WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

Olsztyn, 2 maja 2023 r

Wydział Finansów i Kontroli
FK-IV.431.4.2023

**Szanowny Pan**
**Andrzej Maciejewski**
**Burmistrz Barczewa**
**Plac Ratuszowy 1**
**11-010 Barczewo**

Stosownie do art. 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U. 2020 poz. 224), przekazuję Panu treść wystąpienia pokontrolnego.

**Wystąpienie pokontrolne**

Kontrolę przeprowadzono w Urzędzie Miejskim w Barczewie[1], Plac Ratuszowy 1, 11-010 Barczewo, NIP jednostki: 739-05-09-553, REGON jednostki: 000527902.

- W okresie objętym kontrolą oraz w czasie prowadzonych czynności kontrolnych kierownikiem kontrolowanej jednostki był Pan **Andrzej Maciejewski** - Burmistrz wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 21.10.2018 r.

- W dniu rozpoczęcia czynności kontrolnych odpowiedzialnymi za realizację zadania objętego kontrolą był Pan **Mateusz Atałap** – Informatyk, zatrudniony na podstawie umowy o pracę od dnia 12.06.2018 r.,

- Osobą bezpośrednio nadzorującą pracownika odpowiedzialnego za realizację zadania był Pan **Damian Pająk** – Inspektor Ochrony Danych, zatrudniony na podstawie umowy o pracę od dnia 31.12.2021 r.

[akta kontroli poz. 18-19]

Kontrolę przeprowadzili pracownicy Wydziału Finansów i Kontroli Warmińsko- Mazurskiego Urzędu Wojewódzkiego w Olsztynie:
**Radosław Gazda** – inspektor wojewódzki; przewodniczący zespołu kontrolnego, 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.0030.153.2023 z 15 lutego 2023 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.
**Michał Wasilewski** – inspektor wojewódzki; członek zespołu kontrolnego, legitymacja służbowa nr 23/2020, wydana przez Dyrektora Generalnego Warmińsko - Mazurskiego Urzędu

[1] Zwanym dalej: Urzędem

Warmińsko-Mazurski Urząd Wojewódzki w Olsztynie
Al. Marsz. J. Piłsudskiego 7/9
10-575 Olsztyn
tel. 89 523 24 44, 89 523 23 33, fax 89 527 74 47
www.olsztyn.uw.gov.pl
info@uw.olsztyn.pl
Skrzynka ESP na ePUAP /WMURZADWOJ/SkrytkaESP

Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr FK-IV.0030.154.2023 z 15 lutego 2023 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli poz. 7]

Kontrolę przeprowadzono w dniach 3 – 24 marca 2023 r., co zostało odnotowane w książce kontroli Urzędu pod pozycją, Nr 3/2023.

[akta kontroli poz. 20]

Kontrola prowadzona była w trybie hybrydowym, tj. w dniu 3 marca br. – rozpoczęto czynności kontrolne w Urzędzie Miejskim w Barczewie oraz dokonano oględziny serwerowni na miejscu w jednostce. Pozostałe dni (6 - 24 marca br.) kontrola była prowadzona zdalnie, bez osobistej obecności kontrolerów Urzędzie, z wykorzystaniem narzędzi informatycznych do zgromadzenia materiału dowodowego, w celu ustalenia stanu faktycznego, a następnie dokonania oceny działalności jednostki kontrolowanej, a także sformułowanie ewentualnych zaleceń pokontrolnych. W dniu rozpoczęcia czynności kontrolnych okazano legitymacje oraz upoważnienia do kontroli, poinformowano o zasadach kontroli w trybie hybrydowym, wymaganych dokumentach do kontroli oraz formach i terminie ich przekazywania.

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 (tj. Dz.U. z 2023 r., poz. 57 ze zm.). Okres objęty kontrolą: od 1 stycznia do 31 grudnia 2022 r.

[akta kontroli poz. 1, 11-12]

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. 2020 poz. 224), art. 28 ust. 1 pkt 2 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (tj. Dz. U. z 2023 r., poz. 190), 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 (tj. Dz.U. z 2023 r., poz. 57 ze zm.)[2], 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 ze zm.)[3], 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 poz. 1, 11-12]

Zastępca Burmistrza upoważnił Pana Damiana Pająka– Audytora w Urzędzie Miejskim w Barczewie, do udzielania informacji i wyjaśnień oraz przekazywania dokumentacji w okresie trwania czynności kontrolnych.

[akta kontroli poz. 30]

---

[2] Zwanej dalej: ustawą

[3] Zwanego dalej: rozporządzeniem KRI

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

Z informacji przekazanych przez Urząd przed rozpoczęciem czynności kontrolnych oraz uzyskanych w trakcie prowadzenia kontroli wynika, że w Urzędzie do realizacji zadań zleconych z zakresu administracji rządowej wykorzystywane są 4 niżej wymienione systemy teleinformatyczne.

Systemy teleinformatyczne wykorzystywane w Urzędzie:

1) **SRP ŹRÓDŁO** – (Rejestr PESEL, Rejestr Stanu Cywilnego, Rejestr dowodów osobistych) bezpłatna aplikacja, która obsługuje wszystkie wymagane polskim prawem działania, w zakresie rejestru PESEL, dowodów osobistych. 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 Rejestr Sprzeciwów (CRS).
2) **PB_USC TECHNIKA** – system wspierający dla urzędów stanu cywilnego, zapewniający wsparcie zarządzania archiwum USC oraz umożliwiający obsługę w zakresie rejestracji stanu cywilnego.
3) **SYSTEM EWIDENCJI LUDNOŚCI i WYBORCÓW (SELWIN, RWWIN)** – realizacja zadań nałożonych ustawą o dowodach osobistych, ewidencji ludności oraz kodeksie wyborczym. Współpracuje z Systemem Rejestrów Państwowych (SRP).
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. Służy również do przekazywania informacji o wydanych zezwoleniach, koncesjach oraz wpisach do rejestrów.

[akta kontroli poz. 9, 13]

## 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 posiada aktywną Elektroniczną Skrzynkę Podawczą **/5889lgadjj/SkrytkaESP**, znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie i odbieranie pism w formie dokumentów elektronicznych. Na stronie głównej BIP Urzędu, podano adresy Elektronicznej Skrzynki Podawczej. Formaty danych przyjmowane za pośrednictwem Elektronicznej Skrzynki Podawczej to m.in.: DOC, RTF, XLS, CSV, TXT, GIF, TIF, BMP, JPG, PDF, ZIP.

Na stronie głównej Portalu Urzędu, w zakładce „Dla Mieszkańców" zawarto odnośniki do różnych informacji przeznaczonych dla mieszkańców Gminy. Jedną z dostępnych zakładek jest E-URZĄD. Po wejściu w zakładkę otwiera się katalog usług świadczonych on-line, umożliwiający złożenie wniosku za pośrednictwem platformy ePUAP. System umożliwia złożenie wniosku w zakresie spraw związanych z:


[akta kontroli poz. 23-28]

Zgodnie z § 5 ust. 2 pkt 1 i 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.
W zakresie publikacji procedur załatwiania spraw realizowanych przez Urząd należy stwierdzić, że na stronie BIP w zakładce „jak załatwić sprawę w urzędzie", opublikowany jest przydatny dla petentów wykaz usług, które realizowane są przez poszczególne wydziału Urzędu.

Ponadto na stronie BIP w powyższej zakładce opublikowane są karty usług oraz wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych wydziałów w Urzędzie.

Urząd świadczył za pomocą ePUAP usługę „Skargi, wnioski, zapytania do urzędu". Usługa umożliwia złożenie skargi, wniosku do wybranego organu administracji publicznej. Zgodnie z obowiązującymi przepisami, obywatele i przedsiębiorcy mają prawo wnosić skargi, wnioski do organów administracji publicznej, a organy te mają obowiązek ich rozpatrzenia. Przez administrację publiczną należy rozumieć organy państwa, organy jednostek samorządu terytorialnego oraz organy samorządowych jednostek organizacyjnych.

Jednocześnie należy zaznaczyć, że Urząd nie świadczył usług związanych z załatwianiem spraw od początku do końca w formie elektronicznej, za pomocą kontrolowanych systemów teleinformatycznych.

[akta kontroli poz. 28-29]

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

**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 nie przekazywał wzorów dokumentów elektronicznych do Centralnego Repozytorium Wzorów Dokumentów prowadzonego przez Ministerstwo Cyfryzacji. Zgodnie z wyjaśnieniem cyt.: *„Urząd nie przekazywał do CRWDE wzorów formularzy e-usług udostępnionych dla mieszkańców i przedsiębiorców. Na stronie BIP Urzędu zamieszczono wzory dokumentów i instrukcję dotyczącą załatwiania spraw w Urzędzie: https://barczewo.biD.net.pl/?c=276.*
*Jednocześnie pragnę poinformować, że istnieje grupa postępowań, gdzie niezbędne jest osobiste stawiennictwo zainteresowanego, ponadto względy prawne rzutują także na grupę spraw, gdzie*

*elektroniczne procedowanie jest niemożliwe z uwagi na np.: brak lub znacznie utrudnione możliwości elektronicznego odwzorowania specyficznych załączników w postępowaniu.*
*W okresie objętym kontrolą do Urzędu nie wpłynęły skargi w sprawie działalności Urzędu w zakresie świadczenia usług w formie elektronicznej, ani wnioski dotyczące usprawnienia tej formy komunikacji z Urzędem.*
*Należy jednocześnie wskazać, że urząd począwszy od 2022 r. podejmuje działania modernizacyjne w obszarze teleinformatycznym i obsługi elektronicznej w ramach programu „Cyfrowa Gmina", który jest w fazie realizacji."*

[akta kontroli poz. 45, 47]

Jednocześnie, na stronie BIP w zakładce „jak załatwić sprawę w urzędzie" opublikowane są karty usług oraz wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących
w zakresie działania poszczególnych wydziałów w Urzędzie.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

**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 https://barczewo.pl/, a strona internetowa BIP Urzędu – pod adresem https://barczewo.bip.net.pl/.
Na stronie głównej Portalu Urzędu, w zakładce „Dla Mieszkańców" zawarto odnośniki do różnych informacji przeznaczonych dla mieszkańców Gminy. Jedną z dostępnych zakładek jest E-URZĄD. Po wejściu w zakładkę otwiera się katalog usług świadczonych on-line przez Urząd, umożliwiający złożenie wniosku za pośrednictwem platformy ePUAP.
Ponadto na stronie BIP w powyższej zakładce opublikowane są karty usług oraz wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych wydziałów w Urzędzie.

[akta kontroli poz. 23-29]

W Urzędzie brak jest formalnych procedur opisujących obsługę oraz monitorowanie usług elektronicznych realizowanych przez kontrolowane systemy teleinformatyczne wykorzystywane do realizacji zadań zleconych z zakresu administracji rządowej ze względu na fakt, że jednostka nie świadczyła usług elektronicznych na zewnątrz za pomocą tych systemów. Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie nie podlegało ocenie.

**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 z Urzędu wynika, że, cyt.: „System SRP Źródło komunikuje się z Rejestrem mieszkańców SELWIN, który znajduje się na serwerze. Komputer podłączony do sieci Źródło ma ustawiony wyjątek na szukanie jedynie oprogramowania SELWIN na wydzielonej sieci kierując się na konkretny serwer, gdzie są wymieniane dane. Komunikacja działa w jedną stronę, z komputera podłączonego do Źródła można się dostać na serwer, w drugą stronę połączenie jest zablokowane."

[akta kontroli poz. 47]

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

### 1.5. Obieg dokumentów w podmiocie publicznym

Z § 20 ust. 2 pkt 9 rozporządzenia KRI wynika, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności 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.

Zarządzeniem Nr 0050.79.2013 Burmistrza Barczewa, wprowadzono w Urzędzie elektroniczny obieg dokumentów przy wykorzystaniu systemu PROTON Firmy Sputnik Software Sp. zo.o.
Zgodnie z informacją opracowaną przez autora systemu - pozwala on na zarządzanie pełnym cyklem obiegu dokumentów i spraw w instytucji publicznej, począwszy od przyjęcia korespondencji, aż do wydania decyzji administracyjnej. Proton może pracować w trybie EZD lub jako system wspomagający obieg tradycyjny, zgodnie z właściwą instrukcją kancelaryjną.
Zgodnie z przekazanym przez Zastępcę Burmistrza wyjaśnieniem, cyt.: *„W Urzędzie Miejskim w Barczewie funkcjonuje w sposób formalny i faktyczny obieg dokumentacji w formie elektronicznej przy wykorzystaniu systemu PROTON. Niniejszy obieg wprowadzono z dniem 1 czerwca 2013 r. na mocy Zarządzenia Burmistrza Barczewa nr 0050.79.2013 z dnia 31 maja 2013 r. w sprawie wprowadzenia Elektronicznego Obiegu Dokumentacji w Urzędzie Miejskim w Barczewie przy wykorzystaniu programu PROTON. Niniejszy system stanowi system wspomagający w stosunku do obiegu tradycyjnego (papierowego). Stosowne kopie Zarządzenia zostały załączone do niniejszego pisma.*

Opracowanie procedur dotyczących wykonywania czynności kancelaryjnych, w których określone są zasady obiegu dokumentów wpływających drogą elektroniczną oraz zakres stosowania elektronicznego obiegu dokumentów, 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. Opracowanie zasad postępowania z dokumentacją elektroniczną (wnioski elektroniczne, e-maile) oraz wymagań organizacyjno-technicznych dotyczących zarządzania tą dokumentacją pozwala właściwie dbać o jej bezpieczeństwo.

[akta kontroli poz. 47-48]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

**1.6. Formaty danych udostępniane przez systemy teleinformatyczne**

Stosownie do:

- § 17 ust. 1 rozporządzenia KRI kodowanie 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 z Urzędu wynika, że, cyt.: „Możliwość wymiany danych pomiędzy systemami teleinformatycznymi użytkowanymi w urzędzie, a innymi publicznymi systemami (sprawy z zakresu USC) zapewniona jest poprzez przenoszenie danych na szyfrowanych nośnikach (pendrive) i są one udostępniane w powszechnie dostępnych formatach plików. Standard kodowania znaków wykorzystuje od 1 do 4 bajtów do zakodowania pojedynczego znaku - (UTF - 8)."

[akta kontroli poz. 47]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

## II. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych

**2.1. Dokumenty z zakresu bezpieczeństwa informacji**

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;
- § 20 ust. 2 rozporządzenia KRI zarządzanie 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 zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

W związku z wejściem w życie 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", w celu stosowania i przestrzegania zasad postępowania w procesie przetwarzania informacji oraz ochrony interesów osób fizycznych, których dane mogą być przetwarzane w zbiorach danych znajdujących się w zasobach Urzędu, zaktualizowano i przyjęto:
- Politykę Bezpieczeństwa Informacji - Zarządzeniem Nr 120.25.2021 z dnia 31 grudnia 2021 Burmistrza Barczewa.
- Politykę Ochrony Danych - Zarządzeniem Nr 120.35.2018 z dnia 6 lipca 2018 r. w sprawie podstawowych warunków technicznych i organizacyjnych stosowanych w celu ochrony danych osobowych przetwarzanych w Urzędzie Miejskim w Barczewie.
- Instrukcję Zarządzania Systemami Informatycznymi - Zarządzeniem Nr 120.26.2021 z dnia 31 grudnia 2021 Burmistrza Barczewa.

[akta kontroli poz. 31-32, 43]

Realizacja zadań w zakresie ochrony danych wymaga od podmiotu publicznego 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 Systemu Zarzadzania Bezpieczeństwem Informacji (SZBI) jest warunkiem niezbędnym, w celu 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.
Przedmiotową dokumentację sporządzono na podstawie obowiązujących przepisów prawa, tj. „RODO". Dokumentacja w zakresie bezpieczeństwa informacji dotyczyła danych przetwarzanych w Urzędzie i służyła zapewnieniu poufności oraz integralności ich przetwarzania, jak również monitorowania zdarzeń naruszających ochronę danych (w tym osobowych), zawierała także opis postępowania w przypadku naruszenia zasad bezpieczeństwa przetwarzanych danych. Przyjęta dokumentacja wchodziła w skład System Zarządzania Bezpieczeństwem Informacji, wymaganego zgodnie z § 20 ust. 1 rozporządzenia KRI, i zapewniała poufność, dostępność i integralność przetwarzanych informacji.

W myśl § 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.

Zgodnie z powyższym rola podmiotu nie kończy się tylko i wyłącznie na opracowaniu i wdrożeniu do eksploatacji systemu zarządzania bezpieczeństwem informacji. Obowiązkiem podmiotu jest także monitorować, przeglądać i utrzymywać jak również doskonalić ten system tak, aby zapewniać poufność, dostępność i integralność informacji. Oznacza to, iż realizacja obowiązku wynikającego z § 20 ust. 1 KRI nie kończy się z momentem wdrożenia do stosowania SZBI, lecz wymaga ona nieustannej uwagi.
Zgodnie z rozdziałem 16 przyjętej Polityki Bezpieczeństwa Informacji – *w celu utrzymania odpowiedniego, wysokiego poziomu bezpieczeństwa informacji w Urzędzie dokonuje się regularnych przeglądów niniejszej Polityki i ewentualnie audytów systemu bezpieczeństwa informacyjnego Urzędu.* ***Przeglądu dokonuje się nie rzadziej niż jeden raz w ciągu roku.*** *IOD koordynuje realizację przeglądów i w zależności od potrzeb zaleca ich wykonanie wewnątrz Urzędu lub na zewnątrz. Przeprowadzenie przeglądu bądź audytu jest dokumentowane w formie protokołu lub raportu, który dołącza się do dokumentacji związanej z bezpieczeństwem i ochroną danych. Ponadto prowadzi się dodatkowe przeglądy Polityki i stosowanych zabezpieczeń*
*w sytuacji, gdy nastąpiły znaczące zmiany mogące wpływać na system bezpieczeństwa.*
*W szczególności dotyczy to sytuacji: przekazania do eksploatacji nowego, kluczowego systemu informatycznego, znaczących zmian organizacyjnych w funkcjonowaniu Urzędu, zmian w obowiązującym prawie.*

W przekazanej dokumentacji, w ramach prowadzonych czynności kontrolnych stwierdzono dowody (raport z przeglądu) świadczące o podejmowaniu dodatkowych działań w zakresie utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji.

[akta kontroli poz. 31-33]

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. Analiza ryzyka jest ważnym wymaganiem nałożonym na administratorów i podmioty przetwarzające. Proces szacowania ryzyka powinien być przeprowadzony i udokumentowany w celu wykazania, że ryzyko zostało oszacowane i wprowadzono odpowiednie środki obrony. Szacowanie ryzyka pozwala na aktywne zarządzanie bezpieczeństwem informacji, w tym na przeciwdziałanie zagrożeniom oraz ograniczanie skutków zmaterializowanych ryzyk, a także wpływa na racjonalne zarządzanie środkami finansowymi poprzez stosowanie zabezpieczeń adekwatnych do oszacowanego poziomu ryzyka. Jednocześnie należy zaznaczyć, że prawidłowo przebiegająca analiza ryzyka nie jest jednorazowym działaniem, lecz regularnie i ciągle monitorowanym procesem.

Zgodnie z wymogiem wynikającym z § 20 ust. 2 pkt 3 rozporządzenia KRI analiza ryzyka utraty integralności, dostępności lub poufności informacji powinna być przeprowadzana okresowo,

a w przypadku stwierdzenia podwyższonego ryzyka w przedmiotowym zakresie, powinny zostać wprowadzone działania minimalizujące to ryzyko. Zgodnie również z zapisami przyjętej w Urzędzie Polityki Bezpieczeństwa Informacji rozdział 3.1 – analizę ryzyka przeprowadza się okresowo nie rzadziej niż raz w roku.

Kontrolującym przedstawiono dokumentację (stanowiącą akta kontroli) świadczącą o przeprowadzeniu okresowej analizy ryzyka utraty integralności, dostępności lub poufności informacji w Urzędzie w 2022 roku.

[akta kontroli poz. 34]

W toku prowadzonych czynności kontrolnych stwierdzono, że w jednostce zgodnie z art. 30 RODO, prowadzony jest rejestr czynności przetwarzania. W jednostce powołano również Administratora Systemu Informatycznego oraz Inspektora Ochrony Danych.

[akta kontroli poz. 34-38]

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.

Kontrolującym przedstawiono inwentaryzację sprzętu komputerowego użytkowanego w Urzędzie sporządzoną zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI. Przedmiotowa inwentaryzacja zgodnie z cyt. powyżej przepisami obejmowała między innymi rodzaj i konfigurację sprzętu.

[akta kontroli poz. 49]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

**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 (bezpieczeństwa informacji) 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 cofania uprawnień do przetwarzania danych osobowych oraz do pracy w określonym zbiorze danych (systemie informatycznym), określone zostały Zarządzeniem Nr 120.25.2021 z dnia 31 grudnia 2021 Burmistrza Barczewa wprowadzającym Politykę Bezpieczeństwa Informacji w Urzędzie Miejskim w Barczewie rozdział 7.2, 7.3.3 oraz Zarządzeniem Nr 120.26.2021 z dnia 31 grudnia 2021 Burmistrza Barczewa wprowadzającym Instrukcję Zarządzania Systemami Informatycznymi w Urzędzie Miejskim w Barczewie rozdział 7 (załącznik nr 1).
Osoby posiadające dostęp do danych osobowych posiadały pisemne upoważnienia do ich przetwarzania oraz do przetwarzania danych osobowych w określonym zbiorze danych wynikającym z zakresu czynności danego pracownika.
Prowadzona była też ewidencja osób upoważnionych do przetwarzania danych osobowych i pracy w określonym zbiorze danych.

[akta kontroli poz. 31-32, 70-73]

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.

Zgodnie z zapisami przyjętej w Urzędzie PBI rozdział 7.2.3 - w miarę posiadanych możliwości ekonomicznych i organizacyjnych Urząd podejmuje działania zmierzające do tego, by wszyscy pracownicy Urzędu zostali odpowiednio przeszkoleni oraz byli regularnie informowani o uaktualnieniach obowiązujących w Urzędzie polityk i procedur, w szczególności niniejszej Polityki, które są związane z wykonywaną przez nich pracą. Szkolenia przeprowadza się przed podjęciem pracy, a w szczególności przed uzyskaniem przez pracownika dostępu do danych podlegających ochronie. Szkolenie powinno obejmować w szczególności: wymagania bezpieczeństwa funkcjonujące w Urzędzie, zabezpieczania wynikające z uregulowań prawnych, naukę korzystania ze środków przetwarzania informacji, z którymi pracownik będzie miał do czynienia, informacje o środkach dyscyplinarnych i karnych związanych z naruszeniami zasad bezpieczeństwa stosowanych w organizacji. Szkolenia prowadzi IOD.

W okresie objętym kontrolą w Urzędzie przeprowadzono jedno szkolenie wynikające z § 20 ust. 2 pkt 6 rozporządzenia KRI, obejmujące:
- Praktyczne warsztaty - dostęp do informacji publicznej a RODO,
- Otwarte dane i ponowne wykorzystywanie informacji sektora publicznego.

Szczegółowa tematyka szkolenia obejmowała:
- ustawa o dostępie do informacji publicznej a przepisy RODO,
- wniosek o udzielenie informacji publicznej,
- informacje chronione na gruncie RODO,

- odmowa udostępnienia danych osobowych, o których udostępnienie wnioskowano w trybie dostępu do informacji publicznej, uzasadnienie decyzji administracyjnej odmawiającej udostępnienia danych osobowych,
- rola Prezesa Urzędu Ochrony Danych Osobowych w obszarze dostępu do informacji publicznej,
- otwarte dane i ponowne wykorzystywanie informacji sektora publicznego: nowa ustawa, nowe obowiązki,
- otwarte dane i dostęp do informacji publicznej - różnice w regulacjach prawnych.
- otwarte dane i inne podstawowe pojęcia na gruncie ponownego wykorzystywania informacji sektora publicznego z zestawieniu z regulacjami dotyczącymi dostępu do informacji publicznej,
- informacja sektora publicznego a informacja publiczna,
- otwarte dane; tryby zapewniania dostępu do informacji,
- zakres podmiotowy oraz ograniczenia prawa do ponownego wykorzystywania informacji sektora publicznego.

Przeprowadzenie ww. szkolenia potwierdzono listą obecności pracowników Urzędu uczestniczącym w szkoleniu.

[akta kontroli poz. 41-42]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

**2.6. Praca na odległość i mobilne przetwarzanie danych**

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

Zasady korzystania z komputerów przenośnych podczas mobilnego przetwarzania danych opracowane zostały w Instrukcji Zarzadzania Systemami Informatycznymi – rozdział 6.
Ponadto z informacji uzyskanych z Urzędu wynika, że cyt.: *„W urzędzie funkcjonuje Regulamin pracy zdalnej wprowadzony zarządzeniem nr 120.13.1.2020 z dnia 19 marca 2020 r. Niniejszy regulamin wprowadzono, w związku z art. 3 ustawy z dnia 2 marca 2020 roku o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacjami kryzysowymi (Dz. U. 2020 poz. 1842 ze zm.). W okresie objętym kontrolą (w 2022 r.) żaden z pracowników nie przebywał na tzw. „pracy zdalnej."*

[akta kontroli poz. 32, 47, 50]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

**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 użytkowane są dwa systemy teleinformatyczne przeznaczone do realizacji zadań zleconych z zakresu administracji rządowej zakupione u zewnętrznych dostawców, tj.:
- **PB_USC TECHNIKA** – system wspierający dla urzędów stanu cywilnego, zapewniający wsparcie zarządzania archiwum USC oraz umożliwiający obsługę w zakresie rejestracji stanu cywilnego.
- **SYSTEM EWIDENCJI LUDNOŚCI i WYBORCÓW (SELWIN, RWWIN)** – realizacja zadań nałożonych ustawą o dowodach osobistych, ewidencji ludności oraz kodeksie wyborczym. Współpracuje z Systemem Rejestrów Państwowych (SRP).

W związku z zakupem ww. systemów podpisane zostały z dystrybutorem stosowne umowy licencyjne, umożliwiające prawidłową eksploatację i rozwój, poprzez możliwość zgłaszania błędów pytań i roszczeń, dotyczących użytkowanego systemu. Zawarte zostały również stosowne umowy powierzenia danych gwarantujące właściwe zabezpieczenie danych w przypadku awarii systemu oraz gwarantujące bezpieczeństwo informacji uzyskanych przez wykonawcę w związku z realizacją umowy.

[akta kontroli poz. 47, 51-52]

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 zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

Instrukcja postępowania w przypadku stwierdzenia zagrożenia w postaci naruszenia ochrony informacji, jak również podejmowanych działań korygujących została uregulowana Zarządzeniem Nr 120.25.2021 z dnia 31 grudnia 2021 Burmistrza Barczewa wprowadzającym Politykę Bezpieczeństwa Informacji w Urzędzie Miejskim w Barczewie rozdział 12.

[akta kontroli poz. 31]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

**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.

Audyt bezpieczeństwa informacji jest procesem przeprowadzanym w celu zidentyfikowania zagrożeń mogących skutkować utratą poufności, integralności lub dostępności informacji. Celem audytu wewnętrznego bezpieczeństwa informacji jest ocena zakresu zgodności Systemu Zarządzania Bezpieczeństwem Informacji jednostki z kryteriami audytu.

Na podstawie okazanej dokumentacji kontrolujący stwierdzili, że w okresie objętym kontrolą przeprowadzono w Urzędzie jedno audytowe zadanie zapewniające pod nazwą: *„Funkcjonowanie systemu bezpieczeństwa informacji w Urzędzie Miejskim w Barczewie - testy praktyczne"*. Celem zadania była ocena funkcjonowania systemu zarządzania bezpieczeństwem informacji w Urzędzie Miejskim w Barczewie, w oparciu o kryterium zgodności z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Dodatkowo w ramach zadania zastosowano testy praktyczne przyjętych sposobów postępowania na wypadek otrzymywania korespondencji elektronicznej nieznanego pochodzenia, która to korespondencja może powodować zagrożenia dla ciągłości funkcjonowania systemów teleinformatycznych.

Mając powyższe na uwadze, należy stwierdzić, że obowiązek wynikający 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 - w 2022 r. został zrealizowany.

[akta kontroli poz. 39]

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.

Zasady tworzenia kopii zapasowych m.in. z systemów teleinformatycznych uregulowane zostały w Instrukcji Zarządzania Systemami Informatycznymi – rozdział 10, załącznik Nr 7 – *„Kopie zapasowe"*. Zgodnie z opracowaną procedurą:

- *Wszystkie dane osobowe przetwarzane w systemie informatycznym są zachowywane w kopiach zapasowych w serwerowni.*
- *Kopie zapasowe tworzy się w taki sposób, aby zapewnić odtworzenie wszystkich informacji w przypadku awarii. Administrator Systemu Informatycznego nadzoruje prawidłowość procesu tworzenia kopii zapasowych.*
- *Kopie zapasowe tworzone są na serwerze oraz dysku kopii zapasowych NAS, do którego dostęp ma wyłącznie Administrator Systemu Informatycznego (ASI).*

Z wyjaśnienia przekazanego z Urzędu w przedmiotowej sprawie wynik, że cyt.: *„W/w wykaz znajduje się w katalogu „Wykonywanie kopi bezpieczeństwa", z podziałem na poszczególne stanowiska pracy. Katalog „Andruczyk" zawiera:*

- *Zrzut ekranu w pliku „l.jpg" - Logi z wykonywania backup-ów dla pracownika Joanny Andruczyk.*
- *Zrzut ekranu w pliku „2.jpg" - Konfiguracja kopii zapasowych dla w/w pracownika. Metoda szyfrowania AES-256*
- *Zrzut ekranu w pliku „3.jpg" - Wskazuje szyfrowane połączenie SFTP do serwera 192.168.1.80 który odpowiada za zapasowy magazyn backup-ów dla pracowników UM Barczewo.*
- *Zrzut ekranu w pliku „4.jpg" - Harmonogram wykonywanych automatycznie kopi dla w/w pracownika UM Barczewo*
- *Plik „logi.txt" - logi z backup-ów dla w/w pracownika.*

*Analogiczne zrzuty ekranów są w katalogach: „Kwapis", „Niezabitowska", co stanowi komplet zrzutów ekranu dla trzech pracowników UM Barczewo wraz z zapisem logów. W katalogu „Logi" znajduje się plik „SQL Backup Master.pfd" gdzie znajdują się logi z wykonywanych kopi bezpieczeństwa programów dziedzinowych UM Barczewo. Są to kopie całościowe. W katalogu „Logi" znajduje się plik „lista.pdf" który zawiera kompletną listę archiwizowanych zasobów.*
*Co do rozdziału 10, załącznik nr 7 Instrukcji zarządzania systemami informatycznymi w katalogu „Wykonywanie kopi bezpieczeństwa" są dwa zrzuty ekranu w pliku „SQL Backup - 1. Jpg", które obrazują wyodrębnioną strukturę przechowywania kopi bezpieczeństwa, wyłącznie dostępną dla Administratora Systemu Informatycznego. Zgodnie z rozdziałem 10, załącznik nr 7 Instrukcji zarządzania systemami informatycznymi plik „SQL Backup - 2.jpg" przedstawia zakres archiwizowanych danych dla jednego wybranego momentu w tym przypadku na dzień 15.03.2023.*

Na podstawie udostępnionej dokumentacji oraz wyjaśnień kontrolujący stwierdzili, że w Urzędzie są wykonywane kopie zapasowe z kontrolowanych systemów.

[akta kontroli poz. 32, 53-63]

W przypadku prowadzenia testów w celu sprawdzenia poprawności wykonywania kopii zapasowych oraz przydatności utworzonych kopii podczas próby symulowanego przywrócenia i uruchomienia oprogramowania, zgodnie z Instrukcją Zarządzania Systemami Informatycznymi - załącznik Nr 7 - *„Kopie zapasowe" – w celu zweryfikowania poprawności danych przechowywanych na kopiach zapasowych oraz możliwości przywrócenia za ich pomocą systemu do stanu sprzed awarii, Administrator Systemu Informatycznego zobowiązany jest do wykonywania okresowych testów odtworzenia kopii zapasowych.*

Zgodnie z wyjaśnieniem w powyższej sprawie, cyt.: *„W/w wykaz znajduje się w katalogu Wykonywanie kopi bezpieczeństwa. Z podziałem na poszczególne stanowiska pracy. Katalog andruczyk zawiera:*

- *Zrzut ekranu w pliku 5.jpg - Przykładową procedurę odtworzeniową backup dla pracownika Joanna Andruczyk. Odtworzenie jest możliwe zarówno całości jak i pojedynczych folderów.*
- *Zrzut ekranu w pliku 6.jpg - Opcje odtwarzania kopi backup.*

*Tylko dla użytkownika Joanna Andruczyk zostały przedstawione przykładowe ustawienia odtwarzania kopi zapasowych, które są analogiczne dla wszystkich zarchiwizowanych danych.*

*Kopie odtworzeniowe baz danych Urzędu Miasta Barczewo wykonywane są w celach sprawdzenia poprawności zapisanych danych, oraz wykluczenia wadliwych kopi. Częstotliwość wykonywania odtworzenia wynosi nie mniej niż raz na dwa miesiące dla każdej z baz danych. Przykładowa procedura odtworzeniowa bazy danych UM Barczewo.*
*W załączniku l.png jest przedstawiony graficzny zapis serwera SQL EXPRESS podczas procedury testów odtworzeniowych dla bazy danych „Bestia". Przedstawia on założenie nowej bazy danych „testbestia"*
*W załączniku 2.png jest informacja o udanej próbie odtworzenia w/w bazy danych W załączniku 3.png jest informacja o udanej próbie połączenia z odtworzoną bazą danych w celach testowych.*
*Takie procedury testów odtworzeniowych dla baz danych odbywają się raz na dwa miesiące dla każdej bazy danych.*

Na podstawie udostępnionej dokumentacji oraz wyjaśnień kontrolujący stwierdzili, że w Urzędzie wykonywane są testy odtworzeniowe kopii zapasowych systemów.

[akta kontroli poz. 32, 44, 64-66]

Regularne testowanie jakości kopii zapasowych jest kluczowym działaniem w celu minimalizowania ryzyka utraty informacji w wyniku awarii. Prawidłowo zdefiniowana polityka kopii bezpieczeństwa oraz gruntownie przetestowane procesy odtwarzania systemów teleinformatycznych są istotnymi aspektami w każdej jednostce, której procesy opierają się na działaniu systemów informatycznych. Prawidłowo zdefiniowana i wykonana procedura pozwala mieć pewność, że w razie awarii systemu, wytworzone backupy spełnią swoje zadanie i nie odbije się to negatywnie na ciągłości działania jednostki.

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 systemy 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. SRP ŹRÓDŁO, CEiDG oraz systemy wspierające zakupione u dostawców zewnętrznych, tj. PB_USC TECHNIKA oraz SYSTEM EWIDENCJI LUDNOŚCI i WYBORCÓW (SELWIN, RWWIN). Na obsługę zainstalowanego w okresie objętym kontrolą oprogramowania (system informatyczny) zawarte zostały stosowne umowy licencyjne (opieka autorska), gwarantujące rozwój systemu i dostosowanie do obowiązujących przepisów prawa. Zakupiony system teleinformatyczny, w razie awarii podlega ekspertyzie technicznej zlecanej firmie dostarczającej.

[akta kontroli poz. 13, 51-52]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

**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 bieżącego dostępu uprawnionym użytkownikom, stosowany jest szereg zabezpieczeń technicznych. Celem zabezpieczeń jest uzyskanie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także np. kradzieżą środków przetwarzania informacji.

Z informacji uzyskanych podczas kontroli wynika, że stosowane są następujące zabezpieczenia: *„Obszarem przetwarzania informacji w tym danych osobowych jest siedziba Urzędu Miejskiego w Barczewie znajdująca się przy ulicy Plac Ratuszowy 1 oraz przy ul. Kopernika 10 — pomieszczenia USC. Budynek główny posiada 3 kondygnacje; budynek USC zajmuje 2 kondygnacje. W budynku zamontowany jest system alarmowy z detekcją ruchu. Teren wokół budynku Urzędu Miejskiego objęty jest monitoringiem wizyjnym. Pomieszczenia, w którym są przechowywane informacje (dokumenty) są zamykane. Dokumentacja jest przechowywana głównie w niemetalowych szafach zamykanych na klucz, oraz w szafach metalowych zamykanych lub też w przypadku USC w formie odrębnego pomieszczenia zamykanego z kontrolą dostępu. Blankiety dokumentów publicznych przechowywane są w miejscu zapewniającym wystarczające środki zabezpieczające przed nieuprawnionym dostępem, utratą lub zniszczeniem. Pomieszczenia, w którym są przechowywane dokumenty publiczne oraz blankiety tych dokumentów, jest zamykane, a dostęp do tego pomieszczenia mają wyłącznie osoby upoważnione. Pomieszczenia w USC posiadają wydzieloną część, w której są przechowywane dokumenty publiczne. Dostęp do pomieszczenia jest rejestrowany.*
*Sprzęt zlokalizowano w sposób uniemożliwiający wgląd do monitora, zarówno osobom pracującym w pomieszczeniu jak i osobom wchodzącym do pomieszczenia. Pracownicy po odejściu od komputera co do zasady wylogowują się (wygaszają monitor). Polityka haseł do systemów, na których wykonywane są operacje wymusza zmianę haseł w interwałach. Zmiany haseł do komputerów są co do zasady dokonywane w interwałach czasowych. Osoby zaangażowane w przetwarzanie informacji posiadają stosowne uprawnienia (dostęp do dokumentów oraz do aplikacji). Pracownicy posiadają upoważnienia i dostęp jedynie do aplikacji i dokumentów związanych z realizacją powierzonych zadań oraz stosownie do obowiązków doraźnego zastępowania wybranych osób w trakcie ich nieobecności. Osoby upoważnione podpisują oświadczenie o poufności. Upoważnienia wydaje się na czas trwania stosunku pracy i zgodnie z zakresem obowiązków. Przyznanie lub cofnięcie upoważnienia w systemie informatycznym lub zbiorze papierowym wraz z uprawnieniami do przetwarzania danych jest realizowane pisemnie. Dostęp do zewnętrznych systemów Ministerstwa Cyfryzacji (Ministerstwa Spraw Wewnętrznych i Administracji) - dostęp do Systemu Rejestrów Państwowych ŹRÓDŁO odbywa się na zasadach certyfikacji zewnętrznej na wniosek. W urzędzie zastosowano środki*

*zapewniające bezpieczeństwo informacji na poziomie infrastruktury informatycznej i telekomunikacyjnej, poprzez zastosowanie UPS zasilającego całą instalację elektryczną, szyfrowanie danych. Programy i bazy są zabezpieczone poprzez uwierzytelnianie dostępu, mechanizmy blokady dostępu, środki uniemożliwiające automatyczną rejestrację identyfikatora użytkownika oraz określenie praw dostępu do wybranego zakresu danych. Kopie zapasowe tworzy się w sposób określony w pkt. II.5. Dostęp do stron www. Zawierających określone treści jest ograniczony dla użytkowników, konta administratora są wydzielone od kont innych użytkowników, w urzędzie stosowane jest oprogramowanie antywirusowe ESET NOD32."*

[akta kontroli poz. 47]

Mając na uwadze powyższe 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 SRP Źródło logowanie odbywa się poprzez imienną kartę dostępową i indywidualne hasło dostępowe,
- w systemie CEIDG logowanie odbywa się za pomocą certyfikatu kwalifikowanego i hasła,
- w systemie PB_USC TECHNIKA - logowanie odbywa się za pomocą loginu i hasła,
- w systemie SELWIN - RWWIN logowanie odbywa się za pomocą loginu i hasła.

Podczas kontroli dokonano oględzin pomieszczenia serwerowni w Urzędzie, w obecności Pana Damiana Pająk - Audytora wewnętrznego / IOD oraz Pana Mateusza Atałap - Informatyka Urzędu Miejskiego w Barczewie. W toku oględzin stwierdzono:

- główny budynek urzędu zabezpieczony alarmem,

- drzwi wejściowe do serwerowni wzmocnione zabezpieczone zamkiem patentowymi oraz zamkiem elektronicznym uruchamianym za pomocą karty dostępowej,
- do pomieszczeń serwerowni dostęp mają tylko wyznaczeni pracownicy,
- urządzenia serwerowe umieszczone w specjalistycznych szafach,
- w pomieszczeniach serwerowni zainstalowano urządzenie klimatyzujące,
- urządzenia serwerowe podłączone są do UPS-a,
- w pomieszczeniu serwerowni zainstalowano czujkę monitorującą aktualną temperaturę, wilgotność oraz ewentualne zadymienie,
- pomieszczeniu serwerowni (szafa) znajduje się urządzenie gaśnicze przeznaczone do gaszenia urządzeń elektrycznych dwutlenkiem węgla.

Powyższe potwierdza dokumentacja fotograficzna i protokół z przeprowadzonych oględzin.

[akta kontroli poz. 15-17]

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.

Zgodnie z § 21 ust. 1 KRI, rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach). Z informacji uzyskanych w trakcie kontroli wynika, że cyt.: *„Działania użytkowników są odnotowywane bezpośrednio w systemach dziedzinowych obsługiwanych w urzędzie; w przypadku każdego programu zawarte są informacje na temat zdarzeń systemowych. Jeżeli chodzi o przechowywanie informacji w dziennikach systemów to są one przechowywane w okresie krótszym niż wynikający z przepisów; dzieje się tak z powodu ograniczonych możliwości gromadzenia informacji o tak dużym rozmiarze. Próby gromadzenia w dziennikach informacji przez tak długi okres prowadziłyby do znacznego zajęcia pamięci i ograniczenia możliwości bieżącego funkcjonowania systemów w urzędzie. Warto w tym miejscu wskazać, że w związku z pracami modernizacji systemów teleinformatycznych w ramach Programu „Cyfrowa gmina" nowa infrastruktura informatyczna będzie uwzględniać potrzebę zwiększenia pamięci w celu zapewnienia przechowywania dużej liczby danych przez długi okres czasu. W załączeniu przesyłam dowody potwierdzające przechowywanie informacji w dziennikach*

*systemów. W katalogu „Logi" znajduje się plik „Security.evt" który zawiera kompletny zestaw logów logowania z jednego z serwerów UM Barczewo dla okresu od 22.02.2023 do 21.03.2023. Z tego pliku jest wyeksportowany plik „Logi Barczewo.pdf', który zawiera w/w logi w bardziej przejrzystej formie".*

[akta kontroli poz. 47, 67]

Odnosząc się do udzielonych wyjaśnień należy stwierdzić, że zgodnie z § 21 ust. 4 rozporządzenia KRI - informacje w dziennikach systemów powinny być przechowywane od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata. Z przekazanego wyjaśnienia wynika, że z przyczyn technicznych w okresie objętym kontrolą informacje przechowywanie w dziennikach systemów (logi) były przechowywane w okresie krótszym niż wynikający z przepisów; z powodu ograniczonych możliwości gromadzenia informacji o tak dużym rozmiarze. Powyższe **należy ocenić jako uchybienie** skutkujące niedopełnieniem obowiązku wynikającego z przepisów KRI. Osobą odpowiedzialną jest pracownik nadzorujący rozliczalność działań w systemach informatycznych.

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

**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.

Każda strona dostępna w Internecie powinna zapewniać maksymalne wsparcie wszystkim grupom wiekowym jak i społecznym. Warunkiem dostępności strony jest dobry kontrast zapewniający swobodny odczyt przedstawionych informacji. Im wyższy jest kontrast, tym łatwiej odróżnić obiekt, zdjęcie czy tekst pierwszego planu od tła. Niski poziom kontrastu utrudnia korzystanie z witryny przede wszystkim użytkownikom o mniejszej ostrości wzroku, a także osobom niedowidzącym. Celem ułatwienia postrzegania tekstu użytkownikom niedowidzącym można również umożliwić zmianę wielkości tekstu bez utraty jego czytelności lub funkcjonalności serwisu internetowego. Zarówno strona internetowa BIP Urzędu, jak i portal www. Urzędu, zawierała elementy umożliwiające korzystanie z treści na niej zawartych przez osoby niedowidzące. Zastosowane ułatwienia to:

- możliwość doboru odpowiedniego kontrastu (ciemny-jasny),
- możliwość powiększenia wielkości liter na stronie,
- moduł wyszukiwania.

Walidacja za pomocą narzędzia http://wave.webaim.org tj. walidatora WAVE-WCAG 2.0 dla strony BIP nie wykazała jakichkolwiek błędów. Walidacja portalu internetowego Urzędu, wykazała 8 błędów.
WAVE-WCAG jest narzędziem do automatycznego testowania dostępności serwisów internetowych. Pomaga administratorom tworzyć bardziej dostępne strony internetowe. W wyniku automatycznej analizy wskazuje ewentualne miejsca, które mogą powodować problemy z dostępnością.
Brak pełnej zgodności z ustawą o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, w tym niepełne dostosowanie portalu do standardów WCAG 2.0, **należy ocenić jako uchybienie**. Przyczyną uchybienia jest brak pełnej dostępności cyfrowej stron internetowych. Skutek uchybienia - brak zapewnienia maksymalnego wsparcia osobom niepełnosprawnym. Odpowiedzialnym za powstanie uchybienia jest osoba nadzorująca portal internetowy kontrolowanej jednostki.

[akta kontroli poz. 68-69]

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

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

**IV. Zalecenia**

Mając na uwadze powyższe ustalenia i oceny, wnoszę o:

1) Zgodnie z § 21 ust. 4 rozporządzenia KRI, przechowywanie informacji w dziennikach systemów od dnia ich zapisu - przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych - przez dwa lata.
2) Podjęcie działań w celu dostosowania portalu internetowego Urzędu do wymogów dostępności, w tym standardów WCAG min. 2.0.

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***
*/podpisano podpisem elektronicznym/*