WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

Olsztyn, 4 listopada 2019 r.

FK-IV.431.40.2019

Szanowny Pan
Marek Leszek Olszewski
Wójt Gminy Srokowo
pl. Rynkowy 1
11-420 Srokowo

Stosownie do art. 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. Nr 185, poz. 1092), zwanej dalej „ustawą o kontroli w administracji rządowej", przekazuję Panu treść wystąpienia pokontrolnego.

Wystąpienie pokontrolne

Kontrolę przeprowadzono w Urzędzie Gminy Srokowo, pl. Rynkowy 1, 11-420 Srokowo, REGON: 000546029, NIP: 7420013295.

W okresie objętym kontrolą oraz w okresie prowadzenia kontroli stanowiska pełnili:

1. **Pan Franciszek Andruszkiewicz -** Wójt wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 16.11.2014 r. pełnił funkcję do dnia 04.11.2018 r. (*kierownik jednostki kontrolowanej*).
2. **Pan Marek Leszek Olszewski** - Wójt wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 04.11.2018 r. (*kierownik jednostki kontrolowanej bezpośrednio nadzorujący pracowników realizujących zadania objęte kontrolą*).
3. **Pan Mariusz Daćko** - Informatyk Urzędu, zatrudniony na podstawie umowy o pracę od dnia 01.12.2009 r. (*realizujący zadania objęte kontrolą*).
4. **Pan Szymon Kubiak** - Inspektor Ochrony Danych Urzędu zatrudniony na podstawie umowy nr 02/10/2018 od dnia 01.10.2018 r. (*realizujący zadania objęte kontrolą*).

[akta kontroli str. 39]

Kontrolę przeprowadził pracownik Wydziału Finansów i Kontroli Warmińsko- Mazurskiego Urzędu Wojewódzkiego w Olsztynie, Radosław Gazda – inspektor wojewódzki; legitymacja służbowa nr 9/2019, wydana przez Dyrektora Generalnego Warmińsko - Mazurskiego Urzędu Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr FK-IV.0030.879.2019 z 16 września 2019 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 38]

Kontrolę przeprowadzono w dniach 26-30 września 2019 r., co zostało odnotowane w książce kontroli Urzędu Gminy w Srokowie pod pozycją Nr 5/2019.

Przedmiotem kontroli była ocena działania systemów teleinformatycznych używanych przez jednostki samorządu terytorialnego do realizacji zadań zleconych z zakresu administracji rządowej, na podstawie art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2017 r. poz. 570 ze zm. - akt prawny obowiązujący do 02.04.2019 r. oraz Dz.U. z 2019 r. poz. 700 ze zm.). Okres objęty kontrolą: od dnia 1 stycznia 2018 r. do dnia 26 września br. (dzień rozpoczęcia czynności kontrolnych).

[akta kontroli str. 1, 19, 38]

Kontrola została przeprowadzona na podstawie art. 2 pkt 1 i art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. Nr 185, poz. 1092) oraz art. 28 ust. 1 pkt 2 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz. U. z 2019 r., poz. 1464) w związku z art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2017 r. poz. 570 ze zm. - akt prawny obowiązujący do 02.04.2019 r. oraz Dz.U. z 2019 r. poz. 700 ze zm.), zwanej dalej „ustawą" oraz rozdziału III i IV 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 (Dz.U. z 2017 r. poz. 2247), zwanego dalej „rozporządzeniem KRI", jak również Wytycznych dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych, zatwierdzonych przez Ministra Cyfryzacji w dniu 15 grudnia 2015 r.

[akta kontroli str. 1, 19, 38]

W czasie trwania czynności kontrolnych informacji i wyjaśnień udzielał Informatyk Urzędu Gminy - upoważniony przez Wójta Gminy.

[akta kontroli str. 40]

Na podstawie ustaleń kontroli, realizację zadań z zakresu działania systemów teleinformatycznych używanych przez Urząd do realizacji zadań zleconych z zakresu administracji rządowej ocenia się **pozytywnie z nieprawidłowościami.**

Ocena działalności jednostki kontrolowanej wynika z następujących ustaleń i ocen dokonanych w poszczególnych obszarach (zagadnieniach) objętych kontrolą.

Z informacji przekazanych przez UG w Srokowie przed rozpoczęciem czynności kontrolnych

oraz uzyskanych w trakcie prowadzenia kontroli wynika, że w Urzędzie do realizacji zadań zleconych z zakresu administracji rządowej wykorzystywane są **3** systemy teleinformatyczne (Źródło, PUMA – 3 moduły, oraz CEIDG).

Systemy teleinformatyczne wykorzystywane w Urzędzie Gminy w Srokowie

1) **ŹRÓDŁO** – (**Rejestr PESEL**, **Rejestr dowodów osobistych, Rejestr stanu cywilnego**) bezpłatna aplikacja, która obsługuje wszystkie wymagane polskim prawem działania w zakresie rejestru PESEL, dowodów osobistych i stanu cywilnego. Dodatkowo umożliwia również realizację zadań Systemu Odznaczeń Państwowych oraz Centralnego Rejestru Sprzeciwów. W efekcie ŹRÓDŁO to uniwersalne narzędzie obsługujące m.in.: Rejestr PESEL, Rejestr Bazy Usług Stanu Cywilnego (BUSC), Rejestr Dowodów Osobistych (RDO), System Odznaczeń Państwowych (SOP), Centralny Rejestru Sprzeciwów (CRS).

2) **PUMA - Moduł Ewidencja Ludności** posiada homologację MSW, a jego zadaniem jest kompleksowa obsługa komórki ewidencji ludności. Aplikacja umożliwia między innymi: gromadzenie, wyszukiwanie, uzupełnianie oraz zmianę w bazie danych wszystkich informacji znajdujących się na Karcie Osobowej Mieszkańca. Program automatyzuje pracę i drukuje zawiadomienia w zakresie: meldowania, wymeldowania, rejestracji urodzeń, zgonów, zmian stanu cywilnego, gromadzenia i dostępu do danych historycznych mieszkańców.
   Moduł Wyborcy – kompleksowa obsługa wyborów. Moduł Wyborcy umożliwia prowadzenie i aktualizację rejestru wyborców, sporządzanie spisów wyborców uprawnionych do udziału w wyborach i referendum, pozwala na generowanie kwartalnych meldunków dla KBW (Krajowego Biura Wyborczego) o stanie wyborców mieście na podstawie bazy danych ewidencyjnych.
   Moduł Stanu Cywilnego – moduł wspomagający dla Źródła służący do migracji danych.

3) **CEIDG** jest to elektroniczny rejestr przedsiębiorców działających na terenie kraju. Portal ułatwia podatnikom prowadzenie działalności gospodarczej. Umożliwia on założenie firmy, aktualizację danych, jak również zamknięcie czy zawieszenie działalności gospodarczej. Służy również do przekazywania informacji o wydanych zezwoleniach, koncesjach oraz wpisach do rejestrów.

Zgodnie z Uchwałą Nr XLVII/195/06 Rady Gminy Srokowo z dnia 28 kwietnia 2006 r. Gmina Srokowo przystąpiła do Mazurskiego Związku Międzygminnego – Gospodarka Odpadami, który to związek zgodnie z Uchwałą Nr XXIII/117/12 Rady Gminy Srokowo z dnia 29 sierpnia 2012 zobowiązany jest do prowadzenia rejestru działalności regulowanej w zakresie odbierania odpadów komunalnych od właścicieli nieruchomości (podstawa prawna - art. 9b ust. 2-3 ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach, t. j. Dz. U. z 2018 r., poz. 1454 ze zm.).

[akta kontroli str. 18, 52-61]

I. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.

1.1. Usługi elektroniczne

Z art. 16 ust. 1a ustawy wynika, że *podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę.*

Zgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI interoperacyjność na poziomie organizacyjnym osiągana jest przez:

a) informowanie przez podmioty realizujące zadania publiczne, w sposób umożliwiający skuteczne zapoznanie się, o sposobie dostępu oraz zakresie użytkowym serwisów dla usług realizowanych przez te podmioty;

b) publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.

Urząd Gminy w Srokowie posiada aktywną Elektroniczną Skrzynkę Podawczą **/ugsrokowo/SkrytkaESP** znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie pism w formie dokumentów elektronicznych. Adres elektronicznej skrzynki podawczej: https://epuap.gov.pl/wps/portal/strefa-klienta/katalog-spraw/klasyfikacjaterytorialna/WARMIŃSKOMAZURSKIE/kętrzyński/Srokowo(gminawiejska). Możliwość bezpośredniego przejścia na główną stronę e-PUAP, zawarto na stronie internetowej Urzędu, w lewym panelu ekranu w zakładce „Polecamy". Formaty danych przyjmowane za pośrednictwem Elektronicznej Skrzynki Podawczej to m.in.: doc, rtf, docx, odt, xls, xlsx, ods, txt, gif, tif, bmp, jpg, pdf.

[akta kontroli str. 62]

Urząd Gminy w Srokowie w związku z posiadaniem aktywnej Elektronicznej Skrzynki Podawczej udostępniał oraz świadczył usługę elektroniczną, z wykorzystaniem ePUAP, tj. „Pismo ogólne do podmiotu publicznego". Usługa pismo ogólne przeznaczone jest do tworzenia pism w postaci elektronicznej wnoszonych za pomocą elektronicznej skrzynki podawczej lub doręczanych przez podmioty publiczne za potwierdzeniem doręczenia, w przypadkach gdy łącznie spełnione są następujące warunki:

- organ administracji publicznej nie określił wzoru dokumentu elektronicznego umożliwiającego załatwienie danej sprawy,
- przepisy prawa nie wskazują jednoznacznie, że jedynym skutecznym sposobem przekazania informacji jest jej doręczenie w postaci papierowej.

Na stronie BIP urzędu (Menu Przedmiotowe) w zakładce E-URZĄD, znajdują się linki do serwisów umożliwiających załatwienie przez Internet sprawy w Urzędzie. Wszystko za

sprawą zrealizowanego projektu „E-Gmina – uruchomienie e-usług i poprawa dostępu do informacji przestrzennej w gminie Srokowo" dofinansowywanego ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Warmińsko – Mazurskiego na lata 2014 -2020. Chcąc dostosować działalność urzędu do najwyższych standardów usług, Gmina Srokowo wprowadziła możliwość kontaktu oraz załatwienia niektórych spraw za pośrednictwem Internetu. E-usługi, które wprowadzono, mają ułatwić kontakt Klienta z Urzędem bez wychodzenia z domu. W ten sposób można między innymi płacić rachunki, składać dokumenty, a także śledzić aktualne zobowiązania wobec urzędu. W wyniku realizacji projektu uruchomiono:

1. **Portal Mieszkańca - eBOI, w którym udostępnionych zostało 16 nowych e-usług (Interaktywne formularze ePUAP) (adres systemu: https://euslugi.gminasrokowo.pl zakładka eBOI).** Nazwa usługi świadczonej w ramach portalu:
   1) Prowadzenie spraw w zakresie podatku od nieruchomości od osób fizycznych,
   2) Prowadzenie spraw w zakresie podatku od nieruchomości od osób prawnych,
   3) Prowadzenie spraw w zakresie podatku rolnego od osób fizycznych,
   4) Prowadzenie spraw w zakresie podatku rolnego od osób prawnych,
   5) Prowadzenie spraw w zakresie podatku leśnego od osób fizycznych,
   6) Prowadzenie spraw w zakresie podatku leśnego od osób prawnych,
   7) Prowadzenie spraw w zakresie podatku od środków transportowych,
   8) Wniosek o wydanie wypisu i wyrysu z miejscowego planu zagospodarowania przestrzennego,
   9) Wniosek o wydanie wypisu i wyrysu ze studium uwarunkowań i kierunków zagospodarowania przestrzennego,
   10) Wniosek o wydanie zaświadczenia o przeznaczeniu działki w obowiązującym miejscowym planie zagospodarowania przestrzennego,
   11) Wniosek o wydanie zaświadczenia o przeznaczeniu działki w obowiązującym studium uwarunkowań i kierunków zagospodarowania przestrzennego,
   12) Wniosek o zwrot podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej,
   13) Wniosek o wydanie zaświadczenia o wielkości gospodarstwa rolnego,
   14) Wniosek o wydanie zaświadczenia o niezaleganiu w podatkach lub stwierdzające stan zaległości,
   15) Wniosek o ulgę w spłacie zobowiązań podatkowych,
   16) Wniosek o wydanie decyzji o warunkach zabudowy i zagospodarowania terenu.

2. **Portal Mieszkańca - ePłatności, za pomocą którego można śledzić bieżące zobowiązania z urzędem (m. in. podatek rolny, podatek leśny, podatek od nieruchomości, podatek od środków transportowych) oraz dokonywać płatności (adres systemu: https://euslugi.gminasrokowo.pl zakładka ePłatności).**

3. **System Informacji Przestrzennej, który został zasilony zdigitalizowanymi mapami zawierającymi warstwy tematyczne (adres systemu: http://sip.gison.pl/srokowo)**

[akta kontroli str. 63]

Zgodnie z § 5 ust. 2 pkt 4 rozporządzenia KRI interoperacyjność na poziomie organizacyjnym osiągana jest przez publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną. Na stronie BIP Urzędu istnieje zakładka „Menu Przedmiotowe" - Procedury załatwiania spraw, w której opisano obowiązujące procedury stosowane przez Urząd przy załatwianiu poszczególnych spraw będących w kompetencjach poszczególnych stanowisk.
W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 63]

1.2. Centralne repozytorium wzorów dokumentów elektronicznych (CRWDE)

Stosownie do art. 19b ust. 3 ustawy, *organy administracji publicznej przekazują do centralnego repozytorium oraz udostępniają w Biuletynie Informacji Publicznej wzory dokumentów elektronicznych. Przy sporządzaniu wzorów dokumentów elektronicznych stosuje się międzynarodowe standardy dotyczące sporządzania dokumentów elektronicznych przez organy administracji publicznej, z uwzględnieniem konieczności podpisywania ich kwalifikowanym podpisem elektronicznym.*

W celu ujednolicenia w skali kraju procedur usług świadczonych przez urzędy drogą elektroniczną, w tym ujednolicenia wzorów dokumentów elektronicznych w CRWDE przechowywane są wzory dokumentów, jakie zostały już opracowane i są używane. W przypadku uruchamiania przez dany podmiot publiczny usługi elektronicznej, która funkcjonuje już na koncie innego podmiotu, dany podmiot publiczny powinien skorzystać z procedury obsługi tej usługi oraz zastosować wzory dokumentów elektronicznych dotyczące tej procedury znajdujące się w CRWDE (nie dotyczy to sytuacji gdy usługa jest usługą centralną, tzn. jest udostępniania przez jeden podmiot, np. właściwego ministra, ale służy do świadczenia usług przez inne podmioty niż udostępniający, np. wszystkie gminy). W przypadku uruchamiania usługi, dla której nie ma wzorów dokumentów w CRWDE, podmiot publiczny jest zobowiązany przekazać do CRWDE procedurę obsługi usługi i wzory dokumentów elektronicznych z nią związanych.

W trakcie kontroli ustalono, że Urząd Gminy w badanym okresie w związku z realizacją projektu „E-Gmina – uruchomienie e-usług i poprawa dostępu do informacji przestrzennej w gminie Srokowo" przekazywał wzory dokumentów elektronicznych do centralnego repozytorium wzorów dokumentów prowadzonego przez Ministerstwo Cyfryzacji. Łącznie do CRWDE przekazano 31 wniosków, z czego na dzień kontroli opublikowane zostały

4 wnioski.

[akta kontroli str. 65-127]

Jednocześnie należy zaznaczyć, iż na stronie BIP kontrolowanego Urzędu w zakładce „Menu Przedmiotowe" - Procedury załatwiania spraw opublikowano w wersji „do pobrania" formularze wzorów dokumentów niezbędnych do załatwienia poszczególnych spraw w Urzędzie. Urząd Gminy udostępniał też oraz świadczył usługę elektroniczną, z wykorzystaniem ePUAP, tj. „Pismo ogólne do podmiotu publicznego".
W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 64]

1.3. Model usługowy

– Z § 15 ust. 2 rozporządzenia KRI wynika, że *zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.*

Strona internetowa Urzędu działa pod adresem http://www.srokowo.warmia.mazury.pl/, a strona internetowa BIP Urzędu – pod adresem http://bip.gminasrokowo.pl/.
Na stronie internetowej Urzędu zamieszczono link do strony BIP Urzędu w dolne lewej części panelu strony. Zarówno na stronie www jak i na stronie głównej BIP Urzędu, zamieszczono link i adres skrzynki podawczej ESP na platformie ePUAP.
Ponadto na stronie internetowej BIP UG, znajdują się linki do najważniejszych serwisów internetowych ułatwiających odbiorcy internetowemu załatwienie podstawowych spraw urzędowych, tj.:

– **OBYWATEL.GOV.PL**, który powstał jako część programu pl.ID, realizowanego w ramach Programu Operacyjnego Innowacyjna Gospodarka (7. Oś priorytetowa – Społeczeństwo informacyjne – budowa elektronicznej administracji) i współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego. Znajduje się tu kilkaset najpopularniejszych usług świadczonych przez administrację publiczną.
– **BIZNES.GOV.PL** - to serwis przeznaczony dla osób zamierzających rozpocząć i prowadzących działalność gospodarczą. Celem portalu jest pomoc w realizacji spraw związanych z zakładaniem i prowadzeniem działalności oraz uproszczenie formalności niezbędnych do założenia i prowadzenia firmy. W serwisie dostępne są opisy urzędowych usług oraz gotowe formularze. Za pomocą serwisu, osoby prowadzące firmę mogą składać wnioski do instytucji państwowych drogą elektroniczną, a także załatwiać swoje biznesowe sprawy przez Internet. Serwis łączy w sobie wiele usług i funkcji nie tylko dla przedsiębiorców, ale także dla administracji państwowej. Przedsiębiorcy znajdą tutaj szczegółowe informacje o obowiązujących przepisach prawa, wymaganych procedurach i formalnościach związanych z zakładaniem i prowadzeniem działalności gospodarczej w Polsce oraz w całej Unii Europejskiej.
– **ePUPAP -** elektroniczna skrzynka podawcza znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie pism w formie dokumentów

elektronicznych.

W Urzędzie brak jest formalnych procedur opisujących obsługę oraz monitorowanie usług elektronicznych, ze względu na fakt, iż instytucja ta nie świadczyły usług elektronicznych na zewnątrz za pomocą systemów teleinformatycznych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej, w związku z powyższym przedmiotowe cząstkowe zagadnienie nie podlegało ocenie.

[akta kontroli str. 63]

1.4. Współpraca systemów teleinformatycznych z innymi systemami

Stosownie do:

- § 5 ust. 3 pkt 3 rozporządzenia KRI *interoperacyjność na poziomie semantycznym osiągana jest przez: stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań;*
- § 16 ust. 1 rozporządzenia KRI *systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.*

Wiele rejestrów w urzędach administracji publicznej przechowuje i przetwarza identyczne informacje, np. o obywatelu/podmiocie, takie jak PESEL, REGON, NIP, dane adresowe itp. Ułatwieniem w załatwieniu spraw dla obywatela lub podmiotu będzie sytuacja, gdy podmiot publiczny nie będzie żądał od obywatela lub podmiotu informacji będących już w posiadaniu urzędów. Realizacja tego postulatu wymaga, aby system informatyczny, w którym prowadzony jest dany rejestr odwoływał się bezpośrednio do danych gromadzonych w innych rejestrach publicznych uznanych za referencyjne w zakresie niezbędnym do realizacji zadań.

Z informacji uzyskanych w wyniku kontroli wynika, że systemy teleinformatyczne zainstalowane i użytkowane w Urzędzie Gminy w Srokowie współpracują w następujących zakresach, cyt.: „*Systemy teleinformatyczne współpracują ze sobą (...) poprzez dedykowane szyny integracyjne pomiędzy systemami znajdującymi się w Urzędzie Gminy Srokowo oraz certyfikatów dla systemów teleinformatycznych służących zapewnieniu bezpieczeństwa wymiany informacji ePUAP.*

1) *(Źródło -> PUMA) Moduł Ewidencji Ludności w systemie PUMA jest zasilany danymi z systemu Źródło za pomocą dedykowanego, szyfrowanego połączenia.*
2) *(Edicta <-> PUMA) System obiegu dokumentów EDICTA jest zintegrowany z modułami systemu PUMA:*
   - Dane z modułu Kontrahenci systemu PUMA widoczne są w module kontrahenci systemu

EDICTA.

- *Dane z formularzy ePUAP dotyczące podatków, które trafiają do systemu EDICTA po zarejestrowaniu sprawy trafiają do modułu podatkowego lub dotyczącego akcyzy w systemie PUMA (5 poziom dojrzałości usługi).*

3) *(Edicta <-> SIP) Dane z formularzy ePUAP dotyczące gospodarki przestrzennej, które trafiają do systemu EDICTA po zarejestrowaniu sprawy trafiają do modułu Systemu Informacji Przestrzennej (3 poziom dojrzałości usługi).*
4) *(Portal Mieszkańca <-> Pośrednik płatności <-> PUMA) Portal mieszkańca prezentuje dane dot. zobowiązań mieszkańca w urzędzie (dane pobierane są z systemu PUMA - podatki, opłaty, koncesje alkohole, dzierżawy, za zajęcie pasa drogowego, faktury). Mieszkaniec za pośrednictwem portalu mieszkańca może zobowiązanie opłacić on-line, za pośrednictwem pośrednika płatności (PayByNet). Po dokonaniu płatności portal mieszkańca komunikuje się z systemem pośrednika płatności w celu pobrania potwierdzenia przelewu po czym dane te przekazywane są do odpowiedniego modułu PUMA celem zaksięgowania."*

Jednocześnie należy wspomnieć, iż Źródło jest to system zarządzany przez Ministerstwo Cyfryzacji o charakterze ogólnopolskim, umożliwia on współpracę z systemem teleinformatycznym PUMA wykorzystywanym w Urzędzie. Stacje robocze na których zainstalowany jest system Źródło pracują w odizolowanej sieci. Dostęp do systemu uprawnieni użytkownicy uzyskują uwierzytelniając się poprzez logowanie do systemu Windows oraz przy pomocy kart kryptograficznych z zainstalowanymi certyfikatami dedykowanymi dla użytkownika aplikacji. W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 50]

1.5. Obieg dokumentów w podmiocie publicznym

Z § 20 ust. 2 pkt 9 rozporządzenia KRI wynika, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególność przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie, m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.*

Zgodnie z zarządzeniem Nr 83/2018 Wójta Gminy Srokowo z dnia 28 grudnia 2018 w sprawie wskazania systemu wykonywania czynności kancelaryjnych oraz określenia zasad funkcjonowania systemu w Urzędzie Gminy Srokowo, podstawowym sposobem dokumentowania przebiegu załatwiania spraw w Urzędzie jest system tradycyjny, tj. system wykonywania czynności kancelaryjnych, dokumentowania przebiegu załatwiania spraw, gromadzenia i tworzenia dokumentacji w postaci nieelektronicznej zgodnie z zasadami określonymi w Rozporządzeniu Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie

organizacji i zakresu działania archiwów zakładowych. System tradycyjny wspomagany jest przez funkcjonujący w Urzędzie elektroniczny system obiegu dokumentów EDICTA.

EDICTA to elektroniczny system obsługi dokumentów określający sposób doręczania i wysyłania korespondencji w postaci elektronicznej. Umożliwia zarzadzanie dokumentami, korespondencją, sprawami (projektami), poleceniami, terminami oraz czasem pracy pracowników, tworząc centralna, uporządkowana bazę dokumentów i informacji. Umożliwia również sprawny dostęp do korespondencji, umów, procedur wewnętrznych itp., kontroluje drogę obiegu korespondencji oraz stan realizacji projektów, usprawnia obsługę klientów.
Określenie zasad obiegu dokumentacji w formie elektronicznej zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI, umożliwia realizację i egzekwowanie, m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 128--137]

1.6. Formaty danych udostępniane przez systemy teleinformatyczne

Stosownie do:

- § 17 ust. 1 rozporządzenia KRI k*odowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków, odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz ze zmianami lub normę ją zastępującą;*
- § 18 ust. 1 rozporządzenia KRI *systemy teleinformatyczne podmiotów realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia;*
- § 18 ust. 2 rozporządzenia *KRI jeżeli z przepisów szczegółowych albo opublikowanych w repozytorium interoperacyjności schematów XML lub innych wzorów nie wynika inaczej, podmioty realizujące zadania publiczne umożliwiają przyjmowanie dokumentów elektronicznych służących do załatwiania spraw należących do zakresu ich działania w formatach danych określonych w załącznikach nr 2 i 3 do rozporządzenia.*

Istotą współdzielenia informacji w urzędach jest stworzenie możliwości wymiany danych pomiędzy różnymi systemami informatycznymi oraz umożliwienie odbiorcom swobodnego dostępu do informacji poprzez wygenerowanie danych w powszechnie znanych i dostępnych formatach plików.
Z informacji przekazanych przez Wójta Gminy Srokowo wynika, że cyt.*: „Wymiana danych pomiędzy systemami odbywa się za pomocą dedykowanej szyny integracyjnej (PUMA-Źródło). Dane pozyskiwane z systemów dziedzinowych generowane i udostępniane są w powszechnie dostępnych formatach plików (m. in. pdf, xls, xml, odt, html) oraz standardach kodowania (m. in. Unicode UTF-8, WIN-1250, Elixir). Systemy dziedzinowe pozwalają na*

przyjmowanie dokumentów elektronicznych służących do załatwiania spraw, w formatach określonych w załączniku 2 i 3 do rozporządzenia KRI."
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 50]

II. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych

2.1. Dokumenty z zakresu bezpieczeństwa informacji

Zgodnie z:

- § 20 ust. 1 rozporządzenia KRI p*odmiot 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 z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;*
- § 20 ust. 2 rozporządzenia KRI z*arządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań związanych z bezpieczeństwem informacji;*
- § 20 ust. 2 pkt 1 rozporządzenia KRI z*arządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.*

Podmiot publiczny 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 (system zarządzania bezpieczeństwem informacji), w tym szeregu regulacji wewnętrznych oraz zapewnienia aktualizacji tych regulacji w zakresie dotyczącym zmieniającego się otoczenia. Kompleksowa dokumentacja SZBI jest warunkiem niezbędnym możliwości skutecznego zarządzania bezpieczeństwem informacji w podmiocie.
Podstawowym dokumentem SZBI jest Polityka Bezpieczeństwa Informacji. Polityka zazwyczaj zawiera wyrażoną przez kierownictwo deklarację stosowania, opisuje organizację i ustala osoby odpowiedzialne oraz ich zakresy odpowiedzialności, wprowadza klasyfikację informacji, sposób postępowania z poszczególnymi rodzajami informacji.

- Zarządzeniem Nr 73/16 Wójta Gminy Srokowo z dnia 23 sierpnia 2016 r. wprowadzono w Urzędzie Gminy z dniem 30 września 2016 do stosowania dokumentację SZBI, miedzy innymi Politykę Bezpieczeństwa Informacji oraz Instrukcje zarzadzania systemami informatycznymi. Przeprowadzono również analizę ryzyka i opracowano plan postępowania z ryzykiem w UG Srokowo.
  Zarządzenia wprowadzono zgodnie z obowiązującymi w tym okresie przepisami prawa, tj.

ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. 2016 r., poz. 922) oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024). Powyższe dokumenty, a w szczególności Instrukcja Zarządzania Systemem Informatycznym w Urzędzie, stanowiły dokumentację przetwarzania danych osobowych w rozumieniu §1 pkt 1 rozporządzenia MSWiA z 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych (…). Służyły one zapewnieniu poufności, integralności i rozliczalności przetwarzanych danych.

- Zarządzeniami Nr 107/15 Wójta Gminy Srokowo z dnia 4 grudnia2015 r. oraz Nr 58/16 Wójta Gminy Srokowo z dnia 15 czerwca 2016 r. wyznaczono w jednostce kolejnych Administratorów Bezpieczeństwa Informacji.

[akta kontroli str. 190-239]

- Zarządzeniem Nr 66/2018 Wójta Gminy Srokowo z dnia 28 września 2018 r. wprowadzono w Urzędzie Gminy z dniem 1 listopada 2018 r. do stosowania dokumentację SZBI, w skład której weszły miedzy innymi Polityka Bezpieczeństwa Danych Osobowych, Instrukcja zarzadzania systemem informatycznym służącym do przetwarzania danych osobowych, Procedura zarzadzania uprawnieniami do przetwarzania danych osobowych.
- Zarządzeniem Nr 58/2019 Wójta Gminy Srokowo z dnia 1 sierpnia 2019 r. zmieniono zarządzenie Nr 66/2018 Wójta Gminy Srokowo z dnia 28 września 2018 r. w zakresie załącznika Nr 2 stanowiącego Instrukcję zarzadzania systemem informatycznym służącym do przetwarzania danych osobowych.

  Dokumentację SZBI sporządzono na podstawie obowiązujących przepisów prawa, tj. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 roku, 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) (Dz. Urz. UE L 119, s.1) – zwanego dalej „RODO”. Dokumentacja w zakresie ochrony danych dotyczyła danych przetwarzanych w Urzędzie i służyła zapewnieniu poufności, integralności przetwarzania danych, jak również monitorowania zdarzeń naruszających ochronę danych (w tym osobowych), zawierała także opis postępowania w przypadku naruszenia zasad bezpieczeństwa danych osobowych.
- W Urzędzie Gminy w Srokowie wyznaczono Inspektora Ochrony Danych (IOD) oraz zgodnie z podpisaną umową ustalono jego ramowy zakres zadań.

[akta kontroli str. 240-376]

W powyższym zakresie kontrolujący stwierdził uchybienie polegające na przyjęciu dokumentacji stanowiącej SZBI w Urzędzie Gminy w Srokowie dopiero w dniu

1 listopada 2018 r., natomiast obowiązek stosowania RODO – to dzień 25 maja 2018 r. Z uzyskanego z Urzędu Gminy wyjaśnienia wynika, że cyt.: *„Przyczyną opóźnienia wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy był brak wystarczającej wiedzy na ten temat oraz nie podjęcie stosownych decyzji przez kierownictwo jednostki.”*
Skutkiem uchybienia był brak wymaganej aktualizacji Polityki zgodnie z § 20 ust. 1 i ust. 2 pkt 1 rozporządzenia KRI, jak również art. 24 ust. 1 i 2 RODO. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki.

[akta kontroli str. 51]

Zgodnie z § 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 z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.
Kontrolujący stwierdził na podstawie udostępnionej do kontroli dokumentacji, że w Urzędzie nie były prowadzone działania w zakresie monitoringu i przeglądu systemu zarządzania bezpieczeństwem informacji, co stanowi uchybienie. Przyczyną powstania uchybienia zgodnie z wyjaśnieniem Wójta Gminy było, cyt.: *„W urzędzie nie były przeprowadzane okresowe kontrole i przeglądy wewnętrzne Systemu Zarządzania Bezpieczeństwem Informacji. Firma, z którą gmina miała zawartą umowę nie wywiązała się z tego zadania.”*
Brak okresowych przeglądów i monitoringu SZBI w jednostce stanowi naruszenie § 20 ust. 1 rozporządzenia KRI. Osobą odpowiedzialną jest IOD, wskazany przez firmę z którą Wójt Gminy Srokowo podpisał umowę na świadczenie usług Inspektora Ochrony Danych.

[akta kontroli str. 51]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami.

2.2. Analiza zagrożeń związanych z przetwarzaniem informacji

Z § 20 ust. 2 pkt 3 rozporządzenia KRI wynika, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.*

Wymogiem skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Kluczowa rola analizy ryzyka wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny i jest zależny od ważności aktywów informatycznych danego podmiotu.

Zgodnie z wymogiem wynikającym z § 20 ust. 2 pkt 3 rozporządzenia KRI, jak również

przyjętej w Urzędzie Metodyce oceny skutków dla ochrony danych osobowych (Załącznik nr 4 do zarządzenia 66/2018 Wójta Gminy Srokowo), przeprowadzona powinna być w Urzędzie analiza ryzyka utraty poufności, integralności i dostępności danych. Z przedstawionej do kontroli dokumentacji nie wynika, aby po przyjęciu zarządzenia Nr 66/2018 Wójta Gminy Srokowo, taka analiza była w Urzędzie Gminy przeprowadzona. Powyższe stanowi nieprawidłowość. Przyczyną powstania nieprawidłowości zgodnie z wyjaśnieniem Wójta Gminy było, cyt.: „*Inspektor Ochrony Danych nie przeprowadził okresowej analizy ryzyka w urzędzie oraz przeglądów ryzyk zawartych w polityce bezpieczeństwa danych. Firma, z którą gmina miała podpisaną umowę nie wywiązała się z powierzonych zadań.”*
Nieprzeprowadzenie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji stanowi naruszenie § 20 ust. 2 pkt 3 rozporządzenia KRI. Osobą odpowiedzialną jest IOD, wskazany przez firmę z którą Wójt Gminy Srokowo podpisał umowę na świadczenie usług Inspektora Ochrony Danych.

[akta kontroli str. 51, 311-313]

Jednocześnie należy wskazać, iż w jednostce był opracowany rejestr czynności przetwarzania danych osobowych zgodnie z RODO.

[akta kontroli str. 377-391]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z nieprawidłowościami.

2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego

Z § 20 ust. 2 pkt 2 rozporządzenia KRI wynika, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.*

Kontrolującemu przedstawiono aktualną inwentaryzację sprzętu komputerowego użytkowanego w Urzędzie Gminy w Srokowie sporządzoną zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI. Przedmiotowa inwentaryzacja obejmowała miedzy innymi rodzaj i konfigurację sprzętu, prowadzona była w systemie tradycyjnym - papierowym. Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 138-188]

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Stosownie do:

- § 20 ust. 2 pkt 4 rozporządzenia KRI z*arządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: podejmowanie działań zapewniających, 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;

- § 20 ust. 2 pkt 5 rozporządzenia KRI z*arządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.*

Istotnym elementem polityki BI jest zarządzanie dostępem do systemów teleinformatycznych przetwarzających informacje. Zarządzanie dostępem ma zapewnić, 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, a w przypadku zmiany zadań następuje również zmiana ich uprawnień.

Zasady nadawania i odbierania uprawnień do przetwarzania danych osobowych oraz do pracy w systemie informatycznym określone zostały zarządzeniem Nr 66/2018 Wójta Gminy Srokowo z dnia 28 września 2018 r. wprowadzającym do stosowania dokumentację SZBI, w skład której weszły miedzy innymi Polityka Bezpieczeństwa Danych Osobowych, Instrukcja zarzadzania systemem informatycznym służącym do przetwarzania danych osobowych, Procedura zarzadzania uprawnieniami do przetwarzania danych osobowych (Rozdział 4-5).

Osoby posiadające dostęp do danych osobowych posiadały pisemne upoważnienie. Prowadzona była też ewidencja osób upoważnionych do przetwarzania danych. Pracownikom posługującym się systemem teleinformatycznym wydane zostały stosowne upoważnienia do pracy w określonym systemie. W Urzędzie Gminy Srokowo prowadzona była również ewidencja wydanych upoważnień w zakresie dostępu do pracy w systemach informatycznych.

[akta kontroli str. 296-304, 392-417]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Z § 20 ust. 2 pkt 6 rozporządzenia KRI wynika, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: a) zagrożenia bezpieczeństwa informacji, b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.*

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 roku, 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) (Dz. Urz. UE L 119, s.1), weszło w życie w dniu 25 maja 2018 r.

Zarządzenie Nr 66/2018 Wójta Gminy Srokowo z dnia 28 września 2018 r. wprowadzające w Urzędzie nową Politykę Bezpieczeństwa Danych Osobowych oraz Instrukcję Zarzadzania Systemem Informatycznym, weszło w życie w dniu 1 listopada 2018 r.

Kontrolujący na podstawie przekazanej dokumentacji stwierdził, że pracownicy uczestniczący w procesie przetwarzania danych osobowych w Urzędzie pomimo wejścia w życie obydwu dokumentów w 2018 roku, przeszkoleni zostali z tematyki bezpieczeństwa danych osobowych dopiero w dniu 25 kwietnia 2019 r. W okresie objętym kontrolą było to jedyne szkolenie dla pracowników z przedmiotowej tematyki. W dokumentacji udostępnionej kontrolującemu nie stwierdzono również programu szkolenia.
Tak późne przeprowadzenie szkolenia stanowi uchybienie. Przyczyną takiego stanu było zgodnie z wyjaśnieniem Wójta Gminy, cyt.: „*Urząd Gminy Srokowo nie posiada programu szkolenia przeprowadzonego 25 kwietnia 2019r. Firma, z którą gmina miała zawartą umowę przeprowadziła tylko jedno szkolenie. Firma nie wywiązała się z tego zadania*."
Skutkiem uchybienia było niedoinformowanie oraz brak wiedzy pracowników uczestniczących w procesie przetwarzania danych osobowych w zakresie nowych przepisów prawa regulujących powyższą tematykę (do dnia szkolenia). Osobą odpowiedzialną jest IOD, wskazany przez firmę z którą Wójt Gminy Srokowo podpisał umowę na świadczenie usług Inspektora Ochrony Danych.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami.

[akta kontroli str. 51, 189]

2.6. Praca na odległość i mobilne przetwarzanie danych

Zgodnie z § 20 ust. 2 pkt 8 rozporządzenia KRI z*arządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.*

Z uzyskanego z Urzędu Gminy wyjaśnienia wynika, że cyt.: *„Komputery przenośne służące do pracy na odległość są zabezpieczone poprzez stosowanie hasła BIOS, wymogu zmiany hasła użytkownika systemu operacyjnego co 30 dni, ograniczenia uprawnień w postaci standardowego użytkownika (bez możliwości ingerencji w konfigurację oraz oprogramowanie), automatycznego włączenia wygaszacza po 15 min. oraz oprogramowania antywirusowego. Ponadto komputery przenośne służą jako terminale do łączenia się z siecią urzędową poprzez szyfrowane połączenie SSL VPN. Brak formalnych regulacji dotyczących pracy na odległość, praca ta jest wykonywana za wiedzą i zgodą wójta. Komputery przenośne są inwentaryzowane. Komputery przenośne nie są wykorzystywane do pracy w systemach teleinformatycznych objętych kontrolą."*

[akta kontroli str. 51]

Przedmiotowe cząstkowe zagadnienie ze względu na wykorzystywanie sprzętu w zakresie systemów teleinformatycznych tylko w siedzibie jednostki (stacjonarny tryb pracy) nie

podlegało ocenie.

2.7. Serwis sprzętu informatycznego i oprogramowania

Stosownie do § 20 ust. 2 pkt 10 rozporządzenia KRI z*arządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.*

W przypadku systemów informatycznych niezbędne jest objęcie tych systemów (w zakresie oprogramowania użytkowego i systemowego, sprzętu oraz rozwiązań telekomunikacyjnych) stosownymi umowami serwisowymi, gwarantującymi odpowiednio szybkie uruchomienie pracy systemu w przypadku awarii oraz gwarantującymi bezpieczeństwo informacji (BI) dla informacji uzyskanych przez wykonawców w związku z ich realizacją.

W Urzędzie Gminy w Srokowie użytkowany jest 1 system teleinformatyczny do realizacji zadań publicznych (składający się z trzech modułów) zakupiony u zewnętrznego dostawcy, tj.: PUMA W związku z zakupem ww. systemu podpisana została umowa licencyjna z firmą ZETO SOFTWARE Sp. z o.o. w Olsztynie.
W treści umowy licencyjnej (asysta techniczna) z firmą dostarczającą system informatyczny PUMA zawarto zapisy w zakresie powierzenia danych, gwarantujące właściwe zabezpieczenie danych w przypadku awarii systemu oraz gwarantująca bezpieczeństwo informacji uzyskanych przez wykonawców w związku z realizacją umowy.

[akta kontroli str. 418-447]

Zgodnie z zarządzeniem Nr 58/2019 Wójta Gminy Srokowo z dnia 1 sierpnia 2019 r. w sprawie zmiany zarządzenia Nr 66/2018 (Rozdział 6) - przegląd i konserwacja sprzętu informatycznego realizowana jest przez upoważnionych pracowników Urzędu Gminy oraz przez podmioty zewnętrzne. Przekazanie sprzętu teleinformatycznego do naprawy poza teren Urzędu jest dopuszczalne jeżeli sprzęt przekazywany jest bez nośników zawierających dane osobowe, przekazanie sprzętu potwierdzone jest protokołem. Wszelkie prace serwisowe wykonywane przez podmioty zewnętrzne wymagają sporządzenia protokołu serwisowego.

[akta kontroli str. 357-358]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.8. Procedury zgłaszania incydentów naruszenia BI

Z § 20 ust. 2 pkt 13 rozporządzenia KRI wynika, że z*arządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określonym i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.*

Instrukcja postępowania w przypadku naruszenia bezpieczeństwa danych osobowych została uregulowana zarządzeniem Nr 66/2018 Wójta Gminy Srokowo z dnia 28 września 2018 r. wprowadzającym w Urzędzie Gminy z dniem 1 listopada 2018 r. do stosowania dokumentację SZBI, w skład której wchodzą miedzy innymi Polityka Bezpieczeństwa Danych Osobowych, Instrukcja zarzadzania systemem informatycznym służącym do przetwarzania danych osobowych, Procedura zarzadzania uprawnieniami do przetwarzania danych osobowych. (Rozdział 10 Polityki Bezpieczeństwa Danych Osobowych).
Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 257-259]

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

Zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.*

W okresie objętym kontrolą tj. od 1 stycznia 2018 rok do dnia rozpoczęcia czynności kontrolnych (26 września 2019 r.) przeprowadzono w kontrolowanej jednostce jedno cząstkowe zadanie audytowe. Czynności audytowe prowadzone były w dniu 14 stycznia 2019 r. W ramach prowadzonego cząstkowego zadania audytowego w zakresie *badania aktualności, adekwatności polityki ochrony danych ze stanem faktycznym*, zostały wydane jednostce rekomendacje (zalecenia). Jednocześnie należy zauważyć, iż przeprowadzony w 2019 r. cząstkowy audyt obejmował swym zakresem jedynie zagadnienia związane z RODO oraz ustawą o ochronie danych osobowych, a nie uwzględniał zagadnień z rozporządzenia KRI w zakresie systemów (§ 20).

[akta kontroli str. 455-457]

W związku z niedopełnieniem w 2018 roku obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI, który stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok – nieprzeprowadzenie audytu wewnętrznego w zakresie bezpieczeństwa informacji w 2018 roku ocenia się jako nieprawidłowość.
Z wyjaśnienia Wójta Gminy wynika, że cyt.: „*Okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji nie był prowadzony. Dotychczasowa firma nie wywiązała się z umowy. Urząd Gminy Srokowo zlecił dla firmy Togatus przeprowadzenie audytu w Urzędzie Gminy Srokowo i w pozostałych jednostkach organizacyjnych (umowa od 1 października 2019r.)”* Skutkiem nieprawidłowości było naruszenie § 20 ust. 2 pkt 14 rozporządzenia KRI. Osobą odpowiedzialną jest IOD, wskazany przez firmę z którą Wójt Gminy Srokowo podpisał umowę na świadczenie usług Inspektora Ochrony Danych.

[akta kontroli str. 51]

W przypadku 2019 roku zaznaczyć należy, że do dnia kontroli (26.09.2019) przeprowadzono jedynie cząstkowy audyt ochrony danych. Wobec powyższego dopełnienie obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI, w przypadku roku 2019 nie podlegało ocenie, ze względu na istniejącą możliwość przeprowadzenia przez jednostkę pełnego wewnętrznego audytu bezpieczeństwa informacji do końca 2019 roku.

[akta kontroli str. 455-457]

2.10. Kopie zapasowe

Z § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI wynika, że z*arządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: minimalizowanie ryzyka utraty informacji w wyniku awarii.*

Jednym z kluczowych sposobów zapobiegania utracie informacji w wyniku awarii jest wykonywanie kopii zapasowych. Tworzenie kopi zapasowych jest elementem planu ciągłości działania. Celem tworzenia kopii zapasowych jest możliwość odzyskania danych i przywrócenia do pracy użytkowej systemu teleinformatycznego wraz z informacjami przechowywanymi przez ten system, np. w bazie danych. Wymóg ten można osiągnąć wykonując regularnie kopie zapasowe całego środowiska pracy danego systemu teleinformatycznego, tj. systemu operacyjnego, jego konfiguracji (w tym konfiguracji zabezpieczeń), systemu informatycznego i informacji w nim przechowywanych.

Zasady tworzenia kopii zapasowych uregulowane zostały zarządzeniem Nr 58/2019 Wójta Gminy Srokowo z dnia 1 sierpnia 2019 r. zmieniono zarządzenie Nr 66/2018 Wójta Gminy Srokowo z dnia 28 września 2018 r. w zakresie załącznika Nr 2 stanowiącego Instrukcję zarzadzania systemem informatycznym służącym do przetwarzania danych osobowych (Rozdział 3).

[akta kontroli str. 355-356, 359-363]

Kontrolującemu udostępniono opracowany harmonogram wykonywania kopii zapasowych, z którego wynikało, że kopie zapasowe danych z kontrolowanego systemu teleinformatycznego PUMA wykonywane są w cyklu dziennym. Kopie bezpieczeństwa wykonywane są na serwerze w jednostce i dodatkowo na zewnętrznym serwerze zgodnie z umową z Warmińsko-Mazurskim Urzędem Marszałkowskim – Samorządowy Ośrodek Przetwarzania Danych.

[akta kontroli str. 448-454]

Z udostępnionego elektronicznego rejestru kopii zapasowych zbiorów danych, wynika, że kopie zapasowe były wykonywane zgodnie z opracowanym harmonogramem.

[akta kontroli str. 458-460]

Jednocześnie kontrolujący (na podstawie udostępnionej dokumentacji) stwierdził, że w Urzędzie Gminy są wykonywane testy w celu sprawdzenia poprawności wykonywania kopii zapasowych oraz sprawdzenie przydatności utworzonych kopii podczas próby symulowanego przywrócenia i uruchomienia oprogramowania po przywróceniu.

[akta kontroli str. 461-464]

Regularne testowanie jakości kopii zapasowych poprzez odtworzenie systemu informatycznego z kopii zwykle na niezależnym od środowiska produkcyjnego sprzętowym środowisku testowym oraz testowanie pracy użytkowej odtworzonego systemu jest kluczowym działaniem w celu minimalizowania ryzyka utraty informacji w wyniku awarii. Wskazane jest przechowywanie kopii zapasowych w innej lokalizacji niż miejsce ich tworzenia, w odległości niezbędnej do uniknięcia uszkodzeń spowodowanych przez katastrofę, która dotknęłaby podstawowy ośrodek przetwarzania danych.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

Stosownie do § 15 ust. 1 rozporządzenia KRI s*ystemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.*

Wykorzystywane w Urzędzie systemy teleinformatyczne wspomagające realizację zadań z zakresu administracji rządowej dzieliły się na systemy centralne tj. ŹRÓDŁO i CEIDG oraz system zakupiony u dostawcy zewnętrznego - PUMA. Na obsługę aktualnie zainstalowanego oprogramowania z firmą dostarczającą system informatyczny zawarto stosowną umowę licencyjną (asysta techniczna), gwarantujące rozwój systemu i dostosowanie do obowiązujących przepisów prawa. System teleinformatyczny, w razie awarii podlega ekspertyzie technicznej zlecanej firmie dostarczającej.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 418-454]

2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji

Z § 20 ust. 2 rozporządzenia KRI wynika, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez:*

- pkt 7 *zapewnienie ochrony przetwarzania informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: a)monitorowanie dostępu do informacji; b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych*
  z przetwarzaniem informacji, c) zapewnienie środków uniemożliwiających

nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
- pkt 9 *zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie;*
- pkt 11 *ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.*

W celu uzyskania odpowiedniego poziomu BI, przy jednoczesnym zapewnieniu właściwego do nich dostępu przez uprawnionych użytkowników stosowany jest szereg zabezpieczeń informatycznych. Celem zabezpieczeń jest uzyskanie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także np. kradzieżą środków przetwarzania informacji.

Z wyjaśnień uzyskanych w Urzędzie Gminy wynika, że w celu zabezpieczenia danych będących w posiadaniu Urzędu oraz uzyskania maksymalnego poziomu bezpieczeństwa ich przetwarzania zastosowano, cyt.: „*W Urzędzie Gminy Srokowo stosowane są następujące zabezpieczenia: po błędnym trzykrotnym wpisaniu hasła BIOS komputer jest blokowany, każda operacja logowania do systemu operacyjnego jest rejestrowana w dzienniku zdarzeń systemu operacyjnego, każde logowanie komputera do sieci urzędu jest rejestrowane na urządzeniu UTM, ustawione są automatyczne wygaszacze po 15 min. bezczynności, codziennie wykonywane są kopie zapasowe z wszystkich komputerów oraz serwerów, monitorowany i filtrowany (blokowane są strony www wg. kategorii lub konkretnych adresów) jest ruch sieciowy dla pracowników, zasoby dyskowe są chronione za pomocą loginów i haseł, pracownicy mają uprawnienia do systemów jako użytkownicy bez możliwości ingerencji w oprogramowanie i konfigurację, na każdym komputerze zainstalowane jest oprogramowanie antywirusowe.”*

[akta kontroli str. 51, 467]

Ponadto w celu zabezpieczenia danych będących w posiadaniu Urzędu:
- wykonywane są kopie zapasowe zarówno danych zgromadzonych na stacjach roboczych użytkowników jak i baz danych systemów informatycznych. Kopie zapasowe tworzone są zgodnie z harmonogramem ich wykonywania.
- budynek posiada system alarmowy oraz monitoring wizyjny przed wejściem i jest zawarta umowa na obsługę i konserwację systemu,
- wydzielone zostało pomieszczenie serwerowni do którego ma dostęp informatyk,
- bezpieczeństwo działania systemów teleinformatycznych realizowane jest również poprzez okresową aktualizację oprogramowania w zakresie działania poszczególnych systemów do najnowszych wersji,
- przeprowadzono szkolenia pracowników z zakresu bezpieczeństwa informacji.

[akta kontroli str. 465-466, 468-475]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Stosownie do:

- § 20 ust. 2 pkt 12 rozporządzenia KRI *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: a) dbałości o aktualizację oprogramowania; b) minimalizowaniu ryzyka utraty informacji w wyniku awarii; c) ochronie przed błędami, nieuprawnioną modyfikacją; d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa; e) zapewnieniu bezpieczeństwa plików systemowych; f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych; g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa; h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;*
- § 20 ust. 4 rozporządzenia KRI *niezależnie od zapewnienia działań, o których mowa w ust. 2, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.*

W punkcie 2.12 wykazano mechanizmy jakie jednostka kontrolowana zastosowała w celu zapewnienia ochrony przetwarzanych informacji, w ramach badanych systemów teleinformatycznych przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. Zapewniono również środki uniemożliwiające nieautoryzowany dostęp oraz zapewniające kontrolę dostępu do systemów teleinformatycznych służących do realizacji zadań zleconych z zakresu administracji rządowej, poprzez:

- w systemie: PUMA, logowanie odbywa się za pomocą przyznanego loginu i hasła, które wymaga okresowej wymiany,
- w systemie CEIDG logowanie odbywa się za pomocą certyfikatu kwalifikowanego i hasła,
- w systemie Źródło logowanie odbywa się poprzez imienną kartę dostępową i indywidualne hasło dostępowe.

Podczas kontroli dokonano także oględzin pomieszczenia serwerowni Urzędu Gminy w Srokowie. W wyniku oględzin stwierdzono, że pomieszczenia budynku w którym znajduje się serwerownia posiadają zabezpieczenie alarmowe. Serwer umieszczono w specjalistycznej szafie. W pomieszczeniu zainstalowano urządzenie klimatyzujące oraz UPS. Przed wejściem do pomieszczenia serwerowni zainstalowano gaśnicę przystosowaną do gaszenia urządzeń pod napięciem. W zakresie monitoringu parametrów środowiskowych pomieszczenie serwerowni wyposażono w czujki: monitorującą temperaturę i zalanie pomieszczenia, zadymienie, zasilanie, otwarcie drzwi głównych szafy serwerowej. W zakresie pomieszczenia serwerowni stwierdzone uchybienie to: zastosowanie zwykłych (wewnętrznych) drzwi

wejściowych nie wzmocnionych. Powyższe potwierdza dokumentacja z przeprowadzonych oględzin. Osobą odpowiedzialną za powstanie uchybienia jest Kierownik kontrolowanej jednostki.

[akta kontroli str. 475-481]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami.

2.14. Rozliczalność działań w systemach informatycznych

Stosownie do:

- § 21 ust. 2 rozporządzenia KRI *w dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do: 1) systemu z uprawnieniami administracyjnymi; 2) konfiguracji systemu, w tym konfiguracji zabezpieczeń; 3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa;*
- § 21 ust. 3 rozporządzenia KRI *poza informacjami wymienionymi w § 21 ust. 2 rozporządzenia KRI są odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci: 1) działań użytkowników nieposiadających uprawnień administracyjnych, 2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu, 3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny – w zakresie wynikającym z analizy ryzyka;*
- § 21 ust. 4 rozporządzenia KRI *informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.*

Z wyjaśnień uzyskanych w Urzędzie Gminy wynika, że cyt.: *„Rozliczalność zapewniona jest przez logi dotyczące identyfikacji użytkowników oraz rejestru wykonanych operacji przez użytkowników w posiadanych systemach dziedzinowych, przechowywane są one w bazie danych danego systemu od momentu wdrożenia przez cały okres eksploatacji.”*
Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 51]

III. Zapewnienie dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych

Uwzględniając potrzeby osób niepełnosprawnych podmiot publiczny powinien zastosować w eksploatowanych systemach teleinformatycznych rozwiązania techniczne umożliwiające osobom niedosłyszącym, niedowidzącym lub niewidomym zapoznanie się z treścią informacji, m.in. poprzez powiększenie czcionki, obrazu, zmianę kontrastu. Zgodnie z § 19

rozporządzenia KRI, w systemie teleinformatycznym podmiotu realizującego zadania publiczne służące prezentacji zasobów informacji należy zapewnić spełnienie przez ten system wymagań Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia KRI.

Systemy informatyczne wspomagające realizację zadań zleconych z zakresu administracji rządowej w Urzędzie, ze względu na brak interakcji z klientami zewnętrznymi za pośrednictwem publicznej sieci Internet nie są objęte wymogami WCAG 2.0.

Zarówno strona internetowa Urzędu Gminy, jak i BIP zawierają elementy umożliwiające zmianę wielkości czcionki oraz w przypadku strony BIP - zmianę jej kontrastu. Zmiany wielkości czcionki w przypadku strony www dokonuje się przy pomocy ikon - A + (umieszczonych w prawym górnym rogu), natomiast w przypadku strony BIP – przy pomocy ikon A A A (umieszczonych w lewym górnym rogu strony). Zmiana kontrastu możliwa jest za pomocą odpowiednio oznaczonej ikony, umieszczonej w przypadku strony BIP Urzędu w lewym górnym rogu strony. Zmiana kontrastu dostępna jest w następujących konfiguracjach: biały/żółty tekst na czarnym tle, niebieski/czarny tekst na białym tle.
Zgodnie z załącznikiem nr 4 do rozporządzenia KRI, strona internetowa Urzędu oraz strona BIP spełniały poniższe zasady:
- postrzeganie – informacje oraz komponenty interfejsu strony były przedstawione użytkownikom w sposób dostępny dla jego zmysłów,
- funkcjonalność – komponenty interfejsu stron umożliwiały korzystanie z nich,
- zrozumiałość – informacje oraz obsługa interfejsu były zrozumiałe.

Walidacja za pomocą narzędzia http://wave.webaim.org tj. walidatora WAVE-WCAG 2.0 dla strony BIP wykazuje 4 błędy, dla strony www. wykazuje 10 błędów.

[akta kontroli str. 482-483]

Powyższe zagadnienie oceniono pozytywnie.

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny wnoszę o:

1) Terminową aktualizację dokumentów wchodzących w skład Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie.
2) Dokonywanie okresowych przeglądów i monitoringu SZBI w jednostce zgodnie z § 20 ust. 1 rozporządzenia KRI.
3) Przeprowadzanie w jednostce okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, zgodnie z § 20 ust. 2 pkt 3 rozporządzenia KRI.
4) Bieżące prowadzenie szkoleń w zakresie bezpieczeństwa danych osobowych dla

pracowników uczestniczących w procesie ich przetwarzania.

5) Zapewnienie w jednostce nie rzadziej niż raz na rok okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI.
6) Zabezpieczenie pomieszczenia serwerowni, poprzez montaż (w miarę możliwości finansowych Urzędu) wzmocnionych drzwi wejściowych o podwyższonej odporności ogniowej.

Proszę Pana Wójta o podjęcie działań mających na celu usunięcie stwierdzonych nieprawidłowości i uchybień oraz o poinformowanie Wojewody Warmińsko – Mazurskiego w terminie 14 dni od dnia otrzymania niniejszego wystąpienia, o sposobie wykorzystania uwag i wniosków oraz wykonania zaleceń, a także o podjętych działaniach lub przyczynach niepodjęcia działań.

Jednocześnie informuję, że stosownie do art. 48 ustawy o kontroli w administracji rządowej od wystąpienia pokontrolnego nie przysługują środki odwoławcze.

WOJEWODA
WARMIŃSKO-MAZURSKI

Artur Chojecki