UODO sprawdza jak pracuje IOD – czyli o co chodzi z listą 27 pytań

Prezes Urzędu Ochrony Danych Osobowych opublikował dnia 30.03.2022 r. listę pytań jakie zamierza skierować do administratorów oraz podmiotów przetwarzających w zakresie ustalenia poprawności powołania Inspektora Ochrony Danych (IOD) oraz prawidłowości wykonywanych przez niego zadań.

Jak podaje UODO w swoim komunikacie, prowadzone przez niego od początku obowiązywania RODO postępowania, często inicjowane na skutek zgłaszanych przypadków nieprzestrzegania przepisów dotyczących inspektorów ochrony danych, posłużyły mu do opracowania listy zagadnień, do których teraz będą musieli odnieść się wezwani przez Prezesa UODO administratorzy lub podmioty przetwarzające. Urząd chce w ten sposób sprawdzić czy podmioty te należycie przestrzegają przepisów odnoszących się do inspektora ochrony danych.

Od chwili obowiązywania RODO czynności kontrolne Prezesa UODO skupiały się na sprawdzaniu prawidłowości wyznaczenia i funkcjonowania IOD – tj. obowiązku wyznaczenia inspektora, zgłoszenia go następnie Prezesowi UODO, opublikowania imienia i nazwiska inspektora na stronie internetowej administratora, jego odwołania, wyznaczenia zastępcy czy włączania go we wszystkie sprawy odnoszące się do przetwarzania danych osobowych w organizacji, w której został powołany. Jak podkreśla UODO, weryfikacja w powyższym zakresie, wypadła pozytywnie w większości przypadków, niemniej jednak, w toku czynności, UODO zauważył pewne nieprawidłowości w poszczególnych instytucjach, które polegały m.in. na:

- braku powołania IOD, tam gdzie było to wymagane,
- wypełnianiu przez IOD zadań bez należytego uwzględnienia ryzyka związanego z operacjami przetwarzania,
- brak angażowania IOD w prowadzone procesy przetwarzania.

Poza nieprawidłowościami, które zostały zidentyfikowane przez UODO podczas czynności kontrolnych, pojawiały się także te zgłaszane przez samych inspektorów ochrony danych. Wymienione poniżej, stanowią idealną wskazówkę dla administratorów i podmiotów przetwarzających w zakresie odnoszącym się do tego o jakich czynnościach powinni pamiętać, jakich unikać oraz jakich zapisów nie umieszczać w procedurach regulujących status i zadania IOD.

- brak opublikowania na stronie internetowej imienia i nazwiska inspektora,
- przyjęcie procedur obciążających inspektora obowiązkami powodującymi konflikt interesów,
- zapisanie w regulaminie organizacyjnym, że IOD może zostać odwołany w każdym czasie,

- brak prawidłowego usytuowania IOD w strukturze organizacyjnej administratora – IOD nie podlegał bezpośrednio najwyższemu kierownictwu,
- brak zapewnienia inspektorowi wsparcia finansowego oraz możliwości aktualizowania wiedzy,
- brak angażowania IOD w sprawy dotyczące przetwarzania danych osobowych.

UODO wskazał także, iż w jednej sprawie wydana została decyzja, w której organ nadzorczy udzielił upomnienia administratorowi stwierdzając naruszenie w postaci wystąpienia konfliktu interesów w zakresie powierzonych IOD zadań i obowiązków. Przywołany konflikt interesów polegał na zobowiązaniu inspektora do nadawania pracownikom administratora upoważnień do przetwarzania danych osobowych. Zobowiązanie to zostało określone w przyjętej przez administratorze procedurze, która regulowała status i zadania IOD. Jak czytamy w uzasadnieniu decyzji: „*możliwe jest udzielenie przez administratora upoważnienia podległemu pracownikowi do przetwarzania danych osobowych, obejmującego swoim zakresem również delegację uprawnienia do wykonywania obowiązków administratora w zakresie nadawania w jego imieniu upoważnień do przetwarzania danych osobowych. Z uwagi jednak na specyfikę działań IOD ogniskujących się na doradzaniu oraz kontrolowaniu działalności administratora pod kątem zgodności operacji przetwarzania danych osobowych z przepisami o ochronie danych osobowych, administrator nie powinien przyznawać IOD uprawnień do nadawania w jego imieniu upoważnień do przetwarzania danych osobowych, pozostawiając IOD w procedurze wydawania upoważnień funkcji doradczej i nadzorczej*". Prezes UODO podkreślił, że IOD cechujący się szczególnym statusem w dziedzinie zapewnienia właściwego przestrzegania przepisów o ochronie danych osobowych musi mieć dla tego celu zagwarantowane odpowiednie warunki funkcjonowania, a więc takie, które pozwolą mu na **efektywną, niezależną oraz prawidłową realizację obowiązków**. Nakładanie na IOD obowiązków prowadzących do powstania konfliktu interesów, zdaniem UODO, stawia pod znakiem zapytania nie tylko możliwość efektywnego wypełniania jego zadań, ale godzi także w same fundamenty instytucji IOD, opartej na niezależności jego funkcjonowania[1].

IOD – JAKIE W TAKIM RAZIE SĄ JEGO KOMPETENCJE?

Inspektor ochrony danych powinien koncentrować się na monitorowaniu przestrzegania przepisów o ochronie danych osobowych i wewnętrznych polityk oraz prawidłowego wykonywania wynikających z nich obowiązków a także na doradzaniu i podnoszeniu świadomości w tym zakresie. IOD informuje administratora, podmiot przetwarzający oraz pracowników o obowiązkach na nich spoczywających a określonych w RODO oraz innych przepisach regulujących zagadnienia ochrony danych osobowych. IOD przede wszystkim monitoruje RODO, inne przepisy a także przyjęte w podmiotach, w których został powołany wewnętrzne polityki oraz pozostałe dokumenty regulujące kwestie przetwarzania danych osobowych. Osoba powołana na stanowisko inspektora podejmuje czynności prowadzące do zwiększenia świadomości poprzez np. szkolenia personelu uczestniczącego w operacjach przetwarzania. IOD pełni w końcu rolę punktu kontaktowego dla organu nadzorczego a także współpracuje z tym organem.

[1] Decyzja Prezesa UODO ZWAD.405.31.331.2019

LISTA 27 PYTAŃ PREZESA UODO

Poniżej przedstawiamy listę 27 pytań, która została opublikowana przez Prezesa UODO i która kierowana będzie do administratorów i podmiotów przetwarzających, zarówno z sektora publicznego jak i prywatnego, celem sprawdzenia czy podmioty te należycie przestrzegają przepisy odnoszące się do inspektora ochrony danych.

1. Czy u administratora został wyznaczony inspektor ochrony danych (IOD)?
2. Czy na administratorze ciąży obowiązek wyznaczenia IOD (jeżeli tak, to na jakiej podstawie prawnej), czy też IOD został wyznaczony mimo braku takiego obowiązku?
3. Czy administrator opublikował imię i nazwisko oraz kontakt do IOD na swojej stronie internetowej lub - jeżeli nie prowadzi swojej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia swojej działalności?
4. Czy ww. informacje znajdują się w ogólnie dostępnym miejscu (proszę wskazać to miejsce, w przypadku strony internetowej proszę wskazać jej adres oraz link do tej informacji) ?
5. Czy Inspektor Ochrony Danych jest pracownikiem administratora, a jeśli nie, to na jakiej podstawie prawnej wykonuje swoje obowiązki?
6. Czy IOD został powołany na wyłączność u administratora, czy wykonuje swoje obowiązki również u innych administratorów?
7. Na podstawie jakich kwalifikacji administrator wyznaczył IOD (np. wykształcenie, doświadczenie, wiedza)?
8. Jakie niezbędne zasoby, o których mowa w art. 38 ust. 2 rozporządzenia 2016/679 administrator zapewnia IOD?
9. W jaki sposób administrator zapewnia zasoby na utrzymanie wiedzy fachowej IOD?
10. Jakie stanowisko zajmuje IOD i komu podlega w strukturze organizacyjnej administratora?
11. Czy administrator powołał zastępcę IOD, jeżeli tak, to kiedy?
12. Czy u administratora funkcjonuje zespół IOD lub inna forma stałego wsparcia IOD w zakresie wykonywania jego zadań?
13. W jaki sposób administrator zapewnia by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych (np. czy zostały opracowane zasady dotyczące tego, jakie sprawy mają być konsultowane z IOD, kto i w jakich sytuacjach powinien zgłaszać się w celu uzyskania konsultacji IOD, czy i na jakich zasadach IOD bierze udział w naradach kierownictwa)
14. W jaki sposób administrator zapewnia IOD dostęp do danych osobowych i operacji przetwarzania?
15. Czy administrator przyjął jakiekolwiek regulacje wewnętrzne dotyczące funkcjonowania IOD (w szczególności w celu zapewnienia poszanowania gwarancji jego niezależności oraz jego uprawnień w zakresie dostępu do danych osobowych i operacji przetwarzania, włączania we wszystkie sprawy dotyczące ochrony danych osobowych, unikania konfliktu interesów), a jeżeli tak, to w jakim akcie wewnętrznym zostały one przewidziane?
16. W jaki sposób administrator zapewnia, aby IOD nie były wydawane instrukcje co do wykonywania zdań przez IOD?

17. W jaki sposób administrator zapewnia, aby IOD nie były karany i odwoływany za wykonywanie swoich zadań?
18. W jaki sposób ADO postępuje w przypadku, gdy nie uwzględnia wskazówek lub rekomendacji IOD, np. czy dokumentuje powody niezastosowania tych wskazówek?
19. W jaki sposób osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych zgodnie z art. 38 ust. 4 rozporządzenia 2016/679 ?
20. Czy inspektor ochrony danych wykonuje również inne obowiązki lub sprawuje inną funkcję poza obowiązkami związanymi z ochroną danych osobowych, jeżeli tak to:
    a) jakie oraz w jakim wymiarze czasu pełni funkcję IOD, a w jakim inne zadania,
    b) w jaki sposób administrator ocenił, że w przypadku każdego z tych zadań nie występuje konflikt interesów, o którym mowa w art. 38 ust 6 rozporządzenia 2016/679?
    c) czy w zakresie wykonywania innych zadań IOD podlega innym osobom niż najwyższe kierownictwo administratora?
    d) czy administrator opracował politykę zarządzania konfliktem interesów lub wprowadził inny mechanizm zapewniający niewystępowanie konfliktu interesów?
21. Czy administrator opracował politykę zarządzania konfliktem interesów lub wprowadził inny mechanizm zapewniający niewystępowanie konfliktu interesów?
22. Czy IOD wykonuje swoje zadania jedynie w siedzibie administratora, a jeżeli nie, to w jakim miejscu i w jaki sposób zapewniona jest stała dostępność IOD dla kierownictwa i pracowników administratora?
23. Czy IOD opracował (systematycznie opracowuje) plan swojej pracy np. w zakresie szkoleń, audytów?
24. Czy taki plan był prezentowany administratorowi w celu umożliwienia dokonania oceny, czy IOD dysponuje wystarczającymi zasobami i uprawnieniami w obszarach, które IOD obejmuje swoimi zadaniami?
25. Jak często i w jaki sposób IOD przekazuje administratorowi wyniki przeprowadzonych audytów?
26. Czy administrator występował do IOD o udzielenie zaleceń co do oceny skutków dla ochrony danych, a jeśli tak, to w jakich sytuacjach?
27. Czy administrator kontroluje pracę inspektora, jeżeli tak, to w jaki sposób?

Wskazana lista 27 pytań charakteryzuje się podziałem na dwie płaszczyzny, które odnoszą się do zasad działania IOD w poszczególnych organizacjach. Pierwsza z nich odnosi się do samego obowiązku wyznaczenia inspektora, jego formalnego powołania oraz publikacji jego danych we wskazanych miejscach. Obszar ten skupia się również na analizie czy IOD posiada właściwą niezależność w ramach wykonywania swoich obowiązków oraz czy zachodzi konflikt interesów w zakresie pełnionych przez niego funkcji. Druga kategoria pytań ma na celu ustalenie czy IOD wykonuje swoje zadania w oparciu o konkretny plan, w tym plan szkoleń czy audytów oraz czy taki plan został zaprezentowany do oceny administratorowi tak aby ten mógł wnieść swoje uwagi czy następnie skontrolować prace IOD.

Karolina Żebrowska - specjalistka ds. ochrony danych osobowych w iSecure Sp. z o.o.