

RO1431.75.2024

PYTANIA:

1. Czy Państwa jednostka wyznaczyła Inspektora Ochrony Danych osobowych (dalej: IOD)?

TAK

2. Na podstawie jakich kwalifikacji administrator wyznaczył IOD (np. wykształcenie prawnicze, doświadczenie, wiedza)? Art 37 ust. 5 RODO inspektor ochrony danych 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. Według UODO Karami administracyjnymi obwarowane są zatem zarówno poszczególne obowiązki administratorów danych dotyczące także wyznaczania IOD. To na administratorze spoczywa ciężar wyznaczenia IOD zgodnie z kwalifikacjami i wiedzą prawniczą:

<https://uodo.gov.pl/pl/225/637> Jednakże warto zrealizować rekonesans - w tym obszarze i dokonać stosownej analizy - wykazując troskę o bezpieczeństwo danych oraz wyznaczanie IOD zgodnie z kwalifikacjami. Tymczasem często na IOD są wybierani osoby nie mające odpowiednich kwalifikacji, wiedzy prawniczej. Co gorsza często takie funkcje piastują osoby z wykształceniem informatycznym. Dzięki kontrolom NIK i UODO oraz działaniom sfer Rządowych (w skali makro) w ostatnim czasie sytuacja ulega poprawie, jednakże bez szybkiej sanacji tego obszaru (w skali mikro) również w Gminach i jednostkach oświatowych, a zwłaszcza w firmach prywatnych - proces ten nadal przebiegał zbyt wolno - często są to osoby przypadkowe lub informatycy. Brak wyznaczenia IOD zgodnie z kwalifikacjami zmusi nas do powiadomienia odpowiednich organów.

IOD został wybrany na podstawie wieloletniego doświadczenia i wiedzy jaką posiada IOD. Realizował zadania wynikające z wcześniejszych ustaw min. z Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

2. W związku z powyższym wnosimy o wykazanie kwalifikacji IOD w zakresie wiedzy prawniczej? Czy IOD jest prawnikiem? Jakie posiada doświadczenie? Kto i w jaki sposób weryfikował kwalifikacje IOD?

IOD nie jest prawnikiem. Tak jak wcześni jest napisane osoba ta jest wieloletnim pracownikiem urzędu. Należycie realizowała i realizuje zadania z zakresu ochrony danych osobowych.

24.11.2015 r. ukończył szkolenie ABI Nowe obowiązki z w opracowywania Polityki

Bezpieczeństwa, zmiany w ustawie o Ochronie Danych osobowych obowiązujące od 15 stycznia 2015 r. 19.10.2016 r. ukończył kurs z zakresu Ochrony Danych Osobowych, 15 maja 2018 r.

Ukończył szkolenie w zakresie zmian ochrony danych osobowych w JST w związku z wejściem w Życie RODO. Później szkolenia w ramach abonamentu organizowane przez wydawnictwo Wolters Kluwer LEX dla samorządu terytorialnego.

4. Nadmieniamy, iż powyższe pytania o informację publiczną - wydają się szczególnie istotne z punktu widzenia interesu publicznego pro publico bono - nawiązując do art. 3 ust. 1 pkt. 1 Ustawy z dnia 6 września o dostępie do informacji publicznej (Dz.U.2018.1330 tj. z 2018.07.10) - gdyż ten

obszar RODO i kwalifikacji IOD, a zwłaszcza doświadczenia i wiedzy prawniczej wydaje się (jak wynika z uprzednio uzyskanych przez nas odpowiedzi) - szczególnie wymagać - wdrożenia procedur aby takie „przypadkowe” osoby nie pełniły takich funkcji.

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

- a) Sprzęt i narzędzia techniczne.
- b) Niezbędny budżet na szkolenia i inne działania.
- c) Dostęp do danych i współpracę wewnętrzną.
- d) Niezbędna ilość czasu.

· w jaki sposób administrator zapewnia zasoby na utrzymanie wiedzy fachowej IOD?

Administrator zapewnia zasoby na utrzymanie wiedzy fachowej IOD poprzez finansowanie szkoleń, dostęp do specjalistycznych narzędzi i literatury, umożliwienie konsultacji z ekspertami, a także przeznaczenie odpowiedniego budżetu i czasu na rozwój IOD.

· jakie stanowisko zajmuje IOD i komu podlega w strukturze organizacyjnej administratora?

Inspektor Ochrony Danych Osobowych podlega bezpośrednio Burmistrzowi.

· w jaki sposób administrator zapewnia by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych?

Administrator zapewnia włączenie IOD we wszystkie sprawy dotyczące ochrony danych osobowych poprzez:

- Wdrożenie formalnych procedur.
- Promowani
- e świadomości roli IOD w organizacji.
- Zapewnienie dostępu do informacji, narzędzi i procesów decyzyjnych.
- Regularne monitorowanie i egzekwowanie tego obowiązku.

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

IOD do danych osobowych i operacji przetwarzania ma dostęp poprzez upoważnienia dostępu do dokumentacji i systemów IT, bieżącą współpracę dotyczącą przetwarzania danych.

· czy administrator przyjął jakiegokolwiek regulacje wewnętrzne dotyczące funkcjonowania IOD (...), a jeżeli tak, to w jakim akcie wewnętrznym zostały one przewidziane?

Tak. Są one ujęte w Zarządzeniu, PBI, Regulaminie organizacyjnym.

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

Nie posiadamy odrębnej dokumentacji dotyczącej Polityki zarządzania konfliktami interesów. Stosujemy inne mechanizmy.

- 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?

Tylko w Urzędzie Miejskim

- czy IOD opracował (systematycznie opracowuje) plan swojej pracy np. w zakresie szkoleń i planów audytów?

IOD realizuje swoje zadania w zakresie planowania i realizacji szkoleń zgodnie z obowiązującymi przepisami. Szczególną uwagę zwraca się na nowe kadry Urzędu Miejskiego.

- 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?

Zadania do wykonania przez IOD uzgadniane są z Burmistrzem. W miarę możliwości wdrażane są nowe - lepsze procedury dotyczące ochrony danych. W związku z większą ilością zadań przewiduje się wprowadzenie zmian dot. IOD.

- jak często i w jaki sposób IOD przekazuje administratorowi wyniki przeprowadzonych audytów

Wynik audytu przedstawiany jest Burmistrzowi po zakończeniu prac.

- czy administrator kontroluje pracę inspektora, jeżeli tak, to w jaki sposób?

IOD podlega najwyższemu kierownictwu wyłącznie w zakresie podporządkowania organizacyjnego,

5. W jaki sposób IOD realizuje swoje zadania (audyty, szkolenia, konsultacje). Wnosimy o dokumentację potwierdzającą realizację zadań przez IOD lub opis jego działań od dnia 25 maja 2018 roku (zadań wynikających z art. 39 rozporządzenia RODO)

W Urzędzie IOD został powołany w dniu 24 maja 2018 r. Również w 2018 roku opracowano Instrukcję zarządzania systemem do przetwarzania danych osobowych. IOD monitoruje na bieżąco przestrzeganie przepisów RODO w Urzędzie. Uczestniczy w realizacji zagadnień związanych z ochroną danych osobowych, w tym koniecznych audytów. IOD organizuje szkolenia nowoprzyjętych pracowników, jak również pozostałych pracowników UM.

6. Czy zostały opracowane i wdrożone przepisy wewnętrzne, procedury, instrukcje i inne dokumenty dotyczące przetwarzania danych osobowych oraz bezpieczeństwa informacji. Jeśli tak to jakie?

Polityka ochrony danych osobowych, Rejestr czynności przetwarzania danych osobowych, rejestr kategorii przetwarzania danych osobowych, Instrukcja zarządzania systemami informatycznymi, Procedura postępowania w przypadku naruszeń ochrony danych osobowych, Upoważnienia do przetwarzania danych osobowych.

7. Wnosimy o opisanie aktualizacji dokumentacji RODO od 2018r.? W szczególności interesuje nas aktualizacja dokumentacji od roku 2022r. (stanowiska ENISA)

1. W Urzędzie Miejskim opracowano i wdrożono Politykę Bezpieczeństwa Informacji oraz Politykę Bezpieczeństwa Systemów Informatycznych służących do przetwarzania danych

osobowych w Urzędzie. Polityka bezpieczeństwa informacji, Polityka ochrony danych osobowych (zawierająca rejestr czynności przetwarzania danych osobowych), Instrukcja zarządzania systemami informatycznymi, Zasady bezpieczeństwa informacji i danych osobowych, Instrukcja postępowania z incydentami, Procedura zarządzania ryzykiem bezpieczeństwa informacji, Plan ciągłości działania. W/w polityki i instrukcje zawierają wymagane i szczegółowe procedury przetwarzania informacji, w tym danych osobowych, zgodnie z obowiązującymi przepisami prawa i normami. Dokumentacja aktualizowana na bieżąco - zawiera elementy wskazane w ENISA.

8. W jaki sposób w roku 2023 i bieżącym były realizowane szkolenia z zakresu ochrony danych osobowych (art. 39 ust.1. lit b RODO), bezpieczeństwa informacji (par. 19 KRI) i Cyberbezpieczeństwa.

09-10.01.2023 r. - Jaką rolę powinien pełnić inspektor ochrony danych w dostępie do informacji publicznej? LEX Cyberatak - zadania IOD w dobie sytuacji kryzysowych LEX. Pracownicy UM.

7 marca 2024 r. - Anonimizacja danych osobowych w sektorze publicznym Szkolenie dostępne w LEX

12.08.2024 r. od godz. 10.00 szkolenie online zwiększenie bezpieczeństwa ochrony danych osobowych przechowywanych w jednostkach samorządowych w formie elektronicznej, nieprawidłowości w umowach o powierzenie danych, nowe techniczne możliwości zabezpieczeń macierzy i taśm archiwizacyjnych przed atakami ransomware poprzez rozwiązania wirtualne i hybrydowe. 5 osób brak listy obecności

9. Wnosimy o informację na temat częstotliwości szkoleń, ponadto (informacje tj. data szkolenia, zakres szkolenia, osoba prowadząca, listy obecności, czas trwania)

Szkolenia dla nowych pracowników z chwilą podpisania umowy o pracę.

Szkolenia okresowe co roku dla pozostałej kadry.

.....
Strona nr 4 wnioskuPo analizie jednostek:

· Jeśli odpowiedź jest twierdząca wnosimy o wykazanie kwalifikacji IOD w zakresie wiedzy prawniczej? Czy Inspektor Ochrony Danych jest prawnikiem?

IOD nie posiada wykształcenia prawniczego

· Kto weryfikował kwalifikacje IOD przed podpisaniem umowy?

Kierownik Jednostki

· Przypominamy, że funkcją IOD dotyczy osoby fizycznej i konkretna osoba musi się legitymować odpowiednimi kwalifikacjami (wiedza praktyczna i prawnicza).

Dodatkowo, w kontekście pytania - w trybie wyżej powołanych przepisów - wnosimy o informację czy administrator posiada dokumenty potwierdzające kwalifikacje IOD np. dyplomy z wykształcenia prawniczego?

IOD nie posiada wykształcenia prawniczego. Posiada stosowne certyfikaty dotyczące szkolenia w zakresie ochrony danych osobowych.

Czy IOD w ramach monitorowania przeprowadza regularne i systematyczne sprawdzenia/audyty w zakresie prawidłowości przetwarzania danych osobowych oraz przestrzegania rozporządzenia RODO, ustawy o.d.o. oraz regulacji wewnętrznych? Dokumentacja w tym zakresie (plany, sprawozdania, raporty, itp.).

IOD należycie wywiązuje się z realizacji swoich obowiązków w zakresie monitorowania i sprawdzania przetwarzania danych osobowych.

Czy jednostka przeprowadziła audyt KRI za rok 2024? Kto przeprowadził audyt? Proszę o wskazanie daty raportu audytu? Czy audyt z KRI przeprowadziła firma zewnętrzna czy Inspektor Ochrony Danych? Czy jest planowany audyt KRI za rok 2025?

Zgodnie z obowiązującym Rozporządzeniem z dnia 21 maja 2024 r. Rady Ministrów (Dz.U. poz. 773), audyt za rok 2024 będzie przeprowadzony w I kwartale 2025 r. Planuje się wykonanie audytu za rok 2025.


BURMISTRZ
Bogdan Kącki

K. Gygiel