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

Warszawa, dnia 2017 r.

BKA-I.0943.5.2017.KZ

**Pan**

**Krzysztof Lissowski**

Generalny Dyrektor Ochrony Środowiska

**SPRAWOZDANIE Z KONTROLI**

Działając na podstawie upoważnienia Ministra Środowiska nr 5/2017 z dnia 8 czerwca 2017 r. zespół kontrolujący przeprowadził w Generalnej Dyrekcji Ochrony Środowiska w dniach 8 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.

Stanowisko Generalnego Dyrektora Ochrony Środowiska pełni od dnia 1 września 2016 r. Pan Krzysztof Lissowski na postawie powołania z dnia 24 sierpnia 2016 r.

**Ustalenia ogólne kontroli**

W Generalnej Dyrekcji Ochrony Środowiska (dalej GDOŚ) dokonano transferu służbowej skrzynki pocztowej pracownika GDOŚ z okresu, gdy był on pracownikiem Regionalnej Dyrekcji Ochrony Środowiska w Warszawie (dalej RDOŚ w Warszawie). W ten sposób pracownik GDOŚ uzyskał dostęp do poczty elektronicznej z okresu, gdy pracował w RDOŚ w Warszawie. Transfer dokonał się bez wiedzy Regionalnego Dyrektora Ochrony Środowiska w Warszawie.

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. GDOŚ nie udokumentował procesu projektowania systemu
z udziałem wszystkich RDOŚ, w tym przeprowadzenia analiz ekonomicznych, co nie pozwala na potwierdzenie, że wprowadzenie jednego systemu dla GDOŚ i wszystkich RDOŚ wpłynęło na uzyskanie oszczędności oraz uwzględniło potrzeby wszystkich instytucji.

W GDOŚ został formalnie ustanowiony i wdrożony system zarządzania bezpieczeństwem informacji oraz system ochrony danych osobowych.

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:

* braku porozumienia, umowy lub dokumentu równoważnego regulującego relacje GDOŚ i RDOŚ w zakresie współdzielenia systemu teleinformatycznego poczty elektronicznej, w tym zasad udostępnienia systemu przez GDOŚ oraz zasad korzystania z systemu przez RDOŚ,
co stanowi naruszenie § 19 Polityki Bezpieczeństwa Teleinformatycznego GDOŚ,
* braku porozumienia, umowy lub dokumentu równoważnego regulującego relacje GDOŚ i RDOŚ w zakresie przetwarzania danych osobowych w systemie poczty elektronicznej, w tym regulującego prawa, obowiązki i odpowiedzialność stron,
* nieuwzględnieniu w rejestrze ryzyk szeregu istotnych ryzyk informatycznych związanych
z ochroną bezpieczeństwa informacji, wobec czego rejestr ten nie zabezpiecza potrzeb Polityki Bezpieczeństwa Informacji,
* błędnym sporządzeniu wniosku o wydanie upoważnienia do przetwarzania danych osobowych (błędna nazwa zbioru danych osobowych), w związku z czym nie jest jasne, czy pracownik został upoważniony do przetwarzania danych w tym zbiorze,
* naruszeniu art. 37 w zw. z art. 31 ust. 3 ustawy *o ochronie danych osobowych* przez dopuszczenie do przetwarzania danych osobowych pracownika, który nie miał wydanego przez administratora tych danych upoważnienia do przetwarzania danych osobowych
w zakresie danych zawartych w poczcie elektronicznej RDOŚ 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 email. Były Pracownik RDOŚ w Warszawie poinformował wówczas, że obecny pracodawca dokonał już częściowego skopiowania zawartości jego służbowej skrzynki
e-mail w RDOŚ 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 Pan Krzysztof Lissowski 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 regionalnych dyrekcji ochrony środowiska 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 nie posiadających 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.

GDOŚ nie określił przy tym w żaden sposób zakresu swojej odpowiedzialności związanej z bezpieczeństwem informacji i ochroną danych osobowych w systemie 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”[[3]](#footnote-3). 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[[4]](#footnote-4).

Dostęp do skrzynek pocztowych pracowników RDOŚ jest możliwy z dowolnego komputera podłączonego do sieci Internet[[5]](#footnote-5).

Generalny Dyrektor Ochrony Środowiska, Pan Krzysztof Lissowski, wyjaśnił, że „zobowiązanie do korzystania z nowego systemu poczty elektronicznej przez wszystkie RDOŚ wynika z faktu produkcyjnego uruchomienia 29.12.2016 r. nowego systemu poczty elektronicznej dla wszystkich RDOŚ oraz konieczności systematycznej redukcji kosztów utrzymania sprzętu i oprogramowania informatycznego, a co za tym idzie racjonalnego i oszczędnego wydatkowania środków publicznych. Ponoszone przez GDOŚ łączne koszty utrzymania systemu poczty elektronicznej są kilkukrotnie niższe niż w przypadku, gdy były one ponoszone przez każdy z RDOŚ osobno[[6]](#footnote-6)”. Generalny Dyrektor Ochrony Środowiska wyjaśnił, że „symulacje kosztów są możliwe do pozyskania z każdej z RDOŚ korzystających z nowego systemu poczty elektronicznej”. Ponadto według Generalnego Dyrektora Ochrony Środowiska decyzja ta przyniosła oszczędności i zmniejszenie wydatkowanych środków publicznych (…). Utworzenie nowego systemu poczty elektronicznej wynikało z potrzeb zgłaszanych w trakcie cyklicznych spotkań kierownictwa GDOŚ z Regionalnymi Dyrektorami Ochrony Środowiska oraz roboczych spotkań pionów IT GDOŚ i RDOŚ”[[7]](#footnote-7).

W opinii Ministerstwa Środowiska decyzja o utworzeniu wspólnego systemu powinna być poprzedzona analizami ekonomicznymi przeprowadzonymi przez GDOŚ wspólnie z RDOŚ, które powinny być potwierdzone stosownymi dokumentami. GDOŚ nie przedstawił, żadnych dokumentów, potwierdzających opinię, że utworzenie wspólnego systemu faktycznie było uzasadnione ekonomicznie. Nie przedstawiono także dokumentów potwierdzających prowadzenie konsultacji co do potrzeb funkcjonalnych systemu. Proces projektowania oraz ustanawiania wspólnego systemu poczty elektronicznej dla GDOŚ i RDOŚ, nie został w powyższym zakresie udokumentowany, wobec czego nie można stwierdzić, że utworzenie systemu dla wszystkich instytucji przyniosło wymierne korzyści.

**1. 1 Wniosek o udzielenie dostępu do zasobów informatycznych GDOŚ**

Regulacje wewnętrzne dotyczące przyznawania dostępu do zasobów informatycznych zostały wprowadzone Zarządzeniem nr 11 Dyrektora Generalnego GDOŚ z dnia 5 grudnia 2016 r. w sprawie udzielania i odbierania dostępu do zasobów informatycznych oraz przydzielania sprzętu komputerowego pracownikom w Generalnej Dyrekcji Ochrony Środowiska. Załącznik do Zarządzenia stanowi „Procedura udzielania i odbierania dostępu do zasobów informatycznych oraz przydzielania sprzętu komputerowego pracownikom”.

Zgodnie z pkt 4.2 powyższej procedury pracownik może uzyskać dostęp do systemów informatycznych jeśli uzyska pisemną zgodę bezpośredniego przełożonego, Właściciela/Sponsora Systemu Informatycznego oraz Kierującego Zespołem ds. Informatyki. W tym celu należy wypełnić wniosek o udzielenie/odebranie dostępu do zasobów informatycznych GDOŚ, stanowiący załącznik
nr 2 do procedury.

W dniu 30 marca 2017 r. Dyrektor Departamentu Realizacji Projektów Środowiskowych GDOŚ podpisał wniosek o udzielenie dostępu do zasobów informatycznych GDOŚ dla pracownika GDOŚ,
w którym to dopisał odręcznie następującą prośbę: „Proszę również o przeniesienie poczty p. (…)
z RDOŚ Warszawa”.

Wzór wniosku, będący załącznikiem nr 2 do procedury zawiera zamknięty katalog systemów informatycznych, do których można przydzielić dostęp pracownikowi. Przy każdym z systemów, należy wskazać odpowiedź „tak” lub „nie” w zależności od tego, czy wnioskuje się o dostęp pracownika do danego systemu. Pracownik otrzymał dostęp do systemu pn. Poczta elektroniczna. Ręczne dopisanie prośby na wniosku o przeniesienie poczty nastąpiło zatem niezgodnie z procedurą. Wniosek został zaakceptowany przez osobę odpowiedzialną merytorycznie za system informatyczny, która pełni jednocześnie funkcję Kierującego Zespołem ds. Informatyki. Zgodnie z pkt. 4.2.2. Procedury udzielania i odbierania dostępu do zasobów informatycznych oraz przydzielania sprzętu komputerowego pracownikom wprowadzonym Zarządzeniem nr 11 Dyrektora Generalnego Generalnej Dyrekcji Ochrony Środowiska z dnia 5 grudnia 2016 r., ostatecznej akceptacji dopuszczenia do użytkowania wskazanych zasobów informatycznych dokonuje Kierujący Zespołem ds. Informatyki.

W związku z powyższym w dniu 5 kwietnia 2017 r. nastąpiło przeniesienie poczty elektronicznej pracownika ze skrzynki RDOŚ w Warszawie do poczty elektronicznej tego pracownika w GDOŚ. Generalny Dyrektor Ochrony Środowiska wyjaśnił, że przeniesiona została korespondencja e-mail ,,przychodząca” z okresu 30 grudnia 2016 r. – 3 kwietnia 2017 r.[[8]](#footnote-8)

1. **Bezpieczeństwo Informacji**

W GDOŚ został wdrożony System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych. W ramach kontroli zweryfikowano jedynie wybrane elementy SZBI, odnoszące się do: istnienia dokumentacji, identyfikacji aktywów i zarządzania ryzykiem.

Stwierdzone uchybienia dotyczyły sporządzonej analizy ryzyka oraz braku formalnie zaakceptowanych zasad korzystania z infrastruktury teleinformatycznej GDOŚ przez RDOŚ.

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 GDOŚ
		1. Dokumentacja z zakresu bezpieczeństwa informacji

Zgodnie 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[[9]](#footnote-9)* (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. 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 skutecznego zarządzania bezpieczeństwem informacji.

W GDOŚ opracowano, ustanowiono i wdrożono System Zarządzania Bezpieczeństwem Informacji. Zarządzenie Nr 21 Generalnego Dyrektora Ochrony Środowiska z dnia 29 listopada 2016 r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Ochrony Środowiska ustanawia SZBI, obejmuje strukturę organizacyjną, polityki, plany działania, zakresy odpowiedzialności, procesy i zasoby. Celem systemu jest zapewnienie poufności, dostępności oraz integralności informacji w komórkach organizacyjnych GDOŚ oraz w systemach informatycznych służących do przetwarzania informacji w GDOŚ. Zarządzanie Bezpieczeństwem Informacji (dalej BI) w GDOŚ odbywa się poprzez opracowaną i wdrożoną Politykę Bezpieczeństwa Informacji (dalej PBI). Zarządzenie ustanawia Dyrektora Generalnego GDOŚ jako zarządzającego i nadzorującego funkcjonowanie SZBI. Zarządzeniem powołany został Zespół do spraw SZBI, który wspiera Dyrektora Generalnego w realizacji jego zadań poprzez praktyczne wdrażanie Polityki Bezpieczeństwa Informacji, jej monitorowanie i doskonalenie. Zespół zajmuje się między innymi szacowaniem ryzyk związanych z BI, analizą incydentów naruszenia BI, określeniem działań korygujących oraz doskonaleniem SZBI. Zarządzenie zobowiązuje dyrektorów komórek organizacyjnych GDOŚ do nadzorowania przestrzegania zasad BI w nadzorowanych komórkach organizacyjnych, a także do współpracy z Zespołem w zakresie szacowania ryzyka BI.

Podstawowym dokumentem SZBI jest „Polityka Bezpieczeństwa Informacji w Generalnej Dyrekcji Ochrony Środowiska” zatwierdzona 29 kwietnia 2015 r. przez Dyrektora Generalnego GDOŚ. PBI określa działania, które mają zapewnić odpowiedni poziom BI w GDOŚ, w tym opisuje organizację i ustala osoby odpowiedzialne oraz ich zakresy odpowiedzialności, wprowadza klasyfikację informacji, sposób postępowania z poszczególnymi rodzajami informacji. PBI określa aktywa oraz ich właścicieli, sposób szacowania ryzyka oraz sposób postępowania z ryzykiem.

Integralną część PBI stanowią, zatwierdzane odrębnie od PBI:

• Polityka bezpieczeństwa teleinformatycznego w Generalnej Dyrekcji Ochrony Środowiska wraz z procedurami i instrukcjami bezpieczeństwa z 16 lutego 2017 r.;

• Polityka bezpieczeństwa ochrony danych osobowych z 11 lipca 2013 r.

* + 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 GDOŚ przeprowadzano okresowe analizy ryzyka utraty integralności, poufności lub dostępności informacji, zgodnie z § 20 ust. 2 pkt 3 rozporządzenia KRI. Regulacją wewnętrzną opisującą sposób zarządzania ryzykiem jest § 14 i 15 PBI. W GDOŚ prowadzony jest rejestr ryzyk, zawierający informacje o zidentyfikowanych ryzykach, ich poziomie oraz sposobie postępowania z ryzykami.

Badany rejestr ryzyk nie w pełni odpowiada potrzebom PBI, gdyż zawiera głównie ryzyka dotyczące zadań planowanych na potrzeby kontroli zarządczej. Rejestr nie uwzględnia szeregu istotnych ryzyk informatycznych związanych z ochroną BI, np. zniszczeń fizycznych (np. ryzyka pożaru serwerowni), ryzyka włamania do systemu informatycznego, awarie oprogramowania. Przykłady zagrożeń dla bezpieczeństwa informacji zostały określone w normie PN-ISO/EIC 27005, zgodnie z którą opracowano Politykę Bezpieczeństwa Informacji w GDOŚ (§ 5 ust. 2). Ponadto zgodnie z § 14 PBI szacowanie ryzyka powinno odbywać się z uwzględnieniem zasad zawartych m.in. w powyższej normie.

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

Zgodnie z § 19 Polityki Bezpieczeństwa Teleinformatycznego w GDOŚ zasady współpracy z podmiotami zewnętrznymi, w szczególności udzielanie dostępu (fizycznego i logicznego) do zasobów teleinformatycznych i systemów teleinformatycznych GDOŚ są określane w zawieranych z podmiotami zewnętrznymi (stronami trzecimi) umowach cywilnoprawnych zawierających postanowienia o zachowanie poufności i nieujawnianiu informacji. Umowy te precyzują zasady i wymagania bezpieczeństwa, jakie muszą spełnić podmioty zewnętrzne (strony trzecie), aby uzyskać dostęp do zasobów teleinformatycznych i systemów teleinformatycznych GDOŚ. Ponadto dostęp do zasobów teleinformatycznych i systemów teleinformatycznych GDOŚ nie może zostać przyznany podmiotom zewnętrznym (stronom trzecim), dopóki nie zostanie podpisana umowa lub oświadczenie o zachowaniu poufności.

Infrastruktura teleinformatyczna jest w części współdzielona przez GDOŚ i RDOŚ w Warszawie
w obszarze systemu teleinformatycznego realizującego świadczenie usługi poczty elektronicznej.
Nie uregulowano pisemnie zasad udostępnienia systemu przez GDOŚ oraz zasad korzystania
z systemu przez RDOŚ w Warszawie. Jest to naruszenie § 19 obowiązującej Polityki Bezpieczeństwa Teleinformatycznego w GDOŚ. Dokument zaczął obowiązywać 16 lutego 2017 r., czyli już po uruchomieniu poczty elektronicznej dla wszystkich RDOŚ (co miało miejsce 29 grudnia 2016 r.), niemniej po jego wprowadzeniu należało doprowadzić do stanu zgodnego z zasadami wprowadzonymi tym dokumentem.

Zasady korzystania z systemu poczty elektronicznej przez RDOŚ w Warszawie nie zostały formalnie przyjęte do stosowania i zaakceptowane przez obie strony. Brak powyższych regulacji w tak strategicznym obszarze jakim są zasoby teleinformatyczne może powodować powstanie 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 następującymi dokumentami:

1. Zarządzenie Nr 29 Generalnego Dyrektora Ochrony Środowiska z dnia 11 lipca 2013 r. zmieniające zarządzenie w sprawie Polityki bezpieczeństwa ochrony danych osobowych
w Generalnej Dyrekcji Ochrony Środowiska.
2. Zarządzenie Nr 28 Generalnego Dyrektora Ochrony Środowiska z dnia 11 lipca 2013 r. zmieniające zarządzenie w sprawie „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”

**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”[[10]](#footnote-10)**.**

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[[11]](#footnote-11)”.

Natomiast Generalny Dyrektor Ochrony Środowiska stwierdził, że „administratorem danych osobowych przetwarzanych w systemach poczty elektronicznej GDOŚ i RDOŚ jest Generalny Dyrektor Ochrony Środowiska”[[12]](#footnote-12).

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. (Dz.U. 2016 poz.353) - 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[[13]](#footnote-13)* 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[[14]](#footnote-14). Dodatkowo pismem z dnia 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.

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.

Na podstawie wyjaśnień GDOŚ udzielonych w trakcie kontroli 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 dokumentu.

**3.3 Zbiór danych osobowych przetwarzanych w poczcie elektronicznej**

W rejestrze zbiorów danych osobowych GDOŚ prowadzonym na stronie BIP GDOŚ został wyodrębniony zbiór danych pn. Usługa katalogowa Active Directory wraz z profilami mobilnymi
i pocztą elektroniczną.Cel przetwarzania danych osobowych został sprecyzowany następująco: *Wszystkie dane osobowe są gromadzone, przechowywane i przetwarzane zgodnie z przepisami ustawy o ochronie danych osobowych oraz ustawy o świadczeniu usług drogą elektroniczną. Udostępnienie danych osobowych jest dobrowolne, przy czym podanie adresu poczty elektronicznej użytkownika jest niezbędne dla realizacji procedury postępowania administracyjnego lub skargowo-wnioskowego realizowanego w GDOŚ – i wynikającej stąd potrzeby uwierzytelnienia użytkowników. Active Directory służy do uwierzytelniania użytkowników w systemach, gdzie są przetwarzane dane, autoryzuje dostęp.*

W świetle powyższych ustaleń dotyczących administratora danych osobowych, zbiór ten nie może obejmować poczty elektronicznej RDOŚ, ponieważ zgodnie z art. 40 i art. 36a ust. 2 pkt. 2) ustawy
*o ochronie danych osobowych* zbiór do rejestracji w GIODO może zgłosić jedynie administrator danych lub rejestr zbiorów przetwarzanych przez administratora danych prowadzi administrator bezpieczeństwa informacji, jeśli został powołany. Jak ustalono w poprzedniej części sprawozdania, GDOŚ nie jest administratorem danych przetwarzanych w systemie poczty elektronicznej i wprowadzonych przez RDOŚ w Warszawie.

* 1. **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. Zatem GDOŚ jako podmiot, któremu powierzono przetwarzanie danych jest zobowiązany do spełnienia powyższych wymogów. Brak wymogu zawarcia umowy powierzenia, o którym mowa w art. 31 ust. 2a ustawy *o ochronie danych osobowych,* nie zwalnia GDOŚ z tego obowiązku.

Natomiast zgodnie z art. 37 ustawy o ochronie danych osobowych do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych. Zatem przed dopuszczeniem do przetwarzania danych osobowych pracowników, powinni zostać oni upoważnieni do przetwarzania danych.

Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym służącym do przetwarzania danych osobowych została opisana w Rozdziale 2 Instrukcji Zarządzania systemem informatycznym służącym do przetwarzania danych osobowych wprowadzonej Zarządzeniem nr 28 Generalnego Dyrektora Ochrony Środowiska z dnia 11 lipca 2013 r. zmieniającym zarządzenie w sprawie „Instrukcji Zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”. Zgodnie z ww. procedurą nadanie uprawnień do przetwarzania danych osobowych w GDOŚ następuje na wniosek złożony zgodnie ze wzorem stanowiącym załącznik do Instrukcji.

Dnia 30 marca 2017 r. sporządzony został wniosek o upoważnienie do przetwarzania danych osobowych w GDOŚ dla pracownika podpisany przez Dyrektora Departamentu Realizacji Projektów Środowiskowych GDOŚ oraz Administratora Bezpieczeństwa Informacji w GDOŚ. Wniosek obejmował dwa zbiory danych osobowych przetwarzanych w GDOŚ:

1. Usługa katalogowa Active Directory
2. Uczestnicy Sieci ,,Partnerstwo: Środowisko dla Rozwoju”.

Według wniosku dane osobowe w powyższych zbiorach przetwarzane są w formie elektronicznej
w systemach informatycznych Intranetu GDOŚ.

W wyniku złożonego wniosku, pracownik otrzymał upoważnienie do przetwarzania danych osobowych nr 25/ABI/2017, ,*,które obejmuje przetwarzanie danych osobowych w systemie informatycznym danych osobowych a także papierowych zbiorów danych w zakresie danych osobowych, które będzie przetwarzać w toku wykonywania obowiązków wynikających z opisu stanowiska pracy”*

Ww. wniosek nie obejmował zbiorów danych osobowych, przetwarzanych w poczcie elektronicznej RDOŚ w Warszawie. GDOŚ w rejestrze zbiorów prowadzonym na stronie BIP posiada zbiór danych osobowych zawierających dane przetwarzane w związku z pocztą elektroniczną GDOŚ (zbiór pn. Usługa katalogowa *Active Directory wraz z profilami mobilnymi i pocztą elektroniczną*). Niemniej jednak wniosek o upoważnienie do przetwarzania danych osobowych w GDOŚ dla pracownika obejmował zbiór o nazwie *Usługa katalogowa Active Directory*.

W związku z tym, że we wniosku nie podano pełnej nazwy zbioru zgodnie z rejestrem zbiorów danych osobowych nie jest jasne, czy pracownik posiadał upoważnienie do poczty elektronicznej GDOŚ i danych osobowych w niej zawartych. Treść wniosku nie wskazuje także, aby pracownik otrzymał upoważnienie do przetwarzania danych osobowych w poczcie elektronicznej RDOŚ w Warszawie, do której miał dostęp w wyniku transferu części poczty. Zatem pracownik w związku
z tym, że nie otrzymał upoważnienia do przetwarzania danych osobowych, których administratorem był RDOŚ w Warszawie, nie powinien uzyskać dostępu do skrzynki pocztowej RDOŚ w Warszawie. Dostęp ten powinien zostać mu odebrany.

Wobec powyższego doszło do naruszenia art. 37 w zw. z art. 31 ust. 3 ustawy o ochronie danych osobowych, przez udostępnienie osobie nieuprawnionej powierzonych do przetwarzania danych osobowych.

Ponadto zgodnie z treścią art. 37, upoważnienie do przetwarzania danych osobowych nadaje **administrator 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, Regionalny Dyrektor Ochrony Środowiska w Warszawie nie upoważnił Generalnego Dyrektora Ochrony Środowiska do wydawania upoważnień do przetwarzania danych osobowych w zakresie poczty elektronicznej RDOŚ w Warszawie.

[dowód: akta kontroli str. 1-453]

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

1. Dokonanie aktualizacji rejestru ryzyk, tak, aby uwzględniał również ryzyka informatyczne związane z ochroną bezpieczeństwa informacji.
2. Uregulowanie relacji GDOŚ i RDOŚ w zakresie współdzielenia systemu teleinformatycznego poczty elektronicznej przez podpisanie przez wszystkie instytucje dokumentu regulującego zasady udostępnienia systemu przez GDOŚ oraz zasad korzystania z systemu przez RDOŚ.
3. Uregulowanie relacji GDOŚ i RDOŚ w zakresie systemu poczty elektronicznej przez podpisanie przez wszystkie instytucje dokumentu regulującego prawa stron, obowiązki i odpowiedzialność
w związku z przetwarzaniem w nim danych osobowych.
4. Upoważnienie do przetwarzania danych osobowych w poczcie elektronicznej GDOŚ pracownika, który został przeniesiony z RDOŚ w Warszawie do GDOŚ.
5. Usunięcie naruszenia art. 37 w zw. z art. 31 ust. 3 ustawy *o ochronie danych osobowych* polegającego na dopuszczeniu do przetwarzania danych osobowych pracownika, który nie miał upoważnienia do przetwarzania danych osobowych w zakresie danych zawartych w poczcie elektronicznej RDOŚ w Warszawie wydanego przez administratora tych danych.

Przedstawiając powyższe sprawozdanie z kontroli, proszę Pana Ministra 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 30 czerwca 2017 r. [↑](#footnote-ref-3)
4. Pismo GDOŚ z 30 czerwca 2017 r. [↑](#footnote-ref-4)
5. Pismo RDOŚ w Warszawie z 10 lipca 2017 r. [↑](#footnote-ref-5)
6. Pismo GDOŚ z 30 czerwca 2017 r. [↑](#footnote-ref-6)
7. Pismo GDOŚ z 30 czerwca 2017 r. [↑](#footnote-ref-7)
8. Pismo GDOŚ z dnia 22 czerwca 2017 r. [↑](#footnote-ref-8)
9. Dz. U. 2016 poz. 113 [↑](#footnote-ref-9)
10. Pismo RDOŚ w Warszawie z dnia 21 czerwca 2017 r. [↑](#footnote-ref-10)
11. Pismo RDOŚ w Warszawie z dnia 21 czerwca 2017 r. [↑](#footnote-ref-11)
12. Pismo GDOŚ z dnia 22 czerwca 2017 r. [↑](#footnote-ref-12)
13. Dz. U. 2016 poz. 353 [↑](#footnote-ref-13)
14. Pismo GDOŚ z dnia 22 czerwca 2017 r. [↑](#footnote-ref-14)