JDP

e-book

Inspektor ochrony danych osobowych w organizacji

Poradnik JDP

wrzesień 2024

jdp-law.pl

Inspektor ochrony danych (IOD) jest odpowiedzialny za budowanie kultury ochrony danych osobowych w organizacji.

Jak po blisko sześciu latach od rozpoczęcia stosowania przepisów RODO wypełniana jest w praktyce ta rola?

Z jakimi problemami mierzą się inspektorzy ochrony danych oraz organizacje, które wyznaczyły IOD?

Jakich rad udziela prezes Urzędu Ochrony Danych samym inspektorom?

Jakie wnioski w zakresie pełnienia tej funkcji można wysnuć na podstawie rozstrzygnięć zagranicznych organów ochrony danych osobowych?

Na te pytania odpowiadają **Anna Matusiak-Wekiera** oraz **Ewelina Kęciek** z działu **Ochrony Danych Osobowych i Compliance** JDP w cyklu artykułów poświęconych praktycznym problemom związanym z powołaniem i funkcjonowaniem inspektora ochrony danych w organizacji.

Teksty powstały na zlecenie dziennika „**Rzeczpospolita**” i były publikowane jako cykl na temat IOD na jego łamach oraz na rp.pl w okresie dnia od lutego do maja 2024 roku.

W niniejszym **Poradniku** prezentujemy fragmenty wszystkich artykułów cyklu. Linki do poszczególnych artykułów znajdują się pod każdym tekstem.

Spis treści:

Inspektor ochrony danych pod lupą prezesa UODO

Anna Matusiak-Wekiera

Ewelina Kęciek

W mniejszych organizacjach inspektor ochrony danych osobowych traktowany jest jak „człowiek orkiestra” – ma znać się na przepisach, ale i aspektach technologicznych czy analizie ryzyka, projektować konkretne rozwiązania, ale również dostrzegać ich luki w procesie monitorowania.

Od momentu rozpoczęcia stosowania przepisów RODO, prezes Urzędu Ochrony Danych Osobowych przeprowadził około 270 kontroli i wydał ponad 8 tys. decyzji administracyjnych (patrz źródło). Choć jedynie w nielicznych rozstrzygnięciach organ odniósł się wprost do kwestii wyznaczenia i sprawowania funkcji inspektora ochrony danych, zagadnienie to zdaje się pozostawać w sferze jego zainteresowań. Przejawem powyższego było opublikowanie przez Prezesa UODO listy 27 pytań dotyczących statusu IOD, które w pierwszym kwartale 2022 r. zostały przesłane do wybranych organizacji.

Gdzie jesteśmy teraz, po blisko sześciu latach od rozpoczęcia stosowania przepisów RODO i blisko dwóch latach od momentu, gdy Prezes UODO wyraził systemowe zainteresowanie funkcją IOD?

BOLĄCZKI INSPEKTORÓW OCHRONY DANYCH

Kiedy młodsi koledzy, rozpoczynający przygodę z IOD-owaniem", czyli pełnieniem funkcji inspektora ochrony danych w organizacji, pytają starszych stażem inspektorów o rady na początek drogi, lista wskazówek zdaje się nie mieć końca. Inspektorzy zwracają uwagę na swoje codzienne bolączki.

Zgodnie z przepisami RODO, inspektorzy powinni być wyznaczani na podstawie kwalifikacji zawodowych, w tym wiedzy fachowej na temat praktyk i prawa w dziedzinie ochrony danych osobowych. Administratorzy powinni zapewnić, aby inspektorzy byli właściwie i niezwłocznie włączani we wszystkie sprawy dotyczące ochrony danych. Jednocześnie, inspektorom należy zapewnić niezbędne zasoby do wykonania tych zadań i trzymania wiedzy fachowej, z jednoczesnym dostępem do danych i operacji przetwarzania. Zgodnie z przepisami, IOD może wykonywać inne zadania i obowiązki niż te związane z ochroną danych, ale rolą organizacji jest zapewnienie, aby nie powodowały one konfliktu interesów.

Inspektor ma być niezależny, czemu służyć ma brak możliwości udzielania mu instrukcji dotyczących wykonywania zadań i podległość jedynie najwyższemu kierownictwu, np. bezpośrednio zarządowi.

JAK TEORIA PRZEKŁADA SIĘ NA PRAKTYKĘ?

Inspektorzy skarżą się na brak zasobów do pełnienia swojej funkcji.

Po pierwsze, inspektorzy narzekają na brak wsparcia administratora w obszarach, w których chcieliby korzystać z wiedzy eksperckiej, a która wykracza poza profil ich wykształcenia lub doświadczenia. W szczególności w mniejszych organizacjach inspektor traktowany jest jak „człowiek orkiestra" – ma znać się na przepisach, ale i aspektach technologicznych czy analizie ryzyka, projektować konkretne rozwiązania, ale również dostrzegać ich luki w procesie monitorowania. Inspektorzy nie mają wsparcia działu prawnego, zewnętrznej kancelarii czy zespołu informatycznego.

Drugi aspekt dotyczący braku zasobów IOD dotyczy zbyt późnego lub przypadkowego włączania IOD w sprawy organizacji. Inspektorzy często zostają włączani w nowy projekt w momencie, gdy wszystkie ustalenia zostaną poczynione, umowy zawarte, a dane w zasadzie „od jutra" mają być przetwarzane. Inspektorzy nie tylko nie mają zatem czasu, by właściwie zapoznać się z projektem, ale w zasadzie działają ze świadomością braku realnych możliwości modyfikacji projektu. To zaś powoduje, że zgłaszane przez nich uwagi często pozostają „papierowe".

Wymieniając swoje problemy, inspektorzy wskazują na trudność w łączeniu zadań IOD z innymi obowiązkami. W takim przypadku inspektorzy nie tylko nie mają wystarczającego czasu na realizację obowiązków IOD, które często są „na dokładkę" do innych, bardziej wiodących ról, ale niepokoją się również możliwością powstania konfliktu interesów. Część z inspektorów raportuje, że jest stawiana w podwójnej roli – z jednej strony musi sporządzać dokumenty, które następnie, w toku monitorowania przestrzegania przepisów RODO, ma sprawdzać. To zaś powoduje naruszenie zasady, że nadzorujący nie może być jednocześnie nadzorowanym.

CO NA TO PREZES UODO?

Wyżej opisane trudności zdają się nie umykać prezesowi UODO. Organ odnosił się do sygnalizowanych zagadnień w swoim biuletynie informacyjnym, odpowiedziach na pytania IOD oraz na konferencjach i szkoleniach kierowanych do inspektorów.

!

Najbardziej znaczące działania w tym zakresie prezes UODO podjął na początku 2022 r., kiedy to opublikował na swojej stronie wspomnianą listę 27 pytań skierowanych do administratorów i podmiotów przetwarzających, dotyczących tego, w jaki sposób sprawowana jest funkcja IOD. Lista pytań została przesłana do 24 podmiotów z sektora prywatnego i publicznego.

Organ, w następstwie analizy otrzymanych od organizacji odpowiedzi, wszczął 4 kontrole i 2 postępowania administracyjne w sprawie naruszenia przepisów o ochronie danych osobowych. Postępowania dotyczyły naruszenia przepisów odnoszących się do prowadzenia rejestru czynności przetwarzania, zgłaszania naruszeń ochrony danych osobowych do organu, jak również przepisów odnoszących się do wykonywania funkcji IOD.

CO NA TO PREZES UODO?

Prezes UODO podsumował „akcję" sprawdzenia administratorów i podmiotów przetwarzających w sprawozdaniu ze swojej działalności za 2022 r., w którym wskazał, że uchybienia w zakresie powierzenia i sprawowania funkcji IOD „dotyczyły takich kwestii jak np.:

- niewłaściwe włączanie inspektora ochrony danych w sprawy dotyczące ochrony danych osobowych,
- niepodejmowanie działań mających na celu zapewnienie inspektorowi ochrony danych zasobów niezbędnych do utrzymania jego wiedzy fachowej,
- brak procedur zapewniających niezależność inspektora ochrony danych, w szczególności dotyczących zakazu otrzymywania instrukcji, wydawania poleceń, jak również zapewnienia, że w ramach wykonywania zadań inspektora ochrony danych nie będzie on odwoływany ani karany,
- wykonywanie przez inspektorów ochrony danych zadań, które z mocy prawa należą do wyłącznych zadań administratorów, jak np. prowadzenie rejestru czynności przetwarzania, czy rejestru naruszeń ochrony danych osobowych" (patrz s. 73 sprawozdania).

CO NA TO PREZES UODO?

Organ dostrzegł więc te same problemy, które zgłaszane były przez „rynek”. I choć jednorazowa akcja kierowania pytań do organizacji wydaje się kroplą w morzu potrzeb, należy pamiętać, że działania prezesa UODO dotyczące IOD mogą mieć również miejsce w toku planowanych kontroli czy kontroli wynikających ze zgłaszanych naruszeń ochrony danych osobowych oraz skarg osób fizycznych.

W toku kontroli prezes UODO zawsze bowiem zadaje pytania o wyznaczenie IOD, publikację jego danych na stronie internetowej i dokumentację w organizacji dotyczącą inspektora. Nawet ogólne zainteresowanie organu związane z wyznaczeniem czy funkcjonowaniem IOD w organizacji wydaje się zatem nie do uniknięcia.

Artykuł powstał dla dziennika „**Rzeczpospolita**” i został opublikowany na jego łamach dnia 26.01.2024.

Link do artykułu >>> **PRZECZYTAJ CAŁY TEKST** <<<

Co grozi za brak wyznaczenia inspektora ochrony danych?

Anna Matusiak-Wekiera

Ewelina Kęciek

Europejskie organy nadzorcze wydają decyzje, w których nakładają na organizacje sankcje za brak wyznaczenia inspektora ochrony danych. Nie tylko nakazują wyznaczenie inspektora ochrony danych (IOD), nakładają także na zobowiązane organizacje administracyjne kary pieniężne.

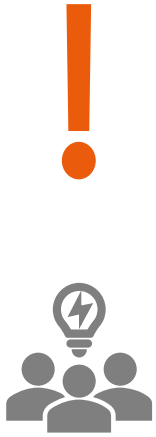
Inspektor ochrony danych (IOD) jest odpowiedzialny za budowanie kultury ochrony danych osobowych w organizacji. Jak po blisko sześciu latach od rozpoczęcia stosowania przepisów RODO wypełniana jest w praktyce ta rola? Z jakimi problemami mierzą się inspektorzy ochrony danych? Jakich rad udziela prezes Urzędu Ochrony Danych Osobowych organizacjom, które wyznaczyły IOD, a także samym inspektorom? Jakie wnioski w zakresie pełnienia tej funkcji można wysnuć na podstawie rozstrzygnięć zagranicznych organów ochrony danych osobowych? Na te pytania odpowiemy w cyklu artykułów poświęconych praktycznym problemom związanym z wyznaczeniem i funkcjonowaniem inspektora ochrony danych w organizacji.

Zasadniczo, przepisy RODO przewidują konieczność wyznaczenia IOD w trzech sytuacjach:

1. gdy przetwarzania dokonują organ lub podmiot publiczny;
2. gdy główna działalność organizacji polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, na dużą skalę;
3. gdy główna działalność organizacji polega na przetwarzaniu na dużą skalę szczególnych kategorii danych lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych.

Powyższe pojęcia, takie jak główna działalność czy duża skala, nie zostały zdefiniowane w przepisach.

To na administratorze lub podmiocie przetwarzającym – a zatem na biznesie – spoczywa obowiązek oceny, czy ze względu na prowadzoną działalność powstaje obowiązek wyznaczenia IOD. Biznes dokonuje oceny samodzielnie, uwzględniając konkretne okoliczności faktyczne związane z przetwarzaniem danych osobowych i posiłkując się wskazówkami na ten temat, zawartymi w wytycznych Grupy Roboczej art. 29 ds. ochrony danych dotyczących inspektorów ochrony danych oraz interpretacjach krajowych organów nadzorczych, w tym wynikających z wydanych decyzji.



EROD – SPRAWOZDANIE DOTYCZĄCE FUNKCJI IOD

Pod koniec 2022 r. Europejska Rada Ochrony Danych (EROD) i wchodzące w jej skład europejskie organy sprawujące nadzór nad ochroną danych osobowych przeprowadziły wspólne badanie dotyczące wyznaczania i pozycji IOD.

Efektem tego działania jest sprawozdanie EROD z 16 stycznia 2024 r., z którego wynika m.in., że wciąż nie wszystkie zobowiązane do tego przez RODO organizacje wyznaczyły IOD.

Co najbardziej zaskakujące, niektórzy administratorzy w sektorze publicznym nie wyznaczyli IOD, gdyż byli w błędnym przekonaniu, że zadania, które wykonują nie stanowią zadań publicznych.

Powyższe wskazuje więc, że nie tylko przesłanki powiązane z zakresem i skalą działalności organizacji sprawiają problemy interpretacyjne, ale również podstawowa przesłanka związana z przetwarzaniem danych przez podmioty publiczne bywa błędnie rozumiana.

To zaś oznacza, że każdy pomiot – publiczny czy prywatny – który podejmuje decyzję o odstąpieniu od wyznaczenia IOD, powinien poprzedzić taką decyzję analizą (braku) obowiązku wyznaczenia IOD. Decyzja udokumentowana zgodnie z zasadą rozliczalności wynikającą z RODO może być, w razie potrzeby, przedstawiona organowi nadzorczemu.

W rezultacie swojego działania EROD zasugerowała, aby krajowe organy nadzorcze kontynuowały działania dotyczące IOD, w tym – jeśli będzie to zasadne – podejmowały działania wykonawcze (np. kontrole, nakazy, administracyjne kary pieniężne).

Warto więc przyjrzeć się tematowi, zarówno w kontekście tego, czy w organizacji przeprowadzono analizę obowiązku wyznaczenia IOD, jak również tego, jak do danego zagadnienia podchodzą organy nadzorcze.

W sierpniu 2019 r. prezes Urzędu Ochrony Danych Osobowych (UODO) wydał wobec spółdzielni mieszkaniowej decyzję (sygn. ZSPR.421. 4.2018), w której nakazał jej dostosowanie operacji przetwarzania danych osobowych do przepisów RODO poprzez wyznaczenie IOD.

Organ wskazał, że w związku ze stosowaniem monitoringu spółdzielnia wykonuje regularne operacje na danych, które polegają m.in. na zapisywaniu, przeglądaniu, udostępnianiu i usuwaniu zarejestrowanych nagrań, a w konsekwencji organizacja podlega pod obowiązek wyznaczenia IOD z uwagi na systematyczne monitorowanie danych na dużą skalę.

Spółdzielnia, oprócz danych lokatorów, przetwarzała dane także innych osób (odwiedzających mieszkańców, korzystających z punktów handlowo-usługowych), dlatego, zdaniem organu, przetwarzała ona dane na dużą skalę.

Decyzja prezesa UODO została zaskarżona do sądu. Wojewódzki Sąd Administracyjny w Warszawie w wyroku o sygn. II SA/Wa 2412/19 uchylił ją w części odnoszącej się do wyznaczenia IOD, podnosząc, że organ nie wykazał dostatecznie potrzeby podjęcia takiego działania.

Wyrok nie jest prawomocny, co wskazuje, że analiza przepisów o obowiązku wyznaczenia IOD nastręcza wiele trudności.

Pojęcia takie jak „duża skala", „główna działalność" czy „monitorowanie" nie posiadają legalnych definicji, a ich konkretne znaczenia ustalane są dla każdej organizacji indywidulanie, uwzględniając to jak, w jakim zakresie i w jakich okolicznościach przetwarza ona dane osobowe.

Dla przykładu, trudność interpretacyjna polega na tym, że „duża skala" dla podmiotu przetwarzającego dane osobowe w ramach marketingu i zatrudniającego 100 osób, ale posiadającego tylko 20 klientów będzie czym innym niż „duża skala" dla prywatnej przychodzi okulistycznej, zatrudniającej 10 osób, ale obsługującej całe województwo.

Powyższe rozstrzygnięcie pokazuje, że organ może zająć odmienne stanowisko od stanowiska organizacji w zakresie wyznaczenia IOD, ale punktem wyjścia winna być zawsze rzetelna analiza obowiązku wyznaczenia IOD, co może również stanowić materiał w trakcie ewentualnego sporu sądowego z organem.

KARA ZA BRAK WYZNACZENIA IOD OBOK KAR ZA INNE UCHYBIENIA

Jak kwestia braku wyznaczenia IOD wygląda na „zagranicznym podwórku”?

Przykładowo, belgijski organ nadzorczy (Autorité de protection des données) w decyzji 21/2022 z 2 lutego 2022 r. (nr DOS-2019-01377) nakazał Interactive Advertising Bureau Europe (IAB) wyznaczenie IOD w związku z przetwarzaniem danych osobowych w ramach narzędzia służącego do łatwego zapisywania preferencji użytkowników w odniesieniu do kwestii reklamowych, tj. Transparency & Consent Framework (TCF). Za brak wyznaczenia IOD oraz pozostałe stwierdzone naruszenia organ nałożył karę w wysokości 250 tys. euro oraz 5 tys. euro za każdy dzień zwłoki w realizacji obowiązków nałożonych decyzją, w tym zwłokę w wyznaczeniu IOD.

W toku postępowania IAB twierdziło, że nie ma obowiązku wyznaczenia IOD. Organ był odmiennego zdania, twierdząc m.in. że IAB przetwarza dane osobowe w związku z czynnością monitorowania osób na dużą skalę z wykorzystaniem standardu TCF, co stanowi działalność o głównym charakterze.

Wskazując, że przetwarzanie odbywa się na dużą skalę, organ podniósł zaś, że narzędzie TCF wykorzystywane jest w wielu państwach UE, dane są udostępniane wielu reklamodawcom i są przetwarzane przez długi okres (tak długo, jak długo konieczne jest wykazanie, że zgoda została uzyskana zgodnie z polityką TCF). Organ uznał więc, że zachodzi obowiązek wyznaczenia IOD z uwagi na w/w okoliczności.

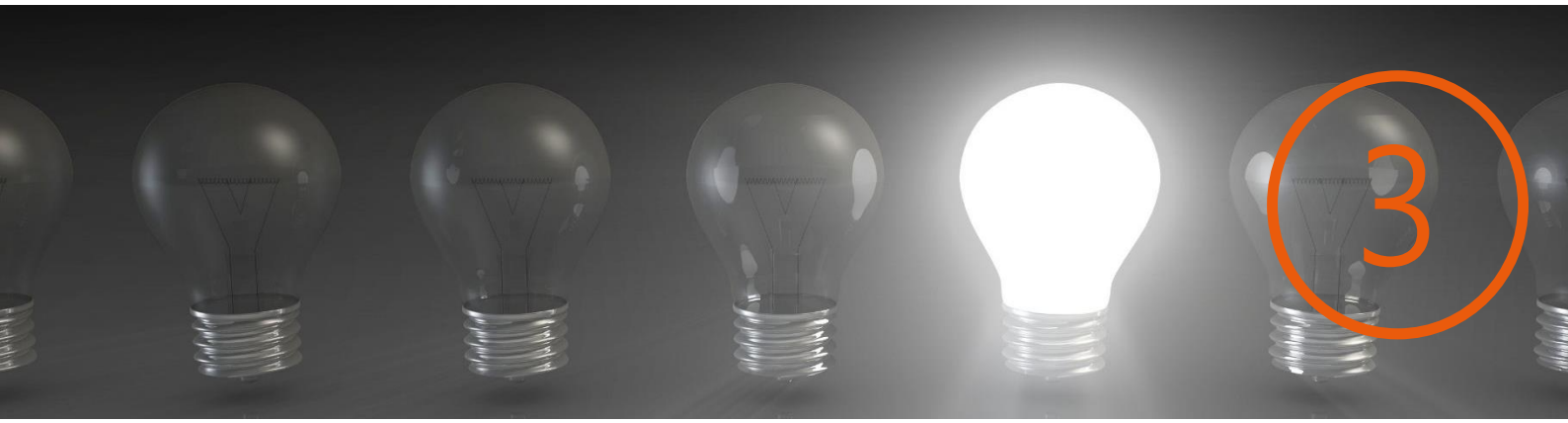
!

Rozstrzygnięcie belgijskiego organu zostało zaskarżone, a obecnie z uwagi na pytania prejudycjalne belgijskiego sądu w zakresie statusu IAB jako administratora oraz w kwestii tego, czy *TC String* (ciągi znaków numerycznych zawierających odpowiednie preferencje użytkowników) stanowi dane osobowe w rozumieniu RODO, finalne rozstrzygnięcie zostało zawieszone do momentu uzyskania odpowiedzi od Trybunału Sprawiedliwości Unii Europejskiej. Odpowiedź na pytania prejudycjalne będzie więc mieć wpływ na ocenę, czy IAB ma obowiązek wyznaczenia IOD oraz przyniesie wskazówki interpretacyjne dla rynku.

Niezależnie od odpowiedzi TSUE, już na etapie decyzji krajowego organu nadzorczego, administratorzy powinni pamiętać, że ocena obowiązku wyznaczenia IOD nie jest analizą oderwaną od okoliczności biznesowych i wymaga dogłębnej znajomości procesów przetwarzania oraz odpowiedzi na liczne pytania, np. jaką rolę pełni podmiot dokonujący analizy w przetwarzaniu danych, z wykorzystaniem jakich narzędzi dane są przetwarzane, jak wiele danych jest zbieranych i jak długo będą przechowywane oraz na czym konkretnie polega mechanizm monitorowania.

Artykuł powstał dla dziennika „**Rzeczpospolita**” i został opublikowany na jego łamach dnia 23.02.2024 roku.

Link do artykułu >>> **PRZECZYTAJ CAŁY TEKST** <<<



Jak wyznaczyć inspektora ochrony danych – poradnik

Anna Matusiak-Wekiera

Ewelina Kęciek

Wyznaczenie inspektora ochrony danych w organizacji wymaga nie tylko sporządzenia i udokumentowania procedur dotyczących jego funkcjonowania, ale także podjęcia czynności formalnych, takich jak skierowanie zawiadomienia do organu nadzorczego czy publikacja danych kontaktowych inspektora. Brak realizacji tych obowiązków stanowi naruszenie przepisów RODO – dostrzegane i karane przez europejskie organy nadzorcze.

Inspektor ochrony danych (IOD) jest odpowiedzialny za budowanie kultury ochrony danych osobowych w organizacji. Jak po blisko sześciu latach od rozpoczęcia stosowania przepisów RODO wypełniana jest w praktyce ta rola? Z jakimi problemami mierzą się inspektorzy ochrony danych? Jakich rad udziela prezes Urzędu Ochrony Danych Osobowych organizacjom, które wyznaczyły IOD, a także samym inspektorom? Jakie wnioski w zakresie pełnienia tej funkcji można wysnuć na podstawie rozstrzygnięć zagranicznych organów ochrony danych osobowych? Na te pytania odpowiemy w cyklu artykułów poświęconych praktycznym problemom związanym z wyznaczeniem i funkcjonowaniem inspektora ochrony danych w organizacji.

1. WYZNACZENIE INSTEKTORA DANYCH – FORMALNA DECYZJA

Organizacje, które zobowiązane są do wyznaczenia IOD zgodnie z przepisami RODO (pisaliśmy o tym w artykule z 23 lutego TUTAJ) lub które podjęły decyzję o wyznaczeniu tej roli z uwagi na standardy ochrony danych osobowych powinny pamiętać, że niezbędne jest dopełnienie wymogów formalnych dla wyznaczenia IOD.

Pierwszym punktem na liście zadań organizacji, która decyduje się na wyznaczenie IOD powinno być sformalizowanie tej decyzji i jej wydanie przez organ uprawniony do prowadzenia spraw w imieniu organizacji – np. poprzez podjęcie stosownej uchwały zarządu, zarządzenia lub w inny przyjęty sposób. Zazwyczaj konieczne może okazać się również podjęcie dodatkowych czynności zapewniających IOD jego status, gwarantujących mu odpowiednie zasoby oraz możliwości raportowania bezpośrednio do najwyższego kierownictwa.

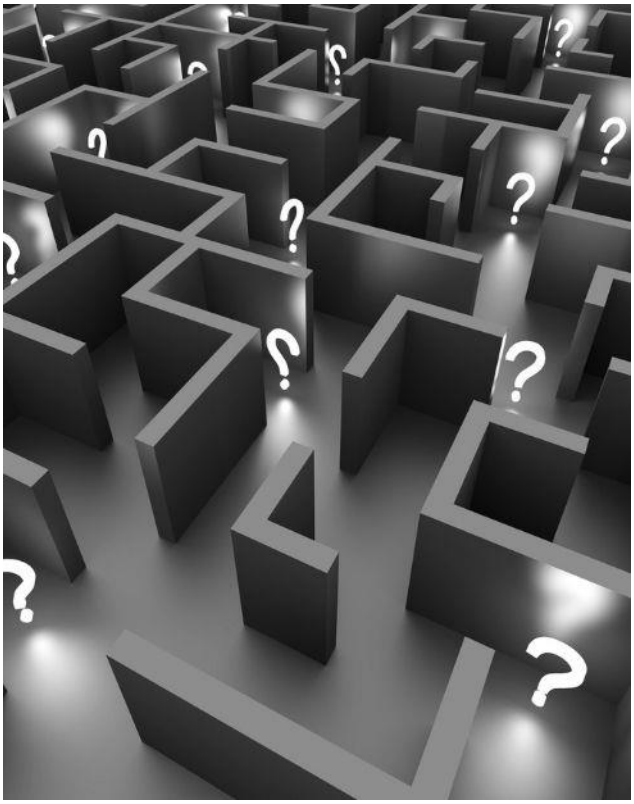
Dobrą praktyką może być również przyjęcie regulaminu biura IOD, który szczegółowo określa procedurę działania inspektora, oraz poinformowanie o zasadach działania inspektora pracowników organizacji. Taki regulamin może być przydatnym narzędziem rozliczalności pracy IOD.

2. WYZNACZENIE IOD W GRUPIE

Zgodnie z przepisami RODO, grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych, o ile można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej.

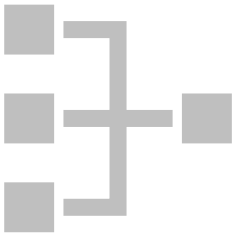
Dla przedsiębiorców sporym ułatwieniem mogłoby być, gdyby formalne wyznaczenie IOD przez jedną spółkę z grupy (co do zasady przez spółkę matkę) pozwalało na przyjęcie, że IOD został wyznaczony także przez inne spółki z tej grupy. W praktyce jednak tak nie jest – każda ze spółek z grupy musi to zrobić samodzielnie.

Boleśnie przekonała się o tym fakcie niemiecka spółka Facebook (Facebook Germany GmbH), na którą hamburski organ ochrony danych osobowych (Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit) nałożył w 2019 r. karę w wysokości 51 tys. euro za brak zawiadomienia o wyznaczeniu IOD przez ten podmiot. Spółka argumentowała przed organem, że IOD został wyznaczony przez spółkę irlandzką i będzie sprawować tę funkcję także wobec innych europejskich spółek z grupy. Zdaniem organu było to niewystarczające, a lokalne spółki powinny były niezależnie wyznaczyć i zawiadomić o wyznaczeniu IOD.



Ułatwieniem w przypadku grupy przedsiębiorstw jest fakt, że funkcję IOD może sprawować ta sama osoba, nie zaś okoliczność, że część spółek może zrezygnować z formalnego wyznaczenia i zawiadomienia o wyznaczeniu IOD lokalnych organów nadzorczych.

Usprawnienie to doznaje jednak pewnych ograniczeń – legislator unijny wskazał bowiem, że dana osoba może pełnić funkcję IOD dla spółek z grupy pod warunkiem, że łatwo będzie można z nią nawiązać kontakt z każdego podmiotu.



Organizacje z jednej grupy, wyznaczające jednego IOD powinny zatem sprawdzić, czy – przykładowo – wyznaczenie IOD posługującego się tylko językiem angielskim będzie funkcjonalne w przypadku, gdy pracownicy spółek z grupy nie mają obowiązku komunikować się w tym języku i bieżące sprawy załatwiają w lokalnych językach, np. po polsku. Powyższe okoliczności mogą bowiem podlegać ocenie organów nadzorczych.

Pewnym rozwiązaniem mogłoby być zapewnienie IOD wsparcia w zakresie tłumaczeń, o ile nie będzie to opóźniało reakcji inspektora.

3. PUBLIKACJA DANYCH KONTAKTOWYCH IOD

Kolejnym obowiązkiem organizacji, która wyznaczyła IOD, jest publikacja danych kontaktowych inspektora i zawiadomienie o nich organu nadzorczego.

Przez publikację danych rozumie się podanie ich do wiadomości wewnętrznie (w ramach organizacji) i zewnętrznie – dla osób, których dane dotyczą i innych potencjalnie zainteresowanych podmiotów. Choć jest to obowiązek bardzo formalny – a wręcz techniczny – brak jego przestrzegania nie umyka organom nadzorczym.

Przykład 1

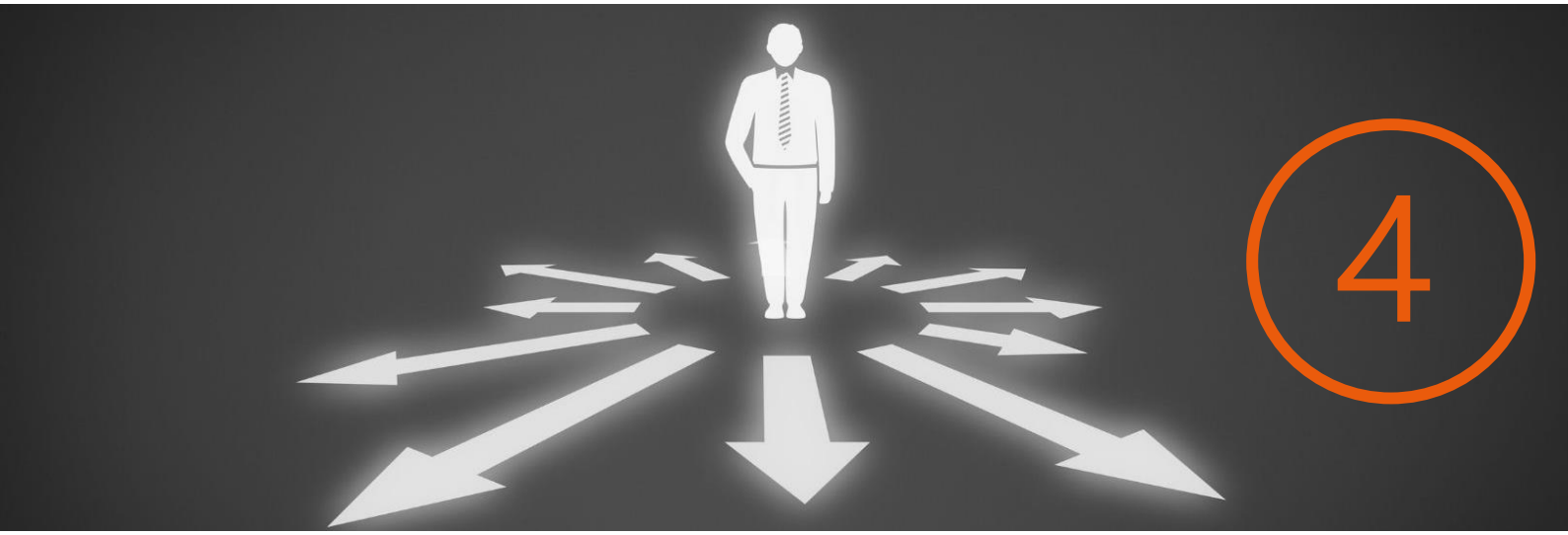
- Luksemburski organ ochrony danych osobowych (La Commission nationale pour la protection des données) nałożył na kontrolowany przez siebie podmiot publiczny karę pieniężną w wysokości 18 tys. euro m.in. za brak podania danych kontaktowych IOD (>patrz decyzja 15 października 2021 r., nr 38FR/2021).
- Organ wskazał, że strona internetowa podmiotu nie zawierała zakładki odnoszącej się do ochrony danych osobowych, a jednocześnie jedyna informacja poświęcona temu zagadnieniu była dostępna w języku angielskim, a więc nie była przekazana w żadnym języku urzędowym Luksemburga. Kontrolowany podmiot jeszcze w toku postępowania naprawił powyższe uchybienia – dodał do swojej strony internetowej odrębną zakładkę poświęconą ochronie danych osobowych, a informacje na ten temat przetłumaczył na francuski i niemiecki.
- Choć organ uznał te działania za właściwe, stwierdził, że zważywszy, że uchybienie w zakresie braku dostatecznego wskazania danych IOD miało miejsce przez jakiś czas – w szczególności w dacie wszczęcia postępowania – nałożenie kary pieniężnej wciąż było zasadne.

Przykład 2

- Na podobnym stanowisku organ luksemburski stanął także w sprawie dotyczącej podmiotu prywatnego, który na swojej stronie internetowej nie zamieścił bezpośrednich danych kontaktowych do IOD, lecz formularz, który co do zasady należało kierować na ogólny adres e-mail lub adres do korespondencji.
- Zdaniem luksemburskiego organu, konieczne było wskazanie danych umożliwiających bezpośredni kontakt z inspektorem – w szczególności zasadne było opublikowanie ich w części polityki prywatności dotyczącej realizacji praw podmiotów danych wynikających z przepisów RODO. M.in. za powyższe uchybienie spółka została ukarana administracyjną karą pieniężną w wysokości 18 tys. 700 euro (patrz decyzja z 27 października 2021 r., nr 41FR/2021).

Artykuł powstał dla dziennika „**Rzeczpospolita**” i został opublikowany na jego łamach dnia 22.03.2024 roku.

Link do artykułu >>> **PRZECZYTAJ CAŁY TEKST** <<<



Niezależność inspektora ochrony danych – kiedy dochodzi do konfliktu interesów?

Anna Matusiak-Wekiera

Ewelina Kęciek

Ostatnie miesiące przyniosły restrykcyjne interpretacje organów dotyczące konfliktu interesów inspektorów ochrony danych i krytyczne wobec tych interpretacji stanowiska biznesu. Warto je poznać, aby zapewnić IOD odpowiedni poziom niezależności.

Inspektor ochrony danych jest odpowiedzialny za budowanie kultury ochrony danych osobowych w biznesie. Jak po blisko sześciu latach od rozpoczęcia stosowania przepisów RODO w praktyce wygląda pełnienie tej roli? Z jakimi problemami mierzą się inspektorzy ochrony danych? Jakich rad udziela prezes Urzędu Ochrony Danych Osobowych organizacjom, które powołały IOD, a także samym inspektorom? Jakie wnioski w zakresie pełnienia tej funkcji można wysnuć na podstawie rozstrzygnięć zagranicznych organów ochrony danych osobowych? Na te pytania odpowiemy w cyklu artykułów poświęconych praktycznym problemom związanym z powołaniem i funkcjonowaniem inspektora ochrony danych w organizacji.

Praktyka ostatnich lat pokazała, że zaprojektowanie efektywnego systemu ochrony danych osobowych, a zatem takiego, który zapewnia realne bezpieczeństwo danych osobowych i chroni biznes przed zarzutem naruszenia przepisów RODO, rozpoczyna się od zapewnienia inspektorowi ochrony danych odpowiedniego statusu w organizacji. Obowiązek zapewnienia warunków organizacyjnych i faktycznych dla prawidłowego wykonywania przez IOD obowiązków powstaje bez względu na to, czy organizacja wyznaczyła IOD z uwagi na swój prawny obowiązek czy też dobrą praktykę. W tym kontekście na szczególną uwagę zasługuje obowiązek, aby IOD nie działał w warunkach konfliktu interesów.

Sposób zapewnienia niezależności inspektorom ochrony danych od dawna jest analizowany przez organizacje, które wyznaczyły IOD i organy nadzorcze. Dobitnym dowodem może być chociażby spotkanie zorganizowane przez prezesa UODO na początku kwietnia 2024 r. „Niezależność inspektora ochrony danych w świetle skoordynowanego działania EROD CEF DPO". Poziom dyskusji, liczba poruszanych problemów, jak również liczba stanowisk praktyków, które pojawiły się po tym wydarzeniu była tak duża, że organ wyznaczył dedykowany adres email, na który można było zgłaszać swoje stanowiska dotyczące konfliktu interesów w ramach sprawowania funkcji IOD.

Licząc na to, że powyższe spotkanie przyniesie nowe rekomendacje organu, już teraz należy zastanowić się, kiedy IOD może mieć do czynienia z konfliktem interesów.

1. KTO ODPOWIE ZA TO, ŻE IOD NIE DZIAŁA PAWIDŁOWO?

Zanim opowiemy o niezależności IOD, przypomnijmy, że to organizacja ponosi odpowiedzialność za naruszenie przepisów RODO dotyczących wykonywania zadań przez inspektora. Zgodnie z przepisami podmioty wyznaczające IOD są zobowiązane do zapewnienia, aby IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych, aby miał niezbędne zasoby do wykonania swoich zadań i utrzymania wiedzy fachowej oraz posiadał stały dostęp do danych osobowych i operacji przetwarzania. W praktyce kwestia ta jest weryfikowana przez organy nadzorcze, co znajduje odzwierciedlenie w wydawanych decyzjach.

Przykładowo, prezes Urzędu Ochrony Danych Osobowych w decyzji z 21 sierpnia 2020 r. dotyczącej Szkoły Głównej Gospodarstwa Wiejskiego nałożył karę pieniężną m.in. za uchybienie polegające na tym, iż IOD wypełniał swoje zadania bez należytego uwzględnienia ryzyka związanego z operacjami przetwarzania oraz z uwagi na brak właściwego angażowania przez administratora w procesy przetwarzania danych osobowych (patrz nasz artykuł TUTAJ).

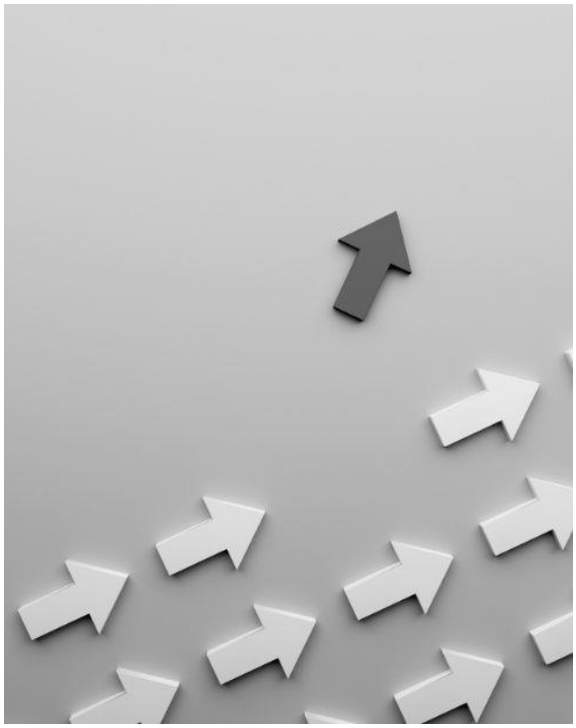
Na europejskim podwórku również nie brakuje kar organów nadzorczych za naruszenie przepisów RODO dotyczących statusu IOD i wykonywania przez niego obowiązków z naruszeniem zakazu konfliktu interesów.

Przykład 1

Berliński organ nadzorczy (Die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI)) w 2022 r. nałożył karę pieniężną w wysokości 525 tys. euro za wyznaczenie na inspektora w spółce zależnej osoby, która była dyrektorem zarządzającym dwóch firm usługowych, które przetwarzały dane osobowe w imieniu tej samej firmy, w której pracownik był zatrudniony jako IOD. Zdaniem organu, IOD w takiej organizacji nie był niezależny. Karę nałożono jednak na spółkę, a nie inspektora.

2. DLACZEGO NIEZALEŻNOŚCI IOD JEST TAK WAŻNA

IOD oprócz licznych zadań o charakterze doradczym i audytorskim, jakie wyznacza mu RODO, pełni również funkcję punktu kontaktowego dla osób fizycznych. Oznacza to, że nie działa on wyłącznie w interesie administratora czy podmiotu przetwarzającego, który go zatrudnia, ale wspiera swoją pracą również osoby fizyczne w realizacji ich praw przewidzianych w RODO, zapewniając klarowną i skuteczną komunikację.



Z drugiej strony, IOD pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych, by umożliwić organowi dostęp do dokumentów i informacji w celu realizacji jego kompetencji. Dzisiaj wiemy już z licznych decyzji, że brak współpracy z organem jest traktowany jako uchybienie, które może skutkować nałożeniem kary pieniężnej.

W praktyce zatem brak współpracy inspektora z organem w tym zakresie może stanowić naruszenie przepisów obciążające administratora. Tutaj należy upatrywać między innymi podstaw dla oceny „delikatnego charakteru stanowiska inspektora”, o którym mowa w „Podręczniku inspektora ochrony danych. Wytyczne dla inspektorów ochrony danych w sektorze publicznym i quasi-publicznym” (obowiązkowa lektura wszystkich IOD).

Wykonywanie zadań IOD jest niemożliwe bez zagwarantowania mu pełnej niezależności, rozumianej jako brak wpływu organizacji na dokonywaną przez IOD wykładnię przepisów oraz działanie w warunkach wolnych od konfliktu interesów przy realizacji wszelkich zadań, w tym w ramach pełnienia funkcji punktu kontaktowego.

!

3. JAKIE SĄ GWARANCJE NIEZALEŻNOŚCI IOD W WYKONYWANIU ZADAŃ

Niezależność inspektora w wykonywaniu zadań opiera się na czterech gwarancjach wskazanych w przepisach RODO, które stanowią jednocześnie obowiązki organizacji, która wyznaczyła IOD.

Gwarancje te są następujące:

- nakaz, aby wykonywanie dodatkowo powierzonych IOD zadań odbywało się w warunkach wyłączających konflikt interesów;
- zakaz wydawania inspektorowi instrukcji dotyczących sposobu wykonywania przez niego zadań;
- zakaz zwolnienia lub karania IOD w związku z wykonywaniem przez niego zadań;
- nakaz, aby inspektor podlegał wyłącznie najwyższemu kierownictwu w organizacji.

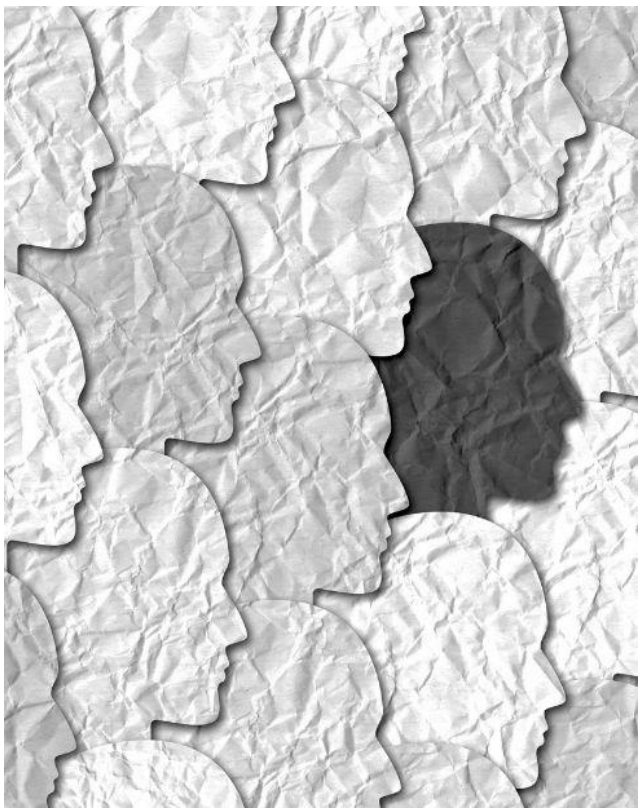
Odpowiedzialnym za zapewnienie statusu niezależnego wykonywania przez IOD zadań jest podmiot, który go wyznaczył – bez względu na to, czy pełni rolę administratora, czy podmiotu przetwarzającego.

Również charakter zatrudnienia IOD nie ma znaczenia dla tego obowiązku – jego treść jest taka sama dla inspektora zatrudnionego w oparciu umowę o pracę, jak i dla IOD zatrudnionego w oparciu o outsourcing usługi.

Praktyczny wymiar powyższych gwarancji nie jest pozbawiony wątpliwości, które rozstrzygane są nie tylko na poziomie krajowym, ale także europejskim.

W wyroku z 9 lutego 2023 r. (C-453/21, X-FAB Dresden GmbH & Co. KG przeciwko FC) Trybunał Sprawiedliwości UE podniósł, że, co do zasady, przepisy krajowe mogą przewidywać możliwość odwołania IOD będącego członkiem personelu jedynie z ważnej przyczyny, nawet jeśli odwołanie nie jest związane z wypełnianiem przez niego zadań.

W omawianej sprawie administrator chciał zakończyć współpracę z IOD z uwagi na fakt, że pracownik został wyznaczony na inspektora w kilku spółkach z grupy, jednocześnie pełniąc funkcję przewodniczącego rady zakładowej oraz wiceprzewodniczącego centralnej rady zakładowej. To, zdaniem pracodawcy, stwarzało ryzyko konfliktu interesów.



TSUE nie przesądził, czy w tej sprawie faktycznie do takiego konfliktu doszło – wskazał jednak, że sąd krajowy powinien to ocenić, biorąc pod uwagę, czy wspomniane dodatkowe zadania inspektora nie powodują ustalania przez IOD celów i sposobów przetwarzania, co stanowiłoby o braku jego niezależności.

Artykuł powstał dla dziennika „**Rzeczpospolita**” i został opublikowany na jego łamach dnia 26.04.2024 roku.

Link do artykułu >>> **PRZECZYTAJ CAŁY TEKST** <<<

Czego inspektor ochrony danych nie zrobi za administratora?

Anna Matusiak-Wekiera

Ewelina Kęciek

Rynek powierza inspektorom wykonywanie wszelkich możliwych zadań w zakresie ochrony danych osobowych, w tym obowiązków wprost przypisanych w RODO do administratora. Co na to prezes UODO i inne organy nadzorcze?

Inspektor ochrony danych (IOD) – to osoba odpowiedzialna za budowanie kultury ochrony danych osobowych w biznesie. Jak po blisko sześciu latach od rozpoczęcia stosowania przepisów RODO w praktyce wygląda pełnienie tej roli? Z jakimi problemami mierzą się inspektorzy ochrony danych? Jakich rad udziela prezes Urzędu Ochrony Danych Osobowych organizacjom, które powołały IOD, a także samym inspektorom? Jakie wnioski w zakresie pełnienia tej funkcji można wysnuć na podstawie rozstrzygnięć zagranicznych organów ochrony danych osobowych? Na te pytania odpowiemy w cyklu artykułów poświęconych praktycznym problemom związanym z powołaniem i funkcjonowaniem inspektora ochrony danych w organizacji.

Analizując obowiązki inspektorów ochrony danych oraz zadania, które nie mogą zostać im powierzone, kluczowa jest ocena kompetencji inspektora ochrony danych. Zgodnie z przepisami RODO, inspektorzy są wyznaczani na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań przypisanych im w przepisach RODO.

Nie dla każdej organizacji te same kwalifikacje

Ocena przydatności kandydata do wykonywania funkcji IOD pozostaje w dyspozycji organizacji wyznaczającej IOD, która zobowiązana jest do ustalenia, czy konkretna osoba posiada wystarczające kwalifikacje, aby pełnić w tej organizacji tę funkcję. RODO nakłada na administratora obowiązek zastosowania odpowiednich środków technicznych i organizacyjnych, które – uwzględniając indywidualny charakter, zakres, kontekst i cele przetwarzania – powinny być dostosowane do zidentyfikowanych ryzyk naruszenia praw lub wolności osób fizycznych. Zasada ta ma również zastosowanie przy wyborze inspektora, który każdorazowo ma być „uszyty na miarę" potrzeb danej organizacji i którego wyznaczenie (a przede wszystkim działanie) wzbogaca listę stosowanych przez organizację środków bezpieczeństwa.

W Polsce ustawodawca nie zdecydował się, wzorem innych państw, na doprecyzowanie wymogów kwalifikacyjnych dla IOD i w tym zakresie obowiązujące są przepisy RODO i wskazane wyżej wymagania. Niezbędny poziom wiedzy fachowej należy więc ustalić w szczególności w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają dane osobowe przetwarzane przez organizację. Oznacza to, że dla różnych organizacji odpowiedni będą inspektorzy posiadający odmienne kwalifikacje, a nawet posiadający różny poziom wiedzy w zakresie ochrony danych osobowych - w szczególności z uwagi na przepisy i praktyki branżowe.

Przykład

Luksemburski organ ochrony danych osobowych (La Commission nationale pour la protection des données) stwierdził, że wyznaczenie na inspektora osoby, która wprawdzie zna i rozumie branżę, ale nie posiada przeszkolenia w kwestiach prawnych, ochrony danych lub IT, ani doświadczenia w tej dziedzinie, nie spełnia wymogów przewidzianych przez przepisy RODO. Administrator uniknął kary pieniężnej, gdyż w momencie wszczęcia postępowania (który był oceniany przez organ) inspektorem była osoba posiadająca odpowiednie umiejętności w zakresie prawa i ochrony danych, która to dopiero została zastąpiona inspektorem o zbyt niskich kwalifikacjach (patrz decyzja z 15 października 2021 r., nr 38FR/2021, o której pisaliśmy w artykule „**Jak wyznaczyć inspektora ochrony danych – poradnik**”).

Obowiązki IOD

Kwalifikacje inspektorów są tym bardziej istotne, że przypisane IOD zadania robią się coraz bardziej skomplikowane. Przepisy RODO określają minimalny katalog zadań inspektora w przedmiocie ochrony danych osobowych. Do głównych kompetencji IOD należy:

- informowanie organizacji o obowiązkach wynikających z przepisów prawa
- monitorowanie przestrzegania przepisów prawa oraz wewnętrznych polityk
- działania zwiększające świadomość w zakresie ochrony danych, w tym szkolenia i audyty
- pełnienie funkcje punktu kontaktowego dla organu nadzorczego oraz dla osób fizycznych, których dane są przetwarzane, w szczególności w zakresie realizacji ich praw
- udzielanie zaleceń dotyczących oceny skutków dla ochrony danych (na żądanie organizacji)

Artykuł powstał dla dziennika „**Rzeczpospolita**” i został opublikowany na jego łamach dnia 31.05.2024 roku.
Link do artykułu >>> **PRZECZYTAJ CAŁY TEKST** <<<

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

Kontakt

Anna Matusiak-Wekiera
Radczyni prawna
Head of Data Protection/ Compliance
anna.matusiak-wekiera@jdp-law.pl