



Stowarzyszenie
Administratorów
Bezpieczeństwa
Informacji

Opinia prawna w przedmiocie wykonywania zadań administratora bezpieczeństwa informacji (ABI)

opracowanie: adw. dr Grzegorz Sibiga

I. PRZEDMIOT I PODSTAWA PRAWNA OPINII

1.1. Przedmiotem niniejszej opinii prawnej jest określenie - w zakresie wykonywania zadań związanych z ochroną danych osobowych - relacji między administratorem bezpieczeństwa informacji (dalej jako: „**ABI**”) oraz innymi komórkami organizacyjnymi powołującego ABI administratora danych (dalej jako „**ADO**”) (np. audyt wewnętrzny, kontrola wewnętrzna) oraz zewnętrznymi usługodawcami świadczącymi usługi dla ADO (np. konsultanci, prawnicy), w tym w szczególności ustalenie, czy dopuszczalna pozostaje działalność wspomnianych innych komórek organizacyjnych oraz usługodawców polegająca na:

- a) kontroli wykonywania zadań przez administratora bezpieczeństwa informacji,
- b) zapewnianiu przestrzegania przepisów o ochronie danych osobowych u administratora danych, poprzez audyty, konsultacje, opinie itp.

1.2. Podstawę prawną niniejszej analizy stanowią, w szczególności, następujące obowiązujące w Rzeczypospolitej Polskiej akty prawne:

- a) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922) – dalej jako „**u.o.d.o.**”;
- b) rozporządzenie Ministra Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych

osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 2015 r., poz. 745) – dalej jako „**rozporządzenie MC**”;

c) dyrektywa 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. U. UE L z 1995 r. nr 281, s. 31 z późn. zm.) – dalej jako „**Dyrektywa 95/46/WE**”;

d) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w 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. U. UE L z 2016 r. nr 119, s. 1) – dalej jako „**RODO**” lub „**rozporządzenie ogólne**”;

e) ustawa z dnia 6 lipca 1982 r. o radcach prawnych (t.j. Dz. U. z 2016 r. poz. 233) – dalej jako „**u.r.p.**”;

f) ustawa z dnia 27 czerwca 1997 r. o służbie medycyny pracy (t.j. Dz. U. z 2014 r. poz. 1184) – dalej jako „**u.s.m.p.**”;

g) ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz. U. z 2013 r. poz. 885 z późn. zm.) – dalej jako „**u.f.p.**”;

h) rozporządzenie Ministra Finansów z dnia 4 września 2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu (Dz. U. z 2015 r., poz. 1480) – dalej jako „**rozporządzenie MF**”;

i) ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2014 r., poz. 1502 z późn. zm.) – dalej jako „**k.p.**”.

II. ANALIZA PRAWNA

[wprowadzenie – podstawowe zasady wykonywania funkcji ABI]

2.1. Z punktu widzenia przedmiotu opinii znaczenia mają następujące zasady wynikające z przepisów o ochronie danych osobowych:

a) [**Kompetencje ABI**] Na ABI obowiązkowo nałożone zostały **zadania** określone w art. 36a ust. 2 u.o.d.o. polegające na zapewnianiu przestrzegania przepisów o ochronie danych osobowych (pkt 1) oraz na prowadzeniu rejestru zbiorów danych osobowych

przetwarzanych przez ADO (pkt 2). W zakresie zadań polegających na zapewnieniu przestrzegania przepisów o ochronie danych osobowych mieszczą się w szczególności: sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych, nadzorowanie opracowania i aktualizowania dokumentacji przetwarzania danych osobowych oraz przestrzegania zasad w niej określonych, zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Powyższe zadania powinny być wykonywane przez ABI w sposób nieprzerwany, a ze względu na ich obligatoryjny charakter zadania te nie mogą zostać – w drodze aktu lub czynności wewnętrznej – odebrane ABI i powierzone do wykonania innej osobie, w ten sposób, że ABI zostanie pozbawiony możliwości ich realizowania.

b) **[Podległość]** Administrator bezpieczeństwa informacji **podlega** bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych (art. 36a ust. 7 u.o.d.o.). Powyższe rozróżnienie na kierownika jednostki organizacyjnej oraz osobę fizyczną (będącą administratorem danych) ma związek z tym, że podmiotem prawa będącym ADO może być zarówno osoba prawna (ew. jednostka organizacyjna nie posiadająca osobowości prawnej), jak i osoba fizyczna. W przypadku gdy status ADO będzie przysługiwał osobie fizycznej to jej podlega ABI. W sytuacji innych, niż osoba fizyczna, podmiotów prawa każdorazowego ustalenia wymaga status kierownika jednostki organizacyjnej, któremu podlega ABI.

c) **[Niezależność]** Administrator bezpieczeństwa informacji wykonuje swoje ustawowe zadania w sposób niezależny, a ADO jest obowiązany zapewniać tą niezależność (art. 36a ust. 8 u.o.d.o.).

d) **[Obowiązki i odpowiedzialność ADO]** Na ADO, pomimo powołania przez niego ABI, spoczywają określone w przepisach prawa obowiązki ochrony danych osobowych oraz związana z nimi odpowiedzialność. To ADO, jako podmiot decydujący o celach i środkach przetwarzania danych osobowych, jest głównym adresatem obowiązków ochrony danych osobowych (w węższym zakresie adresatem obowiązków będzie podmiot przetwarzający powierzone dane osobowe) i ponosi odpowiedzialność za niewykonanie tych obowiązków. W związku z tym to również ADO podejmuje decyzje w jaki sposób wykonywać poszczególne rodzaje obowiązków ochrony danych osobowych.

[niezależne wykonywanie zadań ABI]

2.2 Warunek niezależności ABI w wykonywaniu swoich zadań jest kluczowy dla zrozumienia jego relacji z innymi osobami, w szczególności w stosunkach wewnątrz jednostki organizacyjnej. W ustawie o ochronie danych osobowych warunek ten został wyrażony w dwóch przepisach w: art. 36a ust. 8 oraz w art. 36a ust. 9.

W art. 36a ust. 8 u.o.d.o. warunek ten powiązано z obowiązkami ADO: „Administrator danych zapewnia środki i organizacyjną odrębność administratora bezpieczeństwa informacji niezbędne do niezależnego wykonywania przez niego zadań, o których mowa w ust. 2”. Natomiast art. 36a ust. 9 u.o.d.o. zawiera upoważnienie dla ministra właściwego do spraw informatyzacji do wydania rozporządzenia określającego tryb i sposób realizacji zadań ABI oraz sposób prowadzenia rejestru zbiorów danych, a w wytycznych co treści rozporządzenia zobligowano ministra w szczególności do uwzględnienia konieczność zapewnienia niezależności i organizacyjnej odrębności w wykonywaniu przez ABI zadań.

Warunek niezależności ABI odnosi się jedynie do wykonywania przez niego zadań (a nie do całego jego statusu w jednostce organizacyjnej ADO), przy czym prawodawca nie dookreśla na czym ta niezależność polega.

Zbliżone rozwiązanie przewidziano w stanowiącej pierwowzór u.o.d.o. dyrektywie 95/46/WE. Zgodnie z art. 18 ust. 2 dyrektywy 95/46/WE zapewnienie przez urzędnika, który jest odpowiednikiem polskiego ABI, stosowania wewnętrznych przepisów prawa krajowego przyjętych na mocy dyrektywy ma następować w niezależny sposób. Natomiast w motywie 49 dyrektywy 95/46/WE podkreśla się, że urzędnik musi mieć możliwość wykonywania swoich funkcji w sposób całkowicie niezależny (*complete independence*).

[pojęcie niezależności]

2.3 Słownik Języka Polskiego PWN wskazuje, że „niezależny” to: (1) niepodporządkowany komuś, czemuś, decydujący o sobie; też: świadczący o braku podporządkowania komuś lub czemuś; (2) niebędący wyznaczonym, zdeterminowanym przez coś; (3) wygłaszający bezstronne opinie, niekierujący się interesem żadnej grupy społecznej, (4) nienależący do żadnej z rywalizujących partii. Zgodnie z definicją dwa główne

elementy niezależności to brak podporządkowania oraz bezstronność, a niezależność jest od kogoś lub czegoś.

[prawne rozumienie niezależności]

2.4 Pojęcie niezależności jest rozwijane i uszczegóławiane na gruncie różnego rodzaju aktów prawnych, w tym w kodeksach etyki i w stanowiskach doktryny.

2.5 Definicję pojęcia niezależności dostarcza Kodeks etyki zawodowych księgowych Międzynarodowej Federacji Księgowych (IFAC)¹ (dalej jako „KEZK”), który na podstawie uchwały nr 4249/60/2011 Krajowej Rady Biegłych Rewidentów z dnia 13 czerwca 2011 r. w sprawie zasad etyki zawodowej biegłych rewidentów został wprowadzony jako zasady etyki biegłych rewidentów (§ 2 tej uchwały). Zgodnie z art. 4 ust. 1 pkt 3 ustawy z dnia 7 maja 2009 r. o biegłych rewidentach i ich samorządzie, podmiotach uprawnionych do badania sprawozdań finansowych oraz o nadzorze publicznym (t.j. Dz. U. z 2016 r., poz. 1000) biegły rewident jest obowiązany w szczególności (...) przestrzegać standardów rewizji finansowej, zasad niezależności oraz etyki zawodowej. Jak wskazuje ust. 6 rozdziału 290 KEZK niezależność obejmuje:

a) niezależność umysłu: stan umysłu, który umożliwia sformułowanie wniosku wolnego od różnego rodzaju wpływów podważających zawodowy osąd – pozwalający danej osobie na działanie uczciwe, obiektywne i nacechowane zawodowym sceptycyzmem, oraz

b) niezależność wizerunku: unikanie faktów i okoliczności na tyle znaczących, że racjonalna i dobrze poinformowana strona trzecia – zaznajomiona ze wszystkimi istotnymi faktami i okolicznościami – mogłaby zasadnie uznać, że uczciwość, obiektywizm lub zawodowy sceptycyzm podmiotu lub członka zespołu wykonującego badanie zostały naruszone.

2.6 Podobną definicję niezależności dostarcza również Kodeks zawodowej etyki w rachunkowości przyjęty przez Stowarzyszenie Księgowych w Polsce². Zgodnie z Rozdziałem 2 zasada niezależności zawodowej osoby zajmującej się rachunkowością polega na wyrażeniu niezależnej opinii w sprawach wymagających rozstrzygnięć przy jej udziale. Zasada ta wiąże się z: niezależnością profesjonalnego osądu, który oznacza

¹ http://www.kibr.webserwer.pl/_doc/uchwaly/uchwala_4249-60-2011.pdf

² <http://www.bielsko.skwp.pl/Kodeks,etyki,zawodowej,w,rachunkowosci,9461.html>

stan umysłu pozwalający osobie zajmującej się rachunkowością na rzetelne, obiektywne i wiarygodne przedstawienie jej zdania, bez ulegania wpływom zniekształcającym profesjonalny osąd oraz dbałością o wizerunek zawodu, co oznacza unikanie przez osobę zajmującą się rachunkowością takich sytuacji i działań, które mogłyby doprowadzić do tego, że inne kompetentne osoby mogłyby wyciągnąć uzasadniony wniosek, że zasada niezależności nie została przez nią zachowana. Co istotne, zgodnie z ust. 2.3. tego Kodeksu niezależność zawodowa nie oznacza braku współpracy z innymi osobami wykonującymi czynności księgowe, czynności wspomagające zarządzanie, rozliczenia podatkowe i inne rozliczenia publicznoprawne i z innymi osobami zatrudnionymi w jednostce zgłaszającymi potrzeby informacyjne pod adresem rachunkowości. Natomiast ust. 2.4. wskazuje, że niezależność zawodowa osoby zajmującej się rachunkowością nie oznacza braku funkcjonalnego podporządkowania. Niezależność w ww. przypadkach rozumie się jako zachowanie postawy niepoddawania się jakimkolwiek wpływom, które mogłyby stanowić zagrożenie dla etycznego (moralnego) i profesjonalnego wykonywania przez osobę zajmującą się rachunkowością czynności księgowych, czynności wspomagających zarządzanie, rozliczeń podatkowych i innych rozliczeń publicznoprawnych (ust. 2.5.). Jednocześnie niezależność powinna być rozumiana jako tylko i wyłącznie konieczna cecha profesjonalnego wykonywania zawodu i nie może być wykorzystywana do osiągnięcia szczególnych przywilejów ani w jednostce, ani poza nią (ust. 2.7.).

- 2.7** Zgodnie z § 7 Zbioru zasad etyki adwokackiej i godności zawodu: *„W czasie wykonywania czynności zawodowych adwokat korzysta z pełnej swobody i niezależności. Na adwokacie spoczywa szczególny obowiązek dbałości o to, aby nie przekroczyć granic prawidłowego reprezentowania interesów klienta”*. W przypadku wykonywania zawodu adwokata niezależność jest rozumiana jako wolność od jakichkolwiek nacisków lub zależności formalnych ze strony władzy państwowej lub innej, a nadto organów własnego samorządu, co oznacza, że nikt nie posiada uprawnień do nakazania adwokatowi podjęcia lub zaniechania określonych działań w danej sprawie. Niezależności nie należy mylić z możliwością prowadzenia kontroli prawidłowości czynności wykonywanych przez adwokata. W określonej sytuacji działania adwokata mogą być przedmiotem oceny sądu dyscyplinarnego lub instytucji ubezpieczeniowej w razie zgłoszenia roszczenia przez klienta, jednak w każdym wypadku jest to kontrolna następcza nieingerująca w wykonywanie czynności

zawodowych przez adwokata (J. Naumann, *Zbiór Zasad Etyki Adwokackiej i Godności Zawodu. Komentarz*. Wyd. 2, Warszawa 2015, Komentarz do §7).

[wnioski - niezależne wykonywanie zadań ABI]

2.8 Uwzględniając przedstawione powyżej rozwiązania niezależność ABI można rozumieć w następujący sposób:

- a) Gwarancja zachowania niezależności dotyczy wykonywania czynności, o których mowa w art. 36a ust. 2 u.o.d.o.
- b) Niezależność obejmuje niezależność umysłu oraz niezależność wizerunku ABI (w rozumieniu analogicznym do przedstawionego w pkt 2.5).
- c) ABI realizuje swoje działania z art. 36a ust. 2 u.o.d.o w sposób samodzielny i bezstronny.
- d) Niezależność należy traktować jako wolność ABI od ingerencji z jakiegokolwiek strony lub z jakiegokolwiek powodu.
- e) W szczególności wykonywanie zadań nie może być uzależnione od wydania poleceń przez kierownika jednostki organizacyjnej, działającego bezpośrednio lub poprzez osoby występujące w jego imieniu.
- f) Również inne działania niż polecenia, takie jak rekomendacje czy wskazówki mogą być traktowane jako naruszenie niezależności ABI, jeżeli wpływają na bezstronność ABI (wpływ pośredni).
- g) Inne obowiązki ABI niż zadania ustawowe określone w art. 36a ust. 2 u.o.d.o. nie mogą naruszać niezależnego wykonywania tych zadań.

[niezależność inspektora ochrony danych w RODO]

2.9 W dniu 25 maja 2018 r. zacznie obowiązywać ogólne rozporządzenie o ochronie danych, które zastąpi obecne obowiązujące przepisy o ochronie danych osobowych. Funkcja ABI zostanie zastąpiona przez inspektora ochrony danych (dalej jako „inspektor”), jednak podtrzymana została zasada jego niezależność. Zgodnie z art. 38 ust. 3 RODO, inspektor nie może otrzymywać instrukcji dotyczących wykonywania swoich zadań. W motywie 97 wyjaśnia się, że inspektor powinien być w stanie wykonywać swoje

obowiązki i zadania w sposób niezależny. W wytycznych Grupy Roboczej Art. 29 dyrektywy 95/46 z dnia 13 grudnia 2016 r. dotyczących inspektora (WP 243) wytłumaczono, że oznacza to, że administrator lub podmiot przetwarzający nie może określać inspektorowi, w jaki sposób powinien zajmować się konkretną sprawą, jaki powinien być wynik jego analizy, w jaki sposób przeprowadzić postępowanie wyjaśniające co do skargi lub czy należy się skonsultować z organem nadzorczym. Inspektor nie może też otrzymywać instrukcji co do tego, jaką interpretację prawa przyjąć. Inspektor musi mieć możliwość wyrażenia swojego zdania odrębnego w sytuacji, w której administrator lub podmiot przetwarzający podejmą decyzję niezgodną z rekomendacją inspektora (pkt 3.3 wytycznych) .

[niezależność a podległość ABI]

2.10 Z jednej strony, jak już powyżej wspomniano, administratorowi bezpieczeństwa informacji ustawa gwarantuje niezależne wykonywanie zadań (art. 36a ust. 8 u.o.d.o.), natomiast z drugiej ta sama ustawa przewiduje podległość ABI bezpośrednio kierownikowi jednostki organizacyjnej. Zgodnie z art. 36a ust. 7 u.o.d.o. *„Administrator bezpieczeństwa informacji podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych”*.

Pomimo pozornej sprzeczności tych dwóch rozwiązań należy zwrócić uwagę, że zostały one wprowadzone w jednej nowelizacji ustawy z dnia 7 listopada 2014 r.³, znajdują się w tej samej jednostce redakcyjnej (artykule), a ustępy zawierające wspomniane przepisy następują bezpośrednio po sobie. Trzeba zatem poszukiwać racjonalności w takiej regulacji ustawowej, a nie konfliktu między zasadami wyrażonymi w przepisach.

Wprowadzona regulacja dotycząca ABI nie jest jedynym rozwiązaniem ustawowym, w którym osoba pozostająca w podległości służbowej ma wykonywać swoje obowiązki niezależnie. Jako przykłady w opinii zostaną przedstawione przypadki radcy prawnego wykonującego zawód w ramach stosunku pracy (tzw. „in-house lawyer”), osób realizujących zadania służby medycyny pracy oraz audytora wewnętrznego.

³ Ustawa z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz. U. 2014 r., poz. 1662).

[niezależność radcy prawnego]

- 2.11** Radca prawny wykonujący zawód w ramach stosunku pracy zgodnie z art. 9 ust. 1 u.r.p. zajmuje samodzielne stanowisko podległe bezpośrednio kierownikowi jednostki organizacyjnej. Jest to konstrukcja podobna do tej stosowanej wobec ABI z art. 36a ust. 7 u.o.d.o. Radcy prawnemu nie można polecać wykonania czynności wykraczającej poza zakres pomocy prawnej. Niezależność radcy prawnego uwidacznia się przede wszystkim poprzez art. 13 u.r.p. zgodnie z którym nie jest on związany poleceniem co do treści opinii prawnej, a wszelkie próby wydawania takich poleceń stanowią naruszenie przepisów ustawowych. Kolejną gwarancją jest konieczność zasięgnięcia przez jednostkę organizacyjną opinii radcy okręgowej izby radców prawnych w przypadku rozwiązania stosunku pracy za wypowiedzeniem z radcą prawnym z powodu nienależytego wykonywania obowiązków radcy prawnego (art. 19 ust. 1 u.r.p.). Jest to przepis szczególny wobec przepisów kodeksu pracy dotyczących rozwiązania umowy za wypowiedzeniem, gdyż zawiera on dodatkowe wymaganie w postaci opinii rady okręgowej izby radców prawnych, w przypadku gdy podstawą wypowiedzenia jest nienależyte wykonywanie obowiązków radcy prawnego (Kwapisz, Krystyna. Art. 19. W: *Ustawa o radcach prawnych. Komentarz*. Wydawnictwo Prawnicze LexisNexis, 2011.). W przypadku, gdy rozwiązanie umowy wynika z innych przyczyn, to pracodawca nie ma obowiązku zwracać się o opinię do rady okręgowej izby radców prawnych (tak np. J. Łoziński, Z. Klatka, *Status prawny radcy prawnego jako pracownika*, MOPR 2005, Nr 3, str. 72). Oznacza, to że „in-house lawyer” poza wykonywaniem obowiązków wchodzących w zakres pomocy prawnej podlega przepisom prawa pracy tak jak pozostali pracownicy w danym zakładzie pracy.
- 2.12** W przypadku zawodu radcy prawnego jako zawodu zaufania publicznego niezależność jest gwarancją ochrony praw i wolności obywatelskich, demokratycznego państwa prawnego oraz prawidłowego funkcjonowania wymiaru sprawiedliwości (art. 7 ust. 1 KERP). Ustęp 2 w art. 7 KERP dostarcza wieloaspektową definicję niezależności jako stanu, w którym radca prawny jest wolny od wszelkich wpływów wynikających z jego osobistych interesów, nacisków z zewnątrz oraz ingerencji z jakiegokolwiek strony lub z jakiegokolwiek powodu. Ponadto na prezentowane przez radcę prawnego stanowisko w sprawie nie mogą wpływać polecenia wyrażone przez kogokolwiek, ograniczające niezależność, sugestie czy wskazówki.

[niezależność służby medycyny pracy]

- 2.13** Zasada niezależności występuje również w przypadku pozycji osób wykonujących obowiązki w ramach służby medycyny pracy. Zgodnie z art. 3 u.s.m.p. „Osoby realizujące zadania służby medycyny pracy przy wykonywaniu czynności zawodowych są niezależne od pracodawców, pracowników i ich przedstawicieli oraz innych podmiotów, na których zlecenie realizują zadania tej służby.” Regulacja ta wprowadza zasadę niezależności osób realizujących zadania służby medycyny pracy od pracodawców, pracowników i innych podmiotów, na zlecenie których realizują zadania tej służby. W doktrynie podkreśla się, że niezależność tych osób od innych podmiotów nie dotyczy wszystkich czynności, tylko wykonywania czynności zawodowych (Kaczocho, Mateusz. Art. 3. W: *Służba medycyny pracy. Komentarz*. System Informacji Prawnej LEX, 2014). Należy podkreślić, że ta niezależność przejawia się poprzez brak wpływu innych podmiotów na tę działalność – jest to „niezależność od...”.

[niezależność audytu wewnętrznego]

- 2.14** Instytucją, która jest również zbliżona konstrukcyjnie do ABI jest audyt wewnętrzny, który jest działalnością niezależną i obiektywną, a jego celem jest wspieranie ministra kierującego działem lub kierownika jednostki w realizacji celów i zadań przez systematyczną ocenę kontroli zarządczej oraz czynności doradcze (art. 272 ust. 1 u.f.p.).
- 2.15** Zgodnie z art. 280 u.f.p. „Kierownik komórki audytu wewnętrznego podlega bezpośrednio kierownikowi jednostki, a w urzędzie administracji rządowej, w którym tworzy się stanowisko dyrektora generalnego urzędu - dyrektorowi generalnemu w zakresie określonym odrębnymi ustawami.” Jak wskazuje się w doktrynie wymóg bezpośredniej podległości należy rozumieć w sposób zgodny ze standardami audytu, o którym mowa w art. 273 ust. 1 u.f.p. (Opiola/Skica w: *Ustawa o finansach publicznych. Komentarz*, red. W. Misiąg, 2014, wyd. 1, Komentarz do art. 280).
- 2.16** Na podstawie Komunikatu nr 2 Ministra Finansów w sprawie standardów audytu wewnętrznego dla jednostek sektora finansów publicznych z dnia 17 czerwca 2013 r. (Dz. Urz. MF z 2013 r., poz. 15) w sektorze finansów publicznych obowiązują Międzynarodowe standardy praktyki zawodowej audytu wewnętrznego. Wymagają one, aby kierownik komórki audytu podlegał funkcjonalnie kierownikowi jednostki, aby

zachować niezależność organizacyjną audytu. Zgodnie ze standardem 1110 („niezależność organizacyjna”) zarządzający audytem wewnętrznym musi podlegać takiemu szczeblowi zarządzania w organizacji, który pozwoli audytowi wewnętrznemu wypełniać jego obowiązki. Ponadto, zgodnie ze standardem 1110.A1 audyt wewnętrzny nie może być narażony na jakiegokolwiek próby narzucenia zakresu audytu, wpływania na sposób wykonywania pracy i informowania o jej wynikach.

- 2.17** Podobnie jak w przypadku ABI zgodnie z art. 282 ust. 1 u.f.p. „Kierownik jednostki, a w urzędzie administracji rządowej, w którym tworzy się stanowisko dyrektora generalnego urzędu - dyrektor generalny, zapewnia warunki niezbędne do niezależnego, obiektywnego i efektywnego prowadzenia audytu wewnętrznego, w tym zapewnia organizacyjną odrębność komórki audytu wewnętrznego oraz ciągłość prowadzenia audytu wewnętrznego w jednostce”. Zapewnienie efektywności należy rozumieć m.in. poprzez wyposażenie w odpowiednią ilość kompetentnych pracowników oraz inne środki pracy. Odrębność organizacyjną jednostki należy rozumieć jako jeden z warunków niezależnego prowadzenia audytu.
- 2.18** Bezpośrednia podległość kierownika komórki audytu kierownikowi jednostki oraz uprawnienia do zarządzania działalnością audytu na podstawie standardów działania (standard 2000-2600) są **postrzegane w doktrynie jako gwarancja niezależności działalności audytu wewnętrznego** (Opióła/Skica w: *Ustawa o finansach publicznych...*). Pogląd ten jest również podzielany przez K. Celarek, której zdaniem *„Niezależność oznacza brak okoliczności zagrażających bezstronnemu wykonywaniu obowiązków przez audyt wewnętrzny lub zarządzającego audytem wewnętrznym. Służy temu bezpośredni i nieograniczony dostęp do kierownictwa jednostki”* (K. Celarek, *Prawne i praktyczne aspekty kontroli i nadzoru nad działalnością samorządu terytorialnego*, 2015, wyd. 1, Legalis). Innymi słowy bezpośrednia podległość kierownikowi jednostki przez audytora wewnętrznego przekłada się na bezpośredni dostęp do tego kierownictwa, co w konsekwencji zapewnia niezależność rozumianą jak brak okoliczności zagrażających bezstronnemu wykonywaniu obowiązków.

[wnioski - niezależność a podległość ABI]

- 2.19** Podobnie jak w przypadku audytora wewnętrznego bezpośrednią podległość ABI kierownikowi jednostki organizacyjnej **należy odczytywać jako gwarancję niezależności ABI w wykonywaniu zadań, a nie jej ograniczenie.** W ten sposób ABI

ma bezpośredni dostęp do kierownika jednostki organizacyjnej oraz zapobiega się sytuacji, w której ABI nadzoruje lub sprawdza osoby, które są usytuowane wyżej od niego w strukturze organizacyjnej.

Nie występuje również konflikt między podległością kierownikowi jednostki organizacyjnej a niezależnym wykonywaniem zadań przez ABI. Ustawodawca wyodrębnia bowiem takie zadania, które ze względu na swój cel (przede wszystkim polegający na ocenie) wymagają bezstronności, co oznacza, że kierownik nie może ingerować w ich merytoryczną realizację. Niezależność wykonującego zadanie służy również interesowi jednostki organizacyjnej polegającemu na umożliwieniu prawidłowego wykonania zadania.

W przypadku ABI problemem jest jednak brak dodatkowych gwarancji trwałości stosunku z ADO wzmacniających jego niezależność, chociaż ograniczonych tak jak w przypadku radcy prawnego. Temat ten wykracza jednak poza zakres niniejszej opinii.

- 2.20** Ustawowa gwarancja niezależności ABI odnosi się jedynie do zadań realizowanych na podstawie art. 36a ust. 2 u.o.d.o. W pozostałym zakresie obowiązków podległość ABI nie będzie w żaden sposób ograniczana przez przepisy o ochronie danych osobowych. Przykładem są obowiązki w zakresie przestrzegania przepisów i zasad bezpieczeństwa i higieny pracy, w których status ABI (będącego pracownikiem) jest identyczny jak innych pracowników. Zgodnie z art. 211 k.p. podstawowym obowiązkiem pracownika jest przestrzeganie przepisów i zasad higieny pracy. W szczególności pracownik powinien znać przepisy i zasady bezpieczeństwa i higieny pracy, wykonywać pracę w sposób zgodny z przepisami i zasadami bezpieczeństwa i higieny pracy oraz stosować się do wydawanych w tym zakresie poleceń i wskazówek przełożonych, a także współdziałać z pracodawcą i przełożonymi w wypełnianiu obowiązków dotyczących bezpieczeństwa i higieny pracy. Korelatem tym obowiązków pracownika są zobowiązania nałożone na osobę kierującą pracownikami w art. 212 k.p., w tym zgodnie z pkt 5 jest ona zobowiązana do egzekwowania przestrzegania przez pracowników przepisów i zasad bezpieczeństwa i higieny pracy. Ponadto zgodnie z art. 237⁴ § 1 k.p. pracodawca jest obowiązany zaznajamiać pracowników z przepisami i zasadami bezpieczeństwa i higieny pracy dotyczącymi wykonywanych przez nich prac. Zaś korelatem tego obowiązku pracodawcy jest art. 237⁴ § 3 k.p., zgodnie z którym pracownik jest obowiązany potwierdzić na piśmie zapoznanie się z przepisami oraz zasadami bezpieczeństwa i higieny pracy.

[status ADO]

2.21 Na ADO, pomimo powołania przez niego ABI, spoczywają określone w przepisach prawa obowiązki ochrony danych osobowych oraz związana z nimi odpowiedzialność. W związku z tym to również ADO podejmuje decyzje w jaki sposób wykonywać poszczególne rodzaje obowiązków ochrony danych osobowych. W tym kontekście rola ABI sprowadza się do wsparcia ADO w realizacji tych obowiązków. Znajduje to potwierdzenie w prawnych formach działania ABI, który może jedynie w sprawozdaniu stwierdzić przypadki naruszenia przepisów o ochronie danych osobowych oraz określić działania przywracające stan zgodny z prawem (art. 36c pkt 7 u.o.d.o.), a w przypadku nadzoru nad dokumentacją może dodatkowo zawiadomić o nieprawidłowościach wraz z przedstawieniem działań naprawczych, a także pouczać lub instruować osoby nieprzestrzegające zasad zawartych w dokumentacji (§ 8 rozporządzenia MC). Decyzję co do wdrożenia zaproponowanego przez ABI działania podejmuje ADO.

W żadnym z przepisów o ochronie danych osobowych nie ogranicza się dopuszczalności korzystania przez ADO z innych możliwości wsparcia w wykonywaniu obowiązków ochrony danych: zarówno w sferze wewnętrznej (np. dział prawny), jak i z zewnątrz (konsultanci, audytorzy, prawnicy). Powołanie ABI nie oznacza jego wyłączności w zakresie wdrażania obowiązków ochrony danych osobowych w jednostce organizacyjnej ADO. Co więcej, ADO może nie zaakceptować stanowiska ABI i podjąć odmienne działania (lub zaniechać działań) niż te, które są proponowane przez ABI. To bowiem na ADO spoczywa decyzja w jaki sposób będzie wykonywał przepisy o ochronie danych osobowych i w zakresie jego statusu pozostaje dobór środków w tym procesie (w tym środków organizacyjnych oraz osób dokonujących czynności). Nie można także odmówić ADO możliwości zasięgnięcia specjalistycznego wsparcia w ocenie pracy samego ABI.

W szczególnych sytuacjach z odrębnych przepisów mogą wynikać kompetencje innych osób do zajmowania się zagadnieniami związanymi z ochroną danych osobowych w jednostce organizacyjnej (zob. 2.30).

Jednak działania innych osób wspierających ADO w realizacji obowiązków ochrony danych osobowych powinny następować w zgodzie z przepisami dotyczącymi ABI. Zdaniem sporządzającego opinię z tych przepisów wynikają trzy podstawowe warunki:

a) Dla ABI – w zakresie potrzebnym do realizacji jego zadań - powinna zostać zapewniona możliwość dostępu do informacji o czynnościach innych osób oraz ich oceny, przynajmniej w ramach dokonywanych przez niego sprawdzeń oraz realizowanego nadzoru nad dokumentacją przetwarzania danych osobowych.

b) Czynności innych osób nie mogą w pełnym zakresie powielać zadań ABI, ani prawnych form jego działania.

c) Inne osoby nie mogą ingerować (bezpośrednio lub pośrednio) w działalność ABI w sposób naruszający jego niezależność, co jednak nie wyklucza kierowania do ABI określonych postulatów, czy sugestii co do jego działalności, pod warunkiem, że następuje to w sposób nie naruszający niezależności ABI.

[relacja ABI - inne osoby wsparcia ochrony danych osobowych]

2.22 Do zadań ABI należy zapewnianie przestrzegania przepisów o ochronie danych osobowych, co w szczególności czyni poprzez sprawdzanie zgodności z przepisami o ochronie danych osobowych oraz nadzór nad dokumentacją przetwarzania danych. W zakres kompetencji ABI wchodzi zatem wszystkie działania podejmowane w jednostce organizacyjnej związane z wykonywaniem przepisów o ochronie danych osobowych. W tym celu przyznano ABI szczegółowe kompetencje do ustalania stanu faktycznego oraz zajmowania własnych stanowisk co do zgodności tego stanu z przepisami o ochronie danych osobowych. Swoje kompetencje ABI może również wykorzystywać względem innych osób zajmujących się ochroną danych osobowych w jednostce ADO. W szczególności może on przeprowadzić sprawdzenie odnoszące się do ich prac oraz nadzorować ich udział w tworzeniu czy wdrażaniu dokumentacji przetwarzania danych osobowych. Oczywiście najbardziej pożądanym scenariuszem jest współpraca ABI z takimi osobami w celu wypracowania optymalnych rozwiązań w zakresie ochrony danych osobowych.

[wyłączność realizacji zadań z art. 36a ust. 2 przez ABI]

2.23 O ile ADO może korzystać ze wsparcia innych osób w realizacji obowiązków ochrony danych osobowych, to już dyskusyjna pozostaje możliwość powielania przez nie działalności ABI. Gdy chodzi o prawne formy działania ABI określone w art. 36a ust. 2-3 i art. 36c u.o.d.o. oraz w rozporządzeniu MC (np. przeprowadzanie czynności

w sprawdzeniu i ich dokumentowanie, opracowywanie sprawozdania, prowadzenie rejestru zbioru danych osobowych) to są one zastrzeżone dla ABI, jeżeli został on powołany przez ADO. Inaczej ujmując, czynności ustawowo przewidziane dla ABI mogą być tylko przez niego przeprowadzane, a jedyny wyjątek w tym względzie ustawa czyni dla zastępcy ABI, gdy został on powołany (art. 36a ust. 6 u.o.d.o.). Jednak nawet gdy działania innych osób nie następują w prawnych formach przewidzianych dla ABI to dopuszczalność tych działań budzi wątpliwości, gdy w pełnym zakresie powielają one zadania ABI. Chodzi tutaj w szczególności o tworzenie komórek stale zajmujących się zgodnością z przepisami o ochronie danych osobowych lub przydzielanie tych zadań innym komórkom organizacyjnych (np. działowi prawnemu). Przykładowo, zadaniem takiej komórki może być stałe monitorowanie stanu przestrzegania przepisów o ochronie danych osobowych i na bieżąco informowanie kierownictwa jednostki organizacyjnej o potrzebnych działaniach w tym względzie.

Zdaniem autora niniejszej opinii, po to ustawodawca nie nałożył obowiązku powoływania ABI, ale przewidział możliwość wyboru alternatywnych opcji, tj. powołania ABI albo samodzielnego wykonywania przez ADO zadania zapewniania zgodności (art. 36b u.o.d.o.), aby ADO, który zamierza tworzyć „własne” struktury zajmujące się wykonaniem obowiązków ochrony danych osobowych uczynił to bez powoływania ABI, realizując nałożony na niego obowiązek, o którym mowa w art. 36b u.o.d.o. Ustawa natomiast nie przewidziała koniunkcji tych dwóch rozwiązań.

[zakaz naruszania niezależności ABI]

- 2.23** Działalność innych osób nie może w jakikolwiek sposób naruszać niezależności ABI. Zakazane pozostaje nie tylko wydawanie poleceń ABI, ale również pośrednia ingerencja taka jak zalecenia, wytyczne czy rekomendacje działań dla ABI. Wynika z tego, że działalność innych osób powinna być skierowana przede wszystkim wobec ADO i nakierowana na jego decyzje w przedmiocie wykonania przepisów o ochronie danych osobowych. Z drugiej strony zarówno dla ADO, jak i ABI może być korzystne dokonywanie oceny działalności ABI i formułowanie postulatów w tym zakresie, ponieważ może się to przyczyniać do polepszenia realizowania jego zadań, a co z tym związane do poprawy przestrzegania przepisów o ochronie danych osobowych. Jednak, jak już wspomniano powyżej, kierowanie postulatów (czy sugestii) wobec ABI nie może

naruszać jego niezależności. Wyznaczenie granicy takich działań wobec ABI jest więc niezwykle trudne i wymaga analizy “od przypadku do przypadku”.

[audyt wewnętrzny]

- 2.24** Przykładem określonej prawnej działalności polegającej na weryfikacji, która może również odnosić się do ochrony danych osobowych jest audyt wewnętrzny (art. 272 i n. u.f.p.). W szczególności audyt ten należy analizować pod kątem jego wpływu na działalność ABI pełniącego swoją funkcję w jednostkach sektora finansów publicznych oraz na jego niezależność.
- 2.25** Jak już wyżej wskazano audyt wewnętrzny jest działalnością niezależną i obiektywną, której celem jest wspieranie ministra kierującego działem lub kierownika jednostki w realizacji celów i zadań przez systematyczną ocenę kontroli zarządczej oraz czynności doradcze (art. 272 ust. 1 u.f.p.). Audyt wewnętrzny prowadzony jest albo przez audytora wewnętrznego zatrudnionego w jednostce albo przez usługodawcę niezatrudnionego w jednostce (art. 275 u.f.p.).
- 2.26** Audytor wewnętrzny ma w ramach prowadzonego audytu prawo wstępu do pomieszczeń jednostki oraz wglądu do wszelkich dokumentów, informacji i danych oraz do innych materiałów związanych z funkcjonowaniem jednostki, w tym do elektronicznych nośników danych. Audytor ma także prawo do sporządzania kopii, odpisów, wyciągów, zestawień lub wydruków, z zachowaniem przepisów o tajemnicy ustawowo chronionej (art. 282 ust. 2 u.f.p.). Ponadto pracownicy jednostki są obowiązani udzielać informacji i wyjaśnień, a także sporządzać kopie, odpisy, wyciągi lub zestawienia, o których mowa w ust. 2 (art. 282 ust. 3 u.f.p.). Z punktu widzenia ustawy o finansach publicznych obowiązki te spoczywają również na ABI, jeżeli jest pracownikiem danej jednostki organizacyjnej.
- 2.27** Zgodnie z § 17 ust. 1 rozporządzenia MF audytor wewnętrzny po przeprowadzeniu czynności audytowych uzgadnia pisemnie z audytowanym wstępne wyniki audytu, w tym w szczególności ustalenia i propozycje zaleceń.
- 2.28** Zgodnie z § 19 ust. 1 rozporządzenia MF kierownik komórki audytu wewnętrznego przekazuje sprawozdanie audytowanemu i kierownikowi jednostki. Następnie (ust. 2) audytowany w terminie 14 dni kalendarzowych od otrzymania sprawozdania, ustala sposób i termin realizacji zaleceń oraz wyznacza osoby odpowiedzialne za realizację

zaleceń, powiadamiając o tym na piśmie kierownika audytu wewnętrznego i kierownika jednostki. Zgodnie z § 2 pkt 5 rozporządzenia zalecenia to propozycje działań służących wyeliminowaniu słabości kontroli zarządczej lub usprawniających funkcjonowanie jednostki. W § 20 rozporządzenia MF określa się obowiązek audytora wewnętrznego do monitorowania realizacji zaleceń. Następnie po upływie realizacji zaleceń audytor przeprowadza czynności sprawdzające (§ 21 ust. 1 rozporządzenia MF). Wynik tych czynności sprawdzających audytor wewnętrzny przedstawia w notatce informacyjnej kierownikowi jednostki i audytowanemu.

- 2.29** Czynności audytowe mogą naruszać niezależność ABI w rozumieniu przedstawionym w pkt 2.8, gdy dotyczą audytowania wykonywanych przez niego zadań. Już same zalecenia stanowią ingerencję w realizację zadań przez ABI. Zalecenia zawarte w sprawozdaniu z audytu wewnętrznego są monitorowane przez audytora wewnętrznego, który po upływie terminu do realizacji zaleceń przeprowadza czynności sprawdzające. To kolejna ingerencja, której nie można pogodzić z niezależnością ABI. Ponadto, w przypadku gdy ABI odmówi wykonania zaleceń, to na podstawie §19 ust. 3 rozporządzenia MF będzie zobowiązany przedstawić pisemne stanowisko kierownikowi jednostki oraz audytorowi wewnętrznemu, podczas gdy formalnie ABI nie może w żaden sposób podlegać audytorowi wewnętrznemu. Wobec powyższego ustawowa gwarancja niezależności ABI stanowi ograniczenia przeprowadzania wobec niego audytu wewnętrznego.

[działanie wykonujące szczególne przepisy prawa]

- 2.30** Odrębnym zagadnieniem do omówienia są sytuacje, gdy działania innych osób oparte na szczególnych przepisach prawa dotyczą kwestii związanych z ochroną danych osobowych w jednostce organizacyjnej.

Przykładem jest audyt w zakresie bezpieczeństwa informacji dokonywany na podstawie § 20 ust. 2 pkt 14 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012 r., poz. 526) (rozporządzenie wykonawcze do ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne).

Zgodnie z tym przepisem zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie: “zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.”.

Przedmiotowy audyt może również objąć zabezpieczenia techniczne i organizacyjne określone w przepisach o ochronie danych osobowych, w tym dokumentację opracowaną na ich podstawie. Dane osobowe to bowiem jeden z rodzajów informacji prawnie chronionej.

W takich przypadkach osoba wykonująca odrębne przepisy w niezbędnym zakresie jest uprawniona dla potrzeb realizacji własnych zadań do weryfikacji spełnienia wymogów określonych w przepisach o ochronie danych osobowych. Za rozwiązanie wzorcowe należy uznać sytuację, gdy swoje działania dotyczące ochrony danych osobowych taka osoba wykonuje we współpracy z ABI.

III. REKOMENDACJE I WNIOSKI

3.1 Podstawową zasadą dotyczącą relacji ABI oraz innych osób w jednostce organizacyjnej jest niezależność ABI w zakresie wykonywanych zadań. Warunek niezależności ABI powinien być rozumiany w następujący sposób:

- a) Gwarancja zachowania niezależności dotyczy wykonywania czynności, o których mowa w art. 36a ust. 2 u.o.d.o.
- b) Niezależność obejmuje niezależność umysłu oraz niezależność wizerunku ABI.
- c) ABI realizuje swoje działania z art. 36a ust. 2 u.o.d.o w sposób samodzielny i bezstronny.
- d) Niezależność należy traktować jako wolność ABI od ingerencji z jakiegokolwiek strony oraz z jakiegokolwiek powodu.
- e) W szczególności wykonywanie zadań przez ABI nie może być uzależnione od wydawanych poleceń.
- f) Również inne działania niż polecenia, takie jak rekomendacje czy wskazówki mogą być traktowane jako naruszenie niezależności ABI, jeżeli wpływają na bezstronność ABI (wpływ pośredni).

g) Inne obowiązki ABI niż zadania ustawowe określone w art. 36a ust. 2 nie mogą naruszać niezależnego wykonywania tych zadań.

3.2 Bezpośrednią podległość ABI kierownikowi jednostki organizacyjnej należy odczytywać jako gwarancję niezależności ABI w wykonywaniu zadań, a nie jej ograniczenie. Bezpośrednia relacja ABI jedynie z kierownikiem uniezależnia ABI od innych zależności w jednostce organizacyjnej. Nie występuje również konflikt między podległością kierownikowi jednostki organizacyjnej a niezależnym wykonywaniem zadań przez ABI. W przypadku wykonywanych niezależnie zawodów lub funkcji w jednostce organizacyjnej kryterium ich realizacji – inne niż polecenie przełożonego – określają przepisy prawa.

3.3 Niezależność ABI nie może być naruszana przez kierownika jednostki organizacyjnej, ale także przez działające na jego polecenie inne komórki organizacyjne administratora danych oraz działające na jego zlecenie podmioty zewnętrzne (prawnicy, konsultanci itp.).

3.4 Na ADO, pomimo powołania przez niego ABI, spoczywają określone w przepisach prawa obowiązki ochrony danych osobowych oraz związana z nimi odpowiedzialność. W związku z tym to również ADO podejmuje decyzje co do wykonywania poszczególnych rodzajów obowiązków ochrony danych osobowych. W tym kontekście rola ABI sprowadza się do wsparcia ADO w realizacji tych obowiązków. Jednak ADO może skorzystać z innych możliwości wsparcia w wykonywaniu obowiązków ochrony danych: zarówno w sferze wewnętrznej (np. dział prawny), jak i z zewnątrz (konsultanci, audytorzy, prawnicy). ADO może także skorzystać z takich osób do oceny pracy ABI.

3.5 Korzystanie przez ADO ze wsparcia, o którym mowa w pkt 3.4 jest ograniczone następującymi warunkami:

a) Dla ABI powinna zostać zapewniona możliwość dostępu do informacji o czynnościach innych osób związanych z ochroną danych osobowych oraz dokonania

ich oceny, przynajmniej w ramach przeprowadzanych przez niego sprawdzeń oraz realizowanego nadzoru nad dokumentacją przetwarzania danych.

b) Czynności innych osób nie mogą w pełnym zakresie powielać zadań ABI, ani prawnych form jego działania.

c) Inne osoby nie mogą ingerować (bezpośrednio lub pośrednio) w działalność ABI w sposób naruszający jego niezależność, nie wyklucza to kierowania do ABI określonych postulatów, czy sugestii co do jego działalności, pod warunkiem, że następuje to w sposób nie naruszający niezależności ABI.

3.6 Przeprowadzanie audytu ABI w zakresie wykonywania jego zadań z art 36a ust. 2 u.o.d.o. przez audytora wewnętrznego w oparciu o przepisy o finansach publicznych, może naruszać niezależność ABI. W związku z tym audytor wewnętrzny powinien powstrzymać się od skierowanych wobec ABI działań, które stanowią ingerencję wkraczającą w sferę niezależności ABI.

3.7 W szczególnych sytuacjach z odrębnych przepisów mogą wynikać kompetencje innych osób do zajmowania się zagadnieniami związanymi z ochroną danych osobowych w jednostce organizacyjnej. Przykładem jest audyt w zakresie bezpieczeństwa informacji wykonywany na podstawie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne. W takich przypadkach osoba wykonująca odrębne przepisy w niezbędnym zakresie jest uprawniona dla potrzeb realizacji własnych zadań do weryfikacji spełnienia wymogów określonych w przepisach o ochronie danych osobowych. Za rozwiązanie wzorcowe należy uznać sytuację, gdy swoje działania dotyczące ochrony danych osobowych taka osoba wykonuje we współpracy z ABI.

dr Grzegorz Sibiga

Adwokat