WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

Olsztyn, 7 maja 2019 r.

FK-IV.431.6.2019

Szanowny Pan
Zbigniew Pietkiewicz
Burmistrz Miasta i Gminy
Frombork, ul. Młynarska 5 A
14 - 530 Frombork

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 Miasta i Gminy Frombork ul. Młynarska 5 A, 14 - 530 Frombork, NIP: 5821577720, REGON: 170747974

W okresie objętym kontrolą oraz w okresie prowadzenia kontroli stanowiska pełnili:
1. **Pan Zbigniew Pietkiewicz** - Burmistrz, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 4 listopada 2018 roku (*kierownik jednostki kontrolowanej*),
2. **Pani Barbara Chomacka** - Sekretarz, powołana na stanowisko w dniu 1 marca 2019 r. roku (*nadzorująca bezpośrednio pracownika realizującego zadania objęte kontrolą*),
3. **Pan Damian Krasiński** - Starszy Informatyk, zatrudniony na podstawie umowy o pracę od dnia 1 kwietnia 2009 roku (*realizujący zadania objęte kontrolą*),

[akta kontroli str. 34]

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 upoważnienie do kontroli nr FK-IV.0030.259.2019 z 20 marca 2019 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 33]

Kontrolę przeprowadzono w dniach 25-26 marca 2019 r., co zostało odnotowane w książce kontroli Urzędu Miasta i Gminy Frombork pod pozycją Nr 9/2019.

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.). Okres objęty kontrolą: od dnia 1 stycznia 2018 r. do dnia 25 marca br. (dzień rozpoczęcia czynności kontrolnych).

[akta kontroli str. 1, 20, 33]

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 (t.j. Dz. U. z 2017 r., poz. 2234) 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 (t.j. Dz.U. z 2017 r. poz. 570 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 j.t.) 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, 20, 33]

W czasie trwania czynności kontrolnych informacji i wyjaśnień udzielali pracownicy upoważnieni przez Burmistrza Miasta i Gminy Frombork, tj.: Sekretarz Urzędu Miasta i Gminy oraz Starszy Informatyk. Bieżąca kontrola była pierwszą kontrolą zewnętrzną z tego zakresu przeprowadzaną w Urzędzie Miasta i Gminy Frombork.

[akta kontroli str. 35-36]

Na podstawie ustaleń kontroli, realizację zadań z zakresu wykorzystania systemów teleinformatycznych używanych przez Urząd Miasta i Gminy Frombork do realizacji zadań zleconych z zakresu administracji rządowej ocenia się **pozytywnie z uchybieniami.**

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

Z informacji przekazanych przez UMiG Frombork przed rozpoczęciem czynności kontrolnych oraz uzyskanych w trakcie prowadzenia kontroli wynika, że w UMiG Frombork do realizacji zadań zleconych z zakresu administracji rządowej wykorzystywane są **4** systemy teleinformatyczne oraz prowadzony jest **1** rejestr publiczny. Ponadto w MGOPS Frombork wykorzystywany jest 1 system teleinformatyczny, tj. SYGNITY, którego właścicielem jest MGOPS Frombork. Kontrolą objęto UMiG Frombork.

Systemy teleinformatyczne wykorzystywane w Urzędzie Miasta i Gminy Frombork:

1) **ŹRÓDŁO** - 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) **AA_USC** - moduł wspomagający w zakresie kompleksowej obsługi stanu cywilnego. Migracja aktów stanu cywilnego do ŹRÓDŁA. Producent Technika IT Sp. z o.o. Wymienione oprogramowanie wspiera tworzenie plików XML z treścią aktów stanu cywilnego, przenoszonych z dotychczasowych systemów PB_USC lub AA_USC do centralnego rejestru stanu cywilnego za pośrednictwem aplikacji ŹRÓDŁO, zgodnie z aktualnymi wymaganiami MC/COI dla tworzonych plików XML

3) **SelWIN -** obsługa z zakresu ewidencji ludności oraz wyborów. SYSTEM EWIDENCJI LUDNOŚCI na platformie systemowej windows (SELWIN) przeznaczony do obsługi procedur administracyjnych związanych z ewidencją ludności wykonywanych w Referatach Ewidencji Ludności podstawowych jednostek podziału administracyjnego kraju. Realizacja funkcji związanych z obsługą procedur administracyjnych jest zgodna z obowiązującą ustawą o ewidencji ludności i dowodach osobistych z dn. 10 kwietnia 1974 r. wraz z późniejszymi zmianami oraz z obowiązującymi wytycznymi MSWiA sformułowanymi w dokumencie „LOKALNY BANK DANYCH PESEL SYSTEM EWIDENCJI LUDNOŚCI" – Wytyczne dla projektanta – programisty.
   SELWIN dedykowany jest do pracy jedno lub wielostanowiskowej pod kontrolą systemu operacyjnego Windows. Dane ewidencyjne o mieszkańcach w postaci kartotek: stałych mieszkańców, czasowych mieszkańców, byłych mieszkańców oraz kartoteka przejściowa utrzymywane są w relacyjnej bazie danych MS SQL Serwer.

4) **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.

Rejestry publiczne prowadzone w Urzędzie Miasta i Gminy Frombork:

Rejestr 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 2017 r., poz. 1289 ze zm.).

[akta kontroli str. 18, 37-38, 39-40]

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 Miasta i Gminy Frombork posiada aktywną Elektroniczną Skrzynkę Podawczą /umigfrombork/SkrytkaESP znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie pism w formie dokumentów elektronicznych. Szczegółowe informacje dotyczące funkcjonowania oraz możliwość bezpośredniego przejścia na główną stronę e-PUAP, zawarto na stronie internetowej BIP Urzędu, w lewym panelu ekranu w zakładce Urząd Miasta i Gminy - ePUAP - Elektroniczna skrzynka podawcza.

W wyniku prowadzonej kontroli stwierdzono, iż w ramach funkcjonującej strony internetowej BIP Urzędu Miasta i Gminy Frombork działa Elektroniczne Biuro Obsługi Interesanta (eBOI). Portal Biuro Obsługi Interesanta służy do komunikacji interesanta z urzędem. Dzięki udostępnieniu przez BOI katalogu spraw w postaci elektronicznej, interesanci mogą załatwić część spraw za pośrednictwem Internetu. Interesant może załatwiać sprawy, bez konieczności wizyty osobistej w urzędzie, może też z tego miejsca pobrać i wydrukować dokumenty niezbędne do załatwienia spraw, w których obecność osobista jest wymagana. Do wypełnienia i wysłania formularzy elektronicznych niezbędne jest posiadanie kwalifikowanego podpisu elektronicznego, bądź też profilu zaufanego na platformie ePUAP. Na portalu interesant może zapoznać się między innymi z katalogiem spraw świadczonych przez dany urząd jak również może sprawdzić na jakim etapie realizacji znajduje się konkretna sprawa.

Urząd Miasta i Gminy udostępniał oraz świadczył również usługi elektroniczne, z wykorzystaniem ePUAP, tj. „Pismo ogólne do podmiotu publicznego" oraz „Petycje, skargi, wnioski, zapytania do urzędu". Usługi te umożliwiają złożenie do wybranego organu administracji publicznej pisma (podania) lub skargi w sprawie.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 40-69]

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.

Z informacji przekazanych przez UMiG Frombork wynika, że w ramach uruchomienia eBOI, w ramach projektu pn. „Rozwój e-usług w Gminie Frombork" zgodnie z umową nr UDA-RPWM.06.01.01-28-001/13-00 dofinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Warmia i Mazury na lata 2007-2013 do centralnego repozytorium w 2014 roku zostały założone następujące karty spraw :

- dostęp do systemu teleinformatycznego,
- ustalenie lokalizacji inwestycji celu publicznego,
- deklaracja na podatek od nieruchomości,
- deklaracja, korekta deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi,
- ustalenie warunków zabudowy,
- zaświadczenie o przeznaczeniu terenu w planie miejscowym,
- jednorazowe zaświadczenie na sprzedaż napojów alkoholowych,
- wydanie zezwolenia na sprzedaż napojów alkoholowych przeznaczonych do spożycia w miejscu lub poza miejscem sprzedaży,
- skargi, wnioski, zapytania do urzędu,

- deklaracja na podatek leśny,
- deklaracja na podatek od środków transportowych,
- deklaracja na podatek rolny,
- informacja w sprawie podatku leśnego,
- informacja w sprawie podatku od nieruchomości,
- informacja w sprawie podatku rolnego,
- zezwolenie na usunięcie drzew i krzewów,
- wypisy i wyrysy z miejscowego planu zagospodarowania przestrzennego,
- zezwolenie na zajęcie pasa drogowego w celu umieszczenia w nim urządzeń infrastruktury technicznej niezwiązanych z potrzebami zarządzania drogami lub potrzebami ruchu drogowego.

Jednocześnie Urząd Miasta i Gminy udostępniał oraz świadczył usługi elektroniczne, z wykorzystaniem ePUAP, na podstawie ogólnego wzoru: „Pismo ogólne do podmiotu publicznego" oraz „Petycje, skargi, wnioski, zapytania do urzędu".
W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 44, 70-104]

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.frombork.pl/, a strona internetowa BIP Urzędu – pod adresem http://frombork.samorzady.pl/.
Na stronie internetowej Urzędu zamieszczono link do strony BIP Urzędu w prawej górnej części panelu strony. Na stronie głównej BIP Urzędu, w lewym panelu ekranu zamieszczono link do skrzynki podawczej ESP na platformie ePUAP.

Na stronie internetowej UMiG, 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.
- Emp@tia portal informacyjno-usługowy. Portal zawiera informacje ważne przy ubieganiu się o świadczenia z pomocy społecznej, świadczenia rodzinne, a także z funduszu alimentacyjnego, informacje o formach opieki nad dzieckiem do lat trzech. Przekazuje również, jakie świadczenia przysługują osobom przemieszczającym się w obrębie Unii

Europejskiej i na czym polega koordynacja systemów zabezpieczenia społecznego.
- CEiDG – portal umożliwiający założenie działalności gospodarczej.

Urząd w ramach działania portalu Elektroniczne Biuro Obsługi Interesanta służącego do komunikacji interesanta z urzędem, oferuje katalogu spraw w postaci elektronicznej, dzięki któremu interesanci mogą załatwić część spraw za pośrednictwem Internetu.

W Urzędzie brak jest formalnych procedur opisujących obsługę oraz monitorowanie usług elektronicznych, ze względu na fakt, że instytucje te 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. 40, 42, 105]

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 cyt.: „*Systemy teleinformatyczne zainstalowane w Urzędzie Miasta i Gminy we Fromborku współpracują z systemami zewnętrznymi w następujących zakresach:*

a) *AA_USC – współpraca z systemem Źrodło /Ministerstwo Cyfryzacji – Rejestry Państwowe/ w zakresie interakcji pośredniej. System pozwala wygenerować plik z obowiązującym formacie XML z danymi jednej, bądź wielu kartotek ze zbiorów Urzędu*

Stanu Cywilnego we Fromborku. Następnie tak utworzony plik wczytywany jest do systemu Źrodło, uzupełniając ogólnopolską bazę danych w zakresie aktów stanu cywilnego. System AA_USC oparty jest na działaniu w aplikacji poprzez przeglądarkę internetową, bezpośredni dostęp do oprogramowania dziedzinowego zainstalowanego na stanowisku pracy użytkownika opiera się na logowaniu trójetapowym: BIOS, logowanie do systemu Windows oraz logowanie do aplikacji za pomocą loginu i hasła uprawnionej osoby. (...).

b) *SelWIN – współpraca z systemem Źrodło /Ministerstwo Cyfryzacji – Rejestry Państwowe/ w zakresie interakcji bezpośredniej. System przy użyciu stosownych certyfikatów wydawanych przez MC /w przypadku gmin miejsko-wiejskich dwa certyfikaty, ważność certyfikatu dla Gminy Frombork – 05.03.2021/ przy pomocy aplikacji Subskrybent_PESEL, stanowiącej moduł SelWIN, zainstalowanej na stacji roboczej na której działa system Źródło, w odpowiednio ustawionych czasookresach, umożliwia komunikację i pobieranie danych, uzupełniając lokalną bazę danych /interakcja jednokierunkowa/. System SelWIN oparty jest na działaniu w zainstalowanej aplikacji, bezpośredni dostęp do oprogramowania dziedzinowego zainstalowanego na stanowisku pracy użytkownika opiera się na logowaniu trójetapowym: BIOS, logowanie do systemu Windows oraz logowanie do aplikacji za pomocą loginu i hasła uprawnionej osoby. (...)*

c) *Źródło – system zarządzany przez Ministerstwo Cyfryzacji o charakterze ogólnopolskim, umożliwia współpracę z wcześniej opisywanymi systemami teleinformatycznymi (lit. a i b). Stacje robocze na których zainstalowany jest system pracują w odizolowanej sieci LAN /brak dostępu do sieci WAN Urzędu, dostęp do sieci LAN jest możliwy tylko w zakresie opisanym w dokumencie „Podłączenie infrastruktury gminnej do sieci dedykowanej OST112" (...) umożliwiając prawidłową wymianę danych. Dostęp do systemu uprawnieni użytkownicy uzyskują uwierzytelniając się trójetapowo: BIOS, logowanie do systemu Windows oraz przy pomocy kart kryptograficznych z zainstalowanymi certyfikatami dedykowanymi dla użytkownika aplikacji Źródło /praca w trybie przeglądarki internetowej/. (...).*

d) *CEIDG - system zarządzany przez Ministerstwo Przedsiębiorczości i Technologii o charakterze ogólnopolskim, oparty na pracy w przeglądarce internetowej. Dostęp do systemu uprawnieni użytkownicy uzyskują uwierzytelniając się trójetapowo: BIOS, logowanie do systemu Windows oraz przy pomocy kart kryptograficznych z zainstalowanymi certyfikatami kwalifikowanymi, bądź przy użyciu Profilu Zaufanego na stronie internetowej https://prod.ceidg.gov.pl/ceidg.cms.engine/ W Urzędzie Miasta i Gminy we Fromborku nie ma zainstalowanego oprogramowania dziedzinowego współpracującego z systemem CEIDG."*

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 108-110]

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.*

W Urzędzie Miasta i Gminy Frombork zgodnie z § 64 pkt 3 Regulaminu Organizacyjnego wprowadzonego zarządzeniem Nr 24/2019 Burmistrza Miasta i Gminy Frombork z dnia 1 marca 2019 r., czynności biurowe i kancelaryjne reguluje rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 roku w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. Nr 14, poz. 67 z późn. zm.) oraz zarządzenie w sprawie instrukcji kancelaryjnej dla Urzędu Miasta i Gminy Frombork oraz instrukcji w sprawie organizacji i zakresu działania archiwum zakładowego z którego wynika, że podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw w Urzędzie Miasta i Gminy Frombork jest system tradycyjny.
Jednocześnie, w okazanej dokumentacji Urzędu brak jest procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby szczegółowe zasady obiegu dokumentów wpływających drogą elektroniczną oraz zakres stosowania elektronicznego obiegu dokumentów (skrzynka podawcza na platformie ePUAP oraz Elektroniczne Biuro Obsługi Interesanta), co zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI, umożliwiłoby realizację i egzekwowanie, m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. Powyższe stanowi uchybienie.
W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie uchybieniami. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki.

[akta kontroli str. 115-175]

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 uzyskanych w wyniku kontroli wynika, że cyt.*: „Zgodnie z opisem systemów teleinformatycznych wykorzystywanych w Urzędzie Miasta i Gminy we Fromborku (ust.1) podstawowym dokumentem służącym wymianie danych jest plik XML zgodny z obowiązującymi standardami i uwarunkowania prawnymi, zastosowano w nim odpowiednie kodowanie na poziomie Unicode UTF-8. Systemy teleinformatyczne są na bieżąco aktualizowane do nowych uwarunkowań legislacyjnych, umożliwiając utrzymanie zasad zachowania bezpieczeństwa informacji na jak najwyższym poziomie. Systemy teleinformatyczne umożliwiają przyjmowanie dokumentów w formatach plików o których mowa w załączniku 2 i 3 rozporządzenia KRI w zakresie niezbędnym do prawidłowego załatwienia sprawy."*
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 110]

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 25/2016 Burmistrza Miasta i Gminy Frombork z dnia 23 marca2016 r. wprowadzono obowiązującą (do 25 maja 2018 r.) Politykę bezpieczeństwa oraz Instrukcję zarządzania systemem informatycznym w Urzędzie Miasta i Gminy Frombork, zgodnie z obowiązującymi w tym okresie przepisami prawa, tj. ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. 2014 r., poz. 1182 ze zm.) 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.

  [akta kontroli str. 176-200]

- Zarządzeniem Nr 26/2018 Burmistrza Miasta i Gminy Frombork z dnia 25 maja 2018 r. w sprawie wprowadzenia Polityki Ochrony Danych w Mieście i Gminie Frombork oraz wyznaczenia Inspektora Ochrony Danych Osobowych przyjęto dokument stanowiący Politykę Ochrony Danych Osobowych oraz wyznaczono IOD w jednostce. Politykę Ochrony Danych Osobowych sporządzono na podstawie obowiązujących przepisów, tj. RODO i ustawy z dnia 10 maja 2018 r. o Ochronie Danych Osobowych (Dz. U. z 2018 r. poz. 1000).
  Dokumentacja w zakresie ochrony danych dotyczyła wszystkich 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.

  [akta kontroli str. 2001-377]

- Zarządzeniem Nr 66/2018 Burmistrza Miasta i Gminy Frombork z dnia 26 listopada 2018

r. w sprawie wprowadzenia „Instrukcji postępowania z kluczami oraz zabezpieczenia pomieszczeń i obiektu Urzędu Miasta i Gminy Frombork", określono zasady zabezpieczenia pomieszczeń Urzędu z uwagi na przetwarzane dane osobowe.

[akta kontroli str. 378-385]

Jednocześnie należy zaznaczyć, że Urząd Miasta i Gminy Frombork, przeprowadzał okresowe przeglądy systemu informatycznego służącego do przetwarzania danych osobowych, kontrole wewnętrzne w zakresie nadzoru nad bezpieczeństwem danych osobowych i dokumentów oraz okresowe kontrole zabezpieczenia systemu informatycznego, jak również przeprowadził analizę i szacowanie ryzyka ochrony danych - szczegółowo w pkt 2.2.

[akta kontroli str. 386-398]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

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.

W dniu wejścia w życie Zarządzenia Nr 26/2018 Burmistrza Miasta i Gminy Frombork z dnia 25 maja 2018 r. w sprawie wprowadzenia Polityki Ochrony Danych w Mieście i Gminie Frombork oraz wyznaczenia Inspektora Ochrony Danych Osobowych przeprowadzona została analiza ryzyka w zakresie ochrony danych osobowych, w której określono źródła ryzyka, dokonano ich oceny (prawdopodobieństwo zdarzenia i konsekwencje) oraz określono działania jakie należy podjąć w celu redukcji wykazanych zagrożeń.

[akta kontroli str. 386-398]

Zgodnie z przyjętą Polityką Ochrony Danych w UMiG Frombork (rozdział XXII), IOD nie rzadziej niż raz na 12 miesięcy dokonuje regularnej oceny ryzyka ochrony danych osobowych. Z wyjaśnienia uzyskanego z Urzędu wynika, że cyt.: „*Zgodnie z terminem wprowadzenia w Urzędzie Miasta i Gminy we Fromborku Polityki Ochrony Danych przypadającej na dzień 25 maja 2018 roku, regularna ocena ryzyka zostanie przeprowadzona do dnia 25 maja 2019 roku, podczas wizytacji IOD w siedzibie Urzędu*."

Jednocześnie należy wskazać, iż w jednostce prowadzony jest rejestr czynności przetwarzania zgodnie z art. 30 RODO.

[akta kontroli str. 399-407]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

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 oprogramowania oraz sprzętu komputerowego. Inwentaryzacja sporządzona została zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI. Przedmiotowa inwentaryzacja obejmowała rodzaj i konfigurację sprzętu oraz dodatkowo informację dotyczącą użytkownika i miejsce użytkowania.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 408-415]

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Stosownie do:

- § 20 ust. 2 pkt 4 rozporządzenia KRI *zarządzanie 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 *zarządzanie 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 w zarządzeniu Nr 26/2018 Burmistrza Miasta i Gminy Frombork z dnia 25 maja 2018 r. w sprawie wprowadzenia Polityki Ochrony Danych w Mieście i Gminie Frombork oraz wyznaczenia Inspektora Ochrony Danych Osobowych, rozdział X – nadawanie i odbieranie uprawnień oraz rozdział XI – procedura

dostępu do danych osobowych w systemie informatycznym. Wszyscy pracownicy złożyli oświadczenie o przestrzeganiu zasad ochrony danych osobowych. W Urzędzie prowadzona była ewidencja osób upoważnionych do przetwarzania danych osobowych oraz ewidencja osób uprawnionych do pracy w systemach.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 223, 247-249, 260-264, 284-285, 416-418]

2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Z § 20 ust. 2 pkt 6 rozporządzenia KRI wynika, że z*arządzanie 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.*

W okresie objętym kontrolą pracownicy UM uczestniczący w procesie przetwarzania danych brali udział w szkoleniach, organizowanych przez zewnętrzną firmę, w zakresie zdobycia wiedzy i umiejętności dotyczących ochrony danych osobowych.
W dniach 12-13 czerwca 2018 r. przeprowadzono szkolenie w zakresie „*Ochrona danych osobowych – zmiany wprowadzone Rozporządzeniem 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."* W dniu 5 marca 2019 r. przeprowadzono szkolenie, które swoim zakresem obejmowało m.in. zmiany aktów prawnych w związku z wejściem w życie RODO, kontrole Urzędu Ochrony Danych Osobowych, zadania IOD, absurdy RODO.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 419-422]

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 informacji uzyskanych w UMiG Frombork wynika że cyt.: *„W Urzędzie Miasta i Gminy we Fromborku obowiązuje (...) Polityka Ochrony Danych, w której w Rozdziale IX (...) znajdują się regulacje dot. pracy użytkowników na odległość za pomocą urządzeń przenośnych. Przetwarzanie danych w ten sposób może odbywać się wyłącznie za pomocą zgody Administratora. Pracownik, uzyskujący taką zgodę, zobowiązany jest do zachowania szczególnej ostrożności podczas transportu, przechowywania i użytkowania urządzeń*

przenośnych. Ponadto, ma całkowity zakaz pozostawiania takich urządzeń bez nadzoru."
Ponadto z uzyskanych z Urzędu wyjaśnień wynika, że pracownicy jednostki pracują tylko i wyłącznie wewnątrz się LAN urzędu, nie ma przypadków pracy „na odległość". Laptopy użytkowane w jednostce służą tylko i wyłącznie do pracy wewnątrz sieci LAN Urzędu np. podczas sesji, czy spotkań. Nie są one wynoszone na zewnątrz strefy administracyjnej. Tylko dwa dyski zewnętrzne zostały dopuszczone do pracy - archiwizacji danych wewnątrz Urzędu, używanie prywatnych nośników danych w Urzędzie jest zabronione.
Przedmiotowe cząstkowe zagadnienie ze względu na wykorzystywanie sprzętu w zakresie systemów teleinformatycznych tylko w siedzibie jednostki (stacjonarny tryb pracy) nie podlegało ocenie.

[akta kontroli str. 111, 222, 227, 288, 522]

2.7. Serwis sprzętu informatycznego i oprogramowania

Stosownie do § 20 ust. 2 pkt 10 rozporządzenia KRI *zarządzanie 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 Miasta i Gminy Frombork użytkowane są 2 systemy teleinformatyczne do realizacji zadań publicznych zakupione u zewnętrznego dostawcy, tj.: AA_USC oraz SelWIN.
W związku z zakupem ww. systemów podpisane zostały umowy licencyjne z firmami: Sputnik Software Sp. z o.o. oraz Technika IT Sp. z o.o. Wraz z umowami licencyjnymi (asysta techniczna) z każdą firmą dostarczającą dany system informatyczny podpisana została właściwa umowa powierzenia danych, gwarantująca poprzez zawarcie określonych zapisów właściwe zabezpieczenie danych w przypadku awarii systemu oraz gwarantująca bezpieczeństwo informacji uzyskanych przez wykonawców w związku z realizacją umowy.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 423-452]

2.8. Procedury zgłaszania incydentów naruszenia BI

Z § 20 ust. 2 pkt 13 rozporządzenia KRI wynika, że *zarządzanie 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.*

Sposób zgłaszania incydentów naruszenia bezpieczeństwa informacji w przypadku Urzędu Miasta i Gminy Frombork został uregulowany Zarządzeniem Nr 26/2018 Burmistrza Miasta i Gminy Frombork z dnia 25 maja 2018 r. w sprawie wprowadzenia Polityki Ochrony Danych w Mieście i Gminie Frombork oraz wyznaczenia Inspektora Ochrony Danych Osobowych – rozdział XXI.
Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 232-234]

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

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

Z dokumentacji audytowej udostępnionej kontrolującemu wynika, że w okresie objętym kontrola przeprowadzone zostały 2 zadania audytowe przez zewnętrzną firmę, tj. Kancelaria Doradztwa Podatkowego Wyrzykowski Sp. z o.o.:

- w dniu 13 czerwca 2018 r. (raport z dnia 12 lipca 2018 r.), przeprowadzono audyt, którego celem była weryfikacja zgodności zasad przetwarzania danych osobowych przez ADO z wymogami RODO. Audytem objęto komórki organizacyjne ADO biorące udział w procesie przetwarzania danych osobowych. W wyniku przeprowadzonego audytu uznano, że poprawy wymaga stopień zabezpieczenia danych osobowych przechowywanych w archiwum, dostęp do serwerowni powinien być należycie zabezpieczony i monitorowany oraz wymagane jest wprowadzenie odgórnie określonej oraz stosowanej przez wszystkich pracowników procedury kluczy.

[akta kontroli str. 453-486]

- w dniu 23 stycznia 2019 r. (raport z dnia 4 marca 2019 r.), przeprowadzono audyt, którego celem była weryfikacja procesów przetwarzania danych i kategorii danych osobowych wykorzystywanych przez pracowników w komórkach organizacyjnych ADO. W wyniku przeprowadzonego audytu rekomendowano jednostce:
  - wszelkie druki i formularze zawierające pole do wypełnienia numeru telefonu bądź adresu e-mail należy zmienić zgodnie z rekomendacjami o dobrowolności ich podania (propozycje zapisów znajdują się w rekomendacjach do każdej komórki organizacyjnej).
  - zgodnie ze stanowiskiem Urzędu Ochrony Danych Osobowych do oznaczania stron postępowania w decyzjach administracyjnych nie można używać numeru PESEL - wystarczającym jest wskazanie: imienia, nazwiska i adresu zamieszkania.
  - w Urzędzie powinna być prowadzona ewidencja pobrania i zdania kluczy.
  - ekrany monitorów pracowników powinny być ustawione w taki sposób, aby interesanci nie mieli do nich dostępu wizyjnego. Obowiązek prawidłowego umiejscowienia

monitorów spoczywa każdorazowo na pracowniku.

- dokumentacja papierowa, zawierająca dane osobowe, powinna być przechowywana
- w zamykanych szafach na klucz. Klucz na koniec dnia powinien być chowany w miejscu znany tylko pracownikom, a z pewnością niewidocznym dla sprzątaczek.
- w ramach dostępu do serwerowni powinny zostać nadane upoważnienia. Należy prowadzić ewidencję wejścia i wyjścia oraz wyposażyć serwerownię w gaśnicę i czujnik wilgoci.
- klucze do drzwi od pomieszczeń nie mogą pozostawać w zamku zewnętrznym w trakcie pracy, ze względu na potencjalne niebezpieczeństwo zabrania ich przez osoby postronne np. interesantów.
- pendrive`y powinny być odpowiednio zabezpieczone poprzez ich szyfrowanie bądź hasłowanie.
- zaleca się prowadzenie ewidencji zewnętrznych nośników danych osobowych.
- rekomendujemy zakupienie skrzynki na klucze do Sekretariatu, która nie byłaby mobilna
- i nie musiałaby być chowana do szafy zamykanej na klucz. Najlepszym rozwiązaniem jest skrzynka kodowana.
- regulamin ZFŚS powinien zostać zmieniony ze względu na przepisy dot. ochrony danych osobowych.

[akta kontroli str. 487-520]

W zakresie realizacji rekomendacji poaudytowych pracownik Urzędu wyjaśnił, że cyt: *„Jeżeli chodzi o wprowadzanie w Urzędzie zaleceń pokontrolnych to są one wprowadzane na bieżąco, dokumenty dostosowywane na stanowiskach pracy do nowych uwarunkowań RODO i stwierdzonych braków pokontrolnych. Wszystkie zalecenia nie wymagające zabezpieczenia, czy wydatkowania dużych nakładów pieniężnych staramy się wprowadzać zaraz po stwierdzeniu braków, a dodatkowe szkolenia prowadzone przez firmę Kancelaria Wyrzykowcy, uświadamiają pracownikom ważność i zasadność stosowanych zabezpieczeń (zachowania zasady czystego burka i drukarki, zamykania szaf, chronienia dokumentów oraz ustawiania ekranów w sposób zapewniającym brak wglądu osobom nieupoważnionym). Dodatkowo wszystkie zalecenia weryfikowane są przez samych audytorów podczas comiesięcznych wizyt w siedzibie Urzędu – najbliższa odbędzie się 15 kwietnia. Po audytach w pokojach w których nie było zamykanych szaf, zostały zakupione nowe spełniające wymagania RODO. Jesteśmy na etapie wdrażania nowej, bardziej restrykcyjnej polityki postepowania z kluczami. Planujemy wnioskować o dofinansowanie doposażenia Serwerowni w nowe zabezpieczenia rejestrujące wejścia i wyjścia, automatyczny system ppoż. oraz przeciwprzepięciowy, system monitorujący parametry pomieszczenia (rozbudowanie istniejącego systemu pomiarowego). Został wprowadzony zakaz stosowania własnych urządzeń przenośnych.”*

[akta kontroli str. 521]

W związku z dopełnieniem 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 - przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.10. Kopie zapasowe

Z § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI wynika, że *zarządzanie 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.

Procedura tworzenia kopii zapasowych w przypadku Urzędu Miasta i Gminy Frombork została uregulowana Zarządzeniem Nr 26/2018 Burmistrza Miasta i Gminy Frombork z dnia 25 maja 2018 r. w sprawie wprowadzenia Polityki Ochrony Danych w Mieście i Gminie Frombork oraz wyznaczenia Inspektora Ochrony Danych Osobowych – rozdział XIII.
Z wyjaśnienia przekazanego przez pracownika Urzędu realizującego zadanie wynika, że *„Każde stanowisko komputerowe oraz pomieszczenie i urządzenia serwerowni wyposażone zostały w dodatkowe zasilanie awaryjne UPS. Kopie bezpieczeństwa wykonywane są z następujących stanowisk komputerowych przetwarzających dane osobowe:*

a) *Pokój nr 9 – Kasa – oprogramowanie HomeBanking – kopia tworzona w cyklu codziennym, zapisywana na serwerze plików NAS TS-459 Pro+, s/n: Q114I05178, 10.89.67.31*
b) *Pokój nr 8 – Płace – oprogramowanie Płatnik – kopia tworzona w cyklu codziennym, zapisywana na serwerze plików NAS TS-459 Pro+, s/n: Q114I05178, 10.89.67.31*
c) *Pokój nr 14 – Serwerownia - SRV-HV2: 9c-8e-99-63-31-92, 10.89.67.4, P/N 661384-001 (667267-001), S/N CZ243307V0, Win Server 2012 64 bit – maszyna wirtualna SRV-SQL – 00-15-5d-43-04-00, 10.89.67.6 – oprogramowanie dziedzinowe wykorzystywane w UMiG Frombork oparte na systemie bazodanowym MS SQL – kopia tworzona w cyklu codziennym zapisywana dwustopniowo:*
   - *na serwerze plików NAS TS-459 Pro+, s/n: Q114I05178, 10.89.67.31*
   - *na serwerze SRV-HV2: 9c-8e-99-63-31-92, 10.89.67.4, P/N 661384-001 (667267-001), S/N CZ243307V0, Win Server 2012 64 bit*
d) *Pokój nr 14 – Serwerownia – oprogramowanie Gravis – kopia tworzona w cyklu codziennym, zapisywana na komputerze Informatyka Picasso MS-500 I5-74-*

00/GT1030/8GB/128GB+1TB/WXP, s/n: FOTP9UVSHMR8, EAN: 6097203886269, 10.89.67.63, Win 10 64 bit

e) *W cyklu miesięcznym kopie zapisywane są na nośniku zewnętrznym SEAGATE Expansion Portable Drive – s/n: NA8NN4ZC*
f) *Kopie zapasowe całych maszyn wirtualnych znajdują się na nośniku WD MyBook E4C GAABGA 4517Q – s/n: VLKKYH0Z*

Lokalne testy przydatności kopii zapasowych wykonywane są w cyklu 6-miesięcznym, przeglądy odnotowywane są w stosownych protokołach z przeprowadzone kontroli. Kopie bezpieczeństwa nie są przechowywane poza granicami strefy administracyjnej Urzędu. (...)".

Zgodnie z protokołem kontroli dotyczącym tworzenia i testu kopii zapasowych w Urzędzie Miasta i Gminy Frombork w dniu 31 października 2018 r. przeprowadzono sprawdzenie poprawności wykonywania kopii zapasowych oraz sprawdzenie przydatności utworzonych kopii podczas próby symulowanego przywrócenia i uruchomienia oprogramowania dziedzinowego po przywróceniu. Ustalenia kontroli wskazywały na prawidłowe wykonywanie i poprawność uruchomionych kopii zapasowych.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 226, 395]

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 2 systemy wspierające zakupione u dostawców zewnętrznych SelWIN oraz AA_USC. Obydwa systemy wspomagających realizację zadań zakupione u zewnętrznego dostawcy współpracują z systemami centralnymi np. ŹRÓDŁO. Na obsługę aktualnie zainstalowanego oprogramowania z każdą firmą dostarczającą dany system informatyczny zawarto stosowne umowy licencyjne (asysta techniczna), gwarantujące rozwój systemu i dostosowanie do obowiązujących przepisów prawa. Systemy teleinformatyczne, w razie awarii podlegają ekspertyzie technicznej zlecanej firmie zewnętrznej. Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 13, 423-452]

2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji

Z § 20 ust. 2 rozporządzenia KRI wynika, że z*arządzanie 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 UMiG Frombork wynika, że cyt.: *„Każda stacja robocza posiada zainstalowane oprogramowanie antywirusowe Eset Endpoint Antivirus NOD32 Client z licencją ważną do 22 sierpnia 2020 roku (Nr certyfikatu: NL2017/029969). Bazy sygnatur aktualizowane są przynajmniej raz dziennie. Dodatkowo zastosowano urządzenie brzegowe firewall Cyberoam CR50iNG /identyfikator urządzenia C16615497591-IGDOWI/, które wyposażono w następujące moduły zabezpieczające zgodnie z licencjami na:*

- *Web and Application Filter – ważna do 16 stycznia 2020*
- *IPS – ważna do 16 stycznia 2020*
- *Gateway Anti Virus – ważna do 16 stycznia 2020*
- *Gateway Anti Spam – ważna do 16 stycznia 2020*
- *8x5 Support – ważna do 16 stycznia 2020*

Urządzenie zapewnia prawidłowy poziom zabezpieczeń między sieciami LAN-WAN, sygnatury aktualizowane zgodnie z harmonogramem producenta urządzenia.
Ponadto, w Urzędzie Miasta i Gminy we Fromborku obowiązuje ww. Polityka Ochrony Danych, w której w Rozdziałach VIII, IX, XI i XIV znajdują się opisane zabezpieczenia techniczno-organizacyjne dostępu do informacji”.

[akta kontroli str. 113, 529]

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 stosowane mechanizmy jakie jednostka kontrolowana zastosowała w celu zapewnienia ochrony przetwarzanych informacji, w ramach badanych systemów teleinformatycznych przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. Odbywa się to również poprzez działania związane z zapewnieniem środków uniemożliwiających nieautoryzowany dostęp oraz kontrolę dostępu do systemów teleinformatycznych służących do realizacji zadań zleconych z zakresu administracji rządowej. W systemach: CEIDG, AA_USC, SelWIN logowanie odbywa się za pomocą przyznanego loginu i hasła, które wymaga okresowej wymiany. W systemie Źródło logowanie odbywa się poprzez imienną kartę dostępową i indywidualne hasło dostępowe.

Oprócz zabezpieczeń systemów teleinformatycznych wykazanych w punkcie 2.12, stosowane są również fizyczne zabezpieczenia na wypadek próby dostępu do danych przetwarzanych przez systemy. Urząd zapewnia fizyczne bezpieczeństwo przetwarzanych informacji, m.in. poprzez, cyt.: „*Budynek Urzędu Miasta i Gminy we Fromborku objęty jest całodobowym monitoringiem wizualnym oraz antywłamaniowym, zgodnie z podpisaną umową z firmą zewnętrzną. Sam obiekt podzielony został na 5 kodowanych stref alarmowych, do których dostęp mają tylko uprawnieni użytkownicy, wprowadzono „Instrukcję postępowania z kluczami oraz zabezpieczenia pomieszczeń i obiektu Urzędu Miasta i Gminy Frombork”.*

[akta kontroli str. 113, 523-528]

Środki ochrony, zastosowane przez Informatyka dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych, obejmują:
- środki ochrony fizycznej,
- środki techniczne,
- środki organizacyjne.

ŚRODKI OCHRONY FIZYCZNEJ DANYCH:

a) Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat,
b) Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych, kontrolowany jest przez system monitoringu z zastosowaniem kamer,
c) Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej szafie,
d) Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej szafie metalowej,
e) Pomieszczenie, w którym przetwarzane są zbiory danych osobowych, zabezpieczone jest przed skutkami pożaru za pomocą wolnostojącej gaśnicy,
f) Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

ŚRODKI OCHRONY TECHNICZNEJ DANYCH:

a) Zastosowano urządzenia typu UPS chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania,
b) Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych,
c) Zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł,
d) Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych,
e) Zastosowano środki ochrony przed szkodliwym oprogramowaniem,
f) Użyto system Firewall do ochrony dostępu do sieci komputerowej,
g) Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej,
h) Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych,
i) Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,
j) Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe,
k) Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

ŚRODKI ORGANIZACYJNE:

a) Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych,
b) Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego,
c) Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,
d) Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane,

e) Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

Podczas kontroli dokonano także oględzin pomieszczenia serwerowni Urzędu Miasta i Gminy Frombork. W wyniku oględzin stwierdzono, że przed wejściem do pomieszczenia serwerowni zainstalowano panel aktywujący dodatkową strefę alarmową jaką objęte jest pomieszczenie serwerowni. Zmiana kodu dodatkowej strefy alarmowej następuje raz do roku. Drzwi wejściowe do serwerowni zabezpieczone zostały dwoma zamkami konwencjonalnymi i umieszczona została na nich tablica z napisem: „Nieupoważnionym wstęp wzbroniony". Jednocześnie należy zaznaczyć, że drzwi wejściowe do serwerowni są to standardowe drzwi wewnętrzne – dodatkowo nie wzmocnione. Należy rozważyć ich wymianę na specjalistyczne drzwi wzmocnione.
Ponadto w pomieszczeniu zainstalowano urządzenie klimatyzujące oraz czujkę monitorującą parametry środowiskowe (temperatura i wilgotność), a panel odczytu parametrów znajduje się bezpośrednio na stanowisku Informatyka. Pomieszczenie wyposażono w gaśnicę przystosowaną do gaszenia urządzeń pod napięciem, Okno serwerowni zabezpieczono kratą stalową. Powyższe potwierdza dokumentacja z przeprowadzonych oględzin.

[akta kontroli str. 530-532]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

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 wyjaśnienia pracownika odpowiedzialnego za realizacje zadania wynika, że cyt.: *„Logi z prowadzonych działań w systemach teleinformatycznych gromadzone są bezterminowo*

poprzez systemy operacyjne oraz aplikacje dziedzinowe zainstalowane na stanowiskach komputerowych użytkowników. Każdy użytkownik otrzymuje indywidulany login i hasło dostępu do komputera /profilu/ przydzielane przez przydzielane przez Administratora Systemów Informatycznych, weryfikowane przez kontroler domeny ActiveDirectory, do aplikacji dziedzinowych przydzielane przez Administratora Systemów Informatycznych bądź przez urzędy certyfikujące w przypadku logowania przy pomocy kart kryptograficznych. Zasady oraz procedury dostępu określone zostały w Polityce Ochrony Danych wprowadzonej Zarządzeniem Burmistrza Miasta i Gminy Frombork nr 26/2018 z dnia 25 maja 2018 roku."
Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 113-114]

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 Miasta i Gminy Frombork, ze względu na brak interakcji z klientami zewnętrznymi za pośrednictwem publicznej sieci Internet nie są objęte wymogami WCAG 2.0.

W toku kontroli dokonano weryfikacji zgodności ze standardem WCAG 2.0 strony internetowej Urzędu oraz BIP Urzędu, za pomocą bezpłatnego validatora on-line https://validator.utilitia.pl/analyses/new. Obydwie strony spełniały kryteria dostępności.

Zarówno strona internetowa BIP jaki i www Urzędu zawierały elementy umożliwiające zmianę kontrastu oraz wielkości czcionki. Dostosowanie to zostało wykonane z możliwością zmiany kontrastu oraz kilku rozmiarów czcionki, za pomocą ikony (wysoki kontrast) oraz (A+ A-) umieszczonej w przypadku obydwu stron w lewym górnym rogu panelu strony. Zgodnie z załącznikiem nr 4 do rozporządzenia KRI, strona internetowa Urzędu oraz BIP Urzędu 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.

Powyższe zagadnienie oceniono pozytywnie.

[akta kontroli str. 539-544]

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny wnoszę o opracowanie wewnętrznych procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby zasady obiegu dokumentów wpływających do Urzędu drogą elektroniczną.

Proszę Pana Burmistrza o podjęcie działań mających na celu usunięcie stwierdzonych 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