WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

Olsztyn, 14 października 2020 r.

FK-IV.431.14.2020

Szanowny Pan
Maciej Leszczyński
Burmistrz Jezioran
Plac Zamkowy 4
11-320 Jeziorany

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 Jezioranach[1], Plac Zamkowy 4, 11-320 Jeziorany, NIP: 739-00-08-905, REGON: 000530293.

W okresie prowadzonych czynności kontrolnych stanowiska pełnili:
1. Pan **Maciej Leszczyński** - Burmistrz wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 21 października 2018 roku (*kierownik jednostki kontrolowanej*).
2. [redacted], zatrudniona na podstawie umowy o pracę od dnia 1 stycznia 2009 roku (*nadzorująca bezpośrednio pracowników realizujących zadania objęte kontrolą*)

Odpowiedzialnymi za realizację zadania w Urzędzie byli:
1. [redacted] - inspektor ds. informacji publicznej i promocji gminy zatrudniona na podstawie umowy o pracę [redacted] roku.
2. [redacted] - starszy informatyk zatrudniony na podstawie umowy o pracę na 1/2 etatu [redacted] roku. Od 8 marca 2019 roku obsługa informatyczna Urzędu – firma zewnętrzna [redacted].
3. [redacted] - inspektor ds. oświaty, ochrony danych zatrudniony na podstawie umowy o pracę [redacted] roku.

[akta kontroli str. 93]

Kontrolę przeprowadzili pracownicy Wydziału Finansów i Kontroli Warmińsko-Mazurskiego Urzędu Wojewódzkiego w Olsztynie:

---

[1] Zwany dalej: Urzędem

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.0030.275.2020 z 20 sierpnia 2020 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.0030.274.2020 z 20 sierpnia 2020 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 23-27]

Kontrolę przeprowadzono w dniach 7-28 września 2020 r., co zostało odnotowane w książce kontroli Urzędu pod pozycją Nr 14/2020.
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 2020 r., poz. 346 ze zm.).
Okres objęty kontrolą: od dnia 1 stycznia 2018 r. do dnia 7 września 2020 r. (dzień rozpoczęcia czynności kontrolnych).

[akta kontroli str. 1-2, 75-85]

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 (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. oraz Dz.U. z 2020 r., poz. 346 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, 75-85]

Burmistrz Jezioran upoważnił do udzielania informacji i wyjaśnień w okresie trwania czynności kontrolnych:

1. Inspektora ds. informacji publicznej i promocji gminy,
2. Inspektora ds. oświaty, ochrony danych.

[akta kontroli str. 94-95]

Na podstawie ustaleń kontroli, realizację zadań z zakresu działania systemów teleinformatycznych używanych przez Urząd do realizacji zadań zleconych z zakresu administracji rządowej ocenia się **pozytywnie z nieprawidłowościami.**
Ocena działalności jednostki kontrolowanej wynika z 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 **3** systemy teleinformatyczne:

1) Źródło (Rejestr PESEL, Rejestr Stanu Cywilnego, Rejestr Dowodów Osobistych),
2) PUMA (ewidencja ludności),
3) CEIDG (działalność gospodarcza).

Systemy teleinformatyczne wykorzystywane w Urzędzie:

1) **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) **PUMA - Moduł Ewidencja Ludności (rejestr mieszkańców)** posiada homologację Ministerstwa Spraw Wewnętrznych, a jego zadaniem jest kompleksowa obsługa komórki ewidencji ludności. Aplikacja umożliwia między innymi: gromadzenie, wyszukiwanie,

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

uzupełnianie oraz zmianę w bazie danych wszystkich informacji znajdujących się na Karcie Osobowej Mieszkańca. Program automatyzuje pracę i drukuje zawiadomienia w zakresie: meldowania, wymeldowania, rejestracji urodzeń, zgonów, zmian stanu cywilnego - gromadzenia i dostępu do danych historycznych mieszkańców.

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

Rejestry publiczne i ewidencje prowadzone w Urzędzie:

- Rejestr działalności regulowanej w zakresie odbierania odpadów komunalnych od właścicieli nieruchomości (podstawa prawna - art. 9b ust. 2-3 ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach, Dz. U. z 2020 r., poz. 1439).
- Ewidencja udzielonych i cofniętych zezwoleń na opróżnianiem zbiorników bezodpływowych i transport nieczystości ciekłych na terenie Gminy (podstawa prawna - art. 7 ust. 6b ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach, Dz. U. z 2020 r., poz. 1439).
- Rejestr instytucji kultury, dla których organizatorem jest Gmina Jeziorany,
- Rejestr obowiązujących miejscowych planów zagospodarowania przestrzennego.
- Ewidencja kąpielisk Gminy Jeziorany.

[akta kontroli str. 205-210, 466]

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 **/281406/skrytka,** znajdującą się

na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie i odbieranie pism w formie dokumentów elektronicznych. Szczegółowe informacje dotyczące funkcjonowania oraz możliwość bezpośredniego przejścia na główną stronę e-PUAP, zawarto na głównej stronie internetowej BIP Urzędu.
Formaty danych przyjmowane za pośrednictwem Elektronicznej Skrzynki Podawczej to m.in.: ODF, ODS, DOC, RTF, XLS, CSV, TXT, PNG, GIF, TIF, BMP, JPG, PDF, ZIP, RAR, 7zip.

W zakresie publikacji procedur załatwiania spraw realizowanych przez Urząd należy stwierdzić, iż na stronie BIP w zakładce Urząd Miejski – Poradnik interesanta, opublikowane są procedury stosowane przy załatwianiu poszczególnych spraw. Na stronie BIP opublikowane są również podstawowe wzory wniosków i formularzy, będących w zakresie poszczególnych komórek organizacyjnych w Urzędzie.
Urząd nie świadczył usług związanych z załatwianiem spraw od początku do końca w formie elektronicznej, za pomocą systemów teleinformatycznych.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 467-470]

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 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 kontrolowanego Urzędu opublikowano w wersji „do pobrania" formularze niektórych wzorów dokumentów niezbędnych do załatwienia poszczególnych spraw w Urzędzie.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 57, 470]

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://jeziorany.com.pl/, a strona internetowa BIP Urzędu – pod adresem http://bip.jeziorany.nowoczesnagmina.pl/.
Na stronie internetowej Urzędu zamieszczono bezpośredni link do strony BIP Urzędu w prawej górnej części panelu strony. Na stronie głównej BIP Urzędu zamieszczono link do skrzynki podawczej ESP na platformie ePUAP.
W Urzędzie brak jest formalnych procedur opisujących obsługę oraz monitorowanie usług elektronicznych za pomocą systemów teleinformatycznych ze względu na fakt, iż instytucja ta nie świadczyła usług elektronicznych na zewnątrz za pomocą systemów teleinformatycznych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej.
W związku z powyższym przedmiotowe cząstkowe zagadnienie nie podlegało ocenie.

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.: *„Źródło-Puma - oddzielne łącze dedykowane dla systemu źródło, puma zainstalowana na tym samym komputerze co źródło. Współpraca programów odbywa się na poziomie wymiany danych. Płatnik-kadry - pliki o rozszerzeniu .XML Generowane są one w systemie kadry i wczytywane do systemu płatnik. Pliki generowane na jednym komputerze, obsługiwane wyłącznie przez 1 osobę. Bestia - program finansowo-księgowy - pliki o rozszerzeniu XML Generowane są w systemie finansowo-księgowym i wczytywane do systemu bestia. Pliki generowane na jednym komputerze."*

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 474]

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 zarządzeniem Nr 56/2020 Burmistrza Jezioran z dnia 23 lipca 2020 r. w sprawie wskazania systemu wykonywania czynności kancelaryjnych w Urzędzie, podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw oraz gromadzenia i tworzenia dokumentacji w Urzędzie jest system tradycyjny, przez który należy rozumieć system wykonywania czynności kancelaryjnych, dokumentowania przebiegu załatwiania spraw, gromadzenia i tworzenia dokumentacji w postaci nieelektronicznej (papierowej) z możliwością wykorzystania narzędzi informatycznych do wspomagania procesu obiegu dokumentacji papierowej.
W zarządzeniu określono sposób postępowania z korespondencją wpływającą i wypływającą z Urzędu w formie papierowej i elektronicznej, co 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.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 137-140]

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.: *„Pliki generowane są lokalnie na komputerze i wczytywane do współpracującego systemu teleinformatycznego. Dane są udostępniane w formatach XML".*

[akta kontroli str. 474]

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.

Zarządzeniem 11/05 Burmistrza Jezioran z dnia 28 lutego 2005 r. r. wdrożono w Urzędzie Politykę bezpieczeństwa systemów informatycznych służącym do przetwarzania danych osobowych.
Zarządzenie wprowadzono zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. 2002 r., Nr 101, poz. 926 Nr 153, poz.1271 oraz z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285.) oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).
Powyższe stanowiło dokumentację przetwarzania danych osobowych w rozumieniu §1 pkt 1 rozporządzenia MSWiA z 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych (...). Służyła ona zapewnieniu poufności, integralności i rozliczalności przetwarzanych danych.

[akta kontroli str. 141-155]

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 Urzędzie dokonano weryfikacji dokumentacji systemu zarządzania bezpieczeństwem informacji i opracowano:

- Zarządzenie wewnętrzne Nr 20/2018 Burmistrza Jezioran z dnia 19 lipca 2018 r. w sprawie Polityki Bezpieczeństwa Ochrony Danych Osobowych w Urzędzie Miejskim w Jezioranach (zmienione zarządzeniami Nr 17/2019 z dnia 24 czerwca 2019 r. oraz Nr 34/2019 z dnia 16 października 2019 r.),

- Zarządzenie wewnętrzne Nr 21/2018 Burmistrza Jezioran z dnia 19 lipca 2018 r. w sprawie Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Jezioranach,

Przedmiotową dokumentację sporządzono na podstawie obowiązujących przepisów prawa, tj. „RODO" oraz ustawy dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000), w brzmieniu obowiązującym w tym okresie. 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. Przedmiotowa dokumentacja wchodząca w skład systemu zarządzania bezpieczeństwem informacji w jednostce obowiązywała do dnia 7 lipca 2020 roku.

[akta kontroli str. 156-204]

W wyniku przeprowadzonej kolejnej weryfikacji dokumentacji SZBI, w dniu 7 lipca 2020 r. przyjęto do stosowania i realizacji zarządzenie wewnętrzne Nr 17/2020 Burmistrza Jezioran w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Jezioranach. Jednym z załączników do przyjętej polityki jest Instrukcja zarządzania systemem informatycznym w Urzędzie Miejskim w Jezioranach (zał. 10).
Dokumentację sporządzono na podstawie obowiązujących przepisów prawa, tj. „RODO" oraz ustawy dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781). Dokumentacja w zakresie ochrony danych dotyczyła danych przetwarzanych w Urzędzie i służyła zapewnieniu poufności, integralności przetwarzania danych, jak również monitorowaniu zdarzeń naruszających ochronę danych (w tym osobowych), zawierała także opis postępowania w przypadku naruszenia zasad bezpieczeństwa danych osobowych.

[akta kontroli str. 312-359]

Burmistrz Jezioran wyznaczył Administratora Systemu Informatycznego w Urzędzie (firma zewnętrzna). Podpisał również stosowne umowy na świadczenie usług Inspektora Ochrony Danych (IOD) w Urzędzie (zgodnie z art. 37 RODO), a po rozwiązaniu umowy z firmą zewnętrzną wyznaczył IOD zgodnie z art. 37 ust. 5-6 RODO. Ponadto każdorazowo dokonywał zgłoszenia zmiany na stanowisku IOD do Urzędu Ochrony Danych Osobowych.

[akta kontroli str. 211-225, 363]

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 §14 pkt 4 zarządzenia wewnętrznego Nr 20/2018 Burmistrza Jezioran z dnia 19 lipca 2018 r. w sprawie Polityki Bezpieczeństwa Ochrony Danych Osobowych (...),

sprawdzeniu podlegają: systemy informatyczne przetwarzające dane osobowe, zabezpieczenia fizyczne, zabezpieczenia organizacyjne, bezpieczeństwo osobowe oraz zgodność stanu faktycznego, z wymaganiami ustawy. IOD przygotowuje plan sprawdzeń, który określa przedmiot, zakres, termin przeprowadzenia poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania. Plan sprawdzeń jest przygotowywany przez IOD na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan sprawdzeń obejmuje co najmniej jedno sprawdzenie. Plan sprawdzeń jest przedstawiany ADO (Administrator Danych Osobowych – Burmistrz Jezioran) nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem. Po zakończeniu sprawdzenia IOD przygotowuje ADO sprawozdanie, nie później niż w terminie 30 dni od zakończenia sprawdzenia. Na jego podstawie ADO inicjuje działania korygujące lub zapobiegawcze.
Jednocześnie zgodnie z §13 pkt 1 zarządzenia wewnętrznego Nr 21/2018 Burmistrza Jezioran z dnia 19 lipca 2018 r. w sprawie Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych, Administrator Sieci Informatycznej (ASI) raz na 3 miesiące wykonuje generalny przegląd systemu informatycznego polegający na ustaleniu poprawności działania tych jego elementów, które są niezbędne do zapewnienia realizacji funkcji wynikających z instrukcji.

Na zadane przez kontrolujących pytanie odnośnie realizacji obowiązku wynikającego z rozporządzenia KRI oraz przyjętych w Urzędzie polityk (§14 pkt 4 zarządzenia wewnętrznego Nr 20/2018 oraz §13 pkt 1 zarządzenia wewnętrznego Nr 21/2018), otrzymano odpowiedź, cyt.: *„Kontrola systemów jest przeprowadzana raz na 3 miesiące i polega na fizycznym sprawdzeniu wszelkich zabezpieczeń począwszy od fizycznych (UPSy, listwy, poprawne działanie komputerów i sprzętu peryferyjnego) po systemowe (np. kopie bezpieczeństwa, firewall, systemy antywirusowe, zmiany haseł, wygaszacze ekranów).*
W przypadku stwierdzenia nieprawidłowości, niezwłocznie są podejmowane działania eliminujące stwierdzone wady".
Z przekazanej odpowiedzi wynika, iż nałożony obowiązek monitorowania, przeglądania oraz utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji nie był w pełni realizowany w jednostce. Zgodnie z otrzymaną odpowiedzią zrealizowano wymóg wynikający z §13 pkt 1 obowiązującego w tym czasie zarządzenia wewnętrznego Nr 21/2018, natomiast obowiązek wynikający z §14 pkt 4 zarządzenia wewnętrznego Nr 20/2018 nie został zrealizowany.
Brak realizacji wymaganych sprawdzeń stanowi nieprawidłowość skutkującą naruszeniem § 20 ust. 1 rozporządzenia KRI oraz przyjętych regulacji wewnętrznych, Osobą odpowiedzialną za powstanie nieprawidłowości jest IOD wyznaczony w jednostce w tym okresie.

[akta kontroli str. 474-475]

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

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.

Z dokumentacji przedstawionej kontrolerom wynika, że analiza ryzyka bezpieczeństwa informacji obejmująca aspekty utraty integralności, dostępności lub poufności informacji przeprowadzona została w Urzędzie dopiero w 2020 r. 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. Pierwsza analiza ryzyka powinna zostać przeprowadzona w dniu wejścia w życie zarządzenia wewnętrznego Nr 20/2018 Burmistrza Jezioran z dnia 19 lipca 2018 r. w sprawie Polityki Bezpieczeństwa Ochrony Danych Osobowych w Urzędzie Miejskim w Jezioranach, a następne w kolejnych latach.

Jednocześnie należy wskazać, że w zarządzeniu wewnętrznym Nr 17/2020 Burmistrza Jezioran w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Jezioranach obowiązującym od dnia 7 lipca 2020 roku, w §15 ust. 1 zawarto zapisy, iż w celu zapewnienia bezpieczeństwa informacji w Urzędzie **minimum raz w roku** przeprowadzana jest analiza ryzyka.

Z wyjaśnienia uzyskanego z Urzędu w powyższej sprawie wynika, że cyt.: *„Brak okresowych analiz i szacowania ryzyka wynikał z braku osoby kompetentnej do przeprowadzenia takich działań w naszym urzędzie. W 2018 roku IOD była osoba powołana osoba z zewnętrznej Kancelarii Prawnej, która takich analiz nie dokonywała. Urząd planuje przeprowadzanie analiz po wdrożeniu nowego oprogramowania w ramach projektu pn. "Opracowanie i wdrożenie e-usług dla społeczeństwa Gminy Jeziorany".*

Brak przeprowadzonych okresowych (lata 2018-2019) analiz ryzyka utraty integralności, dostępności lub poufności informacji w jednostce stanowi nieprawidłowość. Obowiązek wynikający z § 20 ust. 2 pkt 3 rozporządzenia KRI, w zakresie 2018-2019 roku nie został spełniony, co skutkowało naruszeniem powyższego przepisu. Osobą odpowiedzialną za powstanie nieprawidłowości jest IOD jednostki pełniący stanowisko w tym okresie.

[akta kontroli str. 226-260, 475]

Jednocześnie należy wskazać, iż zgodnie z art. 30 ust. 1 RODO, w jednostce jest opracowany i prowadzony rejestr czynności przetwarzania danych.

[akta kontroli str. 261-287]

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

2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego

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

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.

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 288-311]

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:

- zarządzeniem wewnętrznym Nr 20/2018 Burmistrza Jezioran z dnia 19 lipca 2018 r. w sprawie Polityki Bezpieczeństwa Ochrony Danych Osobowych w Urzędzie Miejskim w Jezioranach (zmienionym zarządzeniami Nr 17/2019 z dnia 24 czerwca 2019 r. oraz Nr 34/2019 z dnia 16 października 2019 r.),
- w §4 zarządzenia wewnętrznego Nr 21/2018 Burmistrza Jezioran z dnia 19 lipca 2018 r. w sprawie Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Jezioranach,
- w §3-5 zarządzenia wewnętrznego Nr 17/2020 Burmistrza Jezioran w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Jezioranach,
- w §3 instrukcji zarządzania systemem informatycznym w Urzędzie Miejskim w Jezioranach.

[akta kontroli str. 159, 182-189, 192, 327-328]

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).

[akta kontroli str. 364-390, 462-464]

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 kontrolującemu wynika, że pracownicy Urzędu zaangażowani w proces przetwarzania informacji, uczestniczyli łącznie w okresie objętym kontrolą w 17 szkoleniach (zorganizowanych przez IOD), dotyczących ochrony danych osobowych, tj.:

- w 2018 roku przeprowadzono 2 szkolenia zbiorowe oraz zapoznano pracowników z dokumentacją Polityki bezpieczeństwa ochrony danych osobowych, jak również z Instrukcją zarządzania systemem informatycznym,
- w 2019 roku przeprowadzono 13 szkoleń, w tym 12 szkolenia - pojedyncze osoby, 1 szkolenie zbiorowe. Ponadto zapoznano pracowników z dokumentacją Polityki bezpieczeństwa ochrony danych osobowych, jak również z Instrukcją zarządzania systemem informatycznym,
- w 2020 roku do dnia kontroli przeprowadzono 1 szkolenia zbiorowe oraz 1 szkolenie - pojedynczej osoby. Ponadto zapoznano pracowników z dokumentacją Polityki

bezpieczeństwa ochrony danych osobowych, jak również z Instrukcją zarządzania systemem informatycznym, wprowadzoną zarządzeniem wewnętrznym Nr 17/2020 Burmistrza Jezioran.

Inspektor Ochrony Danych powołany w jednostce przedstawił również certyfikaty z odbytych w 2020 roku 2 szkoleń dotyczących: „RODO – najnowsze wytyczne" oraz „Powierzenie przetwarzania danych osobowych w praktyce".

[akta kontroli str. 391-432]

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 uzyskanych podczas kontroli informacji wynika, że cyt.: *„W Urzędzie Miejskim w Jezioranach pracownicy nie wykonują pracy na odległość. Przetwarzanie danych osobowych odbywa się w siedzibie Urzędu. Jednakże ze względu na posiadanie laptopów, w Zarządzeniu wewnętrznym nr 21/2018 Burmistrza Jezioran z dnia 19 lipca 2018 r. w § 6 opisano procedury Zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej, w tym komputerów przenośnych".*

[akta kontroli str. 475]

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

2.7. Serwis sprzętu informatycznego i oprogramowania

Stosownie do § 20 ust. 2 pkt 10 rozporządzenia KRI *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 użytkowany jest 1 system teleinformatyczny przeznaczony do realizacji zadań zleconych z zakresu administracji rządowej zakupiony u zewnętrznego dostawcy, tj.: PUMA. W związku z zakupem ww. systemu podpisana została z firmą ZETO SOFTWARE Sp. z o.o.

w Olsztynie umowa licencyjna (opieka autorska), umożliwiająca prawidłową eksploatację i rozwój systemu poprzez możliwość zgłaszania błędów pytań i roszczeń dotyczących użytkowanego systemu.

[akta kontroli str. 456-461]

W ramach prowadzonych czynności kontrolnych stwierdzono, że Urząd zawarł z firmą ZETO SOFTWARE Sp. z o.o. w Olsztynie stosowną umowę powierzenia danych na wypadek awarii systemu oraz konieczności ingerencji firmy jako autora oprogramowania w bazy danych zawierające dane osobowe.

[akta kontroli str. 433-438]

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 zarządzeniami:

- Nr 20/2018 Burmistrza Jezioran z dnia 19 lipca 2018 r. w sprawie Polityki Bezpieczeństwa Ochrony Danych Osobowych w Urzędzie Miejskim w Jezioranach (zmienionym zarządzeniami Nr 17/2019 z dnia 24 czerwca 2019 r. oraz Nr 34/2019 z dnia 16 października 2019 r.) – Rozdział V,
- Nr 17/2020 Burmistrza Jezioran z dnia 7 lipca 2020 roku w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Jezioranach - §14.

[akta kontroli str. 162-166, 325]

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 okresie objętym kontrolą tj. od 1 stycznia 2018 r. do dnia rozpoczęcia czynności kontrolnych (7 września 2020 r.), w jednostce nie przeprowadzano audytu wewnętrznego w zakresie bezpieczeństwa informacji.

Z wyjaśnienia uzyskanego z jednostki wynika, że: *„Umowa z audytorem wewnętrznym została podpisana 15.10.2018 r. Zgodnie z planem audytu w 2018 r. przeprowadzono czynności organizacyjne, w tym planowanie i sprawozdawczość. Opracowano Księgę procedur Audytu Wewnętrznego Gminy Jeziorany, która została wprowadzona Zarządzeniem Burmistrza. Po przeprowadzeniu analizy ryzyka z określeniem szacowanego poziomu ryzyka w danym obszarze 27 grudnia 2018 r. przyjęto Plan audytu na rok 2019. W związku z bardzo niskim poziomem ryzyka w zakresie informatycznym i teleinformatycznym, oszacowanym na 43% , procedury audytu w tym zakresie nie zostały podjęte. W związku z wysokim poziomem ryzyka w obszarze gospodarki finansowej i procedur zamówień publicznych (96%) audytor podjął kontrolę procedur w sferze najwyższego zagrożenia. W 2020 r. w planie audytu również ujęto zadanie o wysokim poziomie ryzyka - 96% dot. gospodarki finansowej (procedury centralizacji rozliczenia przez Gminę Jeziorany podatku od towarów i usług). Jednakże w związku z istniejącym obowiązkiem przeprowadzenia audytu wewnętrznego w zakresie bezpieczeństwa informacji, zgodnie z rozporządzeniem KRI, audyt ten zostanie ujęty w planie audytu na 2021 r.*
Obecnie przygotowujemy się do realizacji projektu pn. "Opracowanie i wdrożenie e-usług dla społeczeństwa Gminy Jeziorany" (umowa Nr RPWM.03.01.00-28-0051/19-00 w ramach osi Priorytetowej 3-Cyfrowy Region, Działania 3.1 - "Cyfrowa dostępność informacji sektora publicznego oraz wysoka jakość e-usług publicznych" Regionalnego Programu Operacyjnego Województwa Warmińsko-Mazurskiego na lata 2014-2020 współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego. Umowę zawarto w dniu 25 października 2019 r. z Województwem Warmińsko -Mazurskim. W związku z powyższym audyt zostanie przeprowadzony po realizacji projektu w 2021 r."

Brak przeprowadzenia audytu wewnętrznego w zakresie bezpieczeństwa informacji w 2018 i 2019 roku skutkuje niedopełnieniem obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI. Osobą odpowiedzialną za powstanie nieprawidłowości jest IOD kontrolowanej jednostki pełniący obowiązki w tym okresie.
W przypadku roku 2020 r., istnieje jeszcze możliwość przeprowadzenia przez jednostkę audytu bezpieczeństwa informacji (do końca bieżącego roku). Wobec powyższego dopełnienie obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI, w zakresie roku 2020, nie podlegało ocenie.

[akta kontroli str. 372-385, 404, 443, 475]

Przedmiotowe cząstkowe zagadnienie w zakresie lat 2018-2019 ocenia się negatywnie.

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.

W okresie objętym kontrolą zasady tworzenia kopii zapasowych uregulowane zostały:

- Zarządzeniem wewnętrznym Nr 21/2018 Burmistrza Jezioran z dnia 19 lipca 2018 r. w sprawie Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Jezioranach (obowiązującym do 7 lipca 2020 r.) które stanowiło, że [redacted]
- Zarządzeniem wewnętrznym Nr 17/2020 Burmistrza Jezioran w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Jezioranach w skład którego weszła Instrukcja zarządzania systemem informatycznym w Urzędzie Miejskim w Jezioranach (zał. 10), która stanowi, że dla zabezpieczenia integralności danych Administrator Systemów Informatycznych [redacted] Zabrania się przechowywania kopii awaryjnych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.

[akta kontroli str. 193, 329]

Z wyjaśnienia przekazanego z Urzędu w powyższej sprawie wynik, iż, cyt.: „[redacted]”

[akta kontroli str. 475, 477-478]

W przypadku wykonywania testów w celu sprawdzenia poprawności wykonywania kopii zapasowych oraz sprawdzenia przydatności utworzonych kopii podczas próby symulowanego

przywrócenia i uruchomienia oprogramowania dziedzinowego po przywróceniu, zgodnie z zapisami przyjętej polityki, ASI ponosi odpowiedzialność za okresowe sprawdzanie kopii pod kątem ich dalszej przydatności do odtworzenia w wypadku awarii systemu.
Kontrolującym nie przedstawiono żadnej dokumentacji potwierdzającej wykonywanie w okresie objętym kontrolą testów w celu sprawdzenia poprawności tworzonych kopii zapasowych. Nie odniesiono się również do przedmiotowego zagadnienia w wyjaśnieniu skierowanym do kontrolujących.

[akta kontroli str. 475]

Brak wykonywania testów w celu sprawdzenia poprawności tworzonych kopii zapasowych należy zakwalifikować jako uchybienie skutkujące naruszeniem § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI. Osobą odpowiedzialną za powstanie uchybienia jest ASI.
Należy wskazać, że regularne 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 z uchybieniami.

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. ŹRÓDŁO i CEiDG oraz system wspierający zakupiony u dostawcy zewnętrznego - PUMA. Na obsługę aktualnie zainstalowanego oprogramowania z firmą dostarczającą system informatyczny zawarto stosowną umowę licencyjną (opieka autorska), gwarantujące rozwój systemu i dostosowanie do obowiązujących przepisów prawa. System teleinformatyczny, w razie awarii podlega ekspertyzie technicznej zlecanej firmie dostarczającej.

Jednocześnie należy wspomnieć, iż obsługę informatyczną Urzędu zapewnia firma zewnętrzna, z którą Burmistrz podpisał stosowne umowy zarówno na zapewnienie bieżącej i nieprzerwanej obsługi w zakresie funkcjonowania sprzętu i oprogramowania, jak również powierzenia danych w ramach świadczonej usługi.

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 440-451, 456-461]

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 przyjętym zarządzeniem wewnętrznym Nr 17/2020 Burmistrza Jezioran w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji, w Urzędzie Miejskim w Jezioranach ustalone zostały następujące zabezpieczenia techniczno-organizacyjne niezbędnych do zapewnienia integralności, poufności oraz możliwości przetwarzania danych osobowych:

Wprowadzone środki fizyczne:

[redacted]

[redacted]

Wprowadzone środki techniczne:

[redacted]

Wprowadzone środki organizacyjne:

[redacted]

[akta kontroli str. 357-358]

Mając na uwadze powyższe wyjaśnienia 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:

[redacted]

- [redacted].

Ponadto zgodnie z wyjaśnieniem uzyskanym w trakcie kontroli, w Urzędzie stosowane są, cyt.: *„(...)* [redacted] *(...).”*

[akta kontroli str. 476]

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.: *„Każde stanowisko ma przypisaną tylko jedną osobę do logowania. Dzienniki logów są gromadzone przez każdy program oddzielnie."*
Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 476]

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, jak i strona www. Urzędu zawierają elementy umożliwiające zmianę wielkości czcionki oraz kontrastu w celu ułatwienia korzystania z treści na niej zawartych przez osoby niedowidzące. Zmiany wielkości czcionki dokonuje się przy pomocy ikony – A +. Zgodnie z załącznikiem nr 4 do rozporządzenia KRI, strony BIP i www. spełniają poniższe zasady:

- postrzeganie – informacje oraz komponenty interfejsu strony były przedstawione użytkownikom w sposób dostępny dla jego zmysłów,
- funkcjonalność – komponenty interfejsu stron umożliwiały korzystanie z nich,
- zrozumiałość – informacje oraz obsługa interfejsu były zrozumiałe.

Walidacja za pomocą narzędzia http://wave.webaim.org tj. walidatora WAVE-WCAG 2.0 dla strony BIP nie wykazała błędów, dla strony www. Urzędu wykazała błędy nie mające wpływu na realizację przedmiotowego zagadnienia.

[akta kontroli str. 452-455]

Powyższe zagadnienie oceniono pozytywnie.

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny wnoszę o:

1. Zgodnie z § 20 ust. 1 rozporządzenia KRI monitorowanie i dokonywanie cyklicznych przeglądów systemu zarządzania bezpieczeństwem informacji, w celu jego doskonalenia i utrzymywania go na odpowiednio wysokim poziomie.
2. Zgodnie z § 20 ust. 2 pkt 3 rozporządzenia KRI oraz zapisami przyjętej w Urzędzie Polityki bezpieczeństwa informacji, przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko.
3. Zapewnienie w jednostce nie rzadziej niż raz na rok okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI.
4. Regularne testowanie jakości wytworzonych kopii zapasowych poprzez odtworzenie danych systemu informatycznego z wytworzonej kopii oraz każdorazowe dokumentowanie wykonywanych testów sprawdzenia poprawności tworzonych kopii zapasowych.

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

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

WOJEWODA
WARMIŃSKO-MAZURSKI

Artur Chojecki