WOJEWODA OPOLSKI

PN.I.431.1.1.2019.RCh

Opole, dnia 15 kwietnia 2019 r.

Pan
Andrzej Buła
Marszałek Województwa Opolskiego
ul. Piastowska 14
45-082 Opole

WYSTĄPIENIE POKONTROLNE

I. Podstawowe informacje formalno-prawne dotyczące kontroli:

1) **Nazwa i adres jednostki kontrolowanej:** Urząd Marszałkowski Województwa Opolskiego (dalej: UMWO; Urząd), ul. Piastowska 14, 45-082 Opole.

2) **Podstawa prawna podjęcia kontroli**:

   a) **art. 25 ust. 1 pkt 3 lit. a** i **ust. 3** ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*[1],

   b) **art. 6 ust. 4 pkt 3** ustawy z dnia 15 lipca 2011 r. *o kontroli w administracji rządowej*[2] – dalej: *ustawa o kontroli*;

3) **Zakres kontroli:**

   a) **Przedmiot kontroli:** Działanie systemów teleinformatycznych i rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej,

   b) **Okres objęty kontrolą:** od 1 stycznia 2019 r. do dnia rozpoczęcia kontroli (z uwzględnieniem okresu wcześniejszego i późniejszego w zakresie niezbędnym do realizacji celu kontroli).

4) **Rodzaj kontroli:** problemowa.

5) **Tryb kontroli:** zwykły.

6) **Termin kontroli:** 12-19 marca 2019 r.

7) **Skład zespołu kontrolnego:**

   a) Radosław Chodziński – Starszy Inspektor Wojewódzki w Oddziale Organizacji, Kontroli i Skarg w Wydziale Prawnym i Nadzoru OUW (kierownik zespołu kontrolnego),

   b) Adam Szkudlarski – Starszy Specjalista w Oddziale Informatyki i Rozwoju w Biurze Obsługi Urzędu OUW (członek zespołu kontrolnego).

8) **Kierownik jednostki kontrolowanej:**

   Funkcję Marszałka Województwa Opolskiego pełni Pan Andrzej Buła, od dnia 12 listopada 2013 r.[3]

[Dowód: akta kontroli, s. 2]

---

[1] Dz. U. z 2017 r. poz. 570 ze zm.

[2] Dz. U. Nr 185, poz. 1092.

[3] Wybrany na stanowisko Marszałka Województwa Opolskiego mocą uchwały nr XXXV/421/2013 Sejmiku Województwa Opolskiego z dnia 12 listopada 2013 r. (w kadencji 2010-2014), a następnie uchwałą nr I/6/2014 Sejmiku Województwa Opolskiego z dnia 28 listopada 2014 r. (w kadencji 2014-2018) oraz uchwałą nr I/3/2018 Sejmiku Województwa Opolskiego z dnia 21 listopada 2018 r. (w kadencji 2018-2023).

II. Ocena skontrolowanej działalności, ze wskazaniem ustaleń, na których została oparta:

Funkcjonowanie UMWO w kontrolowanym zakresie **oceniono pozytywnie z uchybieniami**[4]. Powyższą ocenę uzasadniają przedstawione niżej ustalenia kontroli.

Ustalenia kontroli:

UMWO wykorzystuje 15 systemów teleinformatycznych do realizacji zadań zleconych z zakresu administracji rządowej, w tym:

- 13 o zasięgu krajowym (w tym 7 rejestrów publicznych) oraz
- 2 o zasięgu wojewódzkim.

Na powyższych systemach pracuje łącznie 44 użytkowników (pracowników) z 6 samodzielnych komórek organizacyjnych Urzędu (departamentów).

[Dowód: akta kontroli, s. 25-30 i 31-36]

Z przedłożonego kontrolującym zestawienia systemów teleinformatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej w UMWO wynika, że każdy z powyższych systemów (dokonując oceny pod względem krytyczności) jest istotny dla realizacji zadań Marszałka Województwa Opolskiego.

[Dowód: akta kontroli, s. 25-30]

Zgodnie z § 20 ust. 1-2 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*[5], dalej: *rozporządzenie KRI*, podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali **System Zarządzania Bezpieczeństwem Informacji** (dalej: *SZBI*) zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie enumeratywnie wymienionych działań, celem zapewnienia bezpieczeństwa informacji.

UMWO jako potwierdzenie spełniania wymagań określonych w przepisach *rozporządzenia KRI*, przedstawił m.in. *Politykę Bezpieczeństwa Urzędu* (dalej: *Polityka Bezpieczeństwa*) wprowadzoną zarządzeniem nr 52/2018 Marszałka Województwa Opolskiego z dnia 24 maja 2018 r. *Polityka Bezpieczeństwa* stanowi załącznik nr 1 do zarządzenia. Natomiast załącznik nr 2 do zarządzenia określa *Instrukcję zarządzenia systemem informatycznym służącym do przetwarzania danych osobowych w UMWO*.

[Dowód: akta kontroli, s. 38-41 i 42-114]

Analiza zapisów *Polityki Bezpieczeństwa* prowadzi do wniosku, że w dokumencie tym bezpieczeństwo informacji jest usytuowane obok ochrony danych osobowych. A nawet można przychylić się do stwierdzenia, że zapisy dotyczące ochrony danych osobowych mają tu charakter dominujący w stosunku do zapisów dotyczących bezpieczeństwa informacji.

[Dowód: akta kontroli, s. 43-94]

[4] Służby kontrolne Wojewody Opolskiego stosują czterostopniową skalę ocen: pozytywna, pozytywna z uchybieniami, pozytywna z nieprawidłowościami i negatywna.
[5] Dz.U. z 2017 r. poz. 2247.

Zgodnie z § 2 ust. 1 powyższego dokumentu: *Polityka Bezpieczeństwa to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych i informacji w Urzędzie. Określa w szczególności cel i sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Jej celem jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie zabezpieczyć dane osobowe.* W § 3 ust. 1 *Polityki Bezpieczeństwa*, w enumeratywnym wyliczeniu aktów prawnych (podstaw prawnych) związanych z bezpieczeństwem danych osobowych i informacji przywołuje się m.in. rozporządzenie 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 osobowych) – RODO*, czy ustawę z dnia 10 maja 2018 r. *o ochronie danych osobowych*[6]. W wykazie tym brak jednak *rozporządzenia KRI*.

[Dowód: akta kontroli, s. 47-49]

Zaznaczyć w tym miejscu wypada, że pojęcie *bezpieczeństwa informacji* jest szersze od pojęcia *bezpieczeństwa (ochrony) danych osobowych*. Dane osobowe są bardzo ważnym, ale tylko jednym z obszarów informacji podlegających ochronie.

Podkreślić też należy, że w § 3 ust. 2 pkt 1 *Polityki Bezpieczeństwa*, widnieje norma PN-ISO/IEC 17799. Powyższa norma została zastąpiona przez normę PN-ISO/IEC 27002.

[Dowód: akta kontroli, s. 49 i 115-116]

Stosownie do wyjaśnień Dyrektora Departamentu Społeczeństwa Informacyjnego i Informatyki UMWO[7]: *Obecnie trwają prace nad aktualizacją zapisów Polityki Bezpieczeństwa, która uwzględni konieczne zmiany w zakresie podstaw prawnych, tj. przywołania rozporządzenia KRI oraz aktualnych wersji norm*.

[Dowód: akta kontroli, s. 117 oraz 13 i 14-15]

Kontrolującym przedłożono zarządzenie nr 85/2018 Marszałka Województwa Opolskiego z dnia 3 września 2018 r. *w sprawie sposobu określania celów i zadań, zarządzania ryzykiem związanym z ich realizacją oraz oceny stopnia ich osiągnięcia*, a ponadto „rejestr ryzyk”[8]. W powyższym rejestrze, w zakresie dotyczącym Departamentu Społeczeństwa Informacyjnego i Informatyki UMWO wymieniono ryzyko utraty dostępności systemów informatycznych oraz ryzyka utraty: poufności, integralności i rozliczalności przetwarzania danych w systemach informatycznych. O okresowych analizach ryzyka utraty integralności, dostępności lub poufności informacji stanowi § 20 ust. 2 pkt 3 *rozporządzenia KRI*. Ryzyko z podkategorii „bezpieczeństwo informacji”, występuje w tym rejestrze, także w innych komórkach organizacyjnych Urzędu. Analiza zapisów ww. zarządzenia nie wzbudziła zastrzeżeń kontrolujących.

[Dowód: akta kontroli, s. 118-136, 16 i 137-160]

Odnosząc się do kwestii inwentaryzacji sprzętu i oprogramowania informatycznego, w myśl wyjaśnień udzielonych kontrolującym przez Dyrektora Departamentu Społeczeństwa Informacyjnego i Informatyki Urzędu – potwierdzonych pozyskanym w tym zakresie materiałem dowodowym – w UMWO funkcjonuje system (GLPI): *służący do kompleksowego*

[6] Dz. U. z 2018 r. poz. 1000.
[7] Do zakresu działania niniejszego Departamentu należy m.in. zapewnienie bezpieczeństwa teleinformatycznego Urzędu.
[8] Przefiltrowany z bazy ryzyk UMWO (na 2019 r.).

zarządzania zasobami informatycznymi. Departament Społeczeństwa Informacyjnego i Informatyki, za pomocą ww. systemu m.in.: zarządza urządzeniami, dostarcza rozwiązania z zakresu helpdesk, prowadzi inwentaryzację sprzętu i oprogramowania. Natomiast: *OCS Inventory NG to oprogramowanie odpowiedzialne za automatyczną inwentaryzację zasobów sprzętowych będących w posiadaniu Urzędu. System ten składa się z kilku komponentów: agentów inwentaryzacji na komputerach klienckich, serwera zbierającego dane, serwera prezentującego dane. Obie usługi są ze sobą zintegrowane w sposób, który przenosi automatycznie zinwentaryzowane elementy z OCS Inventory NG do GLPI. W GLPI dodatkowo ręcznie są dodawane elementy, których nie można automatycznie zinwentaryzować (...).*

[Dowód: akta kontroli, s. 161-163]

Ocena zebranego w trakcie kontroli materiału dowodowego nie sprzeciwia się przyjęciu, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji. Proces zarządzania uprawnieniami do systemów teleinformatycznych w UMWO, odbywa się w module SKU – System Kontroli Uprawnień (portalu IKAR). Z kolei w przypadku korzystania z systemu informatycznego niebędącego w zasobach Urzędu, przy równoczesnym braku podstawy wyznaczenia Administratora Systemu Informatycznego (merytorycznego) stosuje się procedurę nadawania uprawnień określonych przez właściciela systemu informatycznego.

[Dowód: akta kontroli, s. 99-100]

Badając zagadnienie szkoleń pracowników zaangażowanych w proces przetwarzania informacji w Urzędzie, zgodnie z przedłożoną informacją, UMWO zapewnia wszystkim swoim pracownikom dostęp do portalu e-learningowego ATENA, stworzonego przez Departament Społeczeństwa Informacyjnego i Informatyki. W ramach ww. portalu udostępnione jest m.in. szkolenie pt.: „Bezpieczeństwo w cyberprzestrzeni", obejmujące szereg zagadnień wpisujących się w dyspozycję § 20 ust. 2 pkt 6 lit. a-c *rozporządzenia KRI*. Stosownie do przedłożonego przez Dyrektora Departamentu Społeczeństwa Informacyjnego i Informatyki UMWO wyjaśnienia: *w powyższym szkoleniu udział wzięło **170 pracowników** Urzędu. Ponadto w 2017 i 2018 r. przeprowadzone zostały szkolenia stacjonarne z zakresu cyberbezpieczeństwa w których udział wzięło **227 pracowników** Urzędu*.

[Dowód: akta kontroli, s. 164-165]

W tym miejscu należy podkreślić, że zgodnie z informacją uzyskaną z Departamentu Organizacyjno-Administracyjnego UMWO, zatrudnienie w Urzędzie wg stanu na dzień 14 marca 2019 r. wynosiło **540 osób**.

[Dowód: akta kontroli, s. 183]

Nie bez znaczenia jest tu fakt, że: *wszyscy pracownicy UMWO zatrudnieni na stanowiskach urzędniczych, pomocniczych i obsługi posiadają dostęp do informacji (na podstawie stosownych upoważnień), w związku z realizacją czynności kancelaryjnych w systemie EZD. Pracownicy (...) posiadają również dostęp do zbiorów danych funkcjonujących w Urzędzie, odpowiednio do posiadanego zakresu obowiązków, uprawnień i odpowiedzialności.*

[Dowód: akta kontroli, s. 183]

Dodatkowo, w myśl wyjaśnień Dyrektora Departamentu Społeczeństwa Informacyjnego i Informatyki Urzędu: *(...) każdy nowozatrudniony pracownik (...) przechodzi szkolenie z zakresu objętego Regulaminem użytkownika systemu informatycznego. Regulamin ten dostępny jest dla wszystkich pracowników (...) poprzez serwis intranetowy Przyjazna Informatyka*.

[Dowód: akta kontroli, s. 165]

Przedłożony kontrolującym *Regulamin użytkownika systemu informatycznego* składa się z 6 punktów zawierających podstawowe zasady postępowania w zakresie: nadzoru nad stacją roboczą (a-e); korzystania z poczty elektronicznej (a-d); korzystania z internetu (a-c); korzystania ze sprzętu i oprogramowania (a-f); bezpieczeństwa sprzętu służbowego (a) i zgłaszania incydentów (a). Analiza zapisów niniejszego *Regulaminu* skłania do wniosku, że jest to zbiór cennych wskazówek dla użytkownika systemu informatycznego. Trudno jednak na jego podstawie przyjąć, że takie jednorazowe szkolenie (instruktaż) nowozatrudnionego pracownika jest wystarczające i wyczerpuje dyspozycję § 20 ust. 2 pkt 6 lit. a-c *rozporządzenia KRI*.

[Dowód: akta kontroli, s. 165]

UMWO przewiduje także szkolenia pracowników w 2019 r. z bezpieczeństwa przetwarzania danych[9]. Z uwagi na fakt, że określenie końcowego stopnia realizacji powyższego założenia (planu) będzie możliwe po upływie bieżącego roku, nie wpływa ono zasadniczo na ocenę przez kontrolujących wypełnienia wymogu *rozporządzenia KRI* w tym zakresie.

[Dowód: akta kontroli, s. 39]

Do kwestii pracy na odległość i mobilnego przetwarzania danych (patrząc przez pryzmat obowiązujących w Urzędzie procedur użytkowania urządzeń mobilnych i elektronicznych nośników informacji), kontrolujący nie wnieśli uwag.

[Dowód: akta kontroli, s. 105-106]

Analiza problemu bezpieczeństwa informacji w kontekście serwisu sprzętu informatycznego i oprogramowania nie sprzeciwiła się deklaracji (samoocenie) UMWO przedstawionej w ankiecie dot. działania systemów teleinformatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej. Brak uwag.

[Dowód: akta kontroli, s. 39 i 184-229]

Kontrolującym przedstawiono Raport z audytu (datowany na dzień 17 grudnia 2018 r.) dotyczący bezpieczeństwa informacji w UMWO zgodnie z wytycznymi § 20 ust. 2 pkt 14 *rozporządzenia KRI*. W efekcie przeprowadzonego audytu sformułowano łącznie 32 propozycje zaleceń. Z przedłożonej kontrolującym informacji wynika, że wg stanu na dzień 12 marca 2019 r. 8 propozycji zaleceń zostało zrealizowanych. Natomiast pozostałe propozycje zaleceń, zostaną wykonane w 2019 r. (z tego 8 w IV kwartale).

[Dowód: akta kontroli, s. 237-258 i 259-261]

Z wyjaśnień Dyrektora Departamentu Społeczeństwa Informacyjnego i Informatyki wynika że, audyt o którym stanowi § 20 ust. 2 pkt 14 *rozporządzenia KRI,* zostanie przeprowadzony również w roku 2019.

[Dowód: akta kontroli, s. 117]

W UMWO prowadzony jest tzw. elektroniczny rejestr incydentów. W rejestrze tym stwierdzono odnotowywanie zdarzeń (incydentów) m.in. o charakterze awarii informatycznych, nienaruszających bezpieczeństwa cywilnej cyberprzestrzeni RP. Tym niemniej, zgodnie z wykazem pt. „Stan realizacji rekomendacji zawartych w Raporcie z audytu bezpieczeństwa z dnia 17 grudnia 2018 r.", wykonanie propozycji zalecenia dotyczącego *zapewnienia prowadzenia rejestru incydentów teleinformatycznych agregujących zdarzenia o charakterze incydentu teleinformatycznego wraz ze zmianami dokumentów regulacyjnych (…)*, nastąpi w roku bieżącym.

[Dowód: akta kontroli, s. 264 i 261]

[9] W ramach cyklicznych szkoleń z obsługi systemu EZD.

W toku kontroli przeprowadzono oględziny wybranych pokoi UMWO, w których funkcjonują sprawdzane systemy teleinformatyczne oraz oględziny serwerowni Urzędu. Podczas tych czynności nie stwierdzono nieprawidłowości.

[Dowód: akta kontroli, s. 265-272]

Zaznaczyć jedynie można, że serwerownia Urzędu mieści się na poziomie zero (przyziemie budynku), co łącząc z możliwym ryzykiem wystąpienia powodzi (niedaleko przepływa rzeka), będzie stanowiło poważne zagrożenie dla bezpieczeństwa informacji UMWO.

[Dowód: akta kontroli, s. 270 i 273]

Stwierdzono tworzenie tzw. kopii zapasowej danych. Brak uwag.

[Dowód: akta kontroli, s. 271 i 280-281]

Zebrany materiał dowodowy potwierdza odnotowywanie działań użytkowników w dziennikach systemów i ich przechowywanie.

[Dowód: akta kontroli, s. 282-306]

Dodatkowo zaznaczyć należy, że:

1) W toku kontroli stwierdzono, iż wyznaczoną w UMWO osobą odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa jest Dyrektor Departamentu Społeczeństwa Informacyjnego i Informatyki Urzędu. Z przedłożonej w tym zakresie dokumentacji wynika, że przekazanie danych – wyżej wymienionego – do Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym, prowadzonego przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (CSIRT NASK), zostało wysłane (i doręczone) w dniu 15 marca 2019 r., a więc w trakcie trwania niniejszej kontroli. Podkreślić w tym miejscu jest konieczne, że nakładająca powyższy obowiązek ustawa z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa*[10], dalej: *ustawa o krajowym systemie cyberbezpieczeństwa,* weszła w życie w dniu 28 sierpnia 2018 r.

   [Dowód: akta kontroli, s. 309-313]

   Wskazać tu także wypada, iż dokumentacja SZBI (*Polityka Bezpieczeństwa*) nie powinna pomijać obowiązków wynikających – dla jednostki samorządu terytorialnego – z ww. ustawy;

2) UMWO udostępnia elektroniczną skrzynkę podawczą na platformie ePUAP.

   [Dowód: akta kontroli, s. 38]

   Opolski Urząd Wojewódzki w toku niniejszej kontroli, prowadził z jednostką kontrolowaną poprzez ePUAP, skuteczną korespondencję;

3) Podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw oraz wykonywania czynności kancelaryjnych w UMWO jest system informatyczny do elektronicznego zarządzania dokumentacją EZD, co z uwagi na istotne wsparcie pracowników Urzędu w wykonywaniu zadań, ocenia się pozytywnie.

   [Dowód: akta kontroli, s. 314-319]

[10] Dz. U. z 2018 r. poz. 1560. Patrz: art. 21 ust. 1 i art 22 ust. 1 pkt 5.

III. Zakres, przyczyny i skutki stwierdzonych nieprawidłowości:

Zidentyfikowane w wyniku kontroli odstępstwa od stanu pożądanego zakwalifikowano jako uchybienia. Dotyczą one przede wszystkim:

- ukierunkowania – w przeważającej mierze – zapisów analizowanej dokumentacji *SZBI* Urzędu na ochronę danych osobowych, zamiast na bezpieczeństwo informacji (pojęcie szersze od ochrony danych osobowych), czego wymownym przykładem jest m.in. brak przywołania *rozporządzenia KRI* w podstawach prawnych *Polityki Bezpieczeństwa,* czy nieuwzględnienie w tym dokumencie obowiązków wynikających – dla jednostki samorządu terytorialnego – z *ustawy o krajowym systemie cyberbezpieczeństwa*,
- niewystarczającego zakresu szkoleń dotyczących bezpieczeństwa informacji tzn. takich które jednocześnie wyczerpują dyspozycję § 20 ust. 2 pkt 6 lit. a-c *rozporządzenia KRI* i ukończyli je wszyscy pracownicy Urzędu zaangażowani w proces przetwarzania informacji,
- stosunkowo późnego (patrząc na problem wyłącznie w kontekście upływu czasu od wejścia w życie *ustawy o krajowym systemie cyberbezpieczeństwa*) zrealizowania obowiązku w zakresie wyznaczenia – w trybie art. 21 ust. 1 wymienionej wyżej ustawy – osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa i związanego z tym przekazania danych tej osoby do CSIRT NASK.

Z uwagi na kwalifikację stwierdzonych w toku kontroli odstępstw od stanu pożądanego jako uchybień, odstępuje się od określania ich przyczyn i skutków.

IV. Kontrolę wpisano do książki kontroli prowadzonej w jednostce kontrolowanej, pod poz. nr: 5/2019.

V. Informacja o zastrzeżeniach zgłoszonych do projektu wystąpienia pokontrolnego i wyniku ich rozpatrzenia lub o niezgłoszeniu zastrzeżeń:

Kierownik jednostki kontrolowanej, nie zgłosił zastrzeżeń do projektu wystąpienia pokontrolnego.

VI. Zalecenia lub wnioski dotyczące usunięcia nieprawidłowości (uchybień) lub usprawnienia funkcjonowania jednostki kontrolowanej:

W związku z ustaleniami kontroli, zalecam:

1) Dokonać przeglądu i wprowadzenia niezbędnych modyfikacji (uzupełnień) dokumentacji *SZBI* Urzędu, celem eliminacji stwierdzonych odstępstw od stanu pożądanego;
2) Zapewnić uczestnictwo w szkoleniach dotyczących bezpieczeństwa informacji – w zakresie o którym stanowi § 20 ust. 2 pkt 6 lit. a-c *rozporządzenia KRI* – wszystkich (bez wyjątku) pracowników UMWO zaangażowanych w proces przetwarzania informacji;
3) Przestrzegać obowiązków wynikających dla jednostki samorządu terytorialnego z *ustawy o krajowym systemie cyberbezpieczeństwa*;
4) Rozważyć możliwość zmiany lokalizacji serwerowni UMWO;
5) Rozważyć możliwość przyspieszenia wykonania dotychczas niezrealizowanych propozycji zaleceń, zawartych w Raporcie z audytu (z dnia 17 grudnia 2018 r.) dotyczącego bezpieczeństwa informacji w UMWO.

VII. Ocena wskazująca na niezasadność zajmowania stanowiska lub pełnienia funkcji przez osobę odpowiedzialną za stwierdzone nieprawidłowości: nie dotyczy.

VIII. Na podstawie art. 49 oraz art. 46 ust. 3 pkt 3 *ustawy o kontroli*, proszę o przekazanie pisemnej informacji o sposobie wykonania zaleceń, wykorzystaniu wniosków lub przyczynach ich niewykorzystania, o podjętych działaniach lub przyczynach ich niepodjęcia, albo o innym sposobie usunięcia stwierdzonych nieprawidłowości (uchybień), w terminie 30 dni od dnia otrzymania niniejszego dokumentu.

IX. Zgodnie z art. 48 *ustawy o kontroli,* od wystąpienia pokontrolnego nie przysługują środki odwoławcze.

Wojewoda Opolski

Adrian Czubak