WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

FK-IV.431.14.2021

Olsztyn, 17 listopada 2021 r.

Szanowny Pan
Piotr Ryszard Feliński
Burmistrz
Miasta i Gminy Ruciane – Nida
Al. Wczasów 4
12-220 Ruciane - Nida

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 Miasta i Gminy Ruciane - Nida[1], Al. Wczasów 4, 12-220 Ruciane – Nida, NIP: 8491001236, Regon: 000530821.

W okresie objętym kontrolą oraz w czasie prowadzonych czynności kontrolnych stanowiska pełnili:

- Pan **Piotr Ryszard Feliński** - Burmistrz, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 21 października 2018 r. (kierownik kontrolowanej jednostki).
- Pani **Danuta Kowalewska** - Sekretarz Gminy, zatrudniona na podstawie umowy o pracę od dnia 1 kwietnia 2015 r. (nadzorująca bezpośrednio pracowników realizujących zadania objęte kontrolą).

W dniu rozpoczęcia czynności kontrolnych odpowiedzialnym za realizację zadania objętego kontrolą w Urzędzie byli:

[redacted]

[akta kontroli str. 66]

Kontrolę przeprowadzili pracownicy Wydziału Finansów i Kontroli Warmińsko-Mazurskiego Urzędu Wojewódzkiego w Olsztynie:
Radosław Gazda – inspektor wojewódzki; przewodniczący zespołu kontrolnego,

[1] Zwanym dalej: Urzędem

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.0030.513.2021 z 15 września 2021 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 Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr FK-IV.0030.514.2021 z 15 września 2021 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 17-18]

Kontrolę przeprowadzono w dniach 24 września – 14 października 2021 r., co zostało odnotowane w książce kontroli Urzędu str. 17-18, pod pozycją, Nr 31/2021.

[akta kontroli str. 64-65]

Kontrola prowadzona była w trybie zdalnym, tj. bez osobistej obecności kontrolerów, 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. Rozpoczęcie kontroli nastąpiło podczas wideokonferencji, w trakcie której okazano legitymacje służbowe kontrolerów, poinformowano o zasadach kontroli w trybie zdalnym, wymaganych dokumentach do kontroli oraz formach i terminie ich przekazywania. Upoważnienia kontrolerów do kontroli zostały przekazane do kontrolowanej jednostki za pośrednictwem platformy e-PUAP.

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 2021 r., poz. 670 ze zm.). Okres objęty kontrolą: od dnia 1 stycznia 2019 r. do dnia 31 grudnia 2020 r.

[akta kontroli str. 1-2, 49-59]

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 (Dz. U. z 2019 r., poz. 1464), w związku z art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne tekst jednolity (Dz.U. z 2017 r. poz. 570 ze zm. - akt prawny obowiązujący do 02.04.2019 r., Dz.U. z 2019 r. poz. 700 ze zm. - akt prawny obowiązujący do 04.03.2020 r., Dz.U. z 2020 r., poz. 346 ze zm. - akt prawny obowiązujący do 12.04.2021 r. oraz Dz.U. z 2021 r., poz. 670

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 str. 1-2, 49-59]

Burmistrz Miasta i Gminy Ruciane – Nida, upoważnił Sekretarza Gminy, Informatyka / Administratora systemów informatycznych oraz Inspektora ochrony danych do udzielania informacji i wyjaśnień w okresie trwania czynności kontrolnych.

[akta kontroli str. 67]

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 wykorzystywanych jest 9 systemów teleinformatycznych:

1) **PUMA** (moduły: Decyzyje, Gospodarka odpadami, Podatki, OPJ, POST, Podatki - osoby fizyczne, Windykacja, Nieruchomości, Kadry, Płace, Zwrot części podatku VAT wliczonego w cenę paliwa wykorzystywanego w produkcji rolnej (moduł PALIWA), ewidencji ludności, raportowania i organizacja wyborów (moduły Ewidencja ludności, Wyborcy, Statystyki dla rejestru mieszkańców),
2) **EWOPIS** (Obsługa urzędu w zakresie ewidencji działek gruntowych),
3) **EWMAPA** (Obsługa urzędu na poziomie graficznym ewidencji działek gruntowych),
4) **Besti@** (Zarządzanie budżetem oraz sprawozdawczość w tym zakresie na potrzeby RIO i MF),
5) **Płatnik** (Obsługa urzędu jako płatnika ZUS),
6) **CEIDG** (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),
7) **SRP Źródło** (bezpłatna aplikacja, która obsługuje wszystkie wymagane polskim prawem

[2] Zwanej dalej: ustawą
[3] Zwanego dalej: rozporządzeniem KRI

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),

8) **eSesja** (Obsługa Rady Miejskiej - Przygotowywanie, prowadzenie, sporządzanie protokołów, transmisja obrad Rady Miejskiej),
9) **Portal eUsługi** (Możliwość załatwiania w formie elektronicznej niektórych spraw urzędowych).

[akta kontroli str. 36-40]

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 posiada aktywną Elektroniczną Skrzynkę Podawczą, znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie i odbieranie pism w formie dokumentów elektronicznych. Ścieżkę bezpośredniego przejścia na główną stronę e-PUAP, zawarto na stronie internetowej BIP Urzędu. Formaty danych przyjmowane za pośrednictwem Elektronicznej Skrzynki Podawczej to m.in.: DOC, RTF, XLS, CSV, TXT, GIF, TIF, BMP, JPG, PDF, ZIP.

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

wybranych spraw załatwianych w Urzędzie, istnieje jednak możliwość złożenia wniosku w formie elektronicznej (np. ePUAP),
W związku z powyższym w BIP Urzędu zamieszczone zostały procedury postępowania określające sposób przyjmowania i załatwiania poszczególnych spraw w Urzędzie, w tym załatwianych przy pomocy wniosku elektronicznego zgodnie z § 5 ust. 2 pkt 1 i 4 KRI.
Obywatel ma prawo wiedzieć o wszystkich okolicznościach, które mogą wpłynąć na ustalenie jego praw i obowiązków w prowadzonym postępowaniu.

W wyniku prowadzonej kontroli stwierdzono, iż w ramach funkcjonującej strony BIP, działa Portal eUsługi - Elektroniczne Biuro Obsługi Interesanta (eBOI). Portal eUsługi 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. Na portalu interesant może zapoznać się między innymi z katalogiem wybranych spraw świadczonych przez Urząd.
Moduł ePłatności umożliwia przegląd danych dotyczących zobowiązań kontrahentów przechowywanych w systemie dziedzinowym oraz umożliwia ich rozliczenie za pomocą płatności online. Kontrahent może sprawdzić listę swoich zobowiązań wobec Urzędu: nieopłaconych, w trakcie realizacji oraz opłaconych wraz z danymi szczegółowymi. System umożliwia zrealizowanie płatności za pomocą internetowych przelewów bankowych lub kart kredytowych oraz przegląd historii wykonywanych za pośrednictwem systemu eUsług poleceń przelewów. Dodatkowo System udostępnia funkcje generowania przelewów bankowych i pocztowych oraz powiadamia o zbliżających się terminach płatności zobowiązania.

Ponadto na stronie BIP opublikowane są niektóre wzory wniosków i formularzy, będących w zakresie poszczególnych referatów w Urzędzie. Urząd udostępniał oraz świadczył również usługi elektroniczne, z wykorzystaniem ePUAP, tj. „Pismo ogólne do urzędu". Usługa te umożliwiają złożenie do wybranego organu administracji publicznej pisma (podania) w sprawie.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 68-69]

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.
W trakcie kontroli ustalono, że Urząd w badanym okresie nie korzystał i nie przekazywał wzorów dokumentów elektronicznych do centralnego repozytorium wzorów dokumentów prowadzonego przez Ministerstwo Cyfryzacji, ze względu na fakt, iż nie uruchamiał nowej usługi, dla której nie ma wzorów dokumentów w CRWDE.

Jednocześnie należy zaznaczyć, iż na stronie BIP Urzędu oraz w ramach Elektronicznego Biura Obsługi Interesanta (eBOI) opublikowano w wersji „do pobrania" formularze wzorów dokumentów niezbędnych do załatwienia poszczególnych spraw w Urzędzie.

[akta kontroli str. 24-35, 69-70, 373-383]

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://www.ruciane-nida.pl/, a strona internetowa BIP Urzędu – pod adresem http://bip.ruciane-nida.pl/.
Na stronie internetowej Urzędu zamieszczono bezpośredni link do strony BIP Urzędu, w lewej górnej części panelu strony. Zarówno na stronie głównej BIP Urzędu, jak i Portalu internetowym Urzędu, zamieszczono ścieżkę do skrzynki podawczej ESP na platformie ePUAP.
W Urzędzie brak jest formalnych procedur opisujących obsługę oraz monitorowanie usług elektronicznych realizowanych przez systemy teleinformatyczne wykorzystywane do realizacji zadań zleconych z zakresu administracji rządowej ze względu na fakt, iż 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.: „[redacted]".

[akta kontroli str. 373-383]

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.*

Zgodnie z informacją przekazaną przez Burmistrza, cyt.: *„(...) w Urzędzie Miasta i Gminy Ruciane - Nida w okresie objętym kontrolą czynności z zakresu modelu obiegu dokumentacji wykonywane były zgodnie z wytycznymi zawartymi w Instrukcji Kancelaryjnej stanowiącej załącznik nr 1 do Rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. 2011 nr 14 poz.67). Jednocześnie nadmieniam, iż w Urzędzie trwają prace związane z wdrożeniem systemu Elektronicznego Zarządzania Dokumentacją do tradycyjnego sposobu dokumentowania przebiegu załatwiania i rozstrzygania spraw."*
Ponadto kontrolującym przedstawiono Zarządzenie Nr 26 /2011Burmistrza Miasta i Gminy Ruciane - Nida z dnia 16maja 2011r. w sprawie wyboru podstawowego systemu dokumentowania przebiegu załatwiania i rozstrzygania spraw w Urzędzie Miasta i Gminy w Rucianem-Nidzie, którego wynika, że podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw w Urzędzie Miasta i Gminy w Rucianem - Nidzie jest system tradycyjny (papierowy) wykonywania czynności kancelaryjnych, dokumentowania przebiegu załatwiania spraw, gromadzenia i tworzenia dokumentacji w postaci nieelektronicznej z możliwością korzystania z narzędzi informatycznych do wspomagania procesu obiegu dokumentacji w tej postaci.

W okazanej dokumentacji Urzędu brak było regulacji wewnętrznych opisujących sposób zarządzania dokumentacją w kontrolowanym podmiocie, w tym procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby również zasady obiegu dokumentów wpływających i wypływających drogą elektroniczną oraz zakres stosowania elektronicznego obiegu dokumentów (np. skrzynka podawcza na platformie ePUAP), 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.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie uchybieniami. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki.

Zastosowanie w przyszłości systemu elektronicznego zarządzania dokumentami elektronicznymi wpłynie na uporządkowanie i usprawnienie przepływu dokumentów

w podmiocie publicznym, znacząco usprawni ich archiwizację oraz zapewni łatwy dostęp do dokumentów archiwalnych, co wpłynie na przyspieszenie załatwianych spraw w tym realizowanych przez podmiot publiczny usług oraz pozwoli na minimalizowanie nakładu pracy a także podniesie poziom Bezpieczeństwa Informacji. Celem wdrożenia systemu elektronicznego zarzadzania dokumentacją jest wyeliminowanie z obiegu wewnętrznego podmiotu publicznego dokumentów papierowych, co spowoduje dodatkowo obniżenie kosztów.

[akta kontroli str. 71, 450]

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.: „[redacted]

[redacted]

[akta kontroli str. 373-383]

Mając powyższe na uwadze 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.*

Realizacja ww. zadań 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 SZBI jest warunkiem niezbędnym, w celu skutecznego zarządzania bezpieczeństwem informacji w podmiocie.

Podstawowym dokumentem SZBI jest Polityka Bezpieczeństwa Informacji. Dokument ten 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. W ramach dokumentacji wchodzącej w skład SZBI w Urzędzie przyjęto:

- Zarządzenie Nr 28/2008 Burmistrza Miasta i Gminy Ruciane - Nida z dnia 31 grudnia 2008 roku w sprawie wprowadzenia Polityki Bezpieczeństwa Ochrony Danych Osobowych (obowiązujące do dnia 11 marca 2019 r.).

- Zarządzenie Nr 80/2018 Burmistrza Miasta i Gminy Ruciane - Nida z dnia 20 grudnia 2018 r. w sprawie wyznaczenia Administratora Systemów Informatycznych oraz wprowadzenia instrukcji zarządzania systemem informatycznym w Urzędzie Miasta i Gminy Ruciane - Nida.

- Zarządzenie NR 19/2019 Burmistrza Miasta i Gminy Ruciane - Nida z dnia 11.03.2019 r. w sprawie wprowadzenia Polityki Ochrony Danych (obowiązujące od dnia 11 marca 2019 r.).

Przedmiotową dokumentację sporządzono na podstawie obowiązujących w danym okresie przepisów prawa, tj. „RODO", ustawy dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000), Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. 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 nr 100 poz. 1024), ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tj. Dz. U. z 2018 r. poz.994 ze zm.).

Dokumentacja w zakresie ochrony danych dotyczyła danych przetwarzanych w Urzędzie i służyła zapewnieniu poufności, integralności przetwarzania danych, jak również monitorowania zdarzeń naruszających ochronę danych (w tym osobowych), zawierała także opis postępowania w przypadku naruszenia zasad bezpieczeństwa danych osobowych.

[akta kontroli str. 113-190]

Burmistrz Rucianego – Nidy, zarządzeniami nr 53/2018 z dnia 30 lipca 2018 r. (obowiązywało do dnia 27 czerwca 2019 r.) oraz nr 55/2019 z dnia 27 czerwca 2019 r. powołał w jednostce Inspektora Ochrony Danych (IOD).

[akta kontroli str. 191-194]

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.
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. Powyższe oznacza, iż realizacja obowiązku wynikającego z § 20 ust. 1 KRI nie kończy się z momentem wdrożenia do stosowania SZBI, lecz wymaga ona nieustannej uwagi.

Z dokumentacji przedstawionej kontrolującym wynika, że IOD w okresie objętym kontrolą dokonał przeglądu SZBI w jednostce. Jednocześnie należy nadmienić - zdaniem kontrolujących, że takie przeglądy powinny odbywać się w jednostce raz do roku.
Jednocześnie wypełniając obowiązek zawarty w pkt 21 Polityki ochrony danych przyjętej w jednostce, IOD dokonywał regularnych (nie rzadziej niż raz na rok) przeglądów polityki.

[akta kontroli str. 195-196, 438-445]

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.
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.

Kontrolującym przedstawiono dokumentację (notatka z wykonanego procesu) informującą o przeprowadzeniu analizy ryzyka utraty integralności, dostępności lub poufności informacji w okresie objętym kontrolą.
Należy jednak podkreślić, że treść notatki, informuje jedynie o czynności jaką było przeprowadzenie analizy ryzyka. Brak jest w niej natomiast zapisów określających czy dokonana okresowa analiza stwierdzała lub nie możliwość utraty integralności, dostępności lub poufności informacji oraz czy podejmowano ewentualnie jakiekolwiek działania minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.

[akta kontroli str. 197]

Jednocześnie należy wskazać, iż zgodnie z zarządzeniem nr 50/2018 Burmistrza Miasta i Gminy Ruciane - Nida z dnia 20 lipca 2018 r., w sprawie wprowadzenia rejestru czynności przetwarzania danych osobowych, zmienionym zarządzeniem nr 16/2021 z dnia 25 marca 2021 r., w jednostce został opracowany i jest prowadzony rejestr czynności przetwarzania danych osobowych.

[akta kontroli str. 198-206]

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 aktualną 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 str. 72-73]

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 odbierania uprawnień do przetwarzania danych osobowych oraz do pracy w określonym zbiorze danych (systemie informatycznym) określone zostały w zarządzeniach:

- Nr 80/2018 Burmistrza Miasta i Gminy Ruciane - Nida z dnia 20 grudnia 2018 r. w sprawie wyznaczenia Administratora Systemów Informatycznych oraz wprowadzenia instrukcji zarządzania systemem informatycznym w Urzędzie Miasta i Gminy Ruciane – Nida (§3).

oraz

- NR 19/2019 Burmistrza Miasta i Gminy Ruciane - Nida z dnia 11.03.2019 r. w sprawie wprowadzenia Polityki Ochrony Danych (pkt 7.4, 12.1).

[akta kontroli str. 113-190]

Osoby posiadające dostęp do danych osobowych posiadały pisemne upoważnienie. Prowadzona była też ewidencja osób upoważnionych do przetwarzania danych osobowych oraz do pracy w określonym zbiorze danych (systemie informatycznym).

Ponadto zgodnie z przyjętą polityką ochrony danych - rozdział 18.1, co najmniej raz na kwartał dokonywana była przez informatyka kontrola uprawnień.

[akta kontroli str. 384-412]

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.*

Z dokumentacji przedstawionej kontrolującym wynika, że pracownicy Urzędu zaangażowani w proces przetwarzania informacji, uczestniczyli w okresie objętym kontrolą w szkoleniach (zorganizowanym przez IOD), dotyczącym ochrony danych osobowych.
W załączeniu przedstawiono listy obecności pracowników uczestniczących w szkoleniach:

- *Najważniejsze obowiązki administratora danych nałożone przez RODO oraz rola IOD w organizacji,*
- *Podstawy prawne ochrony danych osobowych – Organy nadzorcze – postępowanie kontrolne, odpowiedzialność za naruszenia.*

Ponadto w związku z wejściem w życie ustawy z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego 1 Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), IOD przekazał do Urzędu drogą elektroniczną materiały w zakresie zmian w poszczególnych ustawach w związku z wejściem w życie RODO.

[akta kontroli str. 74-110]

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.*

Z informacji uzyskanych z Urzędu wynika, że, cyt.: „[redacted]”

Kontrolującym przedstawiono zarządzenie nr 75/2020 Burmistrza Miasta i Gminy Ruciane – Nida z dnia 02.11.2020 r. w sprawie wprowadzenia ramowych zasad organizacji pracy zdalnej i rotacyjnej w Urzędzie Miasta i Gminy Ruciane - Nida

[akta kontroli str. 373-383, 413-417]

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.

Zgodnie z procedurą wykonywania przeglądów i konserwacji systemów i nośników informacji służących do przetwarzania danych, ujętą w zarządzeniu Nr 80/2018 Burmistrza Miasta i Gminy Ruciane - Nida z dnia 20 grudnia 2018 r. w sprawie wyznaczenia Administratora Systemów Informatycznych oraz wprowadzenia instrukcji zarządzania systemem informatycznym w Urzędzie Miasta i Gminy Ruciane – Nida - rozdział IX - ASI jest odpowiedzialny za dokonywanie przeglądu i konserwacji elementów systemu informatycznego. W wypadku wystąpienia potrzeby dokonania przeglądu i konserwacji,

przedmiotowe czynności mogą być zlecone podmiotowi zewnętrznemu specjalizującemu się w tego typu działaniach, ASI informuje podmiot, który na podstawie umowy zawartej z ADO, dokonuje przeglądu i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych, o konieczności podjęcia stosownych czynności. W wypadku przekazania sprzętu lub nośników informacji służących do przetwarzania danych osobowych podmiotowi trzeciemu, pozbawia się je zapisanych danych osobowych w sposób, który uniemożliwi ich odtworzenie, W obydwu przypadkach, zostaną zachowane szczególne warunki ostrożności, w celu zabezpieczenia danych osobowych przed dostępem osób nieuprawnionych.

Z informacji uzyskanych podczas kontroli oraz wyjaśnienia przekazanego w powyższej sprawie wynika, że cyt.: „[redacted]".

W związku z zakupem systemów podpisane zostały z poszczególnymi firmami umowy licencyjne umożliwiające prawidłową eksploatację i rozwój systemu 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 str. 36-40, 180-190, 304-371, 373-383, 452-480]

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 danych osobowych oraz podejmowanych działań korygujących została uregulowana zarządzeniem NR 19/2019 Burmistrza Miasta i Gminy Ruciane - Nida z dnia 11.03.2019 r. w sprawie wprowadzenia Polityki Ochrony Danych – załącznik nr 17.

[akta kontroli str. 113-179]

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.*

Na podstawie okazanej dokumentacji kontrolujący stwierdzili, iż w 2019 r., w jednostce przeprowadzono jedno zadanie audytowe w zakresie bezpieczeństwa informacji. Zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI, w dniach od 17 stycznia 2019 r. do 4 lutego 2019 r. przeprowadzony został audyt bezpieczeństwa informacji przez firmę Centrum Bezpieczeństwa Informatycznego Krasnystaw. Przeprowadzone zadania audytowe obejmowały m.in. następujące zagadnienia:

1. Inwentaryzacja sprzętu i oprogramowania.
2. Ochrona przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.
3. Urządzenia mobilne i praca na odległość.
4. Zabezpieczenia informacji w sposób uniemożliwiający nieuprawnione jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.
5. Zasady postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.
6. Poziom bezpieczeństwa w systemach teleinformatycznych.
7. Okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji.

- Analiza podatności systemu informatycznego,
- Skanowanie sieci lokalnej,
- Skanowanie od strony sieci Internet,
- Analiza podatności strony internetowej,
- Wykaz załączników do raportu,
- Analiza wykorzystania sprzętu, audyt zainstalowanego oprogramowania,
- Identyfikacja zasobów ogólnodostępnych sieci lokalnej.

[akta kontroli str. 111-112]

W przypadku 2020 r. na podstawie okazanej dokumentacji kontrolujący stwierdzili, że IOD w dniu 5 sierpnia 2020 roku przeprowadził w Urzędzie Miasta i Gminy Ruciane Nida audyt dotyczący stosowania środków fizycznych, technicznych i organizacyjnych służących do ochrony danych osobowych, analizę przetwarzania danych osobowych w kadrach, analizę obszarów powierzenia przetwarzania danych osobowych podmiotom zewnętrznym.

[akta kontroli str. 422-437]

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 – został zrealizowany.

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.

Z dokumentacji przedstawionej kontrolującym wynika, że procedury w zakresie tworzenia i testowania kopii zapasowych zbiorów danych osobowych, określone zostały w *Instrukcji zarządzania systemem informatycznym*, stanowiącym załącznik do zarządzenia Nr 80/2018 Burmistrza Miasta i Gminy Ruciane - Nida z dnia 20 grudnia 2018 r. w sprawie wyznaczenia Administratora Systemów Informatycznych oraz wprowadzenia instrukcji zarządzania systemem informatycznym w Urzędzie Miasta i Gminy Ruciane – Nida oraz uszczegółowione (w zakresie tworzenia kopii) w załączniku Nr 12 do zarządzenia NR 19/2019 Burmistrza Miasta i Gminy Ruciane - Nida z dnia 11.03.2019 r. w sprawie wprowadzenia Polityki Ochrony Danych.

Z informacji uzyskanych w powyższej sprawie podczas kontroli wynika, że cyt.: „[redacted]

[redacted]

Zgodnie z przekazaną kontrolującym dokumentacją (dziennik testów, zrzuty ekranu potwierdzające wykonywanie automatycznej kopii bazy danych) obowiązek minimalizowania ryzyka utraty informacji w wyniku awarii, poprzez wykonywanie i testowanie kopii zapasowych jest realizowany.

[akta kontroli str. 113-179, 180-190, 373-383, 446-449]

Regularne tworzenie i testowanie jakości kopii zapasowych jest kluczowym działaniem w celu minimalizowania ryzyka utraty informacji w wyniku awarii. Wskazane jest przechowywanie kopii zapasowych w innej lokalizacji niż miejsce ich tworzenia, w odległości niezbędnej do uniknięcia uszkodzeń spowodowanych przez katastrofę, która dotknęłaby podstawowy ośrodek przetwarzania danych.

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

Stosownie do § 15 ust. 1 rozporządzenia KRI *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.

[redacted]

Na obsługę aktualnie zainstalowanego oprogramowania z firmami zewnętrznymi dostarczającymi dany system informatyczny zawarte zostały stosowne umowa licencyjne (opieka autorska), gwarantujące rozwój systemu i dostosowanie do obowiązujących przepisów prawa. Zakupione systemy teleinformatyczne, w razie awarii podlegają ekspertyzie technicznej zlecanej firmie dostarczającej.

[akta kontroli str. 304-371, 373-383, 452-480]

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 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.

Zgodnie z wyjaśnieniem uzyskanym w trakcie kontroli, cyt.: „[redacted]

[redacted]

[akta kontroli str. 373-383]

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, cyt.: [redacted]

[akta kontroli str. 373-383]

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 wyjaśnień uzyskanych z Urzędu w powyższej sprawie wynika, że cyt.: „[redacted]”

[akta kontroli str. 373-383]

Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

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. W toku kontroli dokonano jednak weryfikacji zgodności ze standardem WCAG 2.0 strony internetowej Urzędu oraz BIP Urzędu.

Dostępność strony internetowej oznacza, że może z niej skutecznie korzystać każdy na dowolnej aplikacji klienckiej, na dowolnym urządzeniu, z dowolnego rodzaju połączenia, w każdych warunkach, bez względu na sprawność swoich zmysłów. Podmioty publiczne zobowiązane są do zapewnienia dostępności cyfrowej swoich stron. Zapewnienie dostępności cyfrowej stron internetowych oznacza spełnienie wielu kryteriów sukcesu zdefiniowanych w Web Content Accessibility Guidelines (WCAG 2.1). Wytyczne wymagają spełnienia czterech głównych zasadami, którymi są:

1. postrzegalność,
2. funkcjonalność,
3. zrozumiałość,
4. kompatybilność.

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.

Walidacja za pomocą narzędzia http://wave.webaim.org tj. walidatora WAVE-WCAG 2.0 Portalu Internetowego Urzędu nie wykazała błędów, natomiast walidacja strony BIP wykazała 4 błędy które nie miały wpływu na realizację zadania.
WAVE-WCAG jest narzędziem do automatycznego testowania dostępności serwisów internetowych. Pomaga projektantom i administratorom tworzyć bardziej dostępne strony internetowe. Wprawdzie nie odpowiada do końca na pytanie, czy zawartość serwisu jest dostępna, bo to może uczynić tylko człowiek-użytkownik, ale poglądowo wskazuje miejsca, które mogą powodować problemy z dostępnością.

[akta kontroli str. 302-303]

Powyższe zagadnienie oceniono pozytywnie.

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 również zasady obiegu dokumentów wpływających i wypływających z 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