



**GENERALNY INSPEKTOR
OCHRONY DANYCH OSOBOWYCH**
dr Edyta Bielak-Jomaa

PRIOTYBILNE

Warszawa, dnia 2013-09-04

Pan
mec. Jacek Trela
Prezes
Naczelnej Rady Adwokackiej
ul. Świętojerska 16
00-202 Warszawa

zwracam się do Pana Prezesa z uprzejmą prośbą o wyrażenie opinii w sprawie dopuszczalności łączenia wykonywania zawodu adwokata 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 stanowiska w przedmiotowym zakresie oraz udzielenia pomocy w rozstrzygnięciu związanych z tym zagadnieniem wątpliwości, w szczególności w obliczu bliskiego terminu wejścia do stosowania rozporządzenia ogólnego o ochronie danych.

Poniżej przedstawiam krótkie omówienie wyznaczników statusu oraz zadań administratora bezpieczeństwa informacji oraz inspektora ochrony danych, a także argumentów, które w mojej



**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

ocenie przemawiają za uznaniem, że nie jest dopuszczalne łączenie funkcji administratora bezpieczeństwa informacji (zwanego dalej również „ABI”) oraz inspektora ochrony danych (zwanego dalej również „IOD” lub „DPO” od „data protection officer”) z wykonywaniem zawodu adwokata.

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 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). Obowiązek ten - jak wskazuje Grupa Robocza art. 29 - nie wyłącza możliwości kontaktowania się inspektora 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

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.giodo.gov.pl/pl/1520296/10056>, str. 13.

² Tamże, str. 19).

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 ABl. 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 ABl, 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 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

³ Tamże, str. 17.

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).

Biorąc pod uwagę powyższe uregulowania prawne oraz odnosząc się do kwestii dopuszczalności jednoczesnego wykonywania zawodu adwokata oraz funkcji administratora bezpieczeństwa informacji/inspektora ochrony danych należy wskazać, że najczęściej wskazywaną przeszkodą dla takiego rozwiązania jest zasada bezpośredniej podległości ABI/IOD kierownictwu

⁴ Tamże, str. 13.

(najwyższemu kierownictwu) administratora danych (lub w przypadku IOD – również podmiotu przetwarzającego). Ze względu na brzmienie art. 1 ust. 3 ustawy z dnia 26 maja 1982 r. Prawo o adwokaturze (Dz. U. z 2016 r. poz. 1999 z późn. zm), zgodnie z którym adwokat w wykonywaniu swoich obowiązków zawodowych podlega tylko ustawom oraz brzmienie § 9 ust. 1 b Kodeksu Etyki Adwokackiej, zgodnie z którym z zawodem adwokata nie wolno łączyć takich zajęć, które ograniczałyby niezawisłość adwokata należałoby uznać, iż adwokat nie może pełnić funkcji administratora bezpieczeństwa informacji, jak również funkcji inspektora ochrony danych.

Ponadto w § 9 ust. 4 Kodeksu Etyki Adwokackiej wśród funkcji, które może pełnić adwokat, uznanych za zgodne z etyką adwokata funkcja ABI nie została wskazana: *„Za zgodne z etyką zawodową uznaje się wykonywanie przez adwokata funkcji syndyka, podejmowanie czynności nadzorcy sądowego, likwidatora i zarządcy działającego na podstawie ustawy Prawo upadłościowe i naprawcze, pełnienie funkcji kuratora we władzach fundacji, w radach nadzorczych, zarządach spółdzielni mieszkaniowych i innych, a także pełnienie obowiązków członka zarządu i prokurenta spółek prawa handlowego z zastrzeżeniem przepisów powyższych, a także dotyczących zasad ochrony tajemnicy adwokackiej. W trakcie pełnienia powyższych funkcji, adwokata obowiązuje stosowanie się do przepisów niniejszych zasad.”*

Ponadto należy mieć również na uwadze art. 4b ust. 1 pkt 1 ustawy z dnia 26 maja 1982 r. Prawo o adwokaturze. (t.j. Dz. U. z 2016 r. poz. 1999 z późn. zm.) w którym został ustanowiony zakaz wykonywania przez adwokata zawodu, jeżeli pozostaje w stosunku pracy. Jedną z cech stosunku pracy jest podległość służbowa.

Niezależność adwokatów podkreślana jest również w orzecznictwie sądowym: *„Adwokat w wykonywaniu swoich obowiązków zawodowych podlega tylko ustawom. Regulacja ta dotyczy wolności zawodu adwokata, jego gwarancji, a co się z tym wiąże - z niezależnością zawodową. Adwokat odpowiada osobiście za podejmowane czynności zawodowe, gdyż korzysta z pełnej swobody i niezależności. Adwokat zawsze wykonuje swoje czynności zawodowe samodzielnie i niezależnie. Nie ma znaczenia, czy źródłem umocowania jest umowa z klientem, czy orzeczenie sądu lub Okręgowej Rady Adwokackiej. Wskazania lub instrukcje, dotyczące merytorycznego prowadzenia zleconej sprawy, udzielane adwokatowi przez jego mocodawcę lub osobę na rzecz, której wykonuje czynności zawodowe, nie są dla adwokata wiążące. Brak związania adwokata treścią wskazań strony nie oznacza oczywiście, by jego czynności nie były zgodne z oczekiwaniami klienta.”* (Wyrok Sądu Apelacyjnego w Krakowie z dnia 22 marca 2016 r. I ACa 1762/15).

Mając powyższe na uwadze uprzejmie proszę o wyrażenie opinii co do prawidłowości powyższego stanowiska. Jednocześnie uprzejmie informuję, że wystąpiłam również do Prezesa Krajowej Rady Radców Prawnych z prośbą o przedstawienie opinii dotyczącej dopuszczalności pełnienia funkcji administratora bezpieczeństwa informacji/inspektora ochrony danych z wykonywaniem zawodu radcy prawnego.