Warszawa, dnia 10-06-2020 r.

MINISTER KLIMATU

BKA-I.0831.7.2019.KZ
1030906.3737091.2929197

Pan
Paweł Ciećko
Główny Inspektor Ochrony Środowiska
ul. Wawelska 52/54
00-922 Warszawa

WYSTĄPIENIE POKONTROLNE

Działając na podstawie upoważnienia Ministra Środowiska[1] nr 7/2019 z 3 października 2019 r. zespół kontrolujący Ministerstwa Klimatu przeprowadził kontrolę planową w Głównym Inspektoracie Ochrony Środowiska (dalej: GIOŚ), ul. Wawelska 52/54 w Warszawie w zakresie funkcjonowania jednostki w zakresie bezpieczeństwa teleinformatycznego oraz ochrony danych osobowych.

Kontrola została przeprowadzona przez zespół kontrolujący w składzie:

- Joanna Matusiak – główny specjalista w Biurze Kontroli i Audytu Wewnętrznego;
- Katarzyna Żebrowska – starszy specjalista w Biurze Kontroli i Audytu Wewnętrznego;
- Mateusz Białek – specjalista w Biurze Kontroli i Audytu Wewnętrznego;
- Dorota Kurczyńska - starszy specjalista w Biurze Dyrektora Generalnego.

Kontrolą objęto okres od 1 stycznia 2017 r. do 20 grudnia 2019 r.

Kontrola została przeprowadzona na podstawie art. 25 ust. 1 pkt 3 lit. b) ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[2] i art. 6 ust. 3 pkt 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[3] w związku z art. 3a ustawy z dnia 20 lipca 1991 r. o Inspekcji Ochrony Środowiska[4] (dalej: ustawa o IOŚ).

Kierownikiem jednostki kontrolowanej jest pan Paweł Ciećko[5]. Poprzednio Głównym Inspektorem Ochrony Środowiska był pan Marek Haliniak.[6]

[1] Zgodnie z rozporządzeniem Prezesa Rady Ministrów z 18 listopada 2019 r. w sprawie szczegółowego zakresu działania Ministra Klimatu - poz. 2266, od 15 listopada 2019 r. Minister Klimatu kieruje działem administracji rządowej – Środowisko. Tym samym stał się następcą prawnym Ministra Środowiska.
[2] t.j. Dz.U. z 2019, poz. 700 ze zm.
[3] Dz. U. z 2011, nr 185 poz. 1092 ze zm.
[4] t.j. Dz. U. z 2019 r., poz. 1355 ze zm.
[5] pełniący obowiązki Głównego Inspektora Ochrony Środowiska w okresie od 30 lipca 2018 r. do 31 października 2018 r. a następnie powołany na stanowisko Głównego Inspektora Ochrony Środowiska od 1 listopada 2018 r.
[6] W okresie od 25 maja 2016 r. do 25 lipca 2018 r.

Dyrektorem Generalnym GIOŚ od 1 października 2018 r. jest pan Andrzej Długołęcki. Wcześniej Dyrektorem Generalnym była pani Anna Jurzyk[7] i pan Radosław Fienko[8].

[Dowód: akta kontroli str. 1, 557-565]

Ocena ogólna kontrolowanej działalności

II. Wybrane zagadnienia ochrony danych osobowych, zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (ogólne rozporządzenie o ochronie danych)

II.1. Organizacja systemu ochrony danych osobowych

Obowiązujące w GIOŚ regulacje wewnętrzne dotyczące systemu ochrony danych osobowych od 25 maja 2018 r. nie były dostosowane do obowiązków i zadań związanych z przetwarzaniem i ochroną danych osobowych wynikających z ogólnego rozporządzenia o ochronie danych.

Obowiązująca w GIOŚ Polityka bezpieczeństwa przetwarzania danych osobowych z 21 czerwca 2017 r., określa obowiązki wynikające z nieobowiązującej ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[194] oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[195]. Polityka GIOŚ określa m.in. definicje, zadania, role i odpowiedzialności poszczególnych osób (m.in. zadania Administratora Bezpieczeństwa Informacji), zasady przetwarzania danych, wykaz zbiorów danych osobowych, opis struktury zbiorów danych, obowiązek wykonywania sprawdzeń, wykaz budynków tworzących obszar, w którym przetwarzane są dane osobowe.

W GIOŚ ustanowiono także Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych z 28 grudnia 2018 r., w której opisano środki ochrony teleinformatycznej systemów, w których przetwarzane są dane osobowe.

Powyższe dokumenty nie określają natomiast procedur dotyczących obowiązków wynikających z ogólnego rozporządzenia o ochronie danych, np. przeprowadzania analizy ryzyka dla naruszenia praw lub wolności osób fizycznych, oceny skutków dla ochrony danych, sposobu realizacji praw osób, których dane dotyczą, zadań Inspektora Ochrony Danych.

[194] Dz. U. z 2016 r. poz. 922
[195] Dz. U. 2004 nr. 100 poz. 1024

Zgodnie z art. 24 ust. 2 ogólnego rozporządzenia o ochronie danych, jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki techniczne i organizacyjne służące ochronie danych osobowych obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

[Dowód: akta kontroli str. 202-258]

Dyrektor Departamentu Organizacyjno-Finansowego odnośnie braku ustanowienia regulacji wewnętrznych określających obowiązki i zadania wynikające z ogólnego rozporządzenia o ochronie danych, w tym ustanowienia nowej Polityki bezpieczeństwa przetwarzania danych osobowych wyjaśnił, że Polityka była w trakcie nowelizacji w związku z reorganizacją Inspekcji Ochrony Środowiska, a brak w obowiązującej Polityce aktualnych obowiązków administratora, czy IOD nie przeszkadzał
w zgodnym z przepisami wypełnianiem obowiązków z uwagi na szczegółowe opisanie tych obowiązków w przepisach. W innych procedurach wewnętrznych stopniowo, gdzie jest to uzasadnione, wprowadzane były elementy związane z ochroną danych osobowych, np. kwestia stosowania obowiązku informacyjnego[196].

[Dowód: akta kontroli str. II/4-9]

Zespół kontrolujący zwraca uwagę, że nowe dokumenty wewnętrzne dotyczące systemu ochrony danych osobowych powinny być ustanowione do dnia rozpoczęcia stosowania ogólnego rozporządzenia o ochronie danych, tj. do 25 maja 2018 r. Zmiany organizacyjne w Inspekcji Ochrony Środowiska nastąpiły z dniem 1 stycznia 2019 r. na podstawie ustawy z dnia 20 lipca 2018 r. o zmianie ustawy o Inspekcji Ochrony Środowiska oraz niektórych innych ustaw[197]. Obowiązki administratora danych są ustanowione przez ogólne rozporządzenie o ochronie danych, jednak szczegółowe rozwiązania proceduralne (dotyczące np. przeprowadzania analizy ryzyka, prowadzenia rejestru czynności przetwarzania i osób za nie odpowiedzialnych) powinny być opisane w wewnętrznych procedurach.

Kontrolujący ocenili kontrolowane zagadnienie negatywnie.

II.2 Analiza ryzyka

W GIOŚ nie była prowadzona analiza ryzyka naruszenia praw i wolności osób fizycznych.

W listopadzie 2018 r. została wykonana analiza ryzyka utraty integralności, dostępności oraz poufności informacji, w której określono jedyne 3 ryzyka (utrata integralności informacji, utrata dostępności
do informacji i utrata poufności informacji), przy czym nie określono skutków zmaterializowania się ryzyk. Przeprowadzona analiza ryzyka nie odnosiła się do praw i wolności osób fizycznych. Nie uwzględniono w niej charakteru, zakresu, kontekstu i celu przetwarzania danych osobowych, a także ryzyka naruszenia praw i wolności osób fizycznych. Zatem nie spełnia ona wymogów ogólnego rozporządzenia o ochronie danych.

[Dowód: akta kontroli str. 259]

Analiza ryzyka naruszenia praw lub wolności osób fizycznych była jedynie przeprowadzona po incydencie, który dotyczył możliwego ujawnienia danych osobowych jednego pracownika GIOŚ (zgubienie legitymacji służbowej) i był przez niego spowodowany.

[Dowód: akta kontroli str. 4-9]

[196] Pismo z 13 grudnia 2019 r. znak: DOF-0701-735/19/WS
[197] Ogłoszona w Dzienniku Ustaw 3 sierpnia 2018 r., Dz. U. poz. 1479

Zgodnie z art. 24 ust. 1 ogólnego rozporządzenia o ochronie danych uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać.

Ponadto w myśl art. 32 ogólnego rozporządzenia o ochronie danych uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

W kwestii zastosowania środków bezpieczeństwa odpowiadających ryzyku Dyrektor Departamentu Organizacyjno-Finansowego wyjaśnił, że środki bezpieczeństwa były stosowane od lat, tj. dużo wcześniej od wejścia w życie ogólnego rozporządzenia o ochronie danych. Zabezpieczenia były udoskonalane wraz z rozwojem technologii i występującymi zagrożeniami. Według Dyrektora wcześniej nie było obowiązku dokumentowania analiz ryzyka w tym zakresie, w związku z czym proces dokumentowania tych analiz jest doskonalony, a procedura będzie zamieszczona w Polityce Bezpieczeństwa Informacji.

[Dowód: akta kontroli str. II/4-9]

Zespół kontrolujący zwraca uwagę, że prowadzenie cyklicznej analizy ryzyka, jest podstawą systemu zarządzania bezpieczeństwem informacji i wymogiem jego skuteczności, co zostało opisane w pkt I.I.3 projektu wystąpienia pokontrolnego. Natomiast obowiązek projektowania zabezpieczeń danych osobowych, które stanowią jedną z kategorii informacji, na podstawie przeprowadzonej analizy ryzyka naruszenia praw i wolności osób fizycznych istnieje od 25 maja 2018 r., tj. od rozpoczęcia stosowania ogólnego rozporządzenia o ochronie danych. O rodzaju i zakresie środków technicznych i organizacyjnych decyduje sam administrator danych na podstawie uprzednio przeprowadzonej analizy ryzyka.

Kontrolujący ocenili kontrolowane zagadnienie negatywnie.

II.3 Szkolenia pracowników

Brak jest systemowego rozwiązania dotyczącego szkoleń pracowników z ochrony danych osobowych.

Pracownicy, GIOŚ, którzy przeszli do pracy z WIOŚ zostali przeszkoleni przed 1 stycznia 2019 r., a część pracowników z dawnego GIOŚ przeszła szkolenia specjalistyczne zewnętrzne. Przed przejęciem pracowników WIOŚ do GIOŚ wykonano rozeznanie jaka część pracowników WIOŚ była przeszkolona w zakresie ochrony danych osobowych po wejściu w życie ogólnego rozporządzenia o ochronie danych, niemniej GIOŚ nie był w stanie przekazać informacji, którzy pracownicy zostali przeszkoleni.

Inspektor ochrony danych wyjaśnił, że nowi pracownicy przeszli wstępne szkolenia przez IOD, a część z nich była szkolona w poprzednich miejscach pracy. W GIOŚ aktualnie pracuje ponad 1200 osób i nie było możliwe stworzenie szczegółowej listy pracowników, którzy zostali przeszkoleni[198].

[Dowód: akta kontroli str. II/10-19]

Niemożliwe było jednoznaczne ustalenie liczby osób, które zostały przeszkolone.

[198] Wyjaśnienia IOD – mail z 13 i l6 grudnia 2019 r.

GIOŚ nie powinien opierać się na fakcie, że pracownicy odbyli szkolenia w poprzednich miejscach pracy w sytuacji, gdy, zakres, cel kontekst przetwarzania danych, a także wdrożone zabezpieczenia mogą się różnić w poszczególnych organizacjach.

Kontrolujący ocenili kontrolowane zagadnienie pozytywnie z zastrzeżeniami.

II.4 Upoważnienia do przetwarzania danych osobowych

Procedura postępowania w zakresie udzielania upoważnienia do przetwarzania danych osobowych została opisana w Polityce bezpieczeństwa przetwarzania danych osobowych z 21 czerwca 2017 r. Osoby otrzymują ogólne upoważnienia do przetwarzania danych osobowych w obszarze nie przekraczającym zakresu czynności i obowiązków pracownika[199]. Inspektor Ochrony Danych prowadził ewidencję upoważnień do przetwarzania danych osobowych, w której jest ok. 1200 osób. Kontrola 6 osób, które mają uprawnienia do dodawania danych osobowych do bazy skarg i wniosków o interwencję wykazała, że wszystkie osoby posiadają upoważnienie do przetwarzania danych osobowych.

[Dowód: akta kontroli str. 202-238, II/20-24]

Kontrolujący ocenili kontrolowane zagadnienie pozytywnie.

II.5 Przetwarzanie danych przez podmioty przetwarzające

W GIOŚ IOD prowadzi rejestr umów powierzenia zawartych pomiędzy WIOŚ i GIOŚ, gdzie GIOŚ w części umów jest administratorem danych, a w części podmiotem przetwarzającym. W rejestrze tym jest zawarta także umowa pomiędzy MŚ a GIOŚ. Według stanu na 9 sierpnia 2019 r. w rejestrze prowadzonym przez IOD zarejestrowano 29 umów powierzenia.

Nie jest natomiast prowadzony rejestr pozostałych umów powierzenia, które były procedowane w komórkach organizacyjnych GIOŚ. W trakcie kontroli GIOŚ nie przekazał także zestawienia tych umów powierzenia. Umowy te nie były uzgadniane z IOD, ponieważ w GIOŚ nie obowiązują wewnętrzne procedury w tym zakresie. Kontrola 2 umów powierzenia danych pomiędzy GIOŚ jako Administratorem danych a WIOŚ jako podmiotem przetwarzającymi, oraz WIOŚ jako Administratorem danych a GIOŚ jako podmiotem przetwarzającym, nie wykazała uchybień.

[Dowód: akta kontroli str. II/25-207]

Zgodnie z art. 38 ust. 1 ogólnego rozporządzenia o ochronie danych, administrator zapewnia, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych. Brak włączenia IOD w proces zawierania wszystkich umów powierzenia jest naruszeniem tego przepisu.

Kontrolujący zwracają uwagę, że brak prowadzenia rejestru wszystkich umów powierzenia stwarza ryzyko braku nadzoru nad podmiotami przetwarzającymi oraz dodatkowo utrudnia monitorowanie przestrzegania przepisów rozporządzenia przez IOD. Należy zwrócić uwagę, że w GIOŚ nie istnieje procedura zawierania umów powierzenia. Ogólne rozporządzenie nie określa szczegółowo obowiązków w tym zakresie, jednak brak uregulowań w tym zakresie w procedurach wewnętrznych rodzi ryzyko powstania uchybień.

Kontrolujący ocenili kontrolowane zagadnienie negatywnie.

[199] Wyjaśnienia IOD – mail z 13 grudnia 2019 r.

II.6 Prawo do przetwarzania danych osobowych

Dla wszystkich zbiorów danych/czynności przetwarzania danych osobowych w GIOŚ zidentyfikowano podstawę prawną ich przetwarzania, co udokumentowano w rejestrze czynności przetwarzania danych osobowych i rejestrze kategorii czynności przetwarzania.

W GIOŚ zidentyfikowano 15 czynności przetwarzania danych osobowych.

W ramach kontroli zweryfikowano przetwarzanie danych osobowych w związku z rozpatrywaniem skarg i wniosków o interwencję (6,6% wszystkich czynności przetwarzania). Stwierdzono spełnienie warunków przetwarzania, określonych w podstawie prawnej przetwarzania i zawartej w rejestrze czynności; zgodność celów przetwarzania z celami, w jakich dane zostały zebrane; przetwarzanie danych wyłącznie w zakresie niezbędnym do realizacji celów ich przetwarzania; przetwarzanie danych w formie umożliwiającej identyfikację osoby, której dane dotyczą.

[Dowód: akta kontroli str. II/208, 266-268]

Kontrolujący ocenili kontrolowane zagadnienie pozytywnie.

II.7 Realizacja praw osób, których dane dotyczą

W GIOŚ opracowano wzory klauzul informacyjnych zgodnych z art. 13 i 14 ogólnego rozporządzenia o ochronie danych.

[Dowód: akta kontroli str. II/209-214]

W okresie objętym kontrolą do GIOŚ nie wpłynęły wnioski o realizację praw osób, których dane dotyczą.

[Dowód: akta kontroli str. II/4-9]

W ramach skontrolowanej czynności przetwarzania danych osobowych był spełniany obowiązek informacyjny, o którym mowa w art. 13 ogólnego rozporządzenia o ochronie danych.

[Dowód: akta kontroli str. II/208]

Kontrolowany zakres oceniono pozytywnie.

II.8 Inspektor ochrony danych

W GIOŚ został powołany Inspektor Ochrony Danych w terminie wynikającym z ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. Dopełniono ustawowego obowiązku zawiadomienia PUODO o powołaniu IOD. Dane kontaktowe do IOD zostały upublicznione na stronie internetowej GIOŚ, w klauzuli informacyjnej dostępnej w zakładce ochrona danych osobowych.
Osoba ta nie zajmuje stanowiska kierowniczego. IOD posiada doświadczenie i wykształcenie niezbędne do pełnienia tej funkcji.

[Dowód: akta kontroli str. II/215-249]

W regulacjach wewnętrznych obowiązujących w GIOŚ nie zapewniono w wystarczający sposób niezależności IOD i podległości pod najwyższe kierownictwo.
Osoba pełniąca funkcję IOD zajmuje Stanowisko do spaw Kontroli, Audytu Wewnętrznego, Spraw Obronnych i Ochrony Informacji Niejawnych, które nadzoruje Dyrektor Generalny w zakresie swoich

wyłącznych kompetencji[200]. Do zadań na tym stanowisku należy m.in. prowadzenie spraw związanych z administrowaniem i ochroną danych osobowych. Natomiast Dyrektor Generalny wykonuje zadania administratora/podmiotu przetwarzającego określone w ustawie o ochronie danych osobowych oraz RODO i nadzoruje czynności, które są związane z przetwarzaniem danych osobowych[201].
Zgodnie z art. 39 ust. 1 ogólnego rozporządzenia o ochronie danych, jednym z zadań IOD jest monitorowanie przestrzegania 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.

Zgodnie z art. 38 ust. 3 ogólnego rozporządzenia o ochronie danych IOD bezpośrednio podlega najwyższemu kierownictwu administratora.

Z powyższego wynika, że osoba na Stanowisku do spraw Kontroli, Audytu Wewnętrznego, Spraw Obronnych i Ochrony Informacji Niejawnych pełniąca funkcję IOD sprawuje nadzór nad przetwarzaniem danych oraz jednocześnie prowadzi sprawy związane z administrowaniem i ochroną danych osobowych. Powierzenie osobie pełniącej funkcję IOD, która m.in. w ramach pełnienia obowiązków służbowych nadzoruje sprawy związane z ochroną danych osobowych, zadań związanych z administrowaniem danymi osobowymi, prowadzi do potencjalnego konfliktu interesów. Zgodnie
z art. 38 ust. 6 ogólnego rozporządzenia o ochronie danych, IOD może wykonywać inne zadania i obowiązki, a administrator zapewnia, by takie zadania i obowiązki nie powodowały konfliktu interesów.

Ponadto do podstawowych obowiązków na Stanowisku do spraw Kontroli, Audytu Wewnętrznego, Spraw Obronnych i Ochrony Informacji Niejawnych należało około 20 zadań, w tym m.in. koordynowanie i prowadzenie kontroli w WIOŚ oraz kontroli wewnętrznych, pełnienie funkcji Rzecznika Dyscyplinarnego GIOŚ, koordynowanie spraw związanych z przeciwdziałaniem korupcji, nadzorowanie realizacji spraw obronnych, prowadzenie spraw związanych z oświadczeniami o stanie majątkowym. Niemniej zadania te nie powodują konfliktu interesów z funkcją IOD.

[Dowód: akta kontroli str. 153-174, II/215-249]

Kontrolujący zwracają uwagę, że powierzenie jednej osobie dużej liczby zadań w dużej organizacji zatrudniającej blisko 1200 osób, mającej oddziały zamiejscowe, przetwarzającej dane osobowe w ramach realizacji swoich ustawowych zadań, może powodować ryzyko nieprawidłowego wypełniania swoich zadań przez IOD, przede wszystkim z powodu braku czasu na realizację zadań.

Dyrektor Departamentu Organizacyjno-Finansowego wyjaśnił, że osoba pełniąca funkcję IOD jest koordynatorem Stanowiska do spraw Kontroli, Audytu Wewnętrznego, Spraw Obronnych i Ochrony Informacji Niejawnych. Przepisy nie zabraniają, aby IOD realizował inne zadania. W związku ze zmianami organizacyjnymi w GIOŚ, a co za tym idzie obsługiwaniem większej liczby pracowników oraz konieczności zmian obowiązujących procedur, komórka ta zostanie wzmocniona dwoma nowymi pracownikami, co powinno doprowadzić do odciążenia osoby pełniącej IOD w pełnieniu swoich zadań.
Odnośnie podległości IOD pod najwyższe kierownictwo, Dyrektor wyjaśnił, że omawiane stanowisko jest specyficzną komórką organizacyjną, a większość zatrudnionych w niej osób pełni samodzielne funkcje, które w zależności od przepisów czy regulaminu organizacyjnego podlegają Głównemu

[200] zgodnie z Regulaminem organizacyjnym GIOŚ z 15 stycznia 2019 r.
[201] Dyrektor Generalny wykonuje, a także m.in. dokonuje czynności z zakresu prawa pracy wobec osób zatrudnionych oraz realizuje politykę personalną, oraz wykonuje kompetencje kierownika zamawiającego w rozumieniu ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych

Inspektorowi Ochrony Środowiska lub Dyrektorowi Generalnemu. Pracownicy organizacyjnie należą do ww. Stanowiska, ale realizując zadania merytoryczne podlegają bezpośrednio tym członkom kierownictwa GIOŚ, którzy sprawują bezpośrednio nadzór merytoryczny nad poszczególnymi zadaniami. Najwyższe kierownictwo w GIOŚ stanowią Główny Inspektor Ochrony Środowiska, jego Zastępca oraz Dyrektor Generalny, wobec tego zdaniem Dyrektora zapewniono podległość IOD najwyższemu kierownictwu[202].

[Dowód: akta kontroli str. II/253-265]

Kontrolujący nie podzielają stanowiska dotyczącego podległości IOD najwyższemu kierownictwu. W związku ze scedowaniem zadań administratora danych na Dyrektora Generalnego, Inspektor Ochrony Danych powinien w regulaminie organizacyjnym być podległy Głównemu Inspektorowi Ochrony Środowiska. Natomiast z regulaminu organizacyjnego wprost wynika, że osoba pełniąca funkcję IOD podlega pod Dyrektora Generalnego.

Kontrolujący ocenili kontrolowane zagadnienie pozytywnie z zastrzeżeniami.

II.9 Rejestrowanie czynności przetwarzania danych osobowych

Rejestr czynności przetwarzania GIOŚ oraz Rejestr kategorii czynności przetwarzania są prowadzone elektronicznie przez IOD. Rejestry zawierają wszystkie elementy wymagane przez art. 30 ogólnego rozporządzenia o ochronie danych.

Rejestr kategorii czynności przetwarzania nie zawiera wszystkich kategorii czynności przetwarzania dokonywanych przez GIOŚ jako podmiotu przetwarzającego na podstawie umów powierzenia danych, tj. czynności związanych z realizacją projektów w ramach POIiŚ 2014-2020 oraz z oferowaniem pracownikom kart wstępu na wydarzenia sportowo-rekreacyjne dla pracowników.

GIOŚ realizuje projekty finansowane ze środków POIiŚ w ramach, których doszło do powierzenia danych osobowych w ramach zbiorów Programu Operacyjnego Infrastruktura i Środowisko na lata 2014-2020 i Centralny System Teleinformatyczny. Dodatkowo należy wskazać, że jednym z obowiązków wskazanych w umowach o dofinansowanie, jest prowadzenie rejestru kategorii czynności przetwarzania. GIOŚ zawarł także umowę powierzenia danych z podmiotem oferującym karty wstępu na wydarzenia sportowo-rekreacyjne dla pracowników. GIOŚ występuje w tym przypadku jako podmiot przetwarzający. Czynność ta powinna być wykazana w rejestrze kategorii czynności przetwarzania.

[Dowód: akta kontroli str. II/63-192, 266-274]

Kontrolujący ocenili kontrolowane zagadnienie pozytywnie z zastrzeżeniami.

Naruszenia ochrony danych

W GIOŚ stwierdzono jeden przypadek naruszenia ochrony danych osobowych dotyczący danych jednego pracownika GIOŚ (zgubienie legitymacji służbowej)[203]. Podjęto działania naprawcze. Procedura postępowania w razie zagrożenia dla bezpieczeństwa przetwarzanych danych osobowych lub naruszenia zasad przetwarzania danych osobowych została opisana w Polityce bezpieczeństwa przetwarzania danych osobowych.

[Dowód: akta kontroli str. 202-238, II/275]

Ocena obszaru

[202]Pismo GIOŚ z 16 grudnia 2019 r.
[203] Rejestr naruszeń ochrony danych osobowych

Kontrolowane zagadnienia zostają ocenione negatywnie.

W GIOŚ do dnia zakończenia kontroli nie ustanowiono systemu ochrony danych zgodnego z ogólnym rozporządzeniem o ochronie danych. Nie została przeprowadzona analiza ryzyka naruszenia praw i wolności osób fizycznych w związku z przetwarzaniem ich danych osobowych w GIOŚ. Wdrożone zabezpieczenia techniczne i organizacyjne nie zostały poprzedzone analizą ryzyka. W szkoleniach z ochrony danych osobowych uczestniczyła część pracowników GIOŚ, jednak jednostka kontrolowana nie była w stanie określić dokładnej liczby tych osób. Rejestr kategorii czynności przetwarzania nie zawierał wszystkich czynności przetwarzania dokonywanych w GIOŚ jako podmiocie przetwarzającym.

W przypadku skontrolowanej czynności przetwarzania danych spełniono warunki przetwarzania, określone w podstawie prawnej przetwarzania, zawartej w rejestrze czynności. Dane były przetwarzane
w celach w jakich zostały zebrane, w sposób adekwatny, w formie umożliwiającej identyfikację osoby, której dane dotyczą. Był wypełniany obowiązek informacyjny wobec osób których dane są zbierane.

Administrator danych wyznaczył IOD w ustawowym terminie. Osoba ta posiada niezbędne wiedzę i doświadczenie. W wewnętrznym regulaminie organizacyjnym, nie zapewniono formalnie podległości IOD bezpośrednio pod kierownika jednostki i wykonywania swoich zadań niezależnie. Osoba pełniąca funkcję IOD pełni również inne obowiązki, których duża liczba może powodować ryzyko dla prawidłowej realizacji obowiązków IOD.

Biorąc pod uwagę powyższe ustalenia i wnioski wnoszę o:

9. Ustanowienie wewnętrznych procedur, w tym polityki ochrony danych osobowych, regulujących zadania i obowiązki wynikające z ogólnego rozporządzenia o ochronie danych osobowych.
10. Opracowanie metodyki przeprowadzenia analizy ryzyka naruszenia praw i wolności osob fizycznych, oraz jej przeprowadzenie
11. Prowadzenie szkoleń z ochrony danych osobowych dla wszystkich pracowników GIOŚ przetwarzających dane osobowe.
12. Prowadzenie rejestru umów powierzenia, zawierającego wszystkie umowy powierzenia zawarte przez GIOŚ.
13. Ustanowienie procedury dotyczącej zawierania umów powierzenia przez GIOŚ.
14. Zapewnienie w dokumentach wewnętrznych GIOŚ podległości IOD pod najwyższe kierownictwo oraz takie opisanie zadań IOD, aby nie powodowały konfliktu interesów.
15. Zapewnienie IOD niezbędnych zasobów (np.. Kadrowych, czasowych, itd.) umożliwiających wykonywanie powierzonych mu zadań i odpowiednie ustalenie priorytetów, sytuacji pełnienia przez niego innych zadań
16. Prowadzenie rejestru kategorii czynności przetwarzania zawierającego wszystkie powierzone czynności przetwarzania.

Przedstawiając powyższe wystąpienie pokontrolne, proszę Pana Prezesa o złożenie pisemnej informacji w sprawie sposobu wykorzystania wyników kontroli oraz o podjętych działaniach zmierzających do realizacji zaleceń pokontrolnych wraz ze stosownymi dokumentami potwierdzającymi podjęte działania **w terminie 1 miesiąca** od daty otrzymania niniejszego pisma.

Z poważaniem

Z up. Ministra
Jacek Ozdoba
Sekretarz Stanu
Ministerstwo Klimatu
/ – podpisany cyfrowo/