Stowarzyszenie Inspektorów Ochrony Danych Osobowych

Warszawa, 29 maja 2024 r.

Sz. P. Mirosław Wróblewski
Prezes Urzędu Ochrony Danych Osobowych

Stanowisko Stowarzyszenia Inspektorów Ochrony Danych Osobowych w sprawie niezależności Inspektora Ochrony Danych

Szanowny Panie Prezesie,

W imieniu SIODO pragniemy złożyć wyrazy podziękowania za otwartość Urzędu oraz podjętą inicjatywę współpracy ze środowiskami zrzeszającymi Inspektorów Ochrony Danych. Jesteśmy przekonani, że podejmowane inicjatywy i zaangażowanie Urzędu przyczynią się do wzmocnienia respektowania konstytucyjnego prawa obywateli do prywatności oraz filozofii i sensu efektywnej realizacji samej istoty stosowania przepisów RODO tj. ochrony praw i wolności osób fizycznych, w szczególności ich prawa do odpowiedniej ochrony danych osobowych.

Doceniamy również inicjatywę mającą na celu wzmocnienie pozycji IOD oraz głos Urzędu wyrażony podczas spotkania pn. „*Niezależność Inspektora Ochrony Danych w świetle skoordynowanego działania EROD CEF DPO*”, a także zapowiadane przez Urząd działania mające na celu wzmacnianie świadomości Administratorów. Godną pochwały jest osobista deklaracja Prezesa UODO o planowaniu bezpośrednich spotkań z kierownictwem organizacji.

Dyskusja podczas spotkania ukazała z jak wieloma praktycznymi problemami borykają się Inspektorzy Ochrony Danych. W sposób stanowczy wskazano jednak, iż IOD nie może wyręczać Administratora w realizacji jego zadań. Powinien natomiast skupiać się na jego wspieraniu poprzez informowanie, budowanie świadomości oraz doradzanie, jednak z zachowaniem ustawowych granic, aby nie prowadzić do konfliktu interesów. Określenie tej "granicy" nie budzi wątpliwości w świetle przepisów, ale pozostaje dość problematyczne w sferze swobodnej interpretacji, ufamy jednak, iż dalsza współpraca UODO ze środowiskiem SIODO pozwoli na stanowcze i konsekwentne budowanie silnej pozycji Inspektorów.

W kontekście przywołanych podczas spotkania atrybutów IOD, takich jak *niezależność*, *obiektywizm* i *skuteczność*, którymi cechować ma się IOD, które potencjalnie zachwiane zostaną poprzez występujący konflikt interesów, a także biorąc pod uwagę budowanie pozycji zawodowej IOD, uważamy, iż warto podjąć szerszą dyskusję na temat tego, jaki ma być kierunek rozwoju statusu IOD – Menedżera systemu ochrony danych osobowych czy Referenta ds. ochrony danych osobowych? Na wariant tego ostatniego nie ma akceptacji środowiska SIODO.

Pragniemy zwrócić szczególną uwagę na rosnącą liczbę nowych aktów prawnych, w szczególności tych dotyczących obszarów bezpieczeństwa informacji i cyberbezpieczeństwa [w skład których, jako aktywo, wchodzą również dane osobowe], których stosowanie będzie ogromnym wyzwaniem dla wielu podmiotów z sektora prywatnego oraz publicznego.

Uważamy, iż profesjonalizacja funkcji IOD powinna być kierunkowana w stronę specjalisty/eksperta w dziedzinie szeroko pojętego bezpieczeństwa informacji o charakterze doradczym, monitorującym, a szczególnie edukacyjnym.

Dyrektywa NIS 2 2022/2555 oraz projekt z dnia 23 kwietnia 2024 r. ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw stanowią doskonały przykład skali wyzwań, stawianych przed Administratorami. Projekt ustawy z dnia 23 kwietnia 2024 r. przewiduje, iż do jej stosowania zobligowane zostaną m.in. Podmioty publiczne tj. jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–6, 8 i 10–13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2023 r. poz. 1270, z późn. zm.), które w myśl przedmiotowej ustawy klasyfikowane są jako podmioty kluczowe. To z kolei implikuje konieczność wdrożenia lub przemodelowania istniejącego dotychczas systemu zarządzania bezpieczeństwem informacji, spełniającego szereg wymagań w myśl obowiązujących przepisów, a którego częścią jest ochrona danych osobowych.

Jest to m.in. prowadzenie systematycznego szacowania ryzyka, opracowywanie oraz wdrażanie do stosowania dokumentacji (procedur, regulaminów etc.), wdrażanie, dokumentowania i utrzymywania planów działania, umożliwiających ciągłe i niezakłócone świadczenie usługi oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, zarządzanie incydentami i wiele innych, w tym również audyty (audyt nie może być przeprowadzony przez osobę realizującą w podmiocie audytowanym zadania, o których mowa w art. 8 i art. 11, lub która realizowała te zadania w podmiocie audytowanym przez rok przed rozpoczęciem audytu.).

Ustawodawca w projekcie ustawy zmieniającej ustawę o krajowym systemie cyberbezpieczeństwa wykluczył możliwość przeprowadzania audytów bezpieczeństwa systemu informacyjnego przez osobę wdrażającą SZBI, prawdopodobnie dopatrując się w tym konfliktu interesów. Analogiczną sytuację dostrzegamy w relacji IOD-Administrator. Jednym z zadań IOD jest monitorowanie przestrzegania RODO, 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. Jeśli zadaniem IOD jest prowadzenie audytów, to opierając się o założenia art. 15 ust. 1 projektu z dnia 23 kwietnia 2024 r. ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw – nie może on samodzielnie realizować obowiązków, które spoczywają na Administratorze.

Projektowana zmiana ustawy kładzie duży nacisk na świadomość i odpowiedzialność Kierownika podmiotu kluczowego i podmiotu ważnego, wskazując na to, jaka powinna być rola Kierownika, a jaka osób go wspierających, w tym również IOD. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), jest zatem drogowskazem jak połączyć świat technologii, prawa i wykonawców.

Ponadto w nowych przepisach wprowadzono pojęcie cyberhigieny[1] (motyw 49 NIS2), które nie miało dotychczas w polskim porządku prawnym zastosowania i nie zostało jeszcze jednoznacznie określone. Jak osiągnąć zadawalający stan zabezpieczenia zasobów, gdy

[1] Polityka cyberhigieny stanowi podstawę pozwalającą chronić infrastrukturę sieci i systemów informatycznych, bezpieczeństwo sprzętu, oprogramowania i aplikacji internetowych oraz dane przedsiębiorstw lub użytkowników końcowych wykorzystywane przez podmioty.

ustawodawca nie wskazuje pozycji formalnej osób funkcyjnych i kompetencji wymaganych w przedmiotowym obszarze?

W kontekście prowadzonej dyskusji na temat niezależności IOD oraz budowania jego pozycji zawodowej, w sposób sceptyczny podchodzimy do zaprezentowanej publicznie podczas spotkania w dniu 9 kwietnia 2024 r. pn. „Niezależność inspektora ochrony danych w świetle skoordynowanego działania EROD CEF DPO", przez przedstawiciela Kancelarii prawnej, formy rozdzielenia możliwości wykonywania funkcji IOD na model statyczny oraz model dynamiczny (prezentacja opinii prawnej z dnia 5 kwietnia 2024 r., pt. „Konflikt interesów w wykonywaniu funkcji inspektora ochrona danych i jego unikanie. Problemy zaistniałe w praktyce i sposoby ich rozwiązania, autorstwa dr hab. Grzegorza Sibigi, prof. INP PAN). Obawiamy się, iż wynikiem tego rodzaju interpretacji przepisów prawa będzie obarczanie IOD wszelkimi możliwymi obowiązkami (w tym również tymi, mającymi charakter dokumentacyjny tj. prowadzenie dokumentacji z zakresu ochrony danych osobowych, RCP, RKP, dokumentacji dot. naruszeń ochrony danych osobowych etc.). UODO prezentuje literalnie czytelny i jednoznaczny status Inspektora, który środowisko SIODO podziela, i którego zdaniem nie jest konieczna nadmiernie rozbudowana, odmienna od oczywistych zapisów opinia.

Wyręczanie Administratora doprowadzi do regresu jego świadomości w zakresie odpowiedzialności, która na nim spoczywa, a także do nasilonej tendencji cedowania zadań spoczywających na ADO na IOD w przyszłości. Z perspektywy rosnącej ilości aktów prawnych, które Administrator powinien znać i stosować, a IOD powinien go w tym zakresie wspierać, ale także z uwagi na fakt, iż Kierownictwo powinno wykazywać przywództwo oraz zaangażowanie w odniesieniu do systemu zarządzania bezpieczeństwem informacji[2] – wydaje się destrukcyjne dla kultury bezpieczeństwa informacji (w tym kultury ochrony danych osobowych) oraz efektywności respektowania prawa do prywatności – skupianie na IOD kompetencji oraz obowiązków Administratora.

Podsumowując, prezentowanie opinii niemających twardego umocowania w przepisach prawa, może być przeciwskuteczne w budowaniu rangi i powagi zawodu zaufania jakim jest Inspektor Ochrony Danych.

Z wyrazami szacunku
w imieniu Zarządu SIODO

Bogdanna Krupińska
Członek Zarządu

Dawid Czerw
Członek Zarządu

[2] PN-EN ISO/IEC 27001