ACTA UNIVERSITATIS WRATISLAVIENSIS
No 3725
PRZEGLĄD PRAWA I ADMINISTRACJI CV
WROCŁAW 2016

KRZYSZTOF WYGODA
Uniwersytet Wrocławski

DOI: 10.19195/0137-1134.105.15

ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI A INSPEKTOR OCHRONY DANYCH NA TLE REGULACJI KRAJOWYCH I UNIJNYCH — WYBRANE ZAGADNIENIA

1. ZAG[redacted]NE

Przepisy zmieniające m.in[redacted]ku obowiązywania ustawy o ochronie danych osobowych ([redacted]Administratora Bezpieczeństwa Informacji (dalej: ABI) w[redacted]a 2015 r. Wprowadziły one do polskiego systemu ochrony [redacted]we rozwiązania w zakresie określenia warunków, jakie ma[redacted]ABI, procedur jego powoływania i rejestracji, uszczegółow[redacted]rzysługujących mu kompetencji i środków działania oraz określenia jego relacji z Administratorem Danych Osobowych (dalej: ADO).

Od dnia 6 maja 2018 mają obowiązywać normy implementujące dyrektywę 2016/680[1], a kilkanaście dni później, 25 maja, będzie znajdować zastosowanie ogólne rozporządzenie o ochronie danych (dalej: r.o.o.d.)[2]. Oba te akty stanowią efekt długo przygotowywanej reformy unijnego prawa ochrony danych osobowych, która ma stanowić remedium na zaistniałą podczas wdrożenia dyrekty-

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, Dz. Urz. UE z 4 maja 2016, L 119/89.

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. Urz. UE z 4 maja 2016, L 119/1.

wy 95/46/WE fragmentaryzację, niepewność prawną oraz upowszechnienie się poglądu, że ochrona osób fizycznych jest znacznie zagrożona, w szczególności w związku z działaniami w internecie. Konieczność możliwie pełnego ujednolicenia reguł ochrony danych była wynikiem konstatacji, iż

różnice w stopniu ochrony praw i wolności osób fizycznych w państwach członkowskich — w szczególności prawa do ochrony danych osobowych — w związku z przetwarzaniem danych osobowych mogą utrudniać swobodny przepływ danych osobowych w Unii. Mogą zatem stanowić przeszkodę w prowadzeniu działalności gospodarczej na szczeblu Unii, zakłócać konkurencję oraz utrudniać organom wykonywanie obowiązków nałożonych na nie prawem Unii[3].

Należy jednak pamiętać, że wprowadzenie nowych rozwiązań unijnych nie spowoduje całkowitej rezygnacji z nom krajowych — choć obecne przepisy z pewnością będą podlegały co najmniej nowelizacji. Dzieje się tak za sprawą wyłączenia z r.o.o.d. kwestii, którym poświęcono nową dyrektywę 2016/680, oraz metody harmonizacji fakultatywnej przyjętej w tym akcie, dającej w kilku przypadkach[4] możliwość określenia rozwiązań krajowych. Na uwadze należy mieć również ograniczony zasięg oddziaływania prawa wtórnego, które nie może wykraczać poza kompetencje powierzone traktatami. Zważywszy na gwarancje wynikające z art. 51 Konstytucji RP, konieczne będzie uregulowanie zagadnień ochrony danych choćby na potrzeby działań w zakresie bezpieczeństwa narodowego, w tym czynności agencji lub jednostek zajmujących się tym bezpieczeństwem. Prowadzić to będzie do kilku różnych konfiguracji podstawy prawnej działania ABI w przypadku podmiotów wyłączonych częściowo spod działania r.o.o.d. Dojdzie wówczas do konieczności swoistego „współstosowania" przepisów tegoż rozporządzenia i ustaw implementujących dyrektywę 2016/680 (np. w sądach) czy przepisów, które pozostają w autonomicznej sferze działania państwa członkowskiego[5] (np. w ABW).

Jak się wydaje, dość istotnym narzędziem mającym zapewnić jednolite przestrzeganie zasad w skali całej UE ma być powoływanie przez administratorów inspektorów ochrony danych (dalej: IOD), którzy stanowią, na gruncie r.o.o.d. i dyrektywy 2016/680, odpowiednik znanego nam ABI. Pełna analiza różnic i podobieństw tych wspierających ADO podmiotów przekracza niestety ramy krótkiego artykułu należy więc skupić się na kilku wątkach, zarysowując jedynie pozostałe zagadnienia.

Głównym tematem analizy będzie zatem kwestia powołania ABI i IOD — czy i kiedy zależy od swobodnej decyzji ADO, a w jakich wypadkach przeradza się w obowiązek prawny. Opis obejmuje również warunki stawiane przed kandydatem na ABI / IOD, proces ich weryfikacji. Na marginesie tych rozważań pojawią

[3] Pkt 9 motywów zawartych w preambule r.o.o.d.

[4] Chodzi np. o: art. 36 ust. 5, art. 83 ust.7 czy art. 88 r.o.o.d.

[5] Kwestią otwartą jest, czy przepisy implementujące dyrektywę 2016/680 i regulujące obszary przetwarzania, wyłączone spod działania r.o.o.d., zostaną ustanowione jako jeden akt normatywny.

się też uwagi dotyczące charakteru relacji między nimi a ADO oraz konsekwencji wynikających z podjęcia decyzji o ich niepowoływaniu.

W Polsce po nowelizacji u.o.d.o. powstało dość spore zamieszanie w związku ze zniesieniem art. 36 ust. 3. Wielu administratorów danych zaczęło zastanawiać się, jak bardzo nowe rozwiązania legislacyjne zmieniają *status quo* w zakresie obowiązku powołania ABI. Czy zastępują wcześniejszy stan obligatoryjności, łagodzonej jedynie niewielkim wyjątkiem (opartym na przesłance przejęcia obowiązków), czy też wprowadzają pełną swobodę w podejmowaniu decyzji o powołaniu tego, bez wątpienia kluczowego w procesie bezpiecznego przetwarzania danych osobowych, pomiotu. Z pespektywy regulacji unijnych takie pytania zdają się nie mieć aż tak istotnego znaczenia, gdyż obie regulacje wprowadzają generalnie obligatoryjność powołania IOD dla określonych grup ADO lub podmiotów przetwarzających dane (*a contrario* wobec wszystkich niespełniających kryteriów należy przyjąć występowanie fakultatywności powoływania IOD). Jednak w przypadku r.o.o.d. kryteria wyznaczające owe grupy zobligowanych nie są do końca precyzyjne.

Kwesta samego powołania ABI–IOD, choć być może najistotniejsza, dla pełniejszego jej zrozumienia wymaga przeanalizowania także wymogów, jakie stawia im prawodawca, oraz choćby zarysowania ich statusu związanego z podległością wobec ADO lub kierownika/kierownictwa jednostki organizacyjnej[6]. Polskie przepisy dotyczące ewentualnego przejęcia jego zadań przez ADO wyraźnie wskazują na szeroki zakres obowiązków obejmujących działania nadzorcze, organizatorskie i koncepcyjne, z których podjęciem powinna wiązać się zdolność ich faktycznej realizacji, co w świetle dotychczasowego podejścia nie zawsze ma miejsce. Na uwagę zasługuje więc również ten problem, gdyż nie znając przesłanek, które potencjalnie uniemożliwiają ADO (funkcjonującym w formie osoby prawnej, podmiotu, jednostki organizacyjnej czy organu) realne sprostanie wymogom realizacji zadań ABI, trudno przesądzać o zakresie swobody, jakim dysponują w odniesieniu do samej decyzji o powołaniu ABI.

Powołanie ABI–IOD rodzi oczywiście też wiele innych problemów, których „techniczny" charakter (obejmujący kwestie formy, trybu, terminów, sposobu realizacji obowiązku oceny spełniania przez kandydata wymogów prawnych itp.) nie czyni z nich mało istotnych zagadnień niezasługujących na analizę — choć być może nie wymaga ona szczególnego pogłębienia.

Określony katalog zagadnień wymaga poruszenia wielu wątków, których pełna analiza będzie *de facto* możliwa dopiero za kilka lat (wielokrotnie prawodawca posługuje się pojęciami domagającymi się praktycznego rozwinięcia oraz ugruntowania ich znaczenia w poglądach doktryny, GIODO, judykatury, jak również

[6] Już w tym miejscu warto wskazać, że rozwiązanie przyjęte w r.o.o.d. (art. 38 pkt 5 „Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego") pozwala uniknąć wątpliwości, jakie budzi regulacja zawarta w u.o.d.o.

wciąż działającej grupy roboczej art. 29[7] czy przewidzianej w r.o.o.d. Europejskiej Rady Ochrony Danych), a obecna próba będzie tylko wstępnym przybliżeniem tematu, nie zawsze dającym jednoznaczne odpowiedzi — choć nawet samo wskazanie punktów zapalnych i istniejących wątpliwości stanowi niejednokrotnie pomoc w praktycznym rozwiązywaniu problemów.

Prawie całkowicie zostanie jednak pominięta problematyka szczegółowego zakresu obowiązków zarówno ABI (wynikających z samej u.o.d.o. i rozporządzeń wykonawczych), jak i IOD. Jest to temat zasługujący z pewnością na odrębną, głęboką analizę, a jego pobieżne omówienie nie stanowi wystarczającego uzasadnienia w rozbudowywaniu i tak dość skomplikowanego wywodu[8].

2. POZYCJA I ROLA ABI–IOD W PROCESACH PRZETWARZANIA DANYCH A OBLIGATORYJNOŚĆ JEGO POWOŁANIA

Nowelizacja u.o.d.o. pozwoliła na zmianę wcześniejszego podejścia, a wydane akty wykonawcze, dookreślając szczegóły zadań ABI, utrudniają deprecjonowanie jego pozycji. Rozbudowana podstawa prawna funkcjonowania ABI odgrywa zatem niewątpliwie rolę gwarancyjną (daleko jej jeszcze do gwarancji udzielanych sędziom, prokuratorom, adwokatom czy radcom prawnym, ale można już zauważyć zarysowującą się tendencję, i to nie tylko na gruncie prawa polskiego[9]), mającą zapewnić mu relatywnie dużą niezależność i środki pozwalające na realizację zadań ustawowych.

[7] Zapowiedzi wydawania wytycznych m.in. w sprawach: oceny ryzyka, certyfikacji czy właśnie IOD przynosi *Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR)*, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

[8] Szerzej na temat obowiązków i roli ABI i/lub IOD zob. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Warszawa 2015, s. 544–578; P. Barta, P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2016, s. 402–438; *Ochrona danych osobowych i informacji niejawnych z uwzględnieniem ogólnego rozporządzenia unijnego*, red. D. Wycióra, Warszawa 2016, s. 91–118; *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016*, red. G. Sibiga, Warszawa 2016; T. Cygan, *Podręcznik administratora bezpieczeństwa informacji*, Wrocław 2016; Ł. Kister, B. Mendyk, *Ochrona danych osobowych w przedsiębiorstwie — poradnik dla MŚP*, Warszawa 2015, s. 23–30; M. Sakowska-Baryła, *Prawo do ochrony danych osobowych*, Wrocław 2015, s. 163–192; *Aktualne Problemy Ochrony Danych Osobowych* 2015, red. G. Sibiga, dodatek „Monitor Prawniczy" 2015, nr 6; G. Sibiga, *Dokumentacja administratora bezpieczeństwa informacji. Wzory dokumentów z objaśnieniami. Omówienie zmienionych przepisów*, Wrocław 2015; K. Wygoda, *Powoływanie administratora bezpieczeństwa informacji jako zasada bezpiecznego przetwarzania danych na gruncie ustawy o ochronie danych osobowych*, „Przegląd Prawa i Administracji" C/2, Wrocław 2015, s. 337–352.

[9] Widać to choćby w omawianych regulacjach UE. Warto też wspomnieć, że słowacka ustawa o ochronie danych osobowych wymaga od IOD zdania egzaminu państwowego, którego organizatorem jest urząd ochrony danych osobowych — choć ten poziom sprawdzenia kwalifikacji jest jednak raczej wyjątkiem niż regułą w UE.

Już sama lektura art. 36a u.o.d.o. pozwala przyjąć, że staje się on organem nadzoru wewnętrznego (z dużymi kompetencjami koordynująco-nadzorczymi) w zakresie zapewniania przestrzegania przepisów o ochronie danych osobowych. Jego funkcjonowanie opierać się ma na pewnej autonomii organizacyjnej (znajdującej umocowanie w normach u.o.d.o.), a możliwość powierzania mu innych obowiązków musi respektować postulat pierwszeństwa prawidłowej realizacji zadań mieszczących się w zakresie jego kompetencji wynikających z u.o.d.o. i aktów wykonawczych (co wprost wynika z art. 36a ust. 4 u.o.d.o.). ABI ma też pewne poboczne zadania administracyjne o charakterze technicznym (prowadzenie jawnego rejestru zbiorów danych przetwarzanych przez ADO), nie stanowiące jednak obszaru działania, mogącego wpływać w sposób istotny na bezpieczeństwo procesów przetwarzania danych czy ochronę praw osób, których dane podlegają przetwarzaniu, choć zwiększając dostępność informacji o części zbiorów, może nieco ułatwiać korzystanie z praw przysługujących jednostce.

Na gruncie regulacji unijnych[10] można dostrzec znaczne podobieństwa dotyczące IOD, ale pojawiają się też różnice obejmujące m.in. możliwość powołania jednego IOD dla wielu administratorów i podmiotów przetwarzających dane (art. 37 ust. 3 r.o.o.d.), pełną swobodę formy prawnej współpracy między ADO a IOD (art. 37 ust. 7 r.o.o.d. — pominięte w dyrektywie 2016/680), pełnienia wobec podmiotów danych funkcji informacyjnych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych, a także z wykonywaniem praw przysługujących im na mocy r.o.o.d. (art. 38 ust. 4 r.o.o.d — pominięte w dyrektywie 2016/680), oraz pełnienia funkcji punktu kontaktowego organu nadzorczego w kwestiach związanych z przetwarzaniem (art. 39 ust. 1 pkt e) r.o.o.d.), brak obowiązku prowadzenia rejestru zbiorów — przy jednoczesnym realizowaniu obowiązków informacyjnych wobec jednostek i organu nadzoru.

Zarówno ABI, jak i IOD mają odgrywać bardzo istotną rolę w realizacji obowiązku, który w polskich przepisach wiąże się z dołożeniem „szczególnej staranności w celu ochrony interesów osób, których dane dotyczą […]", który w swym minimalnym wymiarze obliguje do zapewnienia: „aby dane te były przetwarzane zgodnie z prawem, […] zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, […] merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane, […] przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania" (art. 26 ust.1 u.o.d.o.

[10] Należy zauważyć, że rozwiązania dotyczące IOD przyjęte w dyrektywie 2016/680 są właściwie dość wierną kopią norm r.o.o.d. — a istniejące różnice wynikają z pominięć niektórych przepisów nieprzystających do przedmiotowej i podmiotowej treści dyrektywy — analiza rozwiązań unijnych dotyczyć więc będzie głównie r.o.o.d., a w przypadku istotniejszych różnic między nim a dyrektywą będzie to sygnalizowane w samym tekście lub przypisach.

— odpowiada mu art. 5 r.o.o.d[11], i 4 ust. 1 dyrektywy 2016/680[12]). Jeśli to właśnie od ABI, a ściślej — od jego wiedzy i kompetencji — zależy w znacznej mierze możliwość realizacji praw podmiotów danych (jego podstawowym obowiązkiem jest przecież zapewnianie przestrzegania przepisów o ochronie danych osobowych, a zatem to on zajmować się będzie głównie kontrolą procesów przetwarzania i proponowaniem rozwiązań zwalczających zauważone nieprawidłowości itp.), to na analizowane przepisy należy spojrzeć również jako na gwarancję realizacji praw osób, których dane przetwarzane są przez administratorów. A zatem mają one charakter gwarancyjny zarówno w odniesieniu do samego ABI, jak i rzeczywistych możliwości przestrzegania praw osób, których dane przetwarza ADO.

W przypadku IOD zależność ta jest równie widoczna, choć do określenia jego roli używa się nieco innych sformułowań[13] — ma on bowiem m.in. monitorować stosowanie przepisów o ochronie danych oraz polityk administratora lub pod-

[11] „Artykuł 5 Zasady dotyczące przetwarzania danych osobowych 1. Dane osobowe muszą być: a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (»zgodność z prawem, rzetelność i przejrzystość«); b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami (»ograniczenie celu«); c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (»minimalizacja danych«); d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (»prawidłowość«); e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą (»ograniczenie przechowywania«); f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (»integralność i poufność«). 2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie (»rozliczalność«)".

[12] „Artykuł 4 Zasady dotyczące przetwarzania danych osobowych 1. Państwa członkowskie zapewniają, by dane osobowe były: a) przetwarzane zgodnie z prawem i rzetelnie; b) zbierane w konkretnych, wyraźnych i uzasadnionych celach i nieprzetwarzane w sposób niezgodny z tymi celami; c) adekwatne, stosowne i nienadmierne do celów, dla których są przetwarzane; d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe, w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane; e) przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów ich przetwarzania; f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. […]".

[13] Por. art. 39 r.o.o.d.

miotu przetwarzającego w dziedzinie ochrony danych osobowych, zwracając przy tym szczególną uwagę na: podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty, a także udzielać na żądanie zaleceń co do oceny skutków dla ochrony danych konkretnych rodzajów przetwarzania (uprzednich w stosunku do rozpoczęcia procesów przetwarzania) oraz monitorować dalsze losy działań objętych udzielonymi zaleceniami[14].

Wskazane podejście implikuje traktowanie również samego ABI/IOD jako elementu gwarancji ochrony i realizacji praw podmiotów danych, czyniąc zeń istotny składnik prawidłowego działania systemu umożliwiającego ADO przestrzeganie nałożonych nań obowiązków. Bez wątpienia sama decyzja o powołaniu ABI/IOD (nie przesadzając w tym miejscu o jej ewentualnym fakultatywnym charakterze) musi być postrzegana jako świadome działanie ADO zmierzające do przeniesienia części kompetencji związanych z zapewnieniem przestrzegania przepisów o ochronie danych na osobę, która mając „odpowiednią wiedzę w zakresie ochrony danych osobowych"[15] czy, jak w przypadku rozwiązań unijnych, kwalifikacje zawodowe, a w szczególności wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia nałożonych nań zadań[16], dawać będzie gwarancję realnego — a nie czysto formalnego — przestrzegania zasad ochrony danych osobowych.

W przypadku wykorzystania regulacji prawnych dających możliwość jego niepowołania[17] ADO, a także podmiot przetwarzający dane, świadomie rezygnuje z pomocy osoby, której rolą jest fachowe wsparcie jego działań w obszarze realizacji obowiązków wynikających obowiązującego prawa dotyczącego ochrony danych osobowych.

Na gruncie polskich regulacji pozycja ABI jako względnie autonomicznego organu kontroli wewnętrznej, z ustawowo zakreślonym zakresem kompetencji, nie może być zazwyczaj zrównoważona przez powołanie innych osób do realizacji zadań, których prawidłowe wykonanie gwarantować ma ABI. Osoby takie nie będą posiadać środków i możliwości działania, jakimi dysponować ma ABI, ich umocowanie do realizacji zadań wynikać będzie wyłącznie z dokumentów o charakterze wewnętrznym i zapewne nie będzie umożliwiało tak kompleksowego podejścia do zdań związanych z ochroną danych. Zapewne w większości

[14] Obowiązek dokonywania oceny skutków jest uregulowany w art. 35 r.o.o.d., a dotyczy on sytuacji, w której „dany rodzaj przetwarzania — w szczególności z użyciem nowych technologii — ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych […]".

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

[16] Por. art. 37 ust. 5 r.o.o.d. i art. 32 ust. 2 dyrektywy 2016/680.

[17] Zarówno tych wynikających z u.o.d.o., jak i przepisów UE oraz norm je implementujących — w dyrektywie 2016/680 w art. 32 ust. 1 wskazuje się, że państwa członkowskie mogą zwolnić z obowiązku powołania IOD sądy i inne niezawisłe organy sądowe w ramach sprawowania przez te organy wymiaru sprawiedliwości.

przypadków będą one też obciążone innymi obowiązkami (analogicznie do stanu obserwowanego przed nowelizacją z 2015 roku) utrudniającymi lub wręcz uniemożliwiającymi prawidłową realizację zadań stawianych w art. 36a ust. 2 pkt 1 u.o.d.o. przed ABI. Taki stan rzeczy może prowadzić do wniosku, że ADO nie podejmuje wszystkich niezbędnych kroków mieszczących się w pojęciu szczególnej staranności w celu ochrony interesów osób, których dane dotyczą. Działania takie są najczęściej uzasadniane koniecznością ekonomiczną — brakiem środków na wynagrodzenia dla dodatkowej osoby (ABI) — zmuszającą do łączenia zadań/etatów w ramach już istniejącej struktury zatrudnienia. Teoretycznie możliwa jest oczywiście sytuacja, w której na mocy regulacji wewnętrznych osoba (osoby) wykonująca obowiązki ustawowo powierzone ABI będzie miała pozycję i środki adekwatne do tych wynikających z u.o.d.o., niemniej jednak wówczas niepowołanie samego ABI (lub ABI i jego zastępców) tym bardziej wydaje się pozbawione racjonalnych podstaw.

Zważywszy na literalne brzmienie art. 36b u.o.d.o., można jednak przyjąć, że co do zasady to sam ADO, oprócz innych swoich obowiązków, wykonywać musi[18] też 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[19].

W przypadku gdy ADO jest osobą prawną, organem kolegialnym czy innym podmiotem niebędącym tożsamym z osobą fizyczną, konieczność sięgania po „pełnomocników" zajmujących się problematyką ochrony danych jest tak naturalna, że niepowoływanie ABI i zastępowanie go innymi „upoważnionymi" zdaje się dodatkowo niewłaściwe z uwagi na rozmywanie się odpowiedzialności za podejmowane działania[20]. Poza oczywistymi w tym wypadku skutkami w postaci naruszania praw osób, których dane są przetwarzane, ze względu na nieza-

[18] „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.

[19] Na tego typu trudności w kontekście działania przedsiębiorców wskazują np. Ł. Kister i B. Mendyk: „Administrator danych osobowych może nie powoływać Administratora bezpieczeństwa informacji. Sytuacja ta występuje wtedy, kiedy administrator danych uznaje, że sam jest w stanie spełnić wszystkie obowiązki z zakresu ochrony danych osobowych. Jest to opcja, która wydaje się najtańsza. Wiąże się jednak z koniecznością samodzielnego przeszkolenia się przez przedsiębiorcę w zakresie ochrony danych osobowych, wdrożenia stosownej dokumentacji, przy jednoczesnym prowadzeniu działalności gospodarczej" — *idem*, *op. cit.*, s. 24.

[20] M. Sakowska-Baryła, przyjmując pełną fakultatywność powoływania ABI, także w przypadkach gdy ADO jest administratorem instytucjonalnym, stwierdza, że „zapewnienie przestrzegania przepisów o ochronie danych osobowych może być dokonane tak, że umocowane do tego w jednostce organizacyjnej organy wskażą osoby fizyczne, które będą wykonywały tak określone zadania w imieniu i na rzecz administratora danych, przy czym nie ulega wątpliwości, że to właśnie administrator danych będzie ponosił odpowiedzialność za ich działania" (M. Sakowska-Baryła, *op. cit.*, s. 167) nie wskazuje jednak na potencjalne trudności z ukaraniem bezpośrednio odpowiedzialnych za naruszenia przepisów i rzeczywistej możliwości egzekwowania jej w ramach wskazania odpowiedzialności

pewnianie przestrzegania przepisów u.o.d.o., może dojść również do problemów w przypadku konieczności ponoszenia odpowiedzialności karnej, co przy braku jednoosobowego podejmowania decyzji może być dość kłopotliwe.

Być może sytuację taką należałoby traktować jako celowe działanie mające niweczyć wysiłki prawodawcy, który zmierza, przez osobę ABI działającą w ramach ustawowych obowiązków, do stworzenia silniejszego mechanizmu egzekwowania odpowiedzialności od konkretnych osób fizycznych zobligowanych do zapewniania przestrzegania przepisów o ochronie danych osobowych. W tym kontekście byłoby to działanie zmierzające do obejścia przepisów, a zatem samo w sobie nielegalne.

W kontekście znaczącego wymiaru obligatoryjności powoływania IOD w r.o.o.d. na uwagę zasługuje przesunięcie akcentu w zakresie roli ABI w relacji do IOD — z zapewnienia przestrzegania przepisów o ochronie danych na obowiązki o charakterze informacyjno-doradczym z mocnym akcentem na bieżące monitorowanie procesów przetwarzania. Polskie rozwiązanie, jak słusznie zauważają P. Barta z P. Litwińskim[21], w którym istnieje możliwość przyjęcia rozumienia obowiązków ABI jako obowiązków rezultatu, może prowadzić do dwojakiego rodzaju problemów. Z jednej strony trudno będzie osiągnąć odpowiedni poziom samodzielności ABI — głównie z uwagi na trudności organizacyjnoformalne. Z drugiej może „prowadzić do problemów na etapie odpowiedzialności ABI za wykonywanie jego obowiązków”[22]. A dzieje się tak głównie ze względu na konieczność liczenia się w ostatecznym rozrachunku efektu starań ABI ze stale występującym czynnikiem podejmowania decyzji przez samego ADO. Przyjęcie w rozwiązaniach unijnych roli IOD jako organu monitorującego, informującego, doradzającego czy opiniującego (ADO, a także inne podmioty) — jednoznacznie pozostawia sferę decyzyjną w rękach ADO lub podmiotu przetwarzającego — a zatem to na nich spoczywa w tym kontekście odpowiedzialność za przetwarzanie. Brak chęci/możliwości powołania ABI na gruncie obecnych przepisów u.o.d.o wydaje się więc nieracjonalny także z tej perspektywy (czyli ewentualnego minimalizowania ryzyka odpowiedzialności po stronie ADO i przerzucania go na ABI).

Nie przesądzając losów samej u.o.d.o. (czy zostanie znowelizowana, czy wydana zostanie nowa ustawa, która ją zastąpi w obszarze nieobjętym r.o.o.d.), powołanie ABI na mocy obowiązujących obecnie przepisów ma również fundamentalne znaczenie z uwagi na zbliżający się 25 maja 2018 roku. Pojawi się wówczas odpowiedzialność finansowa, którą ponosić będzie bezpośrednio ADO — w tym wypadku niepowołanie ABI/IOD w sytuacjach wskazanych przez rozporządzenie unijne (a część przesłanek wynikających szczególnie z art. 37 ust. 1 pkt b i c r.o.o.d. może budzić, przynajmniej początkowo, wątpliwości interpretacyjne) samo w so-

poszczególnych członków organów kolegialnych wyznaczających, inne niż ABI, osoby realizujące przypisane mu obowiązki.

[21] Zob. szerzej P. Barta, P. Litwiński, *op. cit.*, s. 425–426.

[22] *Ibidem*.

bie będzie przesłanką jej zaistnienia, jego powołanie zaś będzie mogło wpływać na odpowiednie przygotowanie się i późniejszą prawidłową realizację zasad ochrony danych wynikających z r.o.o.d., a tym samym prowadzić do uniknięcia kar finansowych określonych w rozporządzeniu też przez tych ADO, którzy potencjalnie są zwolnieni z takiego obowiązku.

Przechodząc do analizy r.o.o.d. w kontekście ustalenia zakresu obligatoryjności powoływania IOD, należy wskazać, że pozostaje on wysoce elastyczny w odniesieniu do wskazania podmiotu powołującego i ewentualnego powołania jednego inspektora dla kilku podmiotów[23]. Pełna swoboda panuje również w zakresie prawnych relacji między IOD a podmiotami, na których rzecz działa[24].

Liczbę adresatów art. 37 ust. 1 r.o.o.d., dla których wyznaczenie IOD jest obowiązkowe, bez wątpienia należy jednak uznać za dużą, gdyż obejmuje zarówno ADO, jak i podmiot przetwarzający gdy:

a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości; b) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

Chcąc choćby w zarysie wyobrazić sobie potencjalny krąg adresatów należący do pierwszej grupy zobowiązanych, należy skupić się w szczególności na pojęciu podmiotu publicznego — kierując się wskazówką zawartą w 154 motywie preambuły r.o.o.d. — można przypuszczać, że w najszerszym rozumieniu będzie ono odnosić się do „podmiotów objętych prawem państwa członkowskiego dotyczącym publicznego dostępu do dokumentów". Jest to więc potencjalnie krąg podmiotów objętych polską ustawą z 6 września 2001 r. o dostępie do informacji publicznej.

Do lepszego zobrazowania zasięgu dwu pozostałych grup zobligowanych należy poddać analizie co najmniej trzy zwroty nieostre: „główna działalność", „regularne i systematycznego monitorowania osób" oraz „na dużą skalę". Jak wskazuje K. Syska, pierwszy z nich „można by, jak się wydaje, rozumieć w ten sposób, że przetwarzanie danych jest niezbędnym, a zarazem istotnym elementem głównej działalności podmiotu"[25]. Kolejne z nich oznaczałoby „obserwację osób (poprzez przetwarzanie ich danych osobowych), następujące w regularnych

[23] Zob. art. 7 ust. 2–4 r.o.o.d.

[24] Art. 37 ust. 6 r.o.o.d. stanowi: „Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług".

[25] K. Syska, *Administrator bezpieczeństwa informacji a inspektor ochrony danych — porównanie przesłanek powołania, statusu i zadań*, [w:] *Ogólne rozporządzenie o ochronie danych. Aktualne problemy...*, s. 76.

odstępach lub w sposób ciągły oraz przeprowadzane w oparciu o jakiś system, metodologię lub plan"[26]. Ostatnie jest bez wątpienia najbardziej enigmatyczne i jego zrozumienie wymagać będzie doprecyzowani w praktyce orzeczniczej, dzisiaj jedną z wskazówek przybliżających jego rozumienie może stanowić istniejąca do pewnego momentu w projekcie r.o.o.d. ilościowa granica przetwarzania średniorocznie informacji o 5000 osób.

Nawet na podstawie tak pobieżnej analizy można przyjąć, że poza niewielkimi podmiotami reszta będzie zobligowana do powołania IOD. W porównaniu z u.o.d.o. grupa zobligowanych do powołania takiego wewnętrznego organu zostanie kolosalnie poszerzona, warto więc zadać sobie pytanie, czy opłacalne jest odwlekanie tego zabiegu i narażenie się na wejście w nowy reżim prawny bez odpowiedniego przygotowania.

3. PRAWNE WYMOGI STAWIANE KANDYDATOM NA ABI/IOD W KONTEKŚCIE ICH WERYFIKACJI W PROCESIE REKRUTACJI

Obowiązujący obecnie w Polsce art. 36a ust. 5 u.o.d.o. wskazuje cztery warunki, jakie należy zweryfikować w procesie powołania ABI, zgodnie z którymi osoba kandydującą musi:

— mieć pełną zdolność do czynności prawnych,
— korzystać z pełni praw publicznych,
— nie być karana za umyślne przestępstwo,
— mieć odpowiednią wiedzę w zakresie ochrony danych osobowych.

Podobnie jak samo powołanie, weryfikacja tych wymogów spoczywa na barkach ADO. Trzy pierwsze mają jasno określone desygnaty, a ich sprawdzenie jest proste, choć oczywiście należy dopełnić pewnych wymogów formalnych — procedura przyjęta przez ADO powinna zatem przewidywać przeprowadzenie czynności sprawdzających, tym bardziej że zgłaszając ABI do rejestru prowadzonego przez GIODO, w końcowym fragmencie formularza[27] (część C) należy potwierdzić, iż osoba powołana spełnia wymogi ustawowe. Już choćby z uwagi na odpowiedzialność wiążącą się z poświadczeniem nieprawdy można zakładać, że w interesie ADO leży uzyskanie pewności co do prawdziwości badanych okoliczności, a tym samym poprawności składanego wniosku.

Pełna zdolność do czynności prawnych wiąże się oczywiście z uzyskaniem pełnoletności (w oparciu o art. 10 i 11 kodeksu cywilnego), a zatem procedura jej sprawdzenia musi obejmować okazanie dokumentu tożsamości i odebranie od

[26] *Ibidem*.

[27] Stanowi on załącznik do rozporządzenia Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji, Dz.U. z 2014 r., poz. 1934.

kandydata oświadczenia, że nie jest on częściowo lub całkowicie ubezwłasnowolniony na mocy postanowienia sądowego.

Pozbawienie praw publicznych[28] jest środkiem karnym orzekanym w myśl art. 40 § 2 k.k. fakultatywnie „w razie skazania na karę pozbawienia wolności na czas nie krótszy od lat 3 za przestępstwo popełnione w wyniku motywacji zasługującej na szczególne potępienie", biorąc pod uwagę, że ustawodawca zakłada weryfikację posiadania pełni praw publicznych, należy uznać, że nawet pozbawienie części uprawnień, które całościowo obejmuje pozbawienie praw publicznych, spowoduje utratę zdolności pełnienia funkcji ABI. Taka sytuacja może mieć więc miejsce także w przypadku popełnienia deliktu konstytucyjnego lub naruszenia ustawy i skazania osoby podlegającej odpowiedzialności konstytucyjnej przed TS na jedną z kar określonych w art. 25 ustawy z dnia 26 marca 1982 r. o Trybunale Stanu[29], czyli: 1) utratę czynnego i biernego prawa wyborczego w wyborach prezydenta, w wyborach do Sejmu i do Senatu, w wyborach do Parlamentu Europejskiego oraz w wyborach do organów samorządu terytorialnego, 2) zakaz zajmowania kierowniczych stanowisk lub pełnienia funkcji związanych ze szczególną odpowiedzialnością w organach państwowych i w organizacjach społecznych, 3) utratę wszystkich albo niektórych orderów, odznaczeń i tytułów honorowych.

O ile pierwsza grupa osób niespełniających przesłanek ustawowych byłaby i tak wyeliminowana z uwagi na konieczność skazania za przestępstwo umyślne[30] (tyko wówczas mamy do czynienia z niskimi pobudkami i możliwością nałożenia tego środka karnego), o tyle druga, nawet jeśli nie popełni przestępstwa, lecz jedynie dopuści się deliktu, będzie eliminowana ze względu na niemożność realizacji pełnego spektrum praw publicznych.

Jak słusznie wskazuje P. Fajgielski sprawdzenie kandydata na ABI w zakresie potwierdzenia niekaralności

powinno polegać na złożeniu do Biura Informacyjnego Krajowego Rejestru Karnego zapytania o udzielenie informacji o osobie (tzw. zapytanie o karalność). Zapytanie takie można obecnie złożyć zarówno drogą tradycyjną w Punktach Informacyjnych Krajowego Rejestru Karnego przy sądach powszechnych na terenie kraju (wykaz punktów dostępny jest na stronie: http://bip.ms.gov.pl/Data/Files/ public/bip/krk/wykaz punkty krk update20150414.pdf) oraz w Biurze Informacyjnym Krajowego Rejestru Karnego wykorzystując w tym celu formularz zapytania o udzielenie informacji

[28] Art. 40 § 1. Pozbawienie praw publicznych obejmuje utratę czynnego i biernego prawa wyborczego do organu władzy publicznej, organu samorządu zawodowego lub gospodarczego, utratę prawa do udziału w sprawowaniu wymiaru sprawiedliwości oraz do pełnienia funkcji w organach i instytucjach państwowych i samorządu terytorialnego lub zawodowego, jak również utratę posiadanego stopnia wojskowego i powrót do stopnia szeregowego; pozbawienie praw publicznych obejmuje ponadto utratę orderów, odznaczeń i tytułów honorowych oraz utratę zdolności do ich uzyskania w okresie trwania pozbawienia praw.

[29] Tekst jedn. Dz.U. z 2002 r. Nr 101, poz. 925 z póź. zm.

[30] Również w doktrynie wskazuje się, że wbrew „systematyce ustawowej, wymóg korzystania z pełni praw publicznych należy łączyć nie z pełną zdolnością do czynności prawnych, a z wymogiem niekaralności", P. Fajgielski, *Ustawowe wymogi wobec administratora bezpieczeństwa informacji*, „Informacja w Administracji Publicznej" 2015, nr 3, s. 17.

o osobie, jak i drogą elektroniczną za pośrednictwem strony http://ekrk.ms.gov.pl. Za udzielenie informacji z KRK pobiera się opłatę w wysokości: 30 zł w przypadku korzystania z drogi tradycyjnej, bądź 20 zł w przypadku skorzystania z systemu ekrk...[31]

Uprawnienie do otrzymania zaświadczenia przysługuje oczywiście osobie, której ono dotyczy, lub zgodnie z art. 6 ust. 1 pkt 10 ustawy z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym[32] pracodawcy w zakresie niezbędnym do zatrudnienia pracownika, co do którego z przepisów ustawy wynika wymóg niekaralności lub korzystania z pełni praw publicznych (przepisem tym jest oczywiście art. 36a ust. 5 u.o.d.o.).

Do momentu rozpoczęcia procesów certyfikacji wiedzy kandydatów, która może przybrać formę egzaminu państwowego, lub weryfikacji jej zakresu organizowanej w ramach samorządu zawodowego (o którym obecnie nie ma jeszcze mowy), jedynym podmiotem uprawnionym do określania kryteriów sprawdzenia tej przesłanki jest sam ADO. Gdyby nawet GIODO podjął się wypracowania referencyjnego zakresu zagadnień, które powinien znać każdy ABI — co bez wątpienia mogłoby przybrać formę wystąpień, wspominanych w art. 19a w związku z art. 12 pkt 6 u.o.d.o., kierowanych do podmiotów reprezentatywnych dla poszczególnych grup administratorów danych z uwagi na formę organizacyjną czy obszar i zakres ich działania — to jego wytyczne nie będą miały mocy wiążącej, a stanowić będą jedynie wskazówki dla konkretnego ADO, co oczywiście nie przeszkadzałoby w upowszechnianiu się tego typu informacji i budowałoby swego rodzaju dobre praktyki w tym obszarze.

Jak słusznie zauważa A. Mednis, spełnienie wymogu odpowiedniej wiedzy

wbrew pierwszym komentarzom po opublikowaniu ustawy, nie oznacza, że ABI musi mieć wykształcenie wyższe. Z drugiej strony, użycie przez ustawodawcę kolejnego wyrażenia nieostrego („odpowiednia wiedza") może nieść dla administratorów danych poważne skutki. Brak odpowiedniej wiedzy może skutkować wykreśleniem ABI z rejestru prowadzonego przez GIODO (art. 46d ust. 2 pkt 1)[33].

A zatem jeśli nie jest wymagane wykształcenie wyższe (chyba że inaczej stanowią przepisy odrębne dla danej grupy zawodowej), jakie warunki musi więc spełniać proces weryfikacji owej wiedzy, by nadać mu choćby minimalne przesłanki obiektywnej oceny? ADO ma w tym zakresie możliwość samodzielnej decyzji, czy będzie się opierać na przesłankach wyłącznie formalnych (przedsta-

[31] *Ibidem*, s. 17–18.

[32] Dz. U. z 2012 r. poz. 654 ze zm. Fakt prowadzenia postępowania weryfikującego uprawnienia ABI i odpowiedni przepis u.o.d.o. należy wskazać w pkt 11 załącznika nr 1 do rozporządzenia Ministra Sprawiedliwości z dnia 5 maja 2014 r. w sprawie udzielania informacji o osobach oraz o podmiotach zbiorowych na podstawie danych zgromadzonych w Krajowym Rejestrze Karnym (Dz.U. z 2015 poz. 660).

[33] A. Mednis, *Administrator bezpieczeństwa informacji po nowelizacji ustawy o ochronie danych osobowych z 7.11.2014 r. — ocena rozwiązań*, „Aktualne problemy ochrony danych osobowych" 2015, s. 21.

wiane przez kandydata dokumenty), czy również materialnych (badanie wiedzy — testy, rozmowy kwalifikacyjne itp.).

Jako obiektywne przesłanki weryfikacji wiedzy traktować można przedstawienie przez kandydatów dyplomów studiów podyplomowych obejmujących kształcenie ABI (np. z kierunków: ochrona danych osobowych, ochrona informacji i danych osobowych, ABI itp.). Innymi dokumentami potwierdzającymi w pewnym stopniu nabycie odpowiedniej wiedzy są wszelakie certyfikaty i dyplomy z różnych kursów, warsztatów czy szkoleń poświęconych ochronie danych osobowych. Jako okoliczność potwierdzającą posiadanie wiedzy można też traktować pełnienie funkcji ABI przed nowelizacją ustawy w jakimś podmiocie podlegającym przepisom u.o.d.o. (jeśli podlegał on w tym okresie kontroli GIODO, w której trakcie nie stwierdzono większych uchybień, można też uznać, że wiedza ABI przeszła również weryfikację merytoryczną). Jeśli nie ma kandydatów spełniających wskazane kryteria, odwołać się można się testu kompetencyjnego sprawdzającego znajomość przepisów i orzecznictwa w zakresie ochrony danych osobowych[34] (jego przygotowanie i ocena powinny być jednak oparte na wiedzy fachowej, co w praktyce może być trudne do realizacji).

W odróżnieniu od rozwiązań polskich w obu regulacjach unijnych nie znajdziemy tak rozbudowanego katalogu wymogów formalnych. Jak można przeczytać w art. 37 ust. 5 r.o.o.d.[35]: „Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39". Widać więc, iż jedyne wymogi wiążące się bezpośrednio z osobą IOD dotyczą *de facto* wyłącznie merytorycznego przygotowania do pełnienia powierzonych mu funkcji.

Decyzja o pominięciu innych przesłanek formalnych, pierwotnie występujące w tekście — „na wzór występujących choćby na gruncie u.o.d.o., jest o tyle zrozumiała, że trudno ustalić ich katalog wspólny w skali europejskiej — przy założeniu, że przesłanki te miałyby mieć jakiś realny wpływ na poprawę bezpieczeństwa przetwarzania danych i ochronę praw podmiotów danych. Podobnie jak w Polsce, wymóg zdobycia formalnego wykształcenia, np. wyższego, nie przekłada się w zasadzie na zdolność do wypełniania obowiązków powierzonych IOD. Wymóg niekaralności właściwy jest raczej funkcjonariuszom publicznym czy osobom

[34] W podobnym duchu wypowiada się P. Fajgielski „wymóg posiadania odpowiedniej wiedzy w zakresie ochrony danych osobowych nie jest równoznaczny z koniecznością przedstawienia dyplomu, świadectwa czy też innego dokumentu potwierdzającego wykształcenie. Ustawodawca wymaga od administratora danych by sprawdził, czy kandydat na ABI posiada odpowiednią wiedzę. Administrator danych dokonując oceny spełnienia tego wymogu może oprzeć się na oświadczeniu kandydata, może próbować w różny sposób weryfikować jego zgodność ze stanem faktycznym, posiłkowo może wykorzystać dokumenty potwierdzające odbyte szkolenia czy kursy […]", — *idem*, *Pozycja prawna i zadania administratora bezpieczeństwa informacji po nowelizacji ustawy o ochronie danych osobowych*, „Aktualne Problemy Ochrony Danych Osobowych 2015", s. 4.

[35] Analogicznie rozwiązanie znajduje się art. 32 ust. 2 dyrektywy 2016/680.

wykonującym zawody zaufania publicznego, a jak na razie funkcja ABI/IOD nie jest zaliczana do tego kręgu. Zważywszy na specyfikę różnorodnych podmiotów, w których przyjdzie mu funkcjonować, trudno też zakładać wypracowanie pełnego wspólnego europejskiego kanonu obejmującego wszystkie potrzebne umiejętności. Przydatność kwalifikacji kandydata, z punktu widzenia ich adekwatności do zadań, jakie realizować on będzie konkretnym miejscu wykonywania swych obowiązków, zawsze musi się wiązać (przynajmniej w jakimś stopniu) z subiektywnymi potrzebami i oceną formułowanymi przez ADO. Podejście to nie przeczy oczywiście możliwości, a nawet potrzebie, wypracowania wiarygodnych kryteriów oceny posiadanych przez ABI/IOD kwalifikacji w poszczególnych obszarach jego działania. Możliwe byłoby zapewne nawet certyfikowanie/egzaminowanie osób kandydujących do pełnienia tych funkcji ze znajomości przepisów (zarówno ogólnych, jak i branżowych), znajomości metod działania niezbędnych do prowadzenia audytów czy też umiejętności interpersonalnych związanych z realizacją zadań punktów kontaktowych (wspomniany już przykład słowacki jest tu dobrym punktem odniesienia[36]).

Choć nie przewiduje tego wprost art. 40 r.o.o.d., zasadne jest dążenie do opracowania kodeksu postępowania w zakresie wyboru IOD — nawet gdyby wytycznych takich nie traktować jako funkcjonalnie mieszczących się w pojęciu „rzetelnego i przejrzystego przetwarzania"[37], to przecież wskazany w tym przepisie katalog ma charakter otwarty — byłby on wprawdzie regulacją „oddolną", ale po wydaniu opinii o jego zgodności z r.o.o.d. przez krajowy organ nadzorczy zostałby zarejestrowany i opublikowany (w jednym kraju członkowskim[38] lub po

[36] Obowiązująca na Słowacji ustawa o ochronie danych osobowych (zob. úplné znenie zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, ako vyplýva zo zmien a doplnení vykonaných zákonom č. 84/2014 Z. z, Zbierka zákonov č. 136/2014) zakłada w § 24 m.in., że ABI może przystąpić do wykonywania obowiązków dopiero po zdaniu egzaminu, a dwuletnia przerwa w wykonywaniu obowiązków ABI lub nieprzystąpienie w tym okresie do ich realizacji skutkuje koniecznością ponownego zdania egzaminu. Zakres oraz terminy i miejsce bezpłatnych egzaminów ustala samodzielnie Úrad na ochranu osobných údajov Slovenskej republiky (zob. załącznik do Vyhláška Úradu na ochranu osobných údajov Slovenskej republiky z 13. júna 2013, ktorou sa ustanovujú podrobnosti o skúške fyzickej osoby na výkon funkcie zodpovednej osoby, Zbierka zákonov č. 165/2013) — pisemny test składa się z 20 pytań rozwiązywanych w ciągu 30 minut (wynik pozytywny uzyskuje się, zdobywając co najmniej 15 pkt, a w przypadku niepowodzenia można doń przystąpić ponownie po upływie 60 dni), które obejmują swym zakresem praktycznie wyłącznie zagadnienia prawne, m.in.: podstawowe prawa człowieka, ustawę o ochronie danych osobowych, prawo cywilne (w zakresie dotyczącym danych osobowych), kwestie przetwarzania danych osobowych przez pracodawcę i zagadnienia prywatności pracownika podczas wykonywania pracy, oraz odpowiedzialność karną za nieupoważnione przetwarzanie danych osobowych — informacje ze strony https://dataprotection.gov.sk/uoou/sk/content/narodny-pravny-ramec (dostęp: 18 listopada 2016).

[37] Art. 40 ust. 2 pkt a r.o.o.d.

[38] Przykładem doprecyzowania ogólnych wymagań na gruncie krajowym może być niemiecka rezolucja organów ochrony danych osobowych zrzeszonych w Düsseldorfer Kreises doprecyzowująca niektóre aspekty Bundesdatenschutzgesetz dotyczące inspektora ochrony danych, obejmująca

uwzględnieniu procedury z art. 40 ust. 7–11 r.o.o.d. oddziaływałby w całej UE). Ciekawe przykłady tego typu regulacji podaje E. Bielak-Jomaa[39], podsumowując je bardzo znaczącym w kontekście oceny kwalifikacji przyszłego IOD przez ADO stwierdzeniem

> prawidłowa realizacja swoich zadań przez inspektorów ochrony danych będzie często wymagała w praktyce posiadania przez nich wiedzy z bardzo różnych dziedzin, nie tylko z zakresu przepisów prawa o ochronie danych osobowych, ale też znajomości funkcjonowania systemów teleinformatycznych, wiedzy z zakresu prowadzenia szkoleń, metodologii prowadzenia kontroli i opracowywania specjalistycznej dokumentacji, a także — a może nawet przede wszystkim — umiejętności współpracy z ludźmi w ramach konsultacji z innymi jednostkami w danej instytucji i poza nią […][40].

Wracając do samego r.o.o.d., należy podkreślić, że jego twórcy jasno wskazali na konieczności sprawdzenia kwalifikacji zawodowych kandydata na IOD w zakresie zarówno wiedzy na temat prawa (która bez wątpienia obejmować powinna nie tylko regulacje ponadnarodowe dotyczące ochrony danych, lecz także krajowe normy dotyczące ich przetwarzania właściwe specyfice przyszłego pracodawcy), jak i praktyk w dziedzinie ochrony danych. Praktyki owe nie powinny być raczej rozumiane w sposób wąski, ograniczony do znajomości orzecznictwa czy wypowiedzi GIODO i doktryny obejmujących ochronę danych, ale należy ujmować je szerzej — dotyczyć powinny również wiedzy na temat technicznych i organizacyjnych sposobów prawidłowego przetwarzania/zabezpieczania danych. Tylko tak szerokie podejście do określenia zakresu niezbędnej wiedzy fachowej daje bowiem IOD szansę na zdobycie umiejętności wypełniania zadań powierzonych mu przez prawodawcę w art. 39 r.o.o.d. Jak wskazuje brzmienie przepisu, kwalifikacje zawodowe wymagane od kandydatów na IOD obejmują nie tylko wiedzę, lecz także praktyczne umiejętności w zakresie:

---

w pkt I omówienie kryteriów fachowości. Obejmuje ono zarówno wiedzę prawną dotyczącą ochrony danych od poziomu ogólnego do branżowego/sektorowego, jak i znajomość środków organizacyjnych i technicznych zabezpieczających dane. Ponadto DSB (IOD) powinien cechować się wiedzą na temat technologii informacyjno-komunikacyjnych (bezpieczeństwa fizycznego i sieciowego, kryptografii, szkodliwego oprogramowania itp.) oraz poznać specyfikę działalności i funkcjonowania ADO. Równie istotne w przypadku DSB są umiejętność praktycznego zarządzania ochroną danych (obejmujące m.in. przeprowadzanie audytów, zarządzanie ryzykiem czy monitoringiem). W dalszych punktach rezolucja odnosi się do innych aspektów funkcjonowania DSB — postulując m.in. zawieranie co najmniej czteroletnich kontraktów z osobami wykonującymi te obowiązki. „Beschluss des Düsseldorfer Kreises vom 24./25. November 2010 Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Abs. 2 und 3 Bundesdatenschutzgesetz (BDSG)", http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/24112010-MindestanforderungenAnFachkunde.pdf?__blob=publicationFile&v=1 (dostep: 18 listopada 2016).

[39] Zob. szerzej E. Bielak-Jomaa, *Wyzwania przed administratorami bezpieczeństwa informacji (inspektorami ochrony danych) w związku z wejściem w życie ogólnego rozporządzenia o ochronie danych*, [w:] *Ogólne rozporządzenie o ochronie danych. Aktualne problemy…*, s. 7–8.

[40] *Ibidem*, s. 8.

— merytorycznego, klarownego przekazywania informacji o obowiązkach wynikających z prawa ochrony danych i prowadzenia doradztwa w zakresie ich prawidłowej realizacji;

— monitorowania, czyli co najmniej okresowej weryfikacji, przestrzegania zasad ochrony danych określonych w przepisach UE, krajowych i wewnętrznych ustanowionych przez ADO (lub podmiot przetwarzający) ze szczególnym uwzględnieniem przydziału obowiązków (jego zakresu, adekwatności do potrzeb, samodzielności decyzyjnej itp.), zwiększania świadomości i szkoleń personelu uczestniczącego w operacjach przetwarzania oraz powiązanych z tym audytów (przy czym nie wszystkie te działania muszą być domeną IOD — choć niewątpliwie ma on badać ich jakość i skuteczność);

— udzielania zaleceń co do oceny skutków dla ochrony danych, planowanych procesów przetwarzania oraz późniejsze ich monitorowanie;

— współpracy z organem nadzorczym i pełnienia dla niego funkcji punktu kontaktowego w kwestiach związanych z przetwarzaniem danych osobowych.

Tak zakreślony katalog umiejętności praktycznych pozwala na przyjęcie założenia, że pewną rękojmię rzeczywistego wypełniania wymogów r.o.o.d. dają na przykład osoby mające praktykę na stanowisku ABI, działające w warunkach zaistniałych po 1 stycznia 2015 roku, albowiem nabywają one stosownych umiejętności, realizując wymogi obowiązującego w prawa (pewne wątpliwości budzić może jedynie umiejętność udzielania zaleceń, która w formie opisanej w r.o.o.d. nie występuje w rozwiązaniach krajowych). Dopóki nie pojawią się konkretne wytyczne na poziomie krajowym lub europejskim, w pełni aktualne zdają się być uwagi dotyczące sposobów weryfikacji kwalifikacji IOD przez ADO, poczynione w trakcie rozważań dotyczących analogicznych działań podejmowanych wobec kandydatów na ABI.

4. PODSUMOWANIE

Prowadzone rozważania miały na celu zwrócenie uwagi na nadchodzący przełomom w zakresie podstaw prawnych procesów przetwarzania danych osobowych. Nawet tak szczątkowa analiza zaledwie kilku wybranych problemów pozwoliła wskazać znaczące różnice w dotychczasowym i przyszłym statusie ABI/IOD, pojawiające się już na etapie jego powołania. Dotyczą one zarówno warunków, które ma spełniać kandydat na to stanowisko, jak i samego obowiązku powołania go przez ADO (lub w przypadku r.o.o.d. również przez podmiot przetwarzający — *processor*). Wyraźnie zarysowuje się tendencja do profesjonalizowania działań ABI/IOD, co ujawnia się choćby w swobodzie wyboru formy prawnych relacji łączących go z ADO czy w możliwości realizacji tych zadań w odniesieniu do wielu pomiotów. Z istotną zmianą podejścia mamy również do

czynienia w zakresie poszerzenia obowiązku powoływania tego organu (którego naruszenie skutkować może dotkliwą karą finansową).

W artykule zabrakło miejsca na dokonanie pełnego porównania regulacji dotyczących ABI i IOD, a co za tym idzie nie zawiera on analizy wszystkich istotnych aspektów zmieniającej się roli tego wewnętrznego organu kontroli. Będą one jednak zapewne przedmiotem wielu innych publikacji poświęconych reformie prawa ochrony danych osobowych.

DATA PROTECTION OFFICER AND DATA PROTECTION INSPECTOR ON THE BACKGROUND OF NATIONAL AND THE EU REGULATIONS — SELECTED ISSUES

Summary

The main aim of this article is the attempt to conduct a comparative analysis of selected issues from the relationship between ABI (Data Protection Officer) / IOD (Data Protection Inspecor) and ADO (Controller). The test area includes mainly issues related to the establishment of inspection bodies. In particular, this problem when it depends on the discretion of the ADO and in which cases turns into a legal obligation. The description includes the conditions set for the candidate for the ABI / IOD, and the process of their verification. Apart from main considerations the article provides also comments on the nature of the relationship between them and the ADO.