DZP
więcej niż prawo

Dane osobowe

UODO – kontrola inspektorów ochrony danych (IOD)

Urząd Ochrony Danych Osobowych rozpoczął kompleksową kontrolę inspektorów ochrony danych (IOD) oraz wezwał wybranych administratorów do złożenia wyjaśnień i przedstawienia dowodów dotyczących stosowania przepisów o IOD.

Przeprowadzenie przez UODO kontroli może wiązać się z koniecznością zweryfikowania stosowanych praktyk oraz przeglądu niezbędnej dokumentacji.

Poniżej znajdą Państwo listę pytań kontrolnych stosowanych przez UODO.

Zespół ochrony danych osobowych DZP opracował wskazówki i wytyczne, jakie działania należy podjąć w przypadku kontroli – w razie zainteresowania takim materiałem zachęcamy do kontaktu.

Cel kontroli

Celem kontroli jest zweryfikowanie, czy administrator danych osobowych (ADO) prawidłowo wykonuje wynikające z przepisów o ochronie danych osobowych (w tym RODO) obowiązki w zakresie dotyczącym inspektora ochrony danych (IOD). W ramach wezwania administratorów do złożenia wyjaśnień rekomendujemy, aby zachować dokładność oraz spójność udzielanych wyjaśnień, bowiem wszelka wątpliwość może skutkować wszczęciem indywidualnego postępowania wyjaśniającego, przeprowadzeniem wewnętrznej (miejscowej) kontroli, a w najgorszym wypadku nałożeniem administracyjnej kary pieniężnej. Nie wszystkie pytania wymagają przedstawienia dowodu na potwierdzenie złożonych wyjaśnień.

Lista pytań

Czy u administratora danych osobowych (ADO) został wyznaczony inspektor ochrony danych (IOD)?
Czy na administratorze ciąży obowiązek wyznaczenia IOD (jeżeli tak, to na jakiej podstawie prawnej), czy też IOD został wyznaczony mimo braku takiego obowiązku?
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?
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)?
Czy IOD jest pracownikiem administratora, a jeśli nie, to na jakiej podstawie prawnej wykonuje swoje obowiązki?

Czy IOD został powołany na wyłączność u administratora, czy wykonuje swoje obowiązki również u innych administratorów?

Na podstawie jakich kwalifikacji administrator wyznaczył IOD (np. wykształcenie, doświadczenie, wiedza)?

Jakie niezbędne zasoby, o których mowa w art. 38 ust. 2 rozporządzenia 2016/679 administrator zapewnia IOD?

W jaki sposób administrator zapewnia zasoby na utrzymanie wiedzy fachowej IOD?

Jakie stanowisko zajmuje IOD i komu podlega w strukturze organizacyjnej administratora?

Czy administrator powołał zastępcę IOD, jeżeli tak, to kiedy?

Czy u administratora funkcjonuje zespół IOD lub inna forma stałego wsparcia IOD w zakresie wykonywania jego zadań?

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)?

W jaki sposób administrator zapewnia IOD dostęp do danych osobowych i operacji przetwarzania?

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?

W jaki sposób administrator zapewnia, aby IOD nie były wydawane instrukcje co do wykonywania zdań przez IOD?

W jaki sposób administrator zapewnia, aby IOD nie był karany i odwoływany za wykonywanie swoich zadań?

W jaki sposób ADO postępuje w przypadku, gdy nie uwzględnia wskazówek lub rekomendacji IOD, np. czy dokumentuje powody niezastosowania tych wskazówek?

W jaki sposób osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych zgodnie z art. 38 ust. 4 rozporządzenia 2016/679 ?

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?

Czy administrator opracował politykę zarządzania konfliktem interesów lub wprowadził inny mechanizm zapewniający niewystępowanie konfliktu interesów?

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?
Czy IOD opracował (systematycznie opracowuje) plan swojej pracy np. w zakresie szkoleń, audytów?
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?
Jak często i w jaki sposób IOD przekazuje administratorowi wyniki przeprowadzonych audytów?
Czy administrator występował do IOD o udzielenie zaleceń co do oceny skutków dla ochrony danych, a jeśli tak, to w jakich sytuacjach?
Czy administrator kontroluje pracę inspektora, jeżeli tak, to w jaki sposób?

Kontakt

Bartosz Marcinkowski
Partner | Szef Zespołu Ochrony Danych Osobowych
E: bartosz.marcinkowski@dzp.pl
M: +48 660 440 329