JDP

Newsletter

Zadania IOD a konflikt interesów

maj 2023

Zadania IOD a konflikt interesów

1. Wyznaczenie, zadania oraz kwalifikacje IOD

IOD jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO.

Definicja odpowiedniego poziomu wiedzy fachowej nie została jednoznacznie określona w RODO, jednak zgodnie z Wytycznymi Grupy Roboczej Art. 29 dotyczącymi inspektorów ochrony danych (WP 243)*, wymagania te muszą odpowiadać charakterowi, stopniowi skomplikowania i ilości danych przetwarzanych przez daną jednostkę.

Wyższy poziom wiedzy może być wymagany w przypadku wyjątkowo skomplikowanych procesów przetwarzania, przetwarzania dużej ilości danych szczególnych kategorii lub podmiotów regularnie przekazujących dane do państw trzecich.

*Dokument dostępny na stronie https://ec.europa.eu/newsroom/article29/items/612048/en [dostęp: 10.05.23 r.].

Do zadań IOD należą w szczególności:

1. Informowanie i szkolenie pracowników organizacji w zakresie ochrony danych osobowych i przepisów prawa dotyczących tej kwestii;
2. Doradztwo w sprawach związanych z przetwarzaniem danych osobowych, w tym w kwestiach zgodności z obowiązującymi przepisami;
3. Monitorowanie przestrzegania przepisów o ochronie danych osobowych w organizacji i reagowanie na wszelkie naruszenia tych przepisów;
4. Współpraca z organem nadzorczym ds. ochrony danych osobowych oraz pełnienie funkcji kontaktowej dla organu nadzorczego w sprawach związanych z ochroną danych osobowych;
5. Współpraca z innymi działami organizacji, takimi jak dział IT czy dział HR, w celu zapewnienia przestrzegania przepisów dotyczących ochrony danych osobowych we wszystkich obszarach działalności organizacji;
6. Pełnienie funkcji puntu kontaktowego dla osób fizycznych i organu;
7. Udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych i monitorowanie jej wykonania.

Jak widać powyżej, zadania IOD są zróżnicowane i wymagają zarówno szerokiej wiedzy z zakresu ochrony danych osobowych, jak i umiejętności analitycznych i organizacyjnych.

2. Konflikt interesów

IOD może zostać zarówno członek personelu administratora lub podmiotu przetwarzającego, jak i osoba spoza grona w/w podmiotów, dlatego w wielu przypadkach może pojawić się problem dotyczący kwestii łączenia tego stanowiska z innymi.

- Samo RODO wskazuje w art. 38 ust. 3 oraz 6, że administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie może on być także odwoływany, ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.

- Kluczowe jest jednak wskazanie, że inspektor ochrony danych może wykonywać inne zadania i obowiązki, jednakże administrator lub podmiot przetwarzający obowiązani są zapewnić, aby by takie zadania i obowiązki nie powodowały konfliktu interesów. Oznacza to, że IOD 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.

- Grupa Robocza w dokumencie opisanym powyżej wskazała także, że wymóg niepowodowania konfliktu interesów jest ściśle związany z wymogiem wykonywania zadań w sposób niezależny. Precyzując, Grupa wskazała, że oznacza to przede wszystkim, że IOD nie może obejmować stanowiska w organizacji, które zapewniałoby mu dostęp do informacji pozwalających mu ustalić cele i sposoby przetwarzania danych osobowych, podając jednak, że jest to oczywiście podyktowane indywidualnymi przypadkami. Problem ten podyktowany jest wystąpieniem sprzecznych priorytetów, które skutkować mogłyby zaniedbaniem obowiązków pełnionych przez IOD.

- Aby uniknąć konfliktów interesów, administrator lub podmiot przetwarzający muszą zadbać o to, aby dodatkowe zadania i obowiązki IOD były zgodne z jego funkcją ochrony danych osobowych i nie kolidowały z jego niezależnością i obowiązkiem dbania o prywatność danych osobowych. W przypadku wystąpienia konfliktu interesów administrator lub podmiot przetwarzający muszą podjąć działania, aby wyeliminować taki konflikt.

3. W jaki sposób można zapewnić brak konfliktu interesów

Urząd Ochrony Danych Osobowych na swojej stronie internetowej* zawiera szereg pytań i odpowiedzi dotyczących wyznaczenie i status IOD. Wiele z nich odnosi się do łączenia funkcji IOD z innymi funkcjami w organizacji.

W każdej sytuacji, która wskazywać by mogła na konflikt interesów, należy dokładnie rozważyć, czy IOD może skutecznie wykonywać swoje obowiązki, gdy pełni jednocześnie inne funkcje.

UODO w jednej z odpowiedzi na swojej stronie internetowej** proponuje m.in.:

1. analizę ilości czasu potrzebnego na wykonywanie poszczególnych obowiązków (w tym na współpracę z innymi służbami kontrolnymi),
2. analizę poziomu trudności i znaczenia zadań w organizacji,
3. zapewnienie rezerwy czasowej na nieplanowane zadania (np. w związku z naruszeniem danych),
4. ilość i rodzaj danych osobowych oraz procesów i systemów informatycznych służących do ich przetwarzania, a także obszary ryzyka, związane z tymi procesami,
5. analizę struktury, wielkości i zasobów kadrowych organizacji, w szczególności, w przypadku IOD zatrudnionego w niepełnym wymiarze czasu pracy.

*Pytania i odpowiedzi dotyczące IOD dostępne są pod adresem: https://uodo.gov.pl/pl/495 [dostęp:10.05.23 r.].
**Pytanie i odpowiedź dotycząca IOD dostępne są pod adresem: https://uodo.gov.pl/pl/495/2371 [dostęp:10.05.23 r.].

Dobre praktyki

Grupa Robocza także wskazuje na szereg dobrych praktyk w celu uniknięcia problemu, jak np.:

1. „określenie stanowisk niezgodnych z funkcją IOD;
2. opracowanie wewnętrznych zasad pozwalających uniknąć konfliktu interesów;
3. zapewnienie bardziej ogólnego wyjaśnienia dotyczącego konfliktu interesów;
4. zadeklarowanie, że DPO nie ma konfliktu interesów w odniesieniu do pełnionej przez siebie funkcji DPO, celem zwiększenia świadomości na temat tego wymogu;
5. wprowadzenie zabezpieczeń do wewnętrznych zasad organizacji oraz zapewnienie, by ogłoszenie o naborze na stanowisko DPO lub umowa o świadczenie usług były wystarczająco jasne i precyzyjne, aby uniknąć konfliktu interesów. W tym kontekście należy również mieć na uwadze, że konflikty interesów mogą przybierać różne formy w zależności od tego, czy rekrutacja na stanowisko DPO ma charakter wewnętrzny lub zewnętrzny.”

4. Wykonywanie poszczególnych funkcji przez IOD

Przyjmuje się niełączenie zadań IOD z wykonywaniem funkcji kierowniczych wyższego szczebla, takich jak dyrektorzy, kierownicy departamentów i działów, ale również na niższych szczeblach, które umożliwiają ustalanie celów i sposobów przetwarzania danych osobowych.

Niedopuszczalne jest powołanie na IOD osoby będącej kierownikiem (zarządzającym) ADO, ale również inne stanowiska kierownicze np.:

- Dyrektor generalny;
- Dyrektor do spraw operacyjnych;
- Dyrektor finansowy;
- Kierownik działu marketingu;
- Kierownik działu HR;
- Kierownik działu IT.

Z szeregu odpowiedzi UODO można wywnioskować, że funkcja IOD:

- może być w Polsce pełniona przez obcokrajowca*;
- może być pełniona przez osobę spokrewnioną z osobą zarządzającą**;
- może pełnić funkcję pełnomocnika do spraw ochrony informacji niejawnych***;
- może być wykonywania jednocześnie z zawodem adwokata - przepisy RODO gwarantują IOD niezależność, co jest również podstawą wykonywania zawodu adwokata****;
- nie powinna być wykonywana łącznie z zawodem radcy prawnego. Krajowa Rada Radców Prawnych (KRRP) przekazała opinię, w której rekomenduje niełączenie wykonywania ról w ramach jednego podmiotu (administratora danych/klienta)*****.

*Pytanie i odpowiedź dotycząca IOD dostępne są pod adresem: https://uodo.gov.pl/pl/495/2399 [dostęp:10.05.23 r.].
**Pytanie i odpowiedź dotycząca IOD dostępne są pod adresem: https://uodo.gov.pl/pl/495/2362 [dostęp:10.05.23 r.].
***Pytanie i odpowiedź dotycząca IOD dostępne są pod adresem: https://uodo.gov.pl/pl/495/2371 [dostęp:10.05.23 r.].
****Pytanie i odpowiedź dotycząca IOD dostępne są pod adresem: https://uodo.gov.pl/pl/495/2347 [dostęp:10.05.23 r.].
*****Ibidem.

5. Decyzje Prezesa UODO dotyczące IOD

NR	DECYZJA	OPIS
1.	DECYZJA ZWAD.405.31.331.2019 Administrator: Szpital Kara: upomnienie	Wewnętrzna procedura Szpitala przewidywała obowiązek IOD do nadawania upoważnień personelowi Szpitala w zakresie przetwarzania danych osobowych. Administrator nie powinien przyznawać IOD uprawnień do nadawania w jego imieniu upoważnień. Przyjęcie odmiennego założenia, w którym IOD byłby odpowiedzialny za wydawanie upoważnień, a jednocześnie miałby monitorować zgodność procesu z przepisami o ochronie danych osobowych, do czego zobowiązuje go RODO, doprowadziłoby w efekcie do sytuacji, gdzie IOD sprawowałby nadzór nad własną działalnością, a więc do **konfliktu interesów.**
2.	DECYZJA ZSOŚS.421.25.2019 Administrator: SGGW w Warszawie Kara: 50.000,00 PLN	SGGW zawiadomiło o kradzieży przenośnego prywatnego laptopa pracownika uczelni, który używał urządzenia do przetwarzania danych osobowych kandydatów na studia. Administrator nie miał wiedzy, że jeden z pracowników używa prywatny sprzęt w celach służbowych. Administrator nie wdrożył odpowiednich środków bezpieczeństwa technicznego i organizacyjnego oraz **nie przeprowadził analizy ryzyka**, ale też dopuścił się szeregu dalszych naruszeń RODO. **IOD wypełniał swoje zadania bez należytego uwzględnienia ryzyka związanego z operacjami przetwarzania. IOD nie był angażowany przez administratora w proces analizy procesu rekrutacji, co przyczyniło się to utrzymania nienależytego poziomu zabezpieczenia tego procesu przetwarzania.**

6. Wyroki/decyzje europejskie dotyczące IOD

NR	DECYZJA	OPIS
1.	LUKSEMBURSKI ORGAN NADZORCZY (CNPD) Decyzja z dnia 27.10.2021 r. Administrator: Podmiot oferujący usługi transportowe Kara: 15 400 EUR	CNPD podczas wykonywania czynności kontrolnych u administratora, wykrył, iż IOD nie został prawidłowo włączony we wszystkie sprawy dotyczące ochrony danych, a także administrator **nie zagwarantował niezależności IOD, ponieważ ten nie podlegał bezpośrednio najwyższemu kierownictwu Spółki.**
2.	Belgian Data Protection Authority (APD) Decyzja z dnia 28.04.2020 r. Administrator: Proximus SA Kara: 50 000 EUR	Organ wskazał m.in., iż Spółka wyznaczyła na IOD osobę pełniącą funkcję Dyrektora ds. Audytu, Ryzyka i Compliance, co doprowadziło do konfliktu interesów oraz braku wystarczającego zaangażowania w ocenę naruszeń ochrony danych osobowych.
3.	Belgian Data Protection Authority (APD) Decyzja z dnia 16.12.2021 r. Administrator: Bank Kara: 75 000 EUR.	W trakcie przeprowadzania kontroli APD stwierdził, iż Administrator wyznaczył na IOD osobę pełniącą funkcję Kierownika Działu Zarządzania Ryzykiem Służb Operacyjnych, Ryzyka Informacyjnego i Specjalnej Jednostki Dochodzeniowej. Według organu, doprowadziło to do sytuacji, w której IOD nie posiadał prawa audytowania wskazanego obszaru, pomimo przetwarzania w nim danych osobowych.

Kontakt

W przypadku dodatkowych pytań, zachęcamy do bezpośredniego kontaktu z naszą ekspertką.

Anna Matusiak-Wekiera

Radca prawny

Head of Data Protection/Compliance Practice

anna.matusiak-wekiera@jdp-law.pl