



TEMAT: „Inspektor Ochrony Danych Osobowych – zadania i rola”

Czy administrator musi podać imię i nazwisko Inspektora Ochrony Danych Osobowych - IOD na stronie internetowej?

- Podanie imienia i nazwiska inspektora ochrony danych na stronie internetowej podmiotu, który go wyznaczył, jest obowiązkowe. Obowiązek ten wynika wprost z przepisów prawa.
- Zgodnie z art. 37 ust. 7 RODO, administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych. Sposób realizacji tego obowiązku doprecyzowany został w art. 11 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. W przepisie tym wskazano, że podmiot, który wyznaczył inspektora, udostępnia dane inspektora w zakresie: imię i nazwisko oraz adres poczty elektronicznej lub nr telefonu inspektora, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności.

Czy dane kontaktowe IOD muszą być łatwo dostępne?

- Celem obowiązku publikowania przez administratora na swojej stronie internetowej imienia i nazwiska oraz adresu poczty elektronicznej lub numeru telefonu inspektora ochrony danych jest zapewnienie, aby osoby, których dane dotyczą, mogły mieć łatwy i bezpośredni kontakt z inspektorem, bez konieczności kontaktowania się z innymi jednostkami podmiotu [Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (WP 243), str. 13, dostępne na stronie internetowej UODO pod linkiem: <https://uodo.gov.pl/pl/10/7>].
- Jeśli administrator prowadzi własną stronę internetową, dane o wyznaczonym IOD powinny znaleźć się w łatwo dostępnym miejscu strony, np. w zakładce: „Kontakt”, „Inspektor ochrony danych”, „RODO” czy „Ochrona danych osobowych”. Za niewłaściwe należy natomiast uznać publikowanie tych danych w miejscach wymagających długiego przeszukiwania, takich jak „Aktualności” czy „Polityka prywatności” (<https://uodo.gov.pl/pl/138/569>).
- Zgodnie z RODO jednym z zadań inspektora ochrony danych (IOD) jest pełnienie roli punktu kontaktowego, czyli pośrednika między administratorem lub podmiotem przetwarzającym a osobami, których dane dotyczą. Unijny prawodawca w art. 38 ust. 4 RODO uprawniał osoby, których dane dotyczą, do kontaktowania się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO. Ta rola inspektora jest mocno powiązana z obowiązkami administratora oraz podmiotu przetwarzającego określonymi w art. 12-22 RODO i ma przyczyniać się do skuteczniejszego ich wykonywania.
- Przykładem może tu być sytuacja, gdy dochodzi do naruszenia ochrony danych, które może powodować wysokie ryzyko naruszenia praw i wolności. W takim przypadku znaczenie praw osób oraz roli inspektora uwydatnia się w sposób szczególny.

Jakie zadania ma IOD?

- Informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

Aby kompetentnie edukować i doradzać innym IOD musi być do tego dobrze przygotowany merytorycznie, musi sam bardzo dobrze znać obowiązki administratorów i podmiotów przetwarzających oraz powiązane z nimi uprawnienia podmiotów danych. Dbanie o edukację osób podejmujących działania i decyzje w zakresie ochrony danych osobowych jest działaniem ciągłym i powtarzalnym, wymagającym umiejętności interpersonalnych i dydaktycznych.

- Monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

Aktywność inspektora ochrony danych w tym zakresie nie powinna mieć charakteru jednorazowego, a charakter ciągły i długofalowy. Zgodnie z Wytycznymi Grupy Roboczej art. 29 dotyczącymi inspektorów ochrony danych monitorowanie to:

- zbieranie informacji w celu identyfikacji procesów przetwarzania; analizowanie i sprawdzanie zgodności przetwarzania;
- informowanie, doradzanie i rekomendowanie określonych działań.

Wykonując ten obowiązek inspektor ochrony danych powinien dostosować sposób i rodzaj przekazywanych informacji do grupy docelowej, tak aby zadanie to było realizowane w sposób efektywny i skuteczny.

- Udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35,

Zgodnie z art. 35 ust. 2 RODO administrator dokonując oceny skutków konsultuje się z IOD, jeżeli został wyznaczony, w celu wydania przez niego zaleceń.

RODO określa, kiedy i jak należy dokonywać oceny skutków dla ochrony danych, natomiast nie zawiera konkretnych wskazówek, w jaki sposób oceny takiej należałoby dokonać. Pomocne w tym zakresie mogą być Wytyczne Grupy Roboczej art. 29, zgodnie z nimi administrator dokonując ww. oceny powinien konsultować się z IOD w następujących kwestiach:

- czy należy przeprowadzić ocenę skutków dla ochrony danych;
- metodologii przeprowadzenia oceny skutków dla ochrony danych;
- czy należy przeprowadzić wewnętrzną ocenę czy też zlecić ją podmiotowi zewnętrznemu;
- zabezpieczeń (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą; prawidłowości przeprowadzonej oceny skutków dla ochrony danych i zgodności jej wyników z RODO (czy należy kontynuować przetwarzanie, czy też nie oraz jakie zabezpieczenia należy zastosować).

Jeśli administrator nie zgadza się z zaleceniami IOD w wyżej wymienionych przypadkach, dokumentacja oceny skutków dla ochrony danych powinna zawierać pisemne uzasadnienie nieuwzględnienia zaleceń IOD.

- Współpraca z Prezesem Urzędu Ochrony Danych Osobowych,

Zgodnie z artykułem 39 ust. 1 lit. D RODO, IOD powinien współpracować z organem nadzorczym w kwestiach związanych z przetwarzaniem danych osobowych oraz w stosownych przypadkach zwracać się do niego.

- Pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,

Pełnienie przez IOD funkcji punktu kontaktowego należy traktować jako pełnienie przez niego roli pośrednika pomiędzy administratorem lub podmiotem przetwarzającym, a organem nadzorczym.

IOD z jednej strony udziela fachowego wsparcia administratorowi w zakresie sposobu wykonania obowiązków nałożonych na administratora wynikających z RODO, z drugiej strony wspomaga go przed organem nadzorczym w wykazaniu zasadności wybranych rozwiązań w ramach prowadzonych przez organ postępowań.

Obowiązek pełnienia roli punktu kontaktowego przez IOD dla organu nadzorczego, wynika z art. 39 ust. 1 lit. e RODO. Wobec czego, jeżeli organ nadzorczy zwróci się do IOD o udzielenie mu informacji w określonych przypadkach (w tym dostępu do dokumentów), inspektor powinien się z tego obowiązku należycie wywiązać.

Poniżej przykłady sytuacji, w których IOD będzie pełnił funkcję punktu kontaktowego.

W przypadku zgłoszenia naruszenia ochrony danych przez administratora Prezesowi Urzędu Ochrony Danych Osobowych, administrator jest zobowiązany do podania danych kontaktowych IOD w celu uzyskania przez organ wszelkich ważnych w tej sprawie informacji. Przepis ten zobowiązuje jednocześnie inspektora ochrony danych do współpracy oraz przekazywania wszelkich niezbędnych informacji Prezesowi Urzędu.

punkt kontaktowy w zakresie uprzednich konsultacji (art. 36 RODO).

Zgodnie z art. 35 RODO na administratora danych nałożony jest obowiązek dokonywania oceny skutków dla ochrony danych oraz konsultowania się w tej sprawie z powołanym IOD. Ponadto, w przypadku, gdy zmienia się ryzyko wynikające z operacji przetwarzania administrator powinien dokonać przeglądu, by stwierdzić czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.

Jeżeli ocena ta wykaże, że przetwarzanie może powodować wysokie ryzyko przy braku zastosowania przez administratora środków dla zminimalizowania tego ryzyka, to zgodnie z art. 36 RODO administrator konsultuje się w tej sprawie z Prezesem Urzędu Ochrony Danych Osobowych. Zasadne jest założenie, że IOD jako doradca administratora, powinien w tej sprawie ściśle współpracować z Prezesem Urzędu, przedstawiając wszystkie istotne aspekty mogące mieć wpływ na treść przyszłego zalecenia.

- Pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.

Osoby, których dane dotyczą, zgodnie z art. 38 ust. 4 RODO, powinny mieć możliwość skontaktowania się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia. W związku z tym, na stronie internetowej administratora lub podmiotu przetwarzającego powinny się znaleźć dane kontaktowe inspektora ochrony danych, umożliwiające kontakt z nim zainteresowanym podmiotom. W dużej organizacji, ilość pytań wpływających do IOD może być tak duża, że mogłoby to powodować trudności w wykonywaniu przez niego innych zadań. W związku z powyższym pożądanym byłoby w takim przypadku, wyznaczenie pracowników lub powołanie zespołu osób, które wspierałyby inspektora ochrony danych w zakresie wykonywania tego zadania.

Zadania inspektora ochrony danych w RODO zostały sformułowane w sposób ogólny, bez wskazania trybu oraz terminów ich realizacji. Taki sposób ujęcia obowiązków inspektora jest wyrazem nowego podejścia do ochrony danych osobowych opartego na analizie ryzyka i zasadzie rozliczalności, zapisanej w art. 5 ust. 2 RODO. Wyznaczenie IOD roli doradczej i weryfikacyjnej wobec działań administratora danych i podmiotu przetwarzającego (oraz ich pracowników) sprawia, że zarówno zadania IOD, jak i sposób ich realizacji są ściśle powiązane nie tylko z obowiązkami administratorów danych lub podmiotów przetwarzających, ale też z nowym sposobem podejścia do ich realizacji.

Należy pamiętać, że podmiotem, który faktycznie podejmuje decyzje i odpowiada za wdrożenie odpowiednich środków technicznych i organizacyjnych, zapewniających odpowiedni stopień bezpieczeństwa oraz wykazanie, że przetwarzanie odbywa się zgodnie z przepisami ochrony danych osobowych jest administrator lub podmiot przetwarzający. Na podstawie art. 24 RODO administratorzy i podmioty przetwarzające są zobowiązani uwzględniać: charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, i odpowiednio do nich - dobierać i wdrażać środki techniczne i organizacyjne, tak, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać.

Środki te powinny być w razie potrzeby poddawane przeglądom i uaktualniane. Ponadto zarówno przy określaniu ilości zbieranych danych osobowych, jak i zakresu ich przetwarzania, okresu przechowywania, dostępności oraz sposobów przetwarzania konieczne jest stosowanie mechanizmów takich jak zapewnienie ochrony danych osobowych na etapie projektowania oraz domyślnej ochrony danych („privacy by design” oraz „privacy by default”), zarówno przed przystąpieniem do przetwarzania danych, jak i w czasie prowadzonego przetwarzania (art. 25 RODO).

Janusz Wyspiański

ŹRÓDŁO DANYCH:

Strona internetowa UODO (uodo.gov.pl). <https://uodo.gov.pl>