizyczną (np. przedsiębiorcą), w tym przypadku podległość ABI wiązać się ma bezpośrednio z tą właśnie osobą fizyczną.

Na marginesie tego podziału zauważyć należy kolejny problem stworzony przez samego ustawodawcę, który podobnie jak w wielu innych sytuacjach dotyczących ochrony danych zachowuje się nie do końca zrozumiale. Biorąc pod uwagę definicję administratora danych[17] pojawiającą się w samej u.o.d.o., można

[16] „Art. 36a ust. 7. Administrator bezpieczeństwa informacji podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych".

[17] Ustawodawca, mówiąc o administratorze danych w słowniku zawartym w art. 7 u.o.d.o, wskazał, że „rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osoby, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych".

odnieść wrażenie, że skoro jednostka organizacyjna jest (obok: organu, podmiotu lub osoby) jedną z form, w jakich działa ADO, to tylko w takich właśnie „jednostkach organizacyjnych" ABI będzie musiał podlegać bezpośrednio kierownikowi tej jednostki. Wykładnia językowa nakazywałaby bowiem sztywne podejście do zdefiniowanego pojęcia, *de facto* pozwalając na odstąpienie od zastosowania tej reguły np. w przypadku osób prawnych będących ADO, mieszczących się przecież wprost w pojęciu osoby.

Mając na uwadze, że: organy, osoby prawne i inne podmioty, które doktryna utożsamia zazwyczaj z tzw. instytucjonalnymi administratorami danych, nie są raczej pozbawione możliwości powołania ABI, warto zapytać, komu ma on podlegać w takiej sytuacji. Racjonalnym podejściem byłoby trzymanie się reguły jego bezpośredniej podległości wobec „władzy kierującej" tymi ADO, czyli np. samego organu (w tym oczywiście organu wieloosobowego, a nie jego przewodniczącego), całego zarządu spółki (a nie wyłącznie prezesa w przypadku zarządów kolegialnych), dyrektora przedsiębiorstwa czy innego „ciała kierującego" podmiotem, tyle tylko, że wykładnia taka odwołuje się do analogii oraz przesłanek celowościowych i funkcjonalnych, wynikających choćby z nakazu zapewnienia przez ADO organizacyjnej odrębności ABI, niezbędnej mu do należytego wykonywania ustawowych obowiązków (art. 36a ust. 8 u.o.d.o.), co zawsze sprawia większą trudność niż oparcie się na prostej regule językowej.

Jak przyjmowano przed wejściem w życie ostatniej nowelizacji, pomimo braku słowa „może", również poprzednia formuła językowa dawała ADO pewną swobodę decyzyjną, jeśli tylko ze swej natury był podmiotem, który jest w stanie sam wykonywać czynności nadzoru. Należy tu zauważyć, że czynności związane z nadzorem nad przestrzeganiem zasad ochrony danych nie były uprzednio dookreślone w u.o.d.o. zatem normatywne wyznaczenie zakresu obowiązków ABI, które miał wykonywać, było domeną samego ADO (wynikać miało np. z polityki bezpieczeństwa) — potencjalnie mógł więc on nie podejmować prawie żadnych działań sprawdzających.

Jeśli więc samo wskazanie możliwości powołania, w odróżnieniu od wcześniejszego „wyznaczenia" administratora, nie stanowi jednoznacznej podstawy do zasadniczej zmiany poglądów, to różnica powinna kryć się w ujęciu przepisu dozwalającego samodzielne wykonywania zadań, przypisywanych ustawowo ABI przez ADO.

Porównanie warstwy językowej obu przepisów odnoszących się do tej kwestii wskazuje, że nowe ujęcie pomija istniejący wcześniej wymóg określany przez doktrynę jako zdolność ADO do tego, by „samodzielnie wykonywać" obowiązki ABI. W art. 36b u.o.d.o. nie pojawia się bowiem fraza: „chyba że sam wykonuje te czynności", a jej miejsce zajmuje sformułowanie, którego sens normatywny oddaje formuła: określone ustawowo zadania ABI „wykonuje administrator danych".

Jak widać, obie te reguły jednoznacznie nakazują wykonywanie zadań ABI nie dowolnemu podmiotowi, ale właśnie ADO. Normy nakładające nań pewne

obowiązki, występujące bardzo często w u.o.d.o., są jednak powszechnie interpretowane jako umożliwiające posiłkowanie się przy ich realizacji właściwie umocowanymi pełnomocnikami, przy czym forma udzielenia pełnomocnictwa jest wysoce elastyczna. Pojawia się zatem problem wynikający z pominięcie słowa „sam", występującego wcześniej, co daje asumpt do twierdzeń[18], których autorzy zdają się wykazywać diametralną zmianę podejścia do kwestii swobody powołania ABI. Wypowiedzi te są jednak równocześnie na tyle lakoniczne, że nie znamy stanowiska ich autorów w odniesieniu do kluczowego w tym wypadku problemu, czyli powierzenia czynności przypisanych ustawowo ABI komukolwiek innemu niż sam ADO.

6. SWOBODA ADO W ZAKRESIE POWOŁANIA ABI W KONTEKŚCIE PRZEJĘCIA JEGO OBOWIĄZKÓW

Już na wstępie należy zauważyć, że nie wszyscy przedstawiciele doktryny wyprowadzali konieczność osobistego przejęcia obowiązków ABI z przesłanki opartej bezpośrednio na frazie „sam wykonuje te czynności". A. Drozd, zauważając możliwość niepowoływania ABI, wskazywał bowiem na fakt, że powinien być on osobą fizyczną, z czego wyprowadzał wniosek, iż administrator danych może być zdolny do przejęcia jego obowiązku tylko wtedy, gdy również jest osobą fizyczną. W tym kontekście sytuacja po nowelizacji stała się wręcz bardziej oczywista — wprowadzenie wymogów dotyczących osoby mającej zostać ABI (art. 36a ust. 5 u.o.d.o. i inne dotyczące choćby rejestracji) nie daje najmniejszych możliwości spekulowania o innym podejściu do tego zagadnienia niż uznanie osobowego charakteru tej funkcji, w którym sam ABI znany ma być z imienia i nazwiska. Można by zatem przyjąć, że ten kierunek interpretacji postanowień u.o.d.o. prowadzić będzie do wniosków identycznych ze wskazanymi w poprzednim stanie prawnym.

Również P. Bata i P. Litwiński nie odwoływali się w swych twierdzeniach bezpośrednio do słowa „sam", wskazując jedynie, że art. 36 ust. 3 u.o.d.o. „ma umożliwić wykonywanie obowiązków administratora bezpieczeństwa informacji samodzielnie przez administratorów danych będących osobami fizycznymi prowadzącymi działalność gospodarczą", odnosząc się zaś do ADO będącego osobą prawną, uznawali, że ze swej istoty nie może on korzystać z możliwości niepowoływania ABI[19]. A zatem i w tym przypadku wnioski wyprowadzone w poprzednim stanie prawnym zdają się pozostawać aktualne.

[18] Przykłady takich komunikatów stanowią choćby, wskazane w przypisach 2 i 10, cytaty — umieszczone pierwotnie na stronach GIODO i RCL.

[19] Por. przypis 12.

Wracając jeszcze na chwilę do samego językowego ujęcia art. 36 ust. 3 u.o.d.o., nie sposób oprzeć się wrażeniu, że z kontekstu użycia w nim zaimka „sam”[20] można oczywiście wyprowadzić wniosek, że wskazana osoba (tu domyślnie ADO) wykonuje jakąś czynność samodzielnie lub z własnej woli, ale równie dobrze można przyjmować, że ustawodawca nie chciał[21] w jednym przepisie powtarzać dwa razy tej samej nazwy, posłużył się więc nim jako swego rodzaju kontekstowo zrozumiałym synonimem nazwy „administrator danych”. W tym przypadku zaimek ten odnosiłby się do osoby wykonującej pewną czynność, wskazując, że ważne jest to, iż właśnie ta osoba ją wykonuje. Biorąc pod uwagę osobowy charakter analizowanego zaimka, ADO niebędący osobą fizyczną być może rzeczywiście „ze swej istoty” nie powinien być objęty możliwościami, jakie stwarzał ów wyjątek. Pomijając jednak ten fakt i przyjmując, że zaimek „sam” odnosił się do ADO działającego w każdej formie organizacyjno-prawnej, należałoby uznać, że wcześniejsza formuła językowa była *de facto* tożsama z użytą obecnie na gruncie art. 36b u.o.d.o., a zatem niezbędne staje się udzielenie odpowiedzi na drugie pytanie.

W poprzednim stanie prawnym powierzenie zadań ABI innym niż sam ADO podmiotom uznawane było dość powszechnie za niemożliwe. Poglądy doktryny i judykatury nawiązujące do faktu, że osoby prawne i jednostki organizacyjne niemające osobowości prawnej działają przez swoje organy, jeżeli innych reguł nie przyjmuje ustawa szczególna, są przecież aktualne. Należy zatem wskazać, czy art. 36a–36c u.o.d.o. stanowią obecnie podstawę do uznania ich za regulację szczególną, z której wynika, że jeżeli ADO jest osoba prawna, organ, jednostki organizacyjne czy podmioty posiadające osobowość prawną, jak i niemające tej osobowości, obowiązana jest powołać ABI.

Biorąc pod uwagę obowiązującą zasadę szczególnej staranności, jaką kierować się ma ADO, chroniąc interesy osób, których dane przetwarza (art. 26 u.o.d.o.), należałoby uznać za co najmniej wątpliwą praktykę, w której powszechnie nadzorem na przetwarzaniem danych, m.in. w aspekcie jego legalizmu, celowości i adekwatności, zajmować by się miał ktoś inny niż przygotowany do tego merytorycznie, dysponujący odpowiednimi środkami i organizacyjnie wyodrębniony ABI. Przyjmując za punkt wyjścia art. 36a ust. 1 i dookreślający skutki niepowołania ABI art. 36b u.o.d.o., należy podkreślić, że takie przypadki powinny być ściśle limitowane i znajdować bezpośrednie potwierdzenie w ustawie, a ta

[20] W sprawie różnych znaczeń zaimka sam zob.: np. http://sjp.pwn.pl/sjp/sam-I;2518978.html.

[21] Mogło się tak stać być może ze źle pojętych względów stylistycznych albo dążenia do osiągnięcia możliwie krótkiej formy ujęcia treści w przepisie — w przypadku pełnego powtórzenia przepis mógłby przybrać formę: Administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1. W przypadku niepowołania administratora bezpieczeństwa informacji zadania określone w ust. 1 wykonuje administrator danych.

wprost ogranicza się do lakonicznego stwierdzenia, że przejęte obowiązki „wykonuje administrator danych".

Uznając za ciągle aktualne uwagi doktryny i judykatury poczynione na tle kwalifikowania ADO jako zdolnego do przejęcia obowiązków ABI, dodać należy, że w obecnym stanie prawnym, to nie kto inny jak sam ustawodawca określił obowiązki ABI, które nie mogą być zniesione czy nawet ograniczone z woli ADO, a zatem nie powinno się bezrefleksyjnie przyjmować, że może on całkowicie dowolnie rozdzielać te czynności pomiędzy inne osoby niespełniające warunków, jakie wymagane są od osoby pełniącej funkcje ABI. Miałoby to miejsce w sytuacji działań podjętych przez tzw. instytucjonalnego administratora danych, który arbitralnie uznając brak potrzeby powołania ABI i nie dysponując możliwością samodzielnego, osobistego przejęcia jego obowiązków, scedowałby te zadania na różne osoby biorące udział w procesach przetwarzania danych. Oceniając tego typu zachowania, należałoby się zastanowić nad tym, czy nie stanowią one próby obejścia u.o.d.o. w szczególności przez tych ADO, którzy przed początkiem 2015 roku stworzyli dokumentację przetwarzania danych opisującą m.in. zadania ABI i dokonali powołania jakiejś osoby do pełnienia tej funkcji.

Jeśli jednak ADO jest osobą fizyczną (np. przedsiębiorcą), to zarówno w poprzednim, jak i obecnym stanie prawnym ma prawo do przejęcia obowiązków ABI w dowolnym momencie, o ile realizował je będzie osobiście.

Dodatkowym argumentem negującym całkowitą swobodę powołania ABI jest istnienie art. 35 ustawy o ułatwieniu wykonywania działalności gospodarczej[22], który ma charakter przepisu przejściowego. Nieco upraszczając, można stwierdzić, że w wyniku jego stosowania z dniem 30 czerwca 2015 r. wszyscy ABI powołani przed 1 stycznia 2015 r. z mocy prawa przestaną pełnić swoją funkcję. Gdyby ustawodawca założył pełną swobodę w kreacji nowego ABI, to ustanawiając dość wysokie standardy w zakresie wymogów osobowo-organizacyjnych, jakim ma sprostać ADO w nowej rzeczywistości prawnej, musiałby się liczyć z masowym niepowoływaniem ABI w nowym standardzie i swobodnym przekazywaniem jego uprawnień (obecnie ustawowo określonych, a zapewne w najbliższej przyszłości również dookreślonych wszystkimi wymaganymi rozporządzeniami) w ręce osób niespełniających zakładanych kryteriów i merytorycznie nieprzygotowanych do wykonywania nałożonych nań obowiązków. Można oczywiście przyjmować, że za działania takie pełną odpowiedzialność ponosiłby ADO, co powinno go odwieść od nieprzemyślanych decyzji, niemniej nie sposób zaprzeczyć, że mogłoby

[22] „Art. 35. Administrator bezpieczeństwa informacji wyznaczony na podstawie art. 36 ust. 3 ustawy zmienianej w art. 9, w brzmieniu dotychczasowym, pełni funkcję administratora bezpieczeństwa informacji w rozumieniu art. 36a ust. 1 ustawy zmienianej w art. 9, w brzmieniu nadanym niniejszą ustawą, do czasu zgłoszenia go do rejestru, o którym mowa w art. 46c ustawy zmienianej w art. 9, w brzmieniu nadanym niniejszą ustawą, nie dłużej jednak niż do dnia 30 czerwca 2015 r." Ustawy z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej, Dz.U. z 2014 r., poz. 1662.

to jednocześnie doprowadzić do drastycznego obniżenia przestrzegania standardów ochrony danych osobowych. Ich realizacja nawet obecnie nie jest oceniana jako wzorcowa, zatem biorąc pod uwagę ewentualne konsekwencje dla gwarantowanego konstytucyjnie w art. 51 standardu ochrony praw osób, których dane podlegają przetwarzaniu, należy przyjąć, że ustawodawca nie dążył do uzależnienia uruchamiania mechanizmu powoływania ABI od całkowicie swobodnej, częstokroć uwzględniającej trudności finansowo-organizacyjne decyzji ADO, którego znajomość zasad i wymogów formalnych ochrony danych osobowych bywa wątpliwa.

7. ZAKOŃCZENIE

Interpretując art. 36a u.o.d.o. w oderwaniu od pozostałych przepisów, łatwo dojąć do wniosku o pełnej swobodzie powoływania ABI. Niemniej zestawiając go z art. 36b u.o.d.o., który stanowi o normatywnych konsekwencjach niepowołania ABI i jest immanentnym elementem normy umożliwiającej swobodną ocenę potrzeby jego powołania, jasno widać, iż zakładane początkowo uprawnienie warunkowane jest możliwością rzeczywistego, realizującego standardy szczególnej staranności, przejęcia części obowiązków złożonych na barki ABI przez ADO. Należy zatem przyjąć, że z możliwości niepowoływania wyspecjalizowanego, wewnętrznego organu zajmującego się zapewnianiem przestrzegania przepisów o ochronie danych osobowych korzystać może (choć oczywiście nie musi) tylko taki ADO, który jest jednocześnie przygotowany do realizacji wskazanych ustawowo zadań A B I. Biorąc pod uwagę różnorodność form organizacyjnych, w jakich działają ADO, nie w każdym wypadku takie przejęcie obowiązków wydaje się uzasadnione.

Przedstawione wyżej wątpliwości co do rzeczywistego zakresu swobody wiążącej się z powoływaniem ABI bez wątpienia ulegać będą stopniowemu wyjaśnieniu w procesie stosowania prawa, gdyż zarówno GIODO, jak i przedstawiciele doktryny oraz judykatura nie będą mogli przechodzić obojętnie wobec pojawiających się problemów interpretacyjnych.

APPOINTMENT OF THE ADMINISTRATOR OF PERSONAL DATA SECURITY AS A PRINCIPLE OF SECURE DATA PROCESSING ON THE BASIS OF THE LAW ON PERSONAL DATA PROTECTION

Summary

On January 1, 2015 amendments changing the legal status of the Administrator of Personal Data Security (Pol. Administrator Bezpieczeństwa Informacji, hereinafter "ABI") were introduced into the Polish Law on Personal Data Protection. Description of the legal consequences of one of the amendments is the subject of the analysis included in this text.

The main theme of the analysis is an attempt to answer the question whether appointing of this person is up to the free decision of a personal data protection administrator or if the decision is subject to certain conditions. Addressing the issue begins with a concise description of a position and role dedicated to ABI in the processing of personal data. Next, there is an indication of the scope of responsibilities entrusted to him. On this background are projected, from the historic perspective, the views of the legal doctrine and judicature on appointing ABI. The consequent linguistic and functional analysis of normative grounds for ABI appointment after the amendment allowed to indicate the scope of discretion in his appointment.