Jakie gwarancje niezależności zostały przyznane IOD w przepisach RODO?

Inspektorzy ochrony danych – bez względu na to, czy są pracownikami administratora, czy też nie – powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny (motyw 97 RODO).

W celu zapewnienia niezależności inspektorowi ochrony danych ogólne rozporządzenie o ochronie danych, wprowadza kilka szczegółowych rozwiązań, które pozwalają na osiągnięcie ww. celu, a mianowicie:

a) bezpośrednia podległość IOD najwyższemu kierownictwu,

b) wspieranie IOD w wypełnianiu jego zadań,

c) zapewnienie udziału IOD we wszystkich zagadnieniach związanych z ochroną danych osobowych,

d) zakaz wydawania instrukcji IOD co do wykonywania przez niego zadań,

e) unikanie konfliktu interesów IOD,

f) zakaz odwoływania i karania IOD,

g) obowiązek zachowania tajemnicy lub poufności co do wykonywania zadań przez IOD,

Jako dobrą praktykę Grupa Robocza art. 29 w swoich wytycznych dotyczących IOD, wskazuje wprowadzenie wewnętrznych regulacji (regulaminów, statutów) gwarantujących inspektorowi ochrony danych niezależność w wykonywaniu przez niego zadań.

a) bezpośrednia podległość IOD najwyższemu kierownictwu

Jednym ze szczegółowych rozwiązań służących niezależności IOD jest umieszczenie go w strukturze organizacyjnej administratora danych lub podmiotu przetwarzającego bezpośrednio pod najwyższym kierownictwem. Zgodnie z art. 38 ust. 3 RODO IOD podlega bezpośrednio najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.

Podległość najwyższemu kierownictwu jest jedną z gwarancji niezależnej, wysokiej pozycji inspektora ochrony danych w strukturze administratora danych, a ponadto skraca drogę raportowania, co ma istotne znaczenie w razie konieczności podejmowania szybkich działań naprawczych w sytuacji naruszenia ochrony danych osobowych.

Bezpośrednia podległość oznacza, że w ramach podejmowanych przez siebie czynności IOD nie może podlegać jakimkolwiek innym osobom lub jednostkom organizacyjnym wchodzącym w skład struktury administratora danych (art. 38 ust. 3 RODO).

Sposób rozumienia terminu najwyższe kierownictwo na pewno zależy od typu podmiotu jakim jest administrator lub podmiot przetwarzający. Tytułem przykładu wskazać można, że „najwyższym kierownictwem” będzie osoba lub osoby wchodzące w skład organu, które kierują jej pracami (ministrowie kierujący działami administracji rządowej, dyrektorzy szkół), albo prowadzą jej sprawy (zarząd spółki, wspólnicy spółki jawnej, właściciel jednoosobowej działalności gospodarczej).

b) wspieranie IOD w wypełnianiu jego zadań

Administrator danych i podmiot przetwarzający są zobowiązani do wspierania inspektora ochrony danych poprzez m.in. zapewnienie mu zasobów niezbędnych do wykonania tych zadań.

Grupa Robocza art. 29 w Wytycznych dotyczących inspektora ochrony danych opowiada się za szerokim rozumieniem zasobów:
- wsparcie IOD ze strony kadry kierowniczej (np. na poziomie zarządu),
- wymiar czasu umożliwiający IOD wykonywanie zadań,
- odpowiednie wsparcie finansowe, infrastrukturalne (pomieszczenia, sprzęt, wyposażenie) i kadrowe, gdy to właściwe,
- oficjalne zakomunikowanie wszystkim pracownikom faktu wyznaczenia IOD i jego zadaniach,
- umożliwienie dostępu do innych działów organizacji, np. HR, działu prawnego, IT itd.
- ciągłe szkolenie. DPO powinien mieć możliwość ciągłego aktualizowania wiedzy z zakresu ochrony danych osobowych. Celem powinno być zwiększanie wiedzy DPO i zachęcanie go do udziału w szkoleniach, warsztatach, forach poświęconych ochronie danych etc.;
- wsparcie kadrowe, np. powołanie zespołu inspektora ochrony danych.

c) zapewnienie udziału IOD we wszystkich zagadnieniach związanych z ochroną danych osobowych

Artykuł 38 RODO zobowiązuje administratora oraz podmiot przetwarzający do zapewnienia, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych. Norma ta ma zapobiegać próbom ograniczania inspektorowi dostępu do niezbędnych dla realizacji jego zadań informacji, a tym samym sprzyja zachowaniu jego niezależności.

Zgodnie z Wytycznymi Grupy Roboczej art. 29 dotyczącymi inspektora ochrony danych niezwykle istotne jest, by IOD był zaangażowany od najwcześniejszego etapu we wszystkie kwestie związane z przetwarzaniem danych osobowych, ponieważ ułatwi to zapewnienie zgodności z RODO. Przepisy ogólnego rozporządzenia o ochronie danych w określonych przypadkach wprost nakazują administratorowi angażowanie IOD w podejmowanie określonych czynności i decyzji, np. nakazują administratorowi konsultowanie się z IOD przy okazji dokonywania takiej oceny skutków. W związku z tym angażowanie inspektora ochrony danych we wszelkie kwestie związane z ich przetwarzaniem powinno być standardową procedurą w organizacji.

Ponadto IOD powinien być postrzegany jako partner w dyskusji i powinien być włączany w prace grup roboczych poświęconych procesom związanym z przetwarzaniem danych osobowych w ramach organizacji. Należy zapewnić mu między innymi: udział w spotkaniach przedstawicieli wyższego i średniego szczebla organizacji, uczestnictwo przy podejmowaniu kluczowych decyzji dotyczących przetwarzania danych osobowych wraz z odpowiednio wcześniejszym udostępnieniem IOD informacji umożliwiających zajęcie mu stanowiska, natychmiastowe konsultowanie się z nim w przypadku stwierdzenia naruszenia albo innego zdarzenia związanego z danymi osobowymi, określenie przez administratora lub podmiot przetwarzający innych przypadków, które wymagają konsultacji z IOD.

Ponadto stanowisko IOD powinno być zawsze brane pod uwagę przez kierownictwo oraz pracowników danego podmiotu. Grupa Robocza art. 29 zaleca, aby w ramach

dobrych praktyk, dokumentować przypadki i powody postępowania niezgodnego z zaleceniem IOD.

d) zakaz wydawania instrukcji IOD co do wykonywania przez niego zadań

Istotną gwarancją w zakresie niezależności inspektora ochrony danych jest niewątpliwie wprowadzenie zakazu wydawania przez administratora lub podmiotu przetwarzającego instrukcji (poleceń) dla IOD dotyczących wykonywania przez niego zadań (art. 38 ust. 3 RODO). Zakaz wydawania instrukcji inspektorowi ochrony danych, oznacza, że w ramach wypełniania swoich zadań inspektor ochrony danych, nie może otrzymywać poleceń dotyczących sposobu załatwienia sprawy, środków jakie mają zostać podjęte, czy też celu jaki powinien zostać osiągnięty. Ponadto, administrator nie powinien uniemożliwiać, bądź ograniczać inspektorowi ochrony danych kontaktu z Prezesa Urzędu Ochrony Danych Osobowych.

W Wytycznych dotyczących inspektora ochrony danych Grupa Robocza art. 29 wskazuje, że IOD nie może również zostać zobligowany do przyjęcia określonego stanowiska w sprawie z zakresu prawa ochrony danych, w tym określonej wykładni przepisów.

Z drugiej strony Grupa Robocza art. 29 podkreśla, że niezależność IOD (w tym również w kontekście zakazu do wydawania instrukcji, co do wykonywania zadań IOD) nie oznacza, iż IOD posiada uprawnienia decyzyjne wykraczające poza zadania z art. 39 RODO. Nie zmienia to faktu, że za zapewnienie zgodności z przepisami o ochronie danych osobowych i wykazanie zgodności odpowiedzialni są administrator i podmiot przetwarzający. W sytuacji podjęcia przez administratora lub podmiot przetwarzający decyzji niezgodnej z przepisami RODO i zaleceniami IOD, inspektor ochrony danych powinien mieć możliwość jasnego przedstawienia swojego stanowiska osobom podejmującym decyzję.

Respektowanie powyższego zakazu może być szczególnie problematyczne na styku wykonywania wewnętrznego audytu różnych sfer działalności podmiotu będącego administratorem danych. Szczególnie ważne, zwłaszcza na początku funkcjonowania omawianego przepisu, może być dokonanie wnikliwej analizy zakresu i celów poszczególnych stanowisk związanych z wewnętrznym audytem, tak aby inne osoby wewnątrz organizacji np. prawnicy, audytorzy mogli realizować swoje zadania, nie naruszając przedmiotowego zakazu.

e) unikanie konfliktu interesów IOD

Zgodnie z art. 38 ust. 6 RODO, istnieje możliwość nakładania na inspektora ochrony danych innych zadań i obowiązków, ale administrator i podmiot przetwarzający muszą zapewnić by nie powodowało to konfliktu interesów. Zatem jak wyjaśnia Grupa Robocza art. 29 w Wytycznych dotyczących inspektora ochrony danych oznacza to m.in., że IOD nie może zajmować w organizacji stanowiska związanego z określaniem sposobów i celów przetwarzania danych. Aspekt ten powinien być analizowany osobno i indywidualne dla każdego podmiotu. Powierzając inspektorowi ochrony danych inne zadania, w celu uniknięcia konfliktu interesów administrator danych lub podmiot przetwarzających, powinni w swojej organizacji zidentyfikować stanowiska niekompatybilne z pełnieniem funkcji IOD.

Cenną podpowiedzią w tym zakresie jest wskazanie, że co do zasady, za powodujące konflikt interesów uważane będą stanowiska kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT), ale również

niższe stanowiska, jeśli biorą udział w określaniu celów i sposobów przetwarzania danych. Ponadto konflikt interesów może powstać wówczas, gdy zewnętrzny IOD zostanie poproszony o reprezentowanie administratora lub podmiotu przetwarzającego przed sądem w sprawie dotyczącej ochrony danych osobowych.

Wskazane byłoby też opracowanie wewnętrznej polityki określającej stanowiska będące w konflikcie interesów oraz opracowanie generalnego dokumentu dotyczącego konfliktu interesów. Ponadto administrator lub podmiot przetwarzający powinni wprowadzić odpowiednie zabezpieczenia do wewnętrznych zasad organizacji celem zapewnienia, by ogłoszenia o rekrutacji na stanowisko inspektora ochrony danych były sformułowane w jasny, precyzyjny sposób i niwelowały ryzyko powstania konfliktu interesów.

f) zakaz odwoływania i karania IOD

Zachowanie niezależności przez inspektora ochrony danych wspiera również art. 38 ust 3 RODO, stanowiący, że administrator lub podmiot przetwarzający nie może odwołać ani karać IOD za wypełnianie przez niego zadań. Oczywiście przepis ten należy odnosić do obiektywnie prawidłowego wykonywania zadań. Nie chodzi tu o ochronę inspektora, który nie wywiązuje się należycie ze swoich zadań. Jest to jedyny przepis w ogólnym rozporządzeniu o ochronie danych dotyczący odwołania IOD.

Zgodnie z Wytycznymi Grupy Roboczej art. 29 dotyczącymi inspektora ochrony danych inspektor nie może zostać odwołany ani ukarany za udzielenie określonego zalecenia, nawet jeśli jest ono niezgodne ze stanowiskiem reprezentowanym przez administratora lub podmiot przetwarzający. Grupa Robocza art. 29 wyjaśnia, że chodzi tu o kary w różnych formach, bezpośrednie albo pośrednie, np. brak albo opóźnienie awansu, utrudnienie rozwoju zawodowego, ograniczenie dostępu do korzyści oferowanych pozostałym pracownikom. Zakaz odwoływania inspektora ochrony danych, nie oznacza natomiast, że IOD nie może zostać odwołany w uzasadnionych sytuacjach z przyczyn innych niż wykonywanie swoich obowiązków (np. z powodu kradzieży). Grupa Robocza art. 29 zaleca stosowanie polityki, że im stabilniejsza podstawa zatrudnienia i szerszy zakres ochrony inspektora ochrony danych przed odwołaniem, tym większa szansa na wykonywanie przez IOD zadań w sposób niezależny.

g) obowiązek zachowania tajemnicy lub poufności co do wykonywania zadań przez IOD

IOD jest zobowiązany do zachowania tajemnicy lub poufności, co do wykonywania swoich zadań zgodnie z prawem Unii lub państwa członkowskiego (art. 38 ust. 5 RODO).

Jeśli chodzi o IOD, to w związku z wykonywaniem swoich zadań będzie on miał niewątpliwie dostęp do danych osobowych, w tym danych osobowych, o których mowa w art. 9 ust. 1 RODO oraz danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o których mowa w art. 10 RODO, jak również informacji dotyczących środków technicznych i organizacyjnych zapewniających przetwarzanie zgodne z przepisami RODO, w tym polityk ochrony danych. IOD będzie również zobowiązany do przestrzegania wszystkich przepisów prawa krajowego i unijnego, które będą miały do niego zastosowanie i na mocy których, określone informacje objęte są prawnie chronionymi tajemnicami. Zobowiązanie inspektora ochrony danych do przestrzegania tajemnicy jest w pełni uzasadnione i służyć będzie nie tylko bezpieczeństwu danych osobowych, ale i wzmocnieniu

zaufania do inspektorów ze strony administratorów danych i podmiotów przetwarzających. Co ważne - w Wytycznych dotyczących inspektora ochrony danych Grupa Robocza art. 29 podkreśla, że obowiązek zachowania tajemnicy oraz poufności nie uniemożliwia IOD kontaktu z Prezesem Urzędu Ochrony Danych Osobowych i zasięgania jego opinii.

2019-02-11 

- **Urząd Ochrony Danych Osobowych**

ul. Stawki 2, 00-193 Warszawa