EVERSHEDS
SUTHERLAND

27 pytań UODO
Działalność IOD pod lupą organu nadzorczego

Urząd Ochrony Dany Osobowych opublikował listę 27 pytań dotyczących inspektorów danych osobowych. W najbliższych miesiącach będzie je kierował do administratorów danych osobowych i podmiotów przetwarzających, w tym do podmiotów z sektora prywatnego.
Celem działań podejmowanych przez UODO jest ocena prawidłowości powoływania i funkcjonowania inspektorów ochrony danych.

UODO, wykorzystując swoje uprawnienia nadzorcze określone w art. 58 RODO, już wcześniej badał przypadki potencjalnych naruszeń przepisów dotyczących inspektora danych osobowych. Naruszenia te dotyczyły najczęściej:

- nieopublikowania na stronie internetowej administratora imienia i nazwiska inspektora
- nieaktualizowania danych inspektora na stronie internetowej administratora
- przyjęcia procedur obciążających inspektora obowiązkami powodującymi konflikt interesów
- zapisania w regulaminie organizacyjnym, że IOD może być odwołany w każdym czasie
- przyczyn odwołania inspektora
- nieprawidłowego usytuowania IOD w strukturze organizacyjnej administratora – IOD nie podlegał bezpośrednio najwyższemu kierownictwu
- niezapewnienia inspektorowi wystarczającej ilości czasu oraz innych zasobów niezbędnych do wykonywania jego zadań
- niezapewnienia inspektorowi wsparcia finansowego, infrastrukturalnego oraz możliwości aktualizowania wiedzy

Kontakt

Piotr Łada
Adwokat
Senior Associate

+48 22 50 50 730
piotr.lada
@eversheds-sutherland.pl

- pomijania inspektora w sprawach dotyczących przetwarzania danych osobowych (w tym takich, w których administratorzy prosili o opinię UODO, nie zwracając się wcześniej o opinię do inspektora)

Na bazie zgłoszeń inspektorów ochrony danych osobowych oraz swoich doświadczeń UODO stworzył szczegółową listę 27 pytań. Będą one kierowane zarówno do administratorów danych osobowych, jak i podmiotów przetwarzających z sektora publicznego i prywatnego.

Poniżej pełna lista pytań opublikowanych przez UODO:

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.
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?

Ze względu na treść pytań oraz cel działań podejmowanych przez UODO w wielu przypadkach konieczne będzie, oprócz udzielenia odpowiedzi na pytania, wykazanie także, że określone procedury, mechanizmy lub środki zostały wdrożone, oraz że funkcjonują w sposób prawidłowy.

Publikacja pytań to właściwy czas, aby dokonać wewnętrznej weryfikacji, czy istnieje potrzeba powołania IOD – a jeśli został on powołany, czy spełnione zostały wymogi RODO odnoszące się do prawidłowości funkcjonowania IOD. Nieprawidłowości mogą bowiem zostać uznane za naruszenie RODO, a w konsekwencji prowadzić do objęcia kontrolą przez UODO innych obszarów związanych z przetwarzaniem danych lub do nałożenia kary pieniężnej. Z podobnymi negatywnymi konsekwencjami można liczyć się w przypadku odmowy udzielenia odpowiedzi na pytania, czy udzielania odpowiedzi w formie niepełnej.

Zachęcamy Państwa do kontaktu w przypadku wszelkich pytań w zakresie przepisów o ochronie danych osobowych, w szczególności związanych z weryfikacją prawidłowości powołania i funkcjonowania IOD.