|  |
| --- |
| **Minister Środowiska** |

Warszawa, dnia 2017 r.

BKA-I.0943.6.2017.KZ

**Pan**

**Arkadiusz Siembida**

Regionalny Dyrektor Ochrony Środowiska w Warszawie

**SPRAWOZDANIE Z KONTROLI**

Działając na podstawie upoważnienia Ministra Środowiska nr 6/2017 z dnia 9 czerwca 2017 r. zespół kontrolujący przeprowadził w Regionalnej Dyrekcji Ochrony Środowiska w Warszawie w dniach
12 czerwca – 10 lipca 2017 r. kontrolę doraźną w zakresie *wybranego zdarzenia dotyczącego bezpieczeństwa informacji.*

Zespół kontrolujący przeprowadził kontrolę w następującym składzie:

* Mateusz Białek – Specjalista w Biurze Kontroli i Audytu Wewnętrznego,
* Artur Konarski – Radca Ministra w Biurze Kontroli i Audytu Wewnętrznego,
* Andrzej Smoliński – Zastępca Dyrektora w Biurze Dyrektora Generalnego,
* Paweł Tudek – Główny Specjalista w Biurze Dyrektora Generalnego,
* Katarzyna Żebrowska – Starszy Specjalista w Biurze Kontroli i Audytu Wewnętrznego.

**Ustalenia ogólne kontroli**

Generalna Dyrekcja Ochrony Środowiska (dalej GDOŚ) udostępnia swoje zasoby teleinformatyczne Regionalnym Dyrekcjom Ochrony Środowiska (dalej RDOŚ) przez udostępnienie tym instytucjom systemu poczty elektronicznej. Od 29 grudnia 2016 r. z tego systemu korzystają wszystkie RDOŚ, natomiast wcześniej korzystało z niego 12 RDOŚ, w tym RDOŚ w Warszawie. RDOŚ zostały zobowiązane przez GDOŚ do korzystania z systemu poczty elektronicznej. Administratorem systemu jest GDOŚ, natomiast RDOŚ korzystają z systemu na prawach użytkownika. W systemie tym przetwarzane są dane osobowe. Korzystanie przez RDOŚ z zasobów teleinformatycznych GDOŚ nie zostało uregulowane w formie pisemnego dokumentu, w związku z czym zasady korzystania przez RDOŚ z zasobów teleinformatycznych GDOŚ nie zostały formalnie ustanowione. Nie został określony także zakres odpowiedzialności poszczególnych instytucji za bezpieczeństwo informacji.

W RDOŚ w Warszawie nie został formalnie ustanowiony i wdrożony system zarządzania bezpieczeństwem informacji. Natomiast ustanowiono i wdrożono system ochrony danych osobowych przetwarzanych w RDOŚ w Warszawie.

Administratorem danych osobowych przetwarzanych w systemie poczty elektronicznej RDOŚ w Warszawie jest Regionalny Dyrektor Ochrony Środowiska w Warszawie. W związku z korzystaniem przez RDOŚ w Warszawie z systemu poczty elektronicznej w zasobach teleinformatycznych GDOŚ, doszło do powierzania przetwarzania danych osobowych przez RDOŚ w Warszawie (administrator danych) do GDOŚ (podmiot, któremu powierzono dane). Nie zawarto umowy powierzenia danych osobowych w systemie poczty elektronicznej pomiędzy GDOŚ a RDOŚ, a tym samym formalnie nie ustanowiono zasad przetwarzania danych osobowych przez GDOŚ. W związku z brakiem zawarcia umowy powierzenia, GDOŚ nie został upoważniony do wydawania swoim pracownikom upoważnień do przetwarzania danych osobowych, których administratorem jest RDOŚ. W związku z tym udostępnienie pracownikowi GDOŚ poczty elektronicznej z okresu, kiedy był on pracownikiem RDOŚ w Warszawie odbyło się w sposób nieuprawniony.

W związku z brakiem formalnego uregulowania zasad korzystania z poczty elektronicznej przez RDOŚ oraz praw i obowiązków każdej ze stron, w tym zasad dotyczących przetwarzania danych osobowych, zdarzenie jakim było dokonanie transferu poczty elektronicznej osoby będącej pracownikiem RDOŚ w Warszawie, a następnie GDOŚ, bez wiedzy RDOŚ w Warszawie, ujawniło słabość systemu poczty elektronicznej utrzymywanej w zasobach teleinformatycznych GDOŚ, w zakresie bezpieczeństwa informacji i posiadania faktycznej kontroli nad przetwarzaniem danych przez instytucję, która je wprowadza do systemu.

Stwierdzone nieprawidłowości polegały na:

* nieodebraniu pracownikowi, który zakończył pracę w RDOŚ w Warszawie dostępu
do systemu poczty elektronicznej z dniem zakończenia pracy oraz braku sporządzenia wniosku o odebranie dostępu, co stanowi naruszenie § 10 i § 12 Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych RDOŚ
w Warszawie.,
* naruszeniu art. 13 ust. 1 ustawy *o informatyzacji działalności podmiotów realizujących zadania publiczne* i § 20 ust. 1 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r.
*w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych* przez niewdrożenie Systemu Zarządzania Bezpieczeństwem Informacji,
* braku porozumienia, umowy lub dokumentu równoważnego regulującego relacje GDOŚ i RDOŚ w zakresie przetwarzania danych osobowych w systemie poczty elektronicznej, w tym regulującego prawa stron, obowiązki i odpowiedzialność, co stanowi naruszenie Rozdziału III, § 8 Pkt 1 Regulaminu Ochrony Danych Osobowych w Regionalnej Dyrekcji Ochrony Środowiska w Warszawie.

**Ustalenia szczegółowe**

Niniejsza kontrola została wszczęta w związku z informacją od Regionalnego Dyrektora Ochrony Środowiska w Warszawie o transferze, bez jego wiedzy zawartości służbowej skrzynki poczty elektronicznej byłego pracownika RDOŚ w Warszawie przez obecnego pracodawcę tego pracownika, tj. Generalną Dyrekcję Ochrony Środowiska.

Pracownik od 1 kwietnia 2017 r. jest zatrudniony w GDOŚ. Do 31 marca 2017 r. pracował w RDOŚ
w Warszawie. Zmiana stanowiska pracy nastąpiła na podstawie przeniesienia służbowego zgodnie
z ustawą *o służbie cywilnej.*

Niezależnie wspomniany pracownik pełnił funkcję sekretarza w Regionalnej Komisji Ocen Oddziaływania na Środowisko (dalej RKOOŚ) na podstawie Zarządzenia nr 2/2010 Regionalnego Dyrektora Ochrony Środowiska w Warszawie z dnia 4 lutego 2010 r. Został odwołany z tego stanowiska na podstawie Zarządzenia nr 21 Regionalnego Dyrektora Ochrony Środowiska
z dnia 19 czerwca 2017 r.

Po ustaniu stosunku pracy w RDOŚ w Warszawie pracownik przyszedł 5 maja 2017 r. do siedziby byłego pracodawcy w celu zdania zaległego sprzętu służbowego (ładowarki do telefonu komórkowego). Podczas wizyty próbował uzyskać od pracowników RDOŚ w Warszawie dokumenty związane z RKOOŚ oraz zawartość służbowej skrzynki e-mail, z której korzystał będąc pracownikiem RDOŚ w Warszawie. Byli współpracownicy odmówili mu przekazania ww. materiałów oraz skopiowania służbowej skrzynki e-mail. Były Pracownik RDOŚ w Warszawie poinformował wówczas, że obecny pracodawca dokonał już częściowego skopiowania zawartości jego służbowej skrzynki e-mail w RDOŚ w Warszawie.

Regionalny Dyrektor Ochrony Środowiska w Warszawie poinformował pisemnie o ww. zdarzeniu Generalnego Dyrektora Ochrony Środowiska, w tym zakwestionował legalność działań pracowników GDOŚ przy procesie kopiowania zawartości skrzynki e-mail z zasobów RDOŚ w Warszawie. Generalny Dyrektor Ochrony Środowiska w piśmie z 30 maja 2017 r. do Regionalnego Dyrektora Ochrony Środowiska w Warszawie poinformował, że „Generalny Dyrektor Ochrony Środowiska jest przełożonym Regionalnego Dyrektora Ochrony Środowiska w Warszawie. Nie zachodzi zatem żadna sprzeczność, tak służbowa, jak i logiczna, aby można było nadal wykorzystywać korespondencję mailową (…) w bieżącej działalności służbowej w Generalnej Dyrekcji Ochrony Środowiska”.

Pracownik natomiast, konieczność posiadania wiadomości e-mail tłumaczył chęcią dokończenia protokołu z posiedzenia RKOOŚ oraz materiałów np. prezentacji, opinii, ustaleń, interpretacji
w dalszej pracy w GDOŚ[[1]](#footnote-1).

1. **System informatyczny poczty elektronicznej**

System poczty elektronicznej RDOŚ jest utrzymywany w zasobach teleinformatycznych GDOŚ. Są to odrębne systemy, którymi administruje GDOŚ. Pracownicy poszczególnych RDOŚ korzystają
z systemu poczty elektronicznej na prawach użytkownika. RDOŚ nie posiada administracyjnych uprawnień w systemie poczty swoich pracowników. Obsługę skrzynek pocztowych pracowników RDOŚ, w tym tworzenie i usuwanie kont realizuje GDOŚ. Pismem z 8 listopada 2016 r. Dyrektor Generalny GDOŚ (dalej Dyrektor Generalny) poinformował wszystkie RDOŚ, że „aktualnie obowiązujący system poczty elektronicznej RDOŚ zostanie wyłączony w dniu 29.12.2016 r. W związku z powyższym wszystkie RDOŚ będą zobowiązane do korzystania z nowego systemu poczty elektronicznej od dnia 29.12.2016 roku, dotyczy to także RDOŚ nieposiadających systemu poczty elektronicznej utrzymywanego w zasobach informatycznych GDOŚ”[[2]](#footnote-2).

System poczty elektronicznej dla wszystkich RDOŚ został zatem produkcyjnie uruchomiony
29 grudnia 2016 r.[[3]](#footnote-3) GDOŚ nie określił przy tym w żaden sposób zakresu swojej odpowiedzialności związanej z bezpieczeństwem informacji i ochroną danych osobowych w zakresie poczty elektronicznej. Przed 29 grudnia 2016 r. z systemu poczty elektronicznej w zasobach GDOŚ korzystały niektóre Regionalne Dyrekcje Ochrony Środowiska, tj. w Białymstoku, Gdańsku, Gorzowie Wielkopolskim, Katowicach, Krakowie, Olsztynie, Opolu, Szczecinie, Warszawie, Poznaniu, Rzeszowie, które „w momencie utworzenia Generalnej Dyrekcji Ochrony Środowiska, wyraziły taką potrzebę ze względu na brak odpowiednich zasobów teleinformatycznych i wysokich kosztów sprzętu oprogramowania niezbędnych do prawidłowego utrzymania systemu poczty elektronicznej we własnym zakresie”[[4]](#footnote-4). Instytucjami, które nie korzystały do 29 grudnia 2016 r. z systemu poczty elektronicznej dostarczanego przez GDOŚ, były RDOŚ we Wrocławiu, w Lublinie, Kielcach i Bydgoszczy[[5]](#footnote-5).

Dostęp do skrzynek pocztowych pracowników RDOŚ jest możliwy z dowolnego komputera podłączonego do sieci Internet[[6]](#footnote-6).

**1.1 Odbieranie uprawnień w systemach informatycznych**

Zgodnie z obowiązującą Instrukcją Zarządzania Systemem Informatycznym służącym
do przetwarzania danych osobowych Regionalnej Dyrekcji Ochrony Środowiska w Warszawie:

§10 W systemie informatycznym RDOŚ może zostać zarejestrowany jedynie użytkownik posiadający upoważnienie do przetwarzania danych osobowych w RDOŚ (…).

§12 Użytkownik jest wyrejestrowany z systemu informatycznego RDOŚ w każdym przypadku utraty przez niego uprawnień do przetwarzania danych osobowych w RDOŚ, co ma miejsce szczególnie
w przypadku: 1) Ustania zatrudnienia w RDOŚ(…)

Zablokowanie dostępu pracownika do poczty elektronicznej nastąpiło dopiero 5 maja 2017 r., czyli ponad miesiąc po ustaniu stosunku pracy pracownika z RDOŚ w Warszawie (data rozwiązania stosunku pracy: 31 marca 2017 r.), pracownik Wydziału Administracyjno-Kadrowego RDOŚ w Warszawie wysłał wówczas wniosek (e-mail) z prośbą o zresetowanie hasła dla konta użytkownika. Do tego czasu pracownik miał dostęp do konta poczty elektronicznej w RDOŚ w Warszawie. Oznacza to, że naruszono zapisy §10 i §12 Instrukcji Zarządzania Systemem Informatycznym służącym
do przetwarzania danych osobowych RDOŚ w Warszawie.

1. **Bezpieczeństwo Informacji**

Zgodnie z art. 13 ust. 1. ustawy *o informatyzacji działalności podmiotów realizujących zadania publiczne*[[7]](#footnote-7) podmiot publiczny używa do realizacji zadań publicznych systemów teleinformatycznych spełniających minimalne wymagania dla systemów teleinformatycznych oraz zapewniających interoperacyjność systemów na zasadach określonych w Krajowych Ramach Interoperacyjności. Zgodnie natomiast z § 20 ust. 1 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych* *[[8]](#footnote-8)* (dalej rozporządzenie KRI) podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża
i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji.

Kontrola wykazała, że w RDOŚ w Warszawie nie został wdrożony System zarządzania bezpieczeństwem informacji, co stanowi naruszenie ww. art. 13 ust. 1 ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* oraz § 20 ust. 1 rozporządzenia KRI.

Wraz z rozwojem elektronicznej formy komunikacji znaczenia nabiera zapewnienie dostępności, integralności i poufności danych posiadanych i przetwarzanych przez urzędy. Dlatego też, szczególnie istotne jest zapewnienie bezpieczeństwa informacji przetwarzanych w użytkowanych przez podmioty publiczne systemach informatycznych. W przeciwnym razie powstaje ryzyko utraty ww. właściwości gwarantujących bezpieczeństwo informacji, a w konsekwencji stabilności pracy urzędów. Podważyć to może zaufanie obywateli do organów administracji publicznej. Jednostka, aby zabezpieczyć swoje informacje powinna zastosować podejście systemowe, w ramach którego będzie zarządzać kompleksowo posiadanymi aktywami informacyjnymi, infrastrukturą przeznaczoną do ich przetwarzania oraz ryzykiem dotyczącym bezpieczeństwa informacji.

* 1. **Wdrożenie systemu zarządzania bezpieczeństwem informacji w systemach teleinformatycznych RDOŚ w Warszawie**
		1. **Dokumenty z zakresu bezpieczeństwa informacji**

Zgodnie z ww. § 20 ust. 1 rozporządzenia KRI podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji. Wymaga to opracowania dokumentacji SZBI, w tym szeregu regulacji wewnętrznych
oraz zapewnienia aktualizacji tych regulacji w zakresie dotyczącym zmieniającego się otoczenia (§ 20 ust. 2 pkt 1 rozporządzenia KRI). Dokumentacja ta jest warunkiem niezbędnym do skutecznego zarządzania bezpieczeństwem informacji.

W RDOŚ w Warszawie nie ustanowiono, nie wdrożono oraz nie opracowano dokumentów regulujących System Zarządzania Bezpieczeństwem Informacji (SZBI). RDOŚ w Warszawie nie powołał komitetu, forum lub zespołu w zakresie Zarządzania Bezpieczeństwem Informacji, który odpowiadałby za zarządzanie Systemem.

Nie ustalono również zakresu Systemu Zarządzania Bezpieczeństwem Informacji. Nie stwierdzono powstania dokumentów dotyczących Polityki Bezpieczeństwa Informacji. Nie udokumentowano stosowanych zabezpieczeń. W RDOŚ w Warszawie nie dokonuje się doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji. Nie stwierdzono stosowania klasyfikacji przetwarzanych informacji.

W związku z brakiem ustanowienia, wdrożenia, dokumentowania i pielęgnowania Systemu Zarządzania Bezpieczeństwem Informacji, przetwarzane informacje, w tym informacje przetwarzane w systemach teleinformatycznych narażone są na niekontrolowany wyciek, utratę lub niedostępność.

* + 1. **Dokonywanie analizy zagrożeń związanych z przetwarzaniem informacji**

Jednym z wymogów skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Na analizę ryzyka składają się: identyfikacja, szacowanie, a następnie określenie sposobu postępowania z ryzykiem oraz deklaracja stosowania zabezpieczeń będąca podstawą podejmowania wszelkich działań minimalizujących ryzyko, stosownie do przeprowadzonej analizy. Analiza ryzyka pozwala na proaktywne zarządzanie BI, w tym na przeciwdziałanie zagrożeniom oraz ograniczanie skutków zmaterializowanych ryzyk. Analiza ryzyka pozwala na racjonalne zarządzanie środkami finansowymi poprzez stosowanie zabezpieczeń adekwatnych do oszacowanego poziomu ryzyka.

W RDOŚ w Warszawie nie przeprowadzano okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, zgodnie z § 20 ust. 2 pkt 3 rozporządzenia KRI, nie stwierdzono prowadzenia rejestru ryzyk, zawierającego informacje o zidentyfikowanych ryzykach, ich poziomie oraz sposobie postępowania z ryzykami.

* 1. Wymiana informacji w postaci elektronicznej pomiędzy GDOŚ i RDOŚ w Warszawie,
	w tym współdzielenie infrastruktury teleinformatycznej przez obie instytucje

Infrastruktura teleinformatyczna jest w części współdzielona przez GDOŚ i RDOŚ w Warszawie
w obszarze systemu teleinformatycznego realizującego świadczenie usługi poczty elektronicznej.
W toku kontroli nie stwierdzono porozumień lub innych dokumentów formalnie regulujących zasady udostępnienia systemu przez GDOŚ oraz zasad korzystania systemu przez RDOŚ w Warszawie.

Zasady korzystania z systemu poczty elektronicznej przez RDOŚ w Warszawie nie zostały formalnie przyjęte do stosowania i zaakceptowane przez obie strony. Brak powyższych regulacji może powodować powstanie/zmaterializowanie ryzyk w bezpieczeństwie informacji oraz w zakresie formalnym, m.in. ustanowienia granic odpowiedzialności za bezpieczeństwo systemu, w tym za bezpieczeństwo danych w nim zgromadzonych, stosowania zabezpieczeń oraz stosowania zasad i procedur przez użytkowników i administratorów systemu.

1. **Ochrona danych osobowych**

Obowiązujące procedury dotyczące ochrony danych osobowych zostały ustanowione Zarządzeniem Nr 63 Regionalnego Dyrektora Ochrony Środowiska z dnia 4 listopada 2016 r. zmieniającym zarządzenie w sprawie wprowadzenia dokumentacji dotyczącej przetwarzania danych osobowych
w Regionalnej Dyrekcji Ochrony Środowiska w Warszawie, do którego załączniki stanowią:

1. Regulamin Ochrony Danych Osobowych Regionalnej Dyrekcji Ochrony Środowiska
w Warszawie
2. Polityka bezpieczeństwa Informacji Regionalnej Dyrekcji Ochrony Środowiska w Warszawie
3. Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych Regionalnej Dyrekcji Ochrony Środowiska w Warszawie.

**3.1. Przetwarzanie danych osobowych w systemie poczty elektronicznej**

Zgodnie z wyjaśnieniem Regionalnego Dyrektora Ochrony Środowiska w Warszawie „w trakcie zatrudnienia w RDOŚ w Warszawie pracownik (tak jak każdy inny pracownik RDOŚ w Warszawie) przetwarzał dane osobowe w systemie pocztowym udostępnionym przez GDOŚ”[[9]](#footnote-9)**.**

Zgodnie z art. 6 ust. 1 ustawy *o ochronie danych osobowych* za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Adresy e-mail osób fizycznych utworzonych w formacie imię.nazwisko@domena.pl będących klientami urzędu, są danymi osobowymi, gdyż taki format adresu e-mail przeważnie bardzo jednoznacznie identyfikuje osobę fizyczną, która z niego korzysta. Co więcej, jeżeli wiadomości
e-mail w swojej treści zawierały dane osobowe, przechowywanie wiadomości na serwerach GDOŚ - dostawcy usługi e-mail, powinno być traktowane jako przetwarzanie tych danych. Również możliwość stworzenia książki adresowej, zawierającej przykładowo imiona, nazwiska i adresy e-mail potencjalnych odbiorców poczty elektronicznej, a następnie przechowywanie jej na serwerze usługodawcy wypełniać będzie definicję przetwarzania danych osobowych.

**3.2. Administrator Danych Osobowych**

Regionalny Dyrektor Ochrony Środowiska w Warszawie stwierdził, że „zarówno Generalna Dyrekcja Ochrony Środowiska jak i poszczególne Regionalne Dyrekcje Ochrony Środowiska
są niezależnymi od siebie administratorami danych osobowych. Każdy z tych podmiotów samodzielnie zbiera dane osobowe (m.in. od swoich pracowników i uczestników prowadzonych postępowań administracyjnych) i decyduje o celach i środkach przetwarzania tych danych[[10]](#footnote-10)”.Natomiast Generalny Dyrektor Ochrony Środowiska stwierdził, że „administratorem danych osobowych przetwarzanych w systemach poczty elektronicznej GDOŚ i RDOŚ jest Generalny Dyrektor Ochrony Środowiska”[[11]](#footnote-11).

Powyższe stwierdzenia są sprzeczne, ponieważ zarówno Regionalny Dyrektor Ochrony Środowiska
w Warszawie jak i Generalny Dyrektor Ochrony Środowiska twierdzi, że każdy z nich
jest administratorem danych osobowych przetwarzanych w systemie pocztowym, z którego korzysta RDOŚ w Warszawie. Dlatego należy dokonać ustalenia, który z powyższych organów
jest administratorem tych danych.

Zgodnie z art. 7 pkt. 4) ustawy *o ochronie danych osobowych* administratorem danych jest organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Zgodnie z komentarzem do ustawy o ochronie danych osobowych: „po pierwsze -
w odniesieniu do podmiotów publicznych o celu i środkach przetwarzania danych osobowych decyduje zazwyczaj ustawodawca, stanowiąc przepisy prawa;(…). Pierwsza ze wskazanych powyżej kwestii jest konsekwencją zasady legalizmu, zgodnie z którą organy władzy publicznej (administracji publicznej) działają na podstawie i w granicach określonych przepisami prawa (por. art. 7 Konstytucji RP oraz art. 6 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (tekst jedn.: Dz. U. z 2013 r. poz. 267 z późn. zm.). Podmioty publiczne są zobowiązane do przetwarzania danych osobowych dla realizacji określonych ustawowo celów. Zazwyczaj także środki, jakie mają służyć przetwarzaniu danych osobowych, wskazane są w przepisach ustawowych lub w wydanych na ich podstawie przepisach aktów wykonawczych (…). Jak słusznie stwierdza R. Hauser (Przetwarzanie danych osobowych: cel i środki, Rzeczpospolita, 6 kwietnia 1999), cel przetwarzania danych osobowych będzie mniej lub bardziej ogólnie wyznaczony przepisami prawa, a określony ich administrator, decydując o celu przetwarzania danych, będzie jedynie konkretyzował jego zakres,
aby odpowiadał on potrzebom bardziej szczegółowo określonego zadania publicznego (J. Barta,
J. Fajgielski, R. Markiewicz, Komentarz do art. 7 ustawy o ochronie danych osobowych w Ochrona danych osobowych, LEX 2015).

Naczelny Sąd Administracyjny w wyroku z dnia 30 stycznia 2002 r. (II SA 1098/01) wskazał,
że za administratora danych nie można uznać każdego dysponenta danych. Administratorem danych osobowych nie jest każdy dysponent danych osobowych tylko ten, kto decyduje o celach i środkach przetwarzania, przy czym zasadnicze znaczenie ma rodzaj i charakter nadanych przez prawo kompetencji z zakresu spraw publicznych. Podobne stanowisko zajął Sąd Najwyższy w postanowieniu z dnia 11 grudnia 2000 r. (II KKN 438/00), w którym rozróżnił administratora i administrującego danymi osobowymi. Za administratora uznał jedynie ten podmiot, który decyduje o środkach przetwarzania danych osobowych, natomiast administrującym podmiot, który zarządza, zawiaduje zbiorem danych osobowych w procesie ich przetwarzania, w tym i powierzonego mu w trybie wskazanym w art. 31 tej ustawy.

Zgodnie z art. 121 ust. 1 ustawy z dnia 3 października 2008 r. o *udostępnieniu informacji
o środowisku, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko[[12]](#footnote-12)* Generalny Dyrektor Ochrony Środowiska jest centralnym organem administracji rządowej powołanym do realizacji zadań, o których mowa w art. 127 ust. 1. Natomiast zgodnie
z art. 123 ust. 1 regionalny dyrektor ochrony środowiska jest organem administracji rządowej niezespolonej, właściwym do realizacji zadań, o których mowa w art. 131 ust. 1, na obszarze województwa. Powyższe przepisy ustawy wskazują, że GDOŚ i RDOŚ są oddzielnymi organami administracji, którym powierzono wykonywanie określonych zadań. Przetwarzanie przez nie danych osobowych będzie odbywało się w celu wypełnienia ustawowych zadań. Oznacza to, że każdy z tych organów jeśli w celu wykonywania zadań ustawowych, będzie przetwarzał dane osobowe, będzie ich administratorem. W związku z tym, że GDOŚ i RDOŚ w Warszawie posiadają oddzielne zadania, każdy z tych organów, będzie administratorem danych przetwarzanych w związku z wypełnianiem swoich zadań.

System poczty elektronicznej jest narzędziem komunikacji pomiędzy pracownikami instytucji oraz podmiotami zewnętrznymi i osobami fizycznymi będącymi klientami instytucji urzędu. Wobec czego system ten jest narzędziem pomocniczym w wykonywaniu zadań urzędu. Dane przetwarzane
w systemie poczty elektronicznej przetwarzane są w związku z realizacją ustawowych zadań instytucji. Generalny Dyrektor Ochrony Środowiska wyjaśnił, że z uwagi na postanowienia
art. 31 ust. 2a w związku z art. 3 ust. 1 ustawy o ochronie danych osobowych nie jest wymagane zawarcie umowy powierzenia[[13]](#footnote-13). Dodatkowo pismem z 30 maja 2017 r. poinformował RDOŚ w Warszawie, że przetransferował maile pracownika ze skrzynki RDOŚ w Warszawie do skrzynki pracownika GDOŚ, zgodnie z art. 31 ust 2a ustawy z dnia 27 kwietnia 2007 r. *o ochronie danych osobowych*, wskazując że ustawodawca przewidział, iż administrator danych może powierzyć innemu podmiotowi przetwarzanie danych bez zawarcia umowy jeżeli ma to miejsce pomiędzy organami państwowymi.

Wynika z tego, że w omawianym przypadku doszło do powierzenia danych osobowych przez RDOŚ w Warszawie do GDOŚ na podstawie art. 31 ustawy *o ochronie danych osobowych*. W związku z tym, że w poczcie elektronicznej RDOŚ w Warszawie były zawarte dane osobowe doszło do przetwarzania danych osobowych przez GDOŚ, w wyniku powierzenia ich przetwarzania przez RDOŚ
w Warszawie, do którego w pełni powinno stosować się przepisy ustawy *o ochronie danych osobowych*. Poprzez korzystanie przez RDOŚ w Warszawie z systemu poczty elektronicznej będącego w zasobach informatycznych GDOŚ, doszło do powierzenia przetwarzania danych osobowych.

Zgodnie bowiem z art. 31 ust. 1 ustawy *o ochronie danych osobowych* administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.

Należy jednak zauważyć, że podmiot, któremu powierza się dane nie staje się automatycznie administratorem tych danych. Potwierdza to komentarz do art. 31 ustawy *o ochronie danych osobowych*: Z treści art. 31 u.o.d.o. można wnioskować, że intencją ustawodawcy było, aby ten, komu powierzono przetwarzanie danych osobowych (zleceniobiorca), nie był traktowany jako administrator danych. (J. Barta, J. Fajgielski, R. Markiewicz, Komentarz do art. 31 ustawy o ochronie danych osobowych w Ochrona danych osobowych, LEX 2015).

W tej sytuacji GDOŚ jako podmiot świadczący usługi poczty elektronicznej dla RDOŚ nie decyduje
o celach i środkach stosowanych przy przetwarzaniu danych, nie może być więc traktowany jako administrator danych osobowych przesyłanych w wiadomościach e-mail za jego pośrednictwem. Rola GDOŚ ma charakter usługodawcy i w procesie wysyłania wiadomości e-mail jest bierna, nie ingeruje on w treść przesyłanych wiadomości. Niemniej jednak przechowywanie danych osobowych przez dostawcę usługi poczty e-mail jest traktowane jako przetwarzanie danych osobowych, do którego stosuje się przepisy ustawy.

Podsumowując, w związku z powyższym, administratorem danych osobowych przetwarzanych
w systemie poczty elektronicznej RDOŚ w Warszawie jest Regionalny Dyrektor Ochrony Środowiska w Warszawie. Analogicznie administratorami danych osobowych w systemie poczty elektronicznej poszczególnych RDOŚ są odpowiedni Regionalni Dyrektorzy Ochrony Środowiska. Generalny Dyrektor Ochrony Środowiska jest natomiast podmiotem, któremu powierzono przetwarzanie tych danych.

Istotną kwestią z punktu widzenia korzystającego z poczty e-mail (administratora danych osobowych) jest fakt, że w przypadku powierzenia przetwarzania danych osobowych odpowiedzialność za przestrzeganie przepisów ustawy przez dostawcę poczty e-mail spoczywa także na administratorze. Będzie on również ponosił odpowiedzialność, w wypadku gdy jego dostawca poczty elektronicznej nie zapewni właściwych środków zabezpieczających przetwarzanie danych oraz nie będzie prowadził dokumentacji opisującej sposób ich przetwarzania. Z tego względu umowa o powierzeniu przetwarzania danych osobowych zawierana z dostawcą usługi e-mail powinna określać obowiązek zastosowania środków technicznych i organizacyjnych zapewniających ochronę danych oraz zasady ponoszenia odpowiedzialności za naruszenie przepisów o ochronie danych osobowych przez podmiot przetwarzający te dane na zlecenie administratora. Odpowiedzialność administratora danych oczywiście nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.

RDOŚ w Warszawie jako administrator danych osobowych w systemie poczty nie dochował należytej staranności przy udostępnianiu i powierzeniu danych w systemie pocztowym utrzymywanym
w zasobach informatycznych GDOŚ. Zgodnie bowiem z art. 31 ust. 3 ustawy *o ochronie danych osobowych* podmiot, któremu powierzono dane, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych. Natomiast w myśl ust. 4 tegoż artykułu odpowiedzialność za przestrzeganie przepisów ustawy spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową. Pomimo braku wymogu zawarcia umowy powierzenia, RDOŚ w Warszawie nie zapewnił sobie prawa kontroli nad przetwarzaniem danych osobowych przez GDOŚ.

Ponadto zgodnie z Rozdziałem III, § 8 Pkt 1Regulaminu Ochrony Danych Osobowych w Regionalnej Dyrekcji Ochrony Środowiska w Warszawie, RDOŚ w Warszawie może powierzyć Przetwarzającemu Dane, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych. Przetwarzający Dane może je przetwarzać wyłącznie w zakresie i celu przewidzianym w umowie.

W związku z powyższym, oraz faktem że system pocztowy, z którego korzysta RDOŚ w Warszawie jest utrzymywany w zasobach informatycznych GDOŚ doszło do naruszenia postanowień niniejszego Regulaminu. Nieistnienie umowy lub dokumentu równoważnego regulującego funkcjonowanie systemu pocztowego i powierzenia przetwarzania danych przez RDOŚ, powoduje brak wskazania podmiotu zobowiązanego do zabezpieczenia zbioru danych osobowych w myśl art. 36-39 ustawy *o ochronie danych osobowych*.

Niemniej należy mieć na uwadze, że RDOŚ w Warszawie został zobowiązany do korzystania z poczty elektronicznej będącej w zasobach GDOŚ pismem Dyrektora Generalnego GDOŚ z 8 listopada 2016 r. Zgodnie bowiem z art. 123 ust. 1a ustawy *o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko*, regionalny dyrektor ochrony środowiska podlega Generalnemu Dyrektorowi Ochrony Środowiska.

Ponadto odnośnie do powierzenia danych osobowych, należy mieć na uwadze, że zgodnie z art. 31 ustawy *o ochronie danych osobowych* administrator danych ma jedynie możliwość, a nie obowiązek, powierzenia przetwarzania danych innemu podmiotowi. W świetle tego przepisu zobowiązanie wszystkich RDOŚ do korzystania z systemu poczty elektronicznej utrzymywanego w zasobach teleinformatycznych GDOŚ powinno odbyć się z poszanowaniem prawa jakie daje art. 31 ustawy
*o ochronie danych osobowych* Regionalnym Dyrektorom Ochrony Środowiska, tj. prawa
do dobrowolności w powierzaniu innym podmiotom danych osobowych, których są administratorami.

Nie jest możliwe stwierdzenie, czy faktycznie RDOŚ dobrowolnie powierzyły dane osobowe w systemie poczty elektronicznej, ponieważ GDOŚ nie posiada żadnych dokumentów świadczących o konsultowaniu z RDOŚ potrzeb co do poczty elektronicznej. GDOŚ wyjaśnił jedynie, że potrzeba utworzenia nowego systemu poczty elektronicznej była konsultowana podczas spotkań z RDOŚ, jednakże nie przedstawiono dokumentów to potwierdzających. Wątpliwości w tym zakresie budzi także fakt, że nie zawarto z RDOŚ umów lub porozumień regulujących korzystanie z systemu poczty.

W odniesieniu do braku obowiązku zawarcia pisemnej umowy powierzenia na gruncie przepisów obecnej ustawy *o ochronie danych osobowych*, trzeba mieć na uwadze, że zgodnie z art. 28 ust. 2 Rozporządzenia 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)* które będzie stosowane od 25 maja 2018 r., przetwarzanie przez podmiot przetwarzający będzie odbywać się na podstawie umowy lub innego instrumentu prawnego, które wiążą podmiot przetwarzający i administratora. Zatem po wejściu w życie ww. rozporządzenia konieczne będzie podpisanie umów powierzenia lub innego dokumentu.

**3.3. Dopuszczenie pracownika do przetwarzania danych osobowych**

Przeniesienie zawartości skrzynki pocztowej RDOŚ w Warszawie do skrzynki pocztowej pracownika GDOŚ, było faktycznym dopuszczeniem pracownika GDOŚ do przetwarzania danych osobowych. Bez znaczenia jest tu fakt, że wcześniej pracownik ten był pracownikiem RDOŚ w Warszawie
i przetransferowana korespondencja była do niego kierowana. Po ustaniu stosunku pracy w RDOŚ pracownik nie miał prawa dostępu do danych osobowych, których administratorem jest RDOŚ
w Warszawie, ponieważ upoważnienie do przetwarzania danych osobowych w RDOŚ w Warszawie wygasło wraz z rozwiązaniem stosunku pracy z pracownikiem. Dostęp do tych danych przez pracownika GDOŚ, mógł odbyć się jedynie na podstawie art. 37 w zw. z art. 31 ust. 3 ustawy
*o ochronie danych osobowych.*

Zgodnie z art. 31 ust. 3 ustawy o ochronie danych osobowych podmiot, któremu powierzono
do przetwarzania dane osobowe, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych.

Natomiast zgodnie z art. 37 ustawy o ochronie danych osobowych do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych. Wobec tego upoważnienie do przetwarzania danych osobowych zawartych w poczcie elektronicznej RDOŚ
w Warszawie powinien wydać Regionalny Dyrektor Ochrony Środowiska w Warszawie, który jest administratorem tych danych, ewentualnie osoba przez niego upoważniona. Wobec tego, że zgodnie
z art. 31 ust. 2a nie zawarto umowy powierzenia, Generalny Dyrektor Ochrony Środowiska nie został upoważniony do wydawania upoważnień do przetwarzania danych osobowych w zakresie poczty elektronicznej RDOŚ w Warszawie.

Pracownik GDOŚ w związku z tym, że nie otrzymał od administratora danych – Regionalnego Dyrektora Ochrony Środowiska w Warszawie upoważnienia do przetwarzania danych osobowych, nie powinien uzyskać dostępu do skrzynki pocztowej RDOŚ w Warszawie.

Sytuacja ta pokazuje, że Regionalny Dyrektor Ochrony Środowiska w Warszawie nie posiada faktycznej kontroli nad danymi osobowymi przetwarzanymi w poczcie elektronicznej, do czego zobowiązuje go ustawa *o ochronie danych osobowych*. Przemawia to tym bardziej za potrzebą zawarcia porozumienia, umowy lub dokumentu równoważnego określającego prawa i obowiązki stron w zakresie korzystania z systemu poczty elektronicznej oraz obejmującego ochronę danych osobowych.

[dowód: akta kontroli str. 1-200]

**Mając na uwadze powyższe ustalenia wnoszę o:**

1. Przestrzeganie Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych Regionalnej Dyrekcji Ochrony Środowiska w Warszawie.
2. Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji, zgodnie z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.*
3. Pisemne określenie zasad z GDOŚ regulujących prawa stron, obowiązki i odpowiedzialność
w związku z przetwarzaniem danych osobowych w systemie poczty elektronicznej utrzymywanej w zasobach informatycznych GDOŚ.

Przedstawiając powyższe sprawozdanie z kontroli, proszę Pana Dyrektora o złożenie pisemnej informacji w sprawie sposobu wykorzystania wyników kontroli oraz o podjętych działaniach zmierzających do realizacji zaleceń pokontrolnych **w terminie 30 dni od dnia otrzymania sprawozdania.**

Zgodnie z art. 52 ust. 5 ustawy z dnia 15 lipca 2011 r. *o kontroli w administracji rządowej,* kierownik jednostki kontrolowanej w terminie 3 dni roboczych od dnia otrzymania sprawozdania ma prawo przedstawić do niego stanowisko, nie wstrzymuje to jednak realizacji ustaleń kontroli.

Stanowisko wnosi się za pośrednictwem dyrektora Biura Kontroli i Audytu Wewnętrznego
w Ministerstwie Środowiska (BKA). W przypadku braku uwag do treści sprawozdania, informację
w tej sprawie należy przekazać bezpośrednio do dyrektora BKA.

1. Protokół z przyjęcia ustnych wyjaśnień z dnia 20 czerwca 2017 r. [↑](#footnote-ref-1)
2. Pismo GDOŚ do RDOŚ z 8 listopada 2016 r. [↑](#footnote-ref-2)
3. Pismo GDOŚ z 22 czerwca 2017 r. [↑](#footnote-ref-3)
4. Pismo GDOŚ z 30 czerwca 2017 r. [↑](#footnote-ref-4)
5. Pismo GDOŚ z 30 czerwca 2017 r. [↑](#footnote-ref-5)
6. Pismo RDOŚ w Warszawie z 10 lipca 2017 r. [↑](#footnote-ref-6)
7. Dz.U. 2017 poz. 570 [↑](#footnote-ref-7)
8. Dz. U. 2016 poz. 113 [↑](#footnote-ref-8)
9. Pismo RDOŚ w Warszawie z dnia 21 czerwca 2017 r. [↑](#footnote-ref-9)
10. Pismo RDOŚ w Warszawie z dnia 21 czerwca 2017 r. [↑](#footnote-ref-10)
11. Pismo GDOŚ z dnia 22 czerwca 2017 r. [↑](#footnote-ref-11)
12. Dz.U. 2016 poz.353 [↑](#footnote-ref-12)
13. Pismo GDOŚ z dnia 22 czerwca 2017 r. [↑](#footnote-ref-13)