



GENERALNY INSPEKTOR
OCHRONY DANYCH OSOBOWYCH
dr Edyta Bielak-Jomaa

DR107012118

Warszawa, dnia 2013-01-04

Pan
mec. Maciej Bobrowicz
Prezes
Krajowej Rady Radców Prawnych
Al. Ujazdowskie 41 lok 2
00-540 Warszawa

zwracam się do Pana Prezesa z uprzejmą prośbą o wyrażenie opinii w sprawie warunków dopuszczalności łączenia wykonywania zawodu radcy prawnego z funkcją:

- 1) administratora bezpieczeństwa informacji wykonywaną obecnie na podstawie art. 36a -36c ustawy o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922), zwanej dalej również „uodo”
- 2) inspektora ochrony danych, która będzie wykonywana w Polsce od 25 maja 2018 r. i która została określona w art. 37-39 rozporządzenia 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 (zwanego dalej rozporządzeniem ogólnym o ochronie danych lub „RODO”).

Moja prośba podyktowana jest potrzebą sformułowania i przekazania administratorom danych oraz administratorom bezpieczeństwa informacji przydatnych zaleceń i wskazówek w przedmiotowym zakresie oraz udzielania pomocy w rozstrzygnięciu związanych z tym zagadnieniem wątpliwości. Opinia samorządu radcowskiego będzie również nieocenioną pomocą dla wszystkich podmiotów przygotowujących się obecnie do stosowania od 25 maja 2018 r. przepisów rozporządzenia ogólnego o ochronie danych. Poniżej przedstawiam krótkie omówienie wyznaczników statusu oraz zadań administratora bezpieczeństwa informacji oraz inspektora ochrony danych oraz dostrzeżonych przeze mnie ułatwień i przeszkód w zakresie możliwości łączenia funkcji



20-LECIE PRAWA DO OCHRONY
DANYCH OSOBOWYCH W POLSCE

ul. Stawki 2, 00-193 Warszawa
tel 22 531-04-04
fax 22 531-04-00
www.gioudo.gov.pl

administratora bezpieczeństwa informacji (zwanego dalej również „ABI”) oraz inspektora ochrony danych (zwanego dalej również „IOD” lub „DPO” od „data protection officer”) z wykonywaniem zawodu radcy prawnego.

Znowelizowane przepisy ustawy o ochronie danych osobowych, które weszły w życie od 1 stycznia 2015 r. w zakresie dotyczącym administratorów bezpieczeństwa informacji nadały tej funkcji kluczowe znaczenie w zapewnianiu przestrzegania przepisów o ochronie danych osobowych u administratorów danych, którzy od tej daty zyskali uprawnienie powołania takiej osoby w swoich jednostkach organizacyjnych. Administrator bezpieczeństwa informacji stał się osobą odpowiedzialną za realizację zadań określonych w art. 36a ust. 2 ustawy o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922), w tym dokonywanie sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych, nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2 uodo, oraz przestrzegania zasad w niej określonych, zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych, a także prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych. Administratorzy bezpieczeństwa informacji zostali zobowiązani również do dokonywania sprawdzeń zgodności przetwarzania danych osobowych z przepisami prawa na zlecenie Generalnego Inspektora Ochrony Danych, w sytuacji przewidzianej w art. 19 b uodo.

Jednym z podstawowych kryteriów wyboru odpowiedniej osoby do pełnienia tej funkcji i jednocześnie warunkiem umożliwiającym wykonywanie funkcji jest **posiadanie odpowiedniej wiedzy w dziedzinie ochrony danych osobowych**. Ustawa o ochronie danych osobowych zobowiązuje administratorów danych do zapewnienia ABI niezależnego sprawowania funkcji i gwarantuje ABI wysoką pozycję w strukturze z organizacyjnej administratora danych. Zgodnie z art. 36a ust. 7 uodo, ABI **podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych**. Ponadto administrator danych zapewnia administratorowi bezpieczeństwa informacji, środki i organizacyjną odrębność niezbędne do **niezależnego wykonywania przez niego zadań** (art. 36a ust. 8 uodo). Administrator danych może powierzyć ABI **inne zadania jedynie wówczas, gdy nie naruszy to prawidłowego wykonania zadań ABI** (art. 36a ust. 4 uodo). Funkcję ABI mogą wykonywać zarówno osoby będące **pracownikami**

administratorów danych, jak i osoby, które zawarły z administratorem danych **umowę cywilnoprawną**.

Wprowadzone wspomnianą nowelizacją ustawy o ochronie danych osobowych rozwiązania polegające na określeniu zasad i warunków sprawowania przez ABI niezależnej wewnętrznej kontroli oraz wymogów, jakie musi on spełniać, stworzyło zarówno osobom pełniącym tę funkcję, jak i administratorom danych szansę na dobre przygotowanie się do stosowania dotyczących inspektora ochrony danych przepisów ogólnego rozporządzenia o ochronie danych. W okresie prac na nowelizacją ustawy o ochronie danych znany był projekt tej nowej unijnej regulacji, wobec czego wiele aspektów statusu i funkcji ABI jest zbliżone do rozwiązań przyjętych w RODO.

Od 25 maja 2018 r., czyli od dnia wejścia do stosowania RODO administratorów bezpieczeństwa informacji zastąpią inspektorzy ochrony danych, a we wszystkich państwach członkowskich Unii Europejskiej obowiązywać będą jednolite kryteria i procedury powołania tych osób, a także zasady dotyczące ich statusu i wykonywanych przez nich zadań. Ich rola w świetle RODO wykracza ponad to, co było przewidziane w Dyrektywie 95/46/WE i to, co przewidywały różne ustawodawstwa krajowe transponujące tę dyrektywę lub inne krajowe uregulowania sektorowe.

Ważną zmianą w stosunku do obecnego systemu fakultatywnego wyznaczania ABI, jest przewidziany przez RODO **obowiązek wyznaczenia inspektora ochrony danych przez określone kategorie administratorów danych**, ale także podmiotów przetwarzających (art. 37 ust. 1 RODO). Często podkreśla się, że dysponujący odpowiednią wiedzą i umiejętnościami inspektorzy mają odegrać kluczową rolę w zapewnieniu zgodności przetwarzania danych osobowych z nowymi unijnymi regulacjami prawnymi i stanowić fundament nowego, skutecznego systemu ochrony danych. Przy czym – co istotne - z rozporządzenia jasno wynika, że to **administrator lub podmiot przetwarzający zobowiązany jest do zapewnienia i udowodnienia zgodności przetwarzania danych osobowych z przepisami prawa** (art. 24 RODO). Przetwarzanie danych zgodne z RODO jest obowiązkiem administratora lub podmiotu przetwarzającego i to te podmioty ponoszą odpowiedzialność za ewentualne niezgodne z RODO działania.

W rozporządzeniu ogólnym o ochronie danych wymóg odpowiedniego fachowego przygotowania inspektora ochrony danych został doprecyzowany poprzez wskazanie w art. 37 ust. 5, że IOD ma **być wyznaczany na podstawie kwalifikacji zawodowych – a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności**

wypełnienia zadań, o których mowa w art. 37 ust. 5 RODO. Poziom wiedzy inspektora ma być ustalany w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają dane osobowe przetwarzane przez administratora lub podmiot przetwarzający (motyw 97 RODO).

W zakresie zadań inspektora ochrony danych art. 39 RODO wymienia na pierwszym miejscu informowanie i doradzanie w zakresie obowiązków ciążących na administratorze, podmiocie przetwarzającym i pracownikach oraz monitorowanie przestrzegania przepisów i polityk w dziedzinie ochrony danych osobowych. Również w Wytycznych Grupy art. 29 dotyczących inspektorów ochrony danych (WP 243)¹ wskazano, że priorytetem DPO powinno być zapewnienie przestrzegania rozporządzenia oraz odgrywanie kluczowej roli w zakresie wspierania „kultury ochrony danych” w ramach podmiotu oraz pomagania w implementacji niezbędnych elementów RODO, w tym zasad przetwarzania danych osobowych, praw osób, których dane dotyczą, ochrony danych w fazie projektowania oraz domyślnej ochrony danych, rejestru czynności przetwarzania, wymogów bezpieczeństwa przetwarzania i zgłoszenia naruszeń.

Ważną sferą działań doradczych i weryfikacyjnych inspektorów ochrony danych będzie przeprowadzanie oceny skutków dla ochrony danych. Zgodnie z art. 39 ust 1 lit. c RODO inspektor ma udzielać na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorować jej wykonanie zgodnie z art. 35 RODO.

Inspektor ochrony danych będzie miał także obowiązek współpracowania z organem nadzorczym, czyli GIODO. W przepisach określono, że inspektor ma pełnić **rolę punktu kontaktowego dla organu nadzorczego** w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach. Jak wskazuje Grupa Robocza art. 29 we wspomnianych Wytycznych² IOD ma pełnić funkcję punktu kontaktowego, by umożliwić organowi nadzorczemu dostęp do dokumentów i informacji w celu realizacji zadań, o których mowa w art. 57 RODO, jak również wykonywania uprawnień w zakresie prowadzonych postępowań, uprawnień naprawczych, uprawnień w zakresie wydawania zezwoleń oraz uprawnień doradczych, zgodnie z art. 58 RODO. Inspektor związany jest tajemnicą i poufnością dotyczącą wykonywania zadań DPO, zgodnie z prawem Unii lub prawem państwa członkowskiego (art. 38 ust. 5 RODO). Obowiązek ten - jak wskazuje Grupa Robocza art. 29 - nie wyłącza możliwości kontaktowania się inspektora

¹ Wytyczne dotyczące inspektorów ochrony danych ('DPO'), przyjęte w dniu 13 grudnia 2016 r., ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r., 16/EN (WP 243 rew.01), dostępne: <http://www.giudo.gov.pl/pl/1520296/10056>, str. 13.

² Tamże, str. 19.

z organem nadzorczym w celu uzyskania porady. Inspektor może konsultować się z organem nadzorczym we wszystkich sprawach, w stosownych przypadkach.

Do zadań inspektora należeć będzie również obowiązek pełnienia **funkcji punktu kontaktowego dla osób, których dane dotyczą**. Art. 38 ust. 4 RODO stanowi, że osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

Kwestia powierzania inspektorowi ochrony danych **innych obowiązków** niż związanych z ochroną danych osobowych została podobnie uregulowana jak w przypadku ABI. Art. 38 ust. 6 ogólnego rozporządzenia o ochronie danych stanowi, że IOD może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by **takie zadania i obowiązki nie powodowały konfliktu interesów**. Jak wskazuje Grupa Robocza art. 29 w Wytycznych „Wymóg niepowodowania konfliktu interesów jest ściśle związany z wymogiem wykonywania zadań w sposób niezależny. I choć DPO mogą posiadać inne zadania i obowiązki, to jednak te nie mogą powodować konfliktu interesów. Oznacza to, że DPO nie może zajmować w organizacji stanowiska pociągającego za sobą określanie sposobów i celów przetwarzania danych. Ze względu na indywidualny charakter każdej organizacji ten aspekt powinien być analizowany osobno dla każdego podmiotu.”³

Tak jak ABI, również inspektor ochrony danych ma **podlegać najwyższemu kierownictwu administratora lub podmiotu przetwarzającego**. Nie są zatem dopuszczalne sytuacje, w których inspektor podlega jakimkolwiek innym osobom lub podmiotom. Podległość najwyższemu kierownictwu jest jedną z gwarancji niezależnej, wysokiej pozycji inspektora ochrony danych w strukturze administratora danych. Ponadto takie umiejscowienie w strukturze organizacyjnej „skraca drogę raportowania”, co ma istotne znaczenie w razie konieczności podejmowania szybkich działań naprawczych w sytuacji naruszenia ochrony danych osobowych.

Inspektor ochrony danych **musi wykonywać swoją funkcję w sposób niezależny**. Motyw 97 ogólnego rozporządzenia o ochronie danych wskazuje, że inspektorzy ochrony danych – **bez względu na to, czy są pracownikami administratora, czy też wykonują swoje usługi na podstawie umowy o świadczenie usług** – powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny. Inspektor może zatem wykonywać swoją funkcję **na podstawie stosunku pracy lub „umowy o świadczenie usług zawartej z osobą fizyczną lub innym podmiotem spoza**

³ Tamże, str. 17.

*organizacji administratora/podmiotu przetwarzającego. W tym ostatnim przypadku konieczne jest, aby każdy członek podmiotu sprawującego funkcję DPO spełniał wszystkie odpowiednie wymogi wskazane w Sekcji 4 RODO (np. konieczne jest, aby każda z osób unikała konfliktu interesów). Równie ważne jest, aby każdą z tych osób objąć ochroną przewidzianą w przepisach RODO (np. aby nie miało miejsca nieuzasadnione rozwiązanie umowy o świadczenie usług w zakresie pełnienia funkcji DPO, ale również aby nie miało miejsca niezgodne z prawem zwolnienie osoby będącej członkiem podmiotu realizującego zadania DPO). Jednocześnie w pracy zespołowej można połączyć indywidualne atuty i umiejętności tak, aby zapewnić wydajniejszą obsługę swoich klientów.*⁴

RODO przewiduje również rozwiązanie, w którym **kilku administratorów danych wyznacza na swojego IOD jedną, tę samą osobę**. Jednego inspektora ochrony danych mogą wyznaczyć administratorzy danych tworzących grupę przedsiębiorstw, np. grupę kapitałową, o ile będzie można nawiązać z nim kontakt z każdej jednostki organizacyjnej (art. 37 ust. 2 RODO). Natomiast zgodnie z art. 37 ust. 3 RODO jednego inspektora będzie mogło powołać - przy uwzględnieniu ich struktury organizacyjnej i wielkości - kilku administratorów danych będących podmiotami publicznymi.

W art. 38 ust. 3 ogólnego rozporządzenia o ochronie danych wprowadzony został obowiązek zapewnienia przez administratorów danych i podmioty przetwarzające, aby inspektor ochrony danych **nie otrzymywał instrukcji co do wykonywania zadań**. Jedną z ważnych i nowych gwarancji niezależności inspektora ochrony danych jest również przepis, zgodnie z którym **inspektor nie może być ukarany lub odwołany za wypełnianie swoich zadań** (art. 38 ust. 3 ogólne rozporządzenie o ochronie danych).

Do ważnych, nowych rozwiązań w zakresie gwarancji niezależności inspektora należy nałożony wprost na administratorów danych i podmioty przetwarzające **obowiązek wspierania inspektora ochrony danych w wypełnianiu przez niego zadań**, m.in. zapewnienie inspektorowi dostępu do danych osobowych i operacji przetwarzania oraz wiedzy o każdej sprawie dotyczącej ochrony danych osobowych. Ten obowiązek ma zapobiegać próbom ograniczania inspektorowi ochrony danych dostępu do niezbędnych dla realizacji jego zadań informacji.

Inspektor związany jest **tajemnicą lub poufnością dotyczącą wykonywania swoich zadań**, zgodnie z prawem Unii lub prawem państwa członkowskiego (art. 38 ust. 5 RODO).

⁴ Tamże, str. 13.

Zestawiając powyższe uregulowania prawne dotyczące administratorów bezpieczeństwa informacji i inspektorów ochrony danych z normami prawnymi dotyczącymi wykonywania zawodu radcy prawnego można wskazać na kilka istotnych podobieństw.

Formy wykonywania zawodu radcy prawnego oraz gwarancje niezależności radcy prawnego zostały określone w ustawie z dnia 6 lipca 1982 r. o radcach prawnych (t.j. Dz. U. z 2017 r. poz. 1870), zwanej dalej „uorp”. Radca prawny może wykonywać zawód w kancelarii radcy prawnego, **w ramach stosunku pracy, na podstawie umowy cywilnoprawnej** oraz w spółce wskazanej w art. 8 ust. 1 pkt 1-3 uorp (art. 8 ust. 1 uorp). Wykonując zawód w ramach stosunku pracy, zajmuje samodzielne stanowisko **podległe bezpośrednio kierownikowi jednostki organizacyjnej** (art. 9. ust. 1 uorp).

Zgodnie z art. 13 uorp radca prawny **nie jest związany poleceniem co do treści opinii prawnej**. Kodeks Etyki Radcy Prawnego w art. 7 ust. 2 stanowi: „Radca prawny, przy wykonywaniu czynności zawodowych, powinien być **wolny od wszelkich wpływów** wynikających z jego osobistych interesów, nacisków z zewnątrz oraz ingerencji z jakiegokolwiek strony lub z jakiegokolwiek powodu. **Wyrażone przez kogokolwiek polecenia, ograniczające niezależność sugestie czy wskazówki, nie mogą wpływać na prezentowane przez niego stanowisko w sprawie**”.

Szczególną w stosunku do przepisów Kodeksu pracy formą ochrony trwałości stosunku pracy radcy prawnego jest tryb przewidziany w art. 19 ust. 1 ustawy o radcach prawnych. **Rozwiązanie stosunku pracy za wypowiedzeniem z radcą prawnym** przez jednostkę organizacyjną z powodu nienależytego wykonywania obowiązków radcy prawnego wynikających z przepisów ustawy o radcach prawnych może nastąpić **po uprzednim zasięgnięciu opinii rady okręgowej izby radców prawnych**.

Zarówno regulacje prawne dotyczące administratorów bezpieczeństwa informacji i inspektorów ochrony danych, jak i przepisy dotyczące wykonywania zawodu radcy prawnego nie zawierają wyraźnego zakazu łączenia funkcji administratora bezpieczeństwa informacji/inspektora ochrony danych z wykonywaniem zawodu radcy prawnego. Co do zasady można by zatem przyjąć - zarówno na gruncie ustawy o ochronie danych osobowych, jak i ogólnego rozporządzenia o ochronie danych - dopuszczalność łączenia obu funkcji z wykonywaniem zawodu radcy prawnego. Niemniej biorąc pod uwagę zarówno różne formy wykonywania zawodu radcy prawnego, jak i

mogący wystąpić konflikt interesów niewątpliwie kwestię tę należałoby zapewne rozważyć szczegółowo w każdej konkretnej sytuacji.

Wiele w tym zakresie może zależeć od formy prawnej wykonywania zawodu radcy prawnego i rodzaju stosunku prawnego, na podstawie którego radca prawny pełniłby funkcję ABI (IOD). Inaczej sytuacja może przedstawiać się w sytuacji ABI/IOD pełniącego funkcję w ramach stosunku pracy łączącego go z administratorem danych, inaczej w sytuacji wykonywania tej funkcji w modelu outsourcingu, zwłaszcza wówczas, gdy osoba taka jednocześnie obsługuje wielu administratorów danych.

Grupa Robocza art. 29 we wspomnianych Wytycznych dotyczących inspektorów ochrony danych wskazuje w odniesieniu do konfliktu interesów, o którym mowa w art. 38 ust. 6 RODO, że konflikt interesów może powstać, gdy zewnętrzny DPO zostanie poproszony o reprezentowanie administratora lub podmiotu przetwarzającego przed sądem w sprawie dotyczącej ochrony danych osobowych⁵.

W przypadku ABI/IOD, którego łączy z administratorem danych umowa cywilnoprawna może pojawić się problem pogodzenia kwestii odpowiedzialności radcy prawnego z tytułu nienależytego wykonania umowy oraz zasady przyjętej w RODO, że DPO nie jest podmiotem, który ponosi odpowiedzialność w przypadkach naruszenia RODO. Na podstawie art. 471 Kodeksu cywilnego radcy prawni w przypadku stosunku umownego odpowiadają wobec klientów za szkody wyrządzone wskutek niewykonania lub nienależytego wykonania zobowiązania. Natomiast jak wskazuje Grupa Robocza art. 29 w odniesieniu do zadania inspektora ochrony danych określonego w art. 39 ust. 1 lit b RODO monitorowanie nie oznacza osobistej odpowiedzialności DPO w przypadkach naruszenia RODO⁶. Z rozporządzenia wynika, iż to administrator, a nie DPO „wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać” (art. 24 ust. 1 RODO). Grupa Robocza art. 29 podkreśla, że spełnianie wymogów rozporządzenia należy do obowiązków korporacyjnych administratora, a nie DPO.

Często wskazuje się też na prawdopodobieństwo wystąpienia konfliktu interesów w sytuacji obsługiwanego przez jednego zewnętrznego ABI/IOD kilku podmiotów, np. w ramach grupy przedsiębiorstw, w szczególności wówczas, gdy zachodzi sprzeczność pomiędzy interesem grupy a

⁵ Tamże, str. 17.

⁶ Tamże, str. 18

poszczególnymi przedsiębiorstwami (administratorami danych) wchodzącymi w jej skład, np. w przypadku występowania istotnych różnic w zakresie charakteru, zakresu, kontekstu i celów przetwarzania oraz związanego z tym ryzyka naruszenia praw i wolności osób, których dane są przetwarzane.

Jednakże w mojej ocenie należy w tym zakresie w pełni oczekiwać, że radcy prawni - jako osoby mające do tego najlepsze kwalifikacje - będą odpowiednio wcześniej identyfikować ryzyko wystąpienia takiego konfliktu i jemu zapobiegać. Radcy prawni mają bowiem obowiązek dokonywania oceny konfliktu interesów w każdym czasie, tj. stałego monitorowania możliwości zaistnienia konfliktu, co ma istotne znaczenie, ponieważ przyczyny zaistnienia konfliktu mogą być bardzo różne i występować również w późniejszym czasie. Art. 15 ustawy o radcach prawnych zobowiązuje radcę do wyłączenia się od wykonania czynności zawodowych we własnej sprawie lub jeżeli przeciwnikiem jednostki organizacyjnej udzielającej mu pełnomocnictwa jest inna zatrudniająca go jednostka organizacyjna albo jeżeli sprawa dotyczy osoby, z którą pozostaje on w takim stosunku, że może to oddziaływać na wynik sprawy. Obowiązki w tym zakresie przewiduje również Kodeks Etyki Radców Prawnych. Art. 10 KERP wskazuje, że obowiązek unikania przez radcę prawnego konfliktu interesów służy zapewnieniu mu niezależności, a także dochowaniu tajemnicy zawodowej oraz lojalności wobec klienta. Zgodnie natomiast z art. 26 ust. 1 KERP radca prawny nie może świadczyć pomocy prawnej, jeżeli wykonywanie czynności zawodowych naruszałoby tajemnicę zawodową lub stwarzało znaczne zagrożenie jej naruszenia, ograniczenia jego niezależności, albo gdy posiadana przez niego wiedza o sprawach innego klienta lub osób, na rzecz których uprzednio wykonywał czynności zawodowe, dawałaby klientowi nieuzasadnioną przewagę. Jeżeli okoliczności, o których mowa w ust. 1, ujawnią się w czasie prowadzenia sprawy, radca prawny obowiązany jest się z niej wyłączyć, a w szczególności wypowiedzieć klientowi pełnomocnictwo (ust. 2).

Warto również nadmienić, że wysuwane są również obawy co do pełnej możliwości pogodzenia funkcji, w którą wpisana jest rola punktu kontaktowego dla organu nadzorczego z obowiązkiem radców prawnych przewidzianym z zasadą lojalności i zaufania. Zgodnie z art. 8 KERP, radca prawny, świadcząc klientowi pomoc prawną, postępuje lojalnie i kieruje się dobrem klienta w celu ochrony jego praw, natomiast art. 45 KERP stosunki pomiędzy radcą prawnym a klientem powinny być oparte na zaufaniu. Rzeczywiście zgodnie z RODO w rolę inspektora ochrony danych wpisany jest obowiązek przekazywania organowi nadzorczemu informacji, nawet wówczas,

gdy informacje te mogą wskazywać na niezgodne z RODO działania administratora lub podmiotu przetwarzającego. Jak już wspomniano, IOD ma pełnić funkcję punktu kontaktowego, by umożliwić organowi nadzorcemu dostęp do dokumentów i informacji w celu realizacji zadań, o których mowa w art. 57 RODO, jak również wykonywania uprawnień w zakresie prowadzonych postępowań, uprawnień naprawczych, uprawnień w zakresie wydawania zezwoleń oraz uprawnień doradczych, zgodnie z art. 58 RODO. Inspektor związany jest tajemnicą i poufnością dotyczącą wykonywania zadań DPO, zgodnie z prawem Unii lub prawem państwa członkowskiego (art. 38 ust. 5 RODO), jednakże obowiązek ten nie dotyczy kontaktów z organem nadzorczym.

W ocenie Generalnego Inspektora Ochrony Danych Osobowych powyższe obawy należy jednak uznać za nieuzasadnione. Realizowanie obowiązku współpracy z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego powinno być postrzegane jako element konsekwentnych i rzetelnych działań radcy prawnego na rzecz interesów klienta. W odniesieniu do zasady lojalności wskazuje się, że *„na podstawie zasady zaufania należy uzupełnić lojalność wobec klienta o jej drugi aspekt, czyli zaufanie rozumiane w sposób generalny, a więc o zaufanie publiczne. Z reguły wymogi ochrony tych stosunków zaufania (generalnych i indywidualnych) nie będą ze sobą sprzeczne, ale często będzie miała miejsce również sytuacja odwrotna, w szczególności wówczas, gdy klient będzie oczekiwał od prawnika działań contra lub praeter legem. Zasada zaufania rozumiana jako ochrona zaufania publicznego do zawodu powinna wtedy posiadać pierwszeństwo i ograniczyć dopuszczalne działania na rzecz klienta. Jest więc ona pierwszym i podstawowym źródłem ograniczeń zasady lojalności. Z drugiej strony, skoro zaufanie między prawnikiem a klientem jest nie tylko stosunkiem faktycznym, ale również regulowanym przez normy etyki zawodowej, to można powiedzieć, że ma ono charakter „stosunku etycznego”. Należy pamiętać, że na tak rozumiane stosunki nakładają się także różnego rodzaju stosunki prawne, w szczególności zobowiązaniowe oraz procesowe”⁷*. Warto dodać, że obowiązek współpracy z organem nadzorczym w ramach wykonywania przez niego swoich zadań nałożony jest również – na mocy art. 31 RODO - na administratora i podmiot przetwarzający.

Wskazuję również, że administrator lub podmiot przetwarzający rozważając wyznaczenie radcy prawnego do pełnienia funkcji ABI/inspektora ochrony danych musi zapewnić mu realną możliwość efektywnego wykonywania jego zadań, w tym odpowiednie zasoby czasu na

⁷ Lojalność wobec klienta jako zasada etyki prawniczej i jej granice w: Etyka prawnicza. Stanowiska i perspektywy 2, str. 87-107, LexisNexis, r. 2011 (*Esej lub rozdział w książce*).

wywiązanie się ze wszystkich nałożonych na niego zadań i obowiązków. Zarówno w przypadku administratora bezpieczeństwa informacji, jak i inspektora ochrony danych, powierzanie innych obowiązków niż te związane z ochroną danych osobowych dopuszczalne jest jedynie wtedy, gdy obowiązki takie nie naruszają prawidłowego wykonywania funkcji ABI (nie będą powodowały konfliktu interesów).

W kontekście zadań inspektora ochrony danych wskazanych w art. 39 RODO (i omówionych uprzednio w niniejszym piśmie) istotnym i wymagającym analizy zagadnieniem może być również zakaz polecania radcy prawnemu wykonywania czynności wykraczających poza zakres pomocy prawnej (w art. 9 ust. 4. ustawy o radcach prawnych), w szczególności w kontekście art. 6 i 7 ustawy o radcach prawnych wskazujących, na czym polega zawód radcy prawnego i pomoc prawna.

Mając powyższe na uwadze uprzejmie proszę o przedstawienie opinii Samorządu Radcowskiego w zakresie wskazanych zagadnień. W przypadku uznania, że łączenie wykonywania zawodu radcy prawnego z funkcją administratora bezpieczeństwa informacji i inspektora ochrony danych jest dopuszczalne będziemy wdzięczni za określenie warunków, jakie powinny być w takich sytuacjach spełnione oraz ewentualnie wskazanie sytuacji, które mogą wykluczać łączenie wymienionych funkcji z wykonywaniem zawodu radcy prawnego. Proszę również o przekazanie wszelkich innych wskazówek, jakie byłyby pomocne zainteresowanym podmiotom w przestrzeganiu obowiązujących w tym zakresie przepisów prawa.

Jednocześnie informuję, że wystąpiłam również do Prezesa Naczelnej Rady Adwokackiej z prośbą o przedstawienie opinii dotyczącej dopuszczalności pełnienia funkcji administratora bezpieczeństwa informacji/inspektora ochrony danych z wykonywaniem zawodu adwokata.