WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

Olsztyn, 9 lutego 2023 r

Wydział Finansów i Kontroli
FK-IV.431.18.2022

**Szanowny Pan**
**Stanisław Bułajewski**
**Burmistrz Mrągowa**
**ul. Królewiecka 60A**
**11-700, Mrągowo**

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 Mrągowie[1], ul. Królewiecka 60A, 11-700, Mrągowo, NIP jednostki: 7420010581, REGON jednostki: 000525671.

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

- W dniu rozpoczęcia czynności kontrolnych odpowiedzialnymi za realizację zadania objętego kontrolą byli:
  - Pan **Cezary Radziszewski** - Starszy informatyk, zatrudniony na podstawie umowy o pracę od dnia 30.10.2006 r.,
  - Pan **Andrzej Doraczyński** - Starszy informatyk, zatrudniony na podstawie umowy o pracę od dnia 15.05.1997 r.

- Osobami bezpośrednio nadzorującymi pracowników odpowiedzialnych za realizację zadania byli: Pani **Małgorzata Chyziak** - Sekretarz, zatrudniona na podstawie umowy o pracę od dnia 01.08.2019 r. - nadzorujący pracownika od 01.05.2021 r., wcześniej Pan **Andrzej Skol** - Kierownik Referatu NZK, zatrudniony na podstawie umowy o pracę od dnia 01.07.2020 r.

[akta kontroli str. 52]

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

[1] Zwanym dalej: Urzędem

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

**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.0030.1000.2022 z 28 listopada 2022 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.0030.1001.2022 z 28 listopada 2022 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 28-33]

Kontrolę przeprowadzono w dniach 2 - 23 grudnia 2022 r., co zostało odnotowane w książce kontroli Urzędu pod pozycją, Nr 3/2022.

[akta kontroli str. 53-54]

Kontrola prowadzona była w trybie hybrydowym, tj. w dniu 2 grudnia – rozpoczęcie czynności kontrolnych w Urzędzie oraz oględziny serwerowni na miejscu w jednostce. Pozostałe dni (5-23 grudnia br.) kontrola prowadzona była zdalnie, bez osobistej obecności kontrolerów w Urzędzie, z wykorzystaniem narzędzi informatycznych do zgromadzenia materiału dowodowego, w celu ustalenia stanu faktycznego, a następnie dokonania oceny działalności jednostki kontrolowanej, a także sformułowanie ewentualnych zaleceń pokontrolnych. W dniu rozpoczęcia czynności kontrolnych okazano legitymację oraz upoważnienia do kontroli, poinformowano o zasadach kontroli w trybie hybrydowym, wymaganych dokumentach do kontroli oraz formach i terminie ich przekazywania.

Przedmiotem kontroli była ocena działania systemów teleinformatycznych używanych przez jednostki samorządu terytorialnego do realizacji zadań zleconych z zakresu administracji rządowej, na podstawie art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2021 r., poz. 2070). Okres objęty kontrolą: od 1 stycznia do 31 grudnia 2021 r.

[akta kontroli str. 1-2, 35-46]

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 2022 r., poz. 135), 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 2021 r., poz. 2070)[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,

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

zatwierdzonych przez Ministra Cyfryzacji w dniu 15 grudnia 2015 r.

[akta kontroli str. 1-2, 35-46]

Zastępca Burmistrza upoważnił obydwie osoby odpowiedzialne za realizację zadania, do udzielania informacji w okresie trwania czynności kontrolnych.

[akta kontroli str. 55]

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 wykorzystywanych jest 5 niżej wymienionych systemów teleinformatycznych.

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) **RESPONS (PUMA)** – Moduły: Ewidencja Ludności, Wyborcy. Posiada homologację Ministerstwa Spraw Wewnętrznych, a jego zadaniem jest kompleksowa obsługa komórki ewidencji ludności. Aplikacja umożliwia między innymi: gromadzenie, wyszukiwanie, uzupełnianie oraz zmianę w bazie danych wszystkich informacji znajdujących się na Karcie Osobowej Mieszkańca. Program automatyzuje pracę i drukuje zawiadomienia w zakresie: meldowania, wymeldowania, rejestracji urodzeń, zgonów, zmian stanu cywilnego - gromadzenia i dostępu do danych historycznych mieszkańców.

3) **BeSTi@** – system do obsługi budżetowej jednostki. Aplikacja do przekazywania sprawozdań finansowych i skonsolidowanych bilansów jednostek samorządu terytorialnego.

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

5) **E-PFRON** - jest oprogramowaniem służącym do składania deklaracji i informacji przez teletransmisję danych w formie dokumentu elektronicznego przez pracodawców zobowiązanych do wpłat lub zwolnionych z wpłat na PFRON.

[akta kontroli str. 25-26]

## 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 **/ummragowo/SkrytkaESP**, znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie i odbieranie pism w formie dokumentów elektronicznych. Na stronie głównej BIP Urzędu – zakładka Informacje Dodatkowe, podano adres Elektronicznej Skrzynki Podawczej. Formaty danych przyjmowane za pośrednictwem Elektronicznej Skrzynki Podawczej to m.in.: DOC, RTF, XLS, CSV, TXT, GIF, TIF, BMP, JPG, PDF, ZIP.

Na stronie głównej BIP Urzędu, w zakładce „e-Płatności" zawarto odnośniki do Platformy eUsług przeznaczonej dla mieszkańców, którzy chcą korzystać z usług jednostek samorządu terytorialnego drogą elektroniczną. Aplikacja ta udostępnia obywatelom dane urzędowe oraz umożliwia sprawną komunikację pomiędzy interesantem i pracownikiem urzędu. Platforma eUsług składa się z następujących modułów:

- Obsługa interesanta i sprawy – wirtualne biuro obsługi interesanta wspiera proces załatwiania spraw w urzędzie. Udostępnia opisy usług świadczonych prze jednostkę samorządu terytorialnego. Dodatkowo umożliwia umówienie się na spotkanie z urzędnikiem.
- Płatności – moduł umożliwia realizację płatności w ramach zobowiązań wynikających z podatków i innych opłat w zakresie usług oferowanych przez urząd. Przykładowym zobowiązaniem jest opłata za podatek od nieruchomości.

Platforma eUsług udostępnia przegląd analiz i zestawień danych o użytkowniku, które zostały zgromadzone w systemie. Aplikacji umożliwia również prezentacje aktualnych informacji na temat gminy oraz planowanych wydarzeń.

Zgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI interoperacyjność na poziomie organizacyjnym osiągana jest przez publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez

podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.
W zakresie publikacji procedur załatwiania spraw realizowanych przez Urząd należy stwierdzić, że na stronie BIP w zakładce „Załatwianie spraw", opublikowany jest przydatny dla petentów wykaz usług, które realizowane są przez poszczególne wydziału Urzędu.
Ponadto na stronie BIP w zakładce „Załatwianie spraw", opublikowane są wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych wydziałów w Urzędzie.
Jednocześnie należy zaznaczyć, że Urząd nie świadczył usług związanych z załatwianiem spraw od początku do końca w formie elektronicznej, za pomocą systemów teleinformatycznych.

[akta kontroli str. 56-58]

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

**1.2. Centralne repozytorium wzorów dokumentów elektronicznych (CRWDE)**

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

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

W trakcie kontroli ustalono, że Urząd przekazywał wzory dokumentów elektronicznych do Centralnego Repozytorium Wzorów Dokumentów prowadzonego przez Ministerstwo Cyfryzacji i wykorzystywał wzory dokumentów zawarte w CRWDE. Ponadto na stronie BIP w zakładce „Załatwianie spraw", opublikowany jest przydatny dla petentów wykaz usług, które realizowane są przez poszczególne wydziału Urzędu. oraz wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych wydziałów w Urzędzie.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 25-26, 59-60]

## 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.mragowo.pl/, a strona internetowa BIP Urzędu – pod adresem https://bipmragowo.warmia.mazury.pl/
Na stronie internetowej Urzędu zamieszczono bezpośredni link do strony BIP Urzędu, w prawej górnej części panelu strony. Na portalu znajdują się również odnośniki do przydatnych dla mieszkańca stron i informacji (np. e-płatności, ).
Na stronie BIP w zakładce „Załatwianie spraw, opublikowany jest przydatny dla petentów wykaz usług, które realizowane są przez poszczególne wydziału Urzędu. oraz wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw.

[akta kontroli str. 61-62]

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, że jednostka nie świadczyła usług elektronicznych na zewnątrz za pomocą tych systemów. Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie nie podlegało ocenie.

## 1.4. Współpraca systemów teleinformatycznych z innymi systemami

Stosownie do:

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

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

Z informacji uzyskanych z Urzędu wynika, że, cyt.: „Jednostronna aktualizacja danych obywateli w zakresie meldunku, dowodów osobistych, stanu cywilnego (dane z systemu Źródło aktualizują dane w systemie lokalnym). Odnośnie topologii komunikacji sieciowej: aplikacja Łącznika Respons zainstalowana na stacji roboczej w sieci Źródła wysyła zapytanie o nowe dane do systemu Źródło zgodnie z harmonogramem czasowym. W momencie otrzymania zwrotnej informacji z danymi aktualizującymi dane mieszkańców aplikacja wysyła te dane na adres IP serwera który jest w innej sieci. Na firewallu obsługującym ruch w sieci Źródła, która jest

odseparowana od innych sieci, ustawiona jest polityka przekierowująca pakiety skierowane na adres serwera Respons do dedykowanego routera sieci Respons - następuje aktualizacja danych mieszkańców w jego bazie danych. Możliwa jest wyłącznie komunikacja z jednego portu Łącznika Respons do głównego serwera Respons, tylko w jedną stronę - nie ma odblokowanej komunikacji od strony serwera Respons w stronę routera i firewalla sieci Źródła. Możliwa jest więc jedynie jednostronna aktualizacja danych mieszkańców w bazie Repons i nic ponadto."

[akta kontroli str. 203-207]

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 Zarządzenie Nr 23/2021 Burmistrza Miasta Mrągowa z dnia 28 kwietnia 2021r w sprawie wprowadzenia zasad wykonywania czynności kancelaryjnych oraz prowadzenia Biuletynu Informacji Publicznej w Urzędzie Miejskim w Mrągowie, podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw jest system tradycyjny (papierowy). Teleinformatyczny system do elektronicznego zarządzania dokumentacją (EZD), funkcjonuje w Urzędzie jako system wspomagający.

[akta kontroli str. 63-78]

W zarządzeniu określono sposób postępowania z korespondencją wpływającą i wypływającą z Urzędu w formie 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.
System EZD - system teleinformatyczny do elektronicznego zarządzania dokumentacją umożliwiający wykonywanie w nim czynności kancelaryjnych, dokumentowanie przebiegu załatwiania spraw oraz gromadzenie i tworzenie dokumentów elektronicznych. Oparty jest on na obowiązujących przepisach prawa, w szczególności kancelaryjnych i archiwalnych. Połączenie systemu EZD z ePUAP umożliwia bezpośrednie pobieranie dokumentów wpływających do elektronicznej skrzynki podawczej podmiotu. System EZD umożliwia wykonanie wszelkich podstawowych czynności w odniesieniu do dokumentu elektronicznego (utworzenie dokumentu, opisanie go metadanymi), ale przekazywanie go dalej zgodnie z procedurą – do kolejnych pracowników.

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

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

Stosownie do:

- § 17 ust. 1 rozporządzenia KRI kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków,

odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz ze zmianami lub normę ją zastępującą;
- § 18 ust. 1 rozporządzenia KRI systemy teleinformatyczne podmiotów realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia;
- § 18 ust. 2 rozporządzenia KRI jeżeli z przepisów szczegółowych albo opublikowanych w repozytorium interoperacyjności schematów XML lub innych wzorów nie wynika inaczej, podmioty realizujące zadania publiczne umożliwiają przyjmowanie dokumentów elektronicznych służących do załatwiania spraw należących do zakresu ich działania w formatach danych określonych w załącznikach nr 2 i 3 do rozporządzenia.

Istotą współdzielenia informacji w urzędach jest stworzenie możliwości wymiany danych pomiędzy różnymi systemami informatycznymi oraz umożliwienie odbiorcom swobodnego dostępu do informacji poprzez wygenerowanie danych w powszechnie znanych i dostępnych formatach plików.

Z informacji uzyskanych z Urzędu wynika, że, cyt.: „System Zeto RESPONS pobiera dane bezpośrednio z systemu COI Źródło za pomocą łącznika dostarczonego przez producenta tj Zeto. Format przekazywanych danych to XML, kodowanie znaków obywa się wg standardu utf-8. Systemy teleinformatyczne używane w Urzędzie umożliwiają udostępnienie danych w powszechnie dostępnych formatach plików XML, PDF, TXT, RTF, ODT, DOC.
Udostępnianie danych obejmuje także ich wymianę, forma kodowania także UTF-8. System obsługujący dokumenty elektronicznych do załatwiania spraw, EZD PUW, robi to w formatach danych określonych w załączniku 2 i 3 do rozporządzenia KRI."

[akta kontroli str. 203-207]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

## II. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych

### 2.1. Dokumenty z zakresu bezpieczeństwa informacji

Zgodnie z:
- § 20 ust. 1 rozporządzenia KRI podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
- § 20 ust. 2 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań związanych z bezpieczeństwem informacji;
- § 20 ust. 2 pkt 1 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

W związku z wejściem w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 roku, w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy

95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s.1) – zwanego dalej „RODO", w celu stosowania i przestrzegania zasad postępowania w procesie przetwarzania danych osobowych oraz ochrony interesów osób fizycznych, których dane mogą być przetwarzane w zbiorach danych znajdujących się w zasobach Urzędu Miejskiego w Mrągowie, zarządzeniem nr 114/2019 Burmistrza Miasta Mrągowo z dnia 5 listopada 2019 r., przyjęto Politykę Ochrony Danych Osobowych.

[akta kontroli str. 96-174]

Realizacja zadań w zakresie ochrony danych wymaga od podmiotu publicznego opracowania dokumentacji SZBI (system zarządzania bezpieczeństwem informacji), w tym szeregu regulacji wewnętrznych oraz zapewnienia aktualizacji tych regulacji w zakresie dotyczącym zmieniającego się otoczenia. Kompleksowa dokumentacja SZBI jest warunkiem niezbędnym, w celu skutecznego zarządzania bezpieczeństwem informacji w podmiocie.
Podstawowym elementem SZBI jest **Polityka Bezpieczeństwa Informacji**. Zgodnie z definicją zawartą w rozporządzeniu KRI §2 pkt 15 *polityka bezpieczeństwa informacji jest to zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia*
*i egzekwowania.*
Polityka zazwyczaj zawiera wyrażoną przez kierownictwo deklarację stosowania, opisuje organizację i ustala osoby odpowiedzialne oraz ich zakresy odpowiedzialności, wprowadza klasyfikację informacji, sposób postępowania z poszczególnymi rodzajami informacji. PBI może określać aktywa oraz ich właścicieli, oraz sposób szacowania ryzyka i postępowania z ryzykiem.
Zazwyczaj w ramach SZBI funkcjonują inne polityki, regulaminy i procedury np.:

- Polityka bezpieczeństwa teleinformatycznego;
- Polityka bezpieczeństwa fizycznego;
- Polityka bezpieczeństwa danych osobowych.
- Procedura zarzadzania ryzykiem;
- Regulamin korzystania z zasobów informatycznych;
- Procedura zarządzania sprzętem i oprogramowaniem;
- Procedura zarządzania konfiguracją;
- Procedura zarządzania uprawnieniami do pracy w systemach teleinformatycznych;
- Procedura monitorowania poziomu świadczenia usług;
- Procedura bezpiecznej utylizacji sprzętu elektronicznego;
- Procedura zarządzania zmianami i wykonywaniem testów;
- Procedura stosowania środków kryptograficznych;
- Procedura określania specyfikacji technicznych wymagań odbioru systemów IT;
- Procedura zgłaszania i obsługi incydentów naruszenia bezpieczeństwa informacji;
- Procedura wykonywania i testowania kopii bezpieczeństwa;
- Procedura monitoringu i kontroli dostępu do zasobów teleinformatycznych, prowadzenia logów systemowych.

Dokumentację SZBI stanowią także:

- Dokumentacja z przeglądów SZBI;
- Dokumentacja z szacowania ryzyka BI;
- Dokumentacja postępowania z ryzykiem;
- Dokumentacja akceptacji ryzyka;
- Dokumentacja audytów z zakresu BI;

- Dokumentacja incydentów naruszenia BI;
- Dokumentacja zarządzania uprawnieniami do pracy w systemach teleinformatycznych;
- Dokumentacja zarządzania sprzętem i oprogramowaniem teleinformatycznym;
- Dokumentacja szkolenia pracowników zaangażowanych w proces przetwarzania informacji.

W Urzędzie nie opracowano i nie wdrożono całościowej SZBI, w szczególności nie wdrożono zaktualizowanej polityki bezpieczeństwa informacji - PBI.

Z wyjaśnienia uzyskanego z Urzędu w powyższej sprawie wynika, że, cyt.: „Zadanie wykonania dokumentacji SZBI, w tym Polityki Bezpieczeństwa Informacji w UM zostało zlecona podmiotowi zewnętrznemu i jest w fazie opracowania."

[akta kontroli str. 203-207]

Opracowana i wdrożona zarządzeniem nr 114/2019 Burmistrza Miasta Mrągowo z dnia 5 listopada 2019 r. dokumentacja w zakresie Polityki Ochrony Danych Osobowych nie obejmowała wszystkich informacji jakie są przetwarzane w Urzędzie, lecz przede wszystkim dane osobowe. Mając na względzie przepisy § 20 ust. 3 rozporządzenia KRI należy uznać, że przyjęta w Urzędzie polityka stanowi tylko jedną ze składowych dokumentacji ustanawiającej SZBI w jednostce i nie dopełnia w całości obowiązku wynikającego z cytowanych powyżej przepisów. Z § 20 ust. 3 rozporządzenia KRI wynika ponadto, że wymagania określone w ust. 1 tego paragrafu uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001 (*Polska Norma PN-EN ISO/IEC 27001:2017 Technika Informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania.*), a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą (*PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem, PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.*).
Jednocześnie w pkt 5.1 Polskiej Normy PN-EN ISO/IEC 27002, wskazano wymóg opracowania i stosowania polityki bezpieczeństwa informacji - PBI.
**Powyższe stanowi nieprawidłowość**, skutkującą naruszeniem § 20 ust. 1 rozporządzenia KRI. Osobą odpowiedzialną za powstanie nieprawidłowości jest IOD pełniący funkcję w tym okresie.

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, że realizacja obowiązku wynikającego z § 20 ust. 1 KRI nie kończy się z momentem wdrożenia do stosowania SZBI, lecz wymaga ona nieustannej uwagi.
W przekazanej dokumentacji, w ramach prowadzonych czynności kontrolnych stwierdzono dowody świadczące o podejmowaniu dodatkowych działań w zakresie utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji.

[akta kontroli str. 203-217]

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

Zgodnie z wymogiem wynikającym z § 20 ust. 2 pkt 3 rozporządzenia KRI analiza ryzyka utraty integralności, dostępności lub poufności informacji powinna być przeprowadzana okresowo, a w przypadku stwierdzenia podwyższonego ryzyka w przedmiotowym zakresie, powinny zostać wprowadzone działania minimalizujące to ryzyko. Zgodnie z przyjętą Polityką Ochrony Danych Osobowych pkt 1.3.5. ppkt 3, analizę ryzyka przeprowadza się cyklicznie lub po znaczących zmianach w przetwarzaniu danych.

Na zadane przez kontrolujących pytanie: czy w 2021 r. przeprowadzono okresową analizę ryzyka. W jakich cyklach przeprowadza się okresową analizę ryzyka w Urzędzie oraz jakiego okresu dotyczy przekazana kontrolującym analiza ryzyka?, kontrolujący uzyskali odpowiedź, cyt.: „Analiza ryzyka przeprowadzana jest raz w roku. Przekazana kontrolującym analiza dotyczy roku 2021."
Kontrolującym przedstawiono dokumentację (stanowiącą akta kontroli) świadczącą o przeprowadzeniu analizy ryzyka utraty integralności, dostępności lub poufności informacji w Urzędzie.

[akta kontroli str. 94-174, 203-207]

W toku prowadzonych czynności kontrolnych stwierdzono, że w jednostce zgodnie z art. 30 RODO oraz załącznikami Nr 06-14A do przyjętej PODO, prowadzony jest rejestr czynności przetwarzania. W jednostce powołano również Administratora Systemów Informatycznych oraz Inspektora Ochrony Danych.

[akta kontroli str. 175, 246-248]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

## 2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego

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

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

[akta kontroli str. 176]

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 uprawnień do przetwarzania danych osobowych oraz do pracy w określonym zbiorze danych (systemie informatycznym), oraz wzór upoważnienia, określone zostały zarządzeniem Nr 114/2019 Burmistrza Miasta Mrągowo z dnia 5 listopada 2019 r. w sprawie wprowadzenia dokumentacji Polityki Ochrony Danych Osobowych - rozdział 2 PODO - zał. 01ARODO oraz 01BRODO.
Osoby posiadające dostęp do danych osobowych posiadały pisemne upoważnienia do ich przetwarzania. Jednocześnie należy nadmienić, że we wzorze upoważnienia do przetwarzania danych osobowych przekazanym kontrolującym wraz z dokumentacją do kontroli, zawarto możliwość wskazania zbiorów (systemu teleinformatycznego) do pracy w którym dany pracownik jest upoważniony. Prowadzona była też ewidencja osób upoważnionych do przetwarzania danych osobowych.

[akta kontroli str. 96-174, 177-180]

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 szkoleniu dotyczących ochrony danych osobowych.
Zakres szkolenia:

- Stosowanie przepisów z zakresu ochrony danych osobowych
- Podstawowe pojęcia
- Podstawa prawna przetwarzania danych osobowych
- Klauzula informacyjna
- Incydenty w ochronie danych osobowych – definicja, procedura działania
- Praktyczne przykłady incydentów w ochronie danych
- Odpowiedzialność za naruszenie przepisów o ochronie danych osobowych
- Ochrona danych osobowych podczas pracy zdalnej, środki kontroli i zapobiegania

W załączeniu przedstawiono listę pracowników uczestniczących w szkoleniu.

[akta kontroli str. 89-93]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

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

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

Zasady korzystania z komputerów przenośnych opracowane zostały w *Regulaminie korzystania z komputerów przenośnych (PODO rozdz. 4)*, a zasady pracy zdalnej w przyjętym zarządzeniem nr 106/2020 Burmistrza Miasta Mrągowo z dnia 30 października 2020 r. *Regulaminie pracy zdalnej (...).*
Z informacji uzyskanych z Urzędu wynika, że, cyt.: "Wystąpiły przypadki przetwarzania danych na odległość."

[akta kontroli str. 203-207, 218-226]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

**2.7. Serwis sprzętu informatycznego i oprogramowania**

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

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

W Urzędzie użytkowany jest jeden system teleinformatyczny przeznaczony do realizacji zadań zleconych z zakresu administracji rządowej zakupiony u zewnętrznego dostawcy, tj.:

- **RESPONS (PUMA)** – Moduły: Ewidencja Ludności, Wyborcy, jego zadaniem jest kompleksowa obsługa komórki ewidencji ludności.

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

[akta kontroli str. 181-192, 227-240]

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 oraz informacji w systemach teleinformatycznych, jak również podejmowanych działań korygujących została uregulowana zarządzeniem Nr 114/2019 Burmistrza Miasta Mrągowo z dnia 5 listopada 2019 r. w sprawie wprowadzenia dokumentacji Polityki Ochrony Danych Osobowych – rozdział 3 PODO.

[akta kontroli str. 96-174]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

**2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji**

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

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

Na podstawie okazanej dokumentacji kontrolujący stwierdzili, że w okresie objętym kontrolą w jednostce przeprowadzono audyt wewnętrzny dotyczący zgodności z Rozporządzeniem 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.
Zadanie audytowe zostało przeprowadzone przez firmę zewnętrzną **WARMIA INKASO GROUP**, co eliminuje niebezpieczeństwo braku zapewnienia obiektywności i bezstronności procesu audytowego. Mając powyższe na uwadze, należy stwierdzić, że obowiązek wynikający z § 20 ust. 2 pkt 14 rozporządzenia KRI – w 2021 r. został zrealizowany.

[akta kontroli str. 79-88]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

**2.10. Kopie zapasowe**

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

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

Zasady tworzenia i testowania kopii zapasowych systemów teleinformatycznych uregulowane zostały zarządzeniem Nr 114/2019 Burmistrza Miasta Mrągowo z dnia 5 listopada 2019 r. w sprawie wprowadzenia dokumentacji Polityki Ochrony Danych Osobowych – Załącznik nr 22RODO.
Zgodnie z procedurą, kopia dzienna jest wykonywana automatycznie przez dedykowane oprogramowanie poza godzinami pracy Urzędu. Kopia robocza-zapasowa przechowywana jest na serwerach zlokalizowanych w sieci komputerowej Jednostki. Zgodnie z procedurą kopia zapasowa jest automatycznie weryfikowana przez system backupowy. Za prawidłowość wytworzenia kopii zapasowych odpowiada ASI oraz IODO Jednostki.

W przypadku prowadzenia testów w celu sprawdzenia poprawności wykonywania kopii zapasowych oraz przydatności utworzonych kopii podczas próby symulowanego przywrócenia i uruchomienia oprogramowania, zgodnie z Polityką Ochrony Danych Osobowych, odzyskiwanie danych z kopii zapasowych jest wykonywane w następujących przypadkach:

- utraty w całości lub części danych na serwerze,
- utraty integralności całości lub części danych na serwerze,
- w celu odtworzenia poprzedniej wersji danych na wniosek Kierownika Referatu.

Regularne testowanie jakości kopii zapasowych jest kluczowym działaniem w celu minimalizowania ryzyka utraty informacji w wyniku awarii. Prawidłowo zdefiniowana polityka kopii bezpieczeństwa oraz gruntownie przetestowane procesy odtwarzania systemów teleinformatycznych są istotnymi aspektami w każdej jednostce, której procesy opierają się na

działaniu systemów informatycznych. Prawidłowo zdefiniowana i wykonana procedura pozwala mieć pewność, że w razie awarii systemu, wytworzone backupy spełnią swoje zadanie i nie odbije się to negatywnie na ciągłości działania jednostki.

Z informacji uzyskanych z Urzędu w powyższej sprawie wynika, że, cyt.: „Oprogramowanie do backupu Veeam Backup & Replication wykonuje po każdej kopii weryfikację jej poprawności. Logi z tego procesu zostały dołączone w poprzedniej przesyłce - pliki 19. Wykonanie i weryfikacja backupu rok wstecz - system nie gromadzi starszych raportów (pula maszyn l).html oraz 19. Wykonanie i weryfikacja backupu rok wstecz - system nie gromadzi starszych raportów (pula maszyn 2).html Logi z tego procesu są przechowywane w aplikacji Veeam przez 12 miesięcy. W przypadku niepowodzenia weryfikacji wysyłany jest email na adres administratora ale nie było jeszcze takiego przypadku, jedynie alerty o niewykonaniu w określonym terminie wykonania kopii np. z powodu zaniku zasilania na dłużej niż działają zasilacze UPS-y. Po przywróceniu zasilania zaległe kopie są wykonywane i weryfikowane automatycznie w kolejnym oknie cyklu. Ponadto co pewien czas przeprowadzane są ręczne odtworzenia kopii jednak system przechowuje logi odtworzenia tyle samo czasu co weryfikacji, 12 miesięcy, w celu niezapełnienia dysku serwera backupu zbędnymi danymi. W załączniku zrzut z podglądu archiwalnego przykładowego odtworzenia."

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

[akta kontroli str. 193-196, 203-207, 241]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

**2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych**

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

Wykorzystywane w Urzędzie systemy teleinformatyczne wspomagające realizację zadań z zakresu administracji rządowej, dzieliły się na systemy centralne tj. ŹRÓDŁO, CEiDG, Bestia, E-PFRON oraz systemy wspierające zakupione u dostawców zewnętrznych – RESPONS (PUMA). Na obsługę zainstalowanego w okresie objętym kontrolą oprogramowania (system informatyczny) zawarte zostały stosowne umowy licencyjne (opieka autorska), gwarantujące rozwój systemu i dostosowanie do obowiązujących przepisów prawa. Zakupiony system teleinformatyczny, w razie awarii podlega ekspertyzie technicznej zlecanej firmie dostarczającej.

[akta kontroli str. 25-26, 181-192]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

**2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji**

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

- pkt 7 zapewnienie ochrony przetwarzania informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: a) monitorowanie dostępu do informacji; b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
- pkt 9 zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie;
- pkt 11 ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.

W celu uzyskania odpowiedniego poziomu BI, przy jednoczesnym zapewnieniu właściwego bieżącego dostępu uprawnionym użytkownikom, stosowany jest szereg zabezpieczeń technicznych. Celem zabezpieczeń jest uzyskanie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także np. kradzieżą środków przetwarzania informacji.
Z informacji uzyskanych podczas kontroli wynika, że w Urzędzie stosowane są następujące zabezpieczenia cyt.: „Sieć LAN zabezpieczona jest firewallem, którego polityki bezpieczeństwa filtrują cały ruch sieciowy. Na serwerach i stacjach roboczych zainstalowany jest oprogramowanie antywirusowe. Komputery pracują w domenie Active Directory a dostęp do niej jest zabezpieczony hasłami i regułami polityk domeny. Trzykrotne podanie nieprawidłowego hasła blokuje konto. Logowanie do komputerów pracowników wykonywane jest w usłudze Windows Hello - zamiast haseł używane są kody PIN generowane i przechowywane w module kryptograficznym TPM danego urządzenia. Trzykrotne podanie złego PIN-u blokuje konto. PIN działa tylko na danym urządzeniu - przechwycenie go nie da dostępu na innych urządzeniach do konta którego dotyczyło. Na każdym komputerze jest zainstalowane oprogramowanie monitorujące pracę użytkownika łącznie z kopiowaniem danych do i z komputera, drukowaniem plików, otwieranymi stronami itd. Logi są analizowane w urządzeniu FortiAnalyzer. Przed utylizacją sprzętu demontowane i komisyjnie niszczone są nośniki danych."
Ponadto, cyt.:
„Wydzielone pomieszczenie serwerowni do którego mają dostęp tylko upoważnieni pracownicy. Klimatyzacja serwerowi. Zasilanie awaryjne serwerów. Zamykanie pokoi na klucz. Redundancja macierzy dyskowych i urządzeń sieciowych. Bezzwłoczna aktualizacja oprogramowania w zakresie działania poszczególnych systemów do najnowszych wersji. Szyfrowanie dysków komputerów przenośnych. Korzystanie z protokołu IMAP dla poczty email z szyfrowaniem połączenia w obie strony. Podpisywanie dokumentów podpisem kwalifikowanym w formacie PADESTak aby podpis był integralną częścią podpisywanego pliku a jego weryfikacja możliwa dla każdego po otworzeniu pliku w Adobe Reader."

[akta kontroli str. 203-207]

Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

**2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych**

Stosownie do:

- § 20 ust. 2 pkt 12 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: a) dbałości o aktualizację oprogramowania; b) minimalizowaniu ryzyka utraty informacji

w wyniku awarii; c) ochronie przed błędami, nieuprawnioną modyfikacją; d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa; e) zapewnieniu bezpieczeństwa plików systemowych; f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych; g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa; h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

- § 20 ust. 4 rozporządzenia KRI niezależnie od zapewnienia działań, o których mowa w ust. 2, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.

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

- w systemie Źródło logowanie odbywa się poprzez imienną kartę dostępową i indywidualne hasło dostępowe,
- w systemie CEIDG logowanie odbywa się za pomocą certyfikatu kwalifikowanego i hasła,
- w systemie RESPONS-PUMA, logowanie odbywa się za pomocą przyznanego loginu i hasła,
- E-PFRON, logowanie odbywa się za pomocą przyznanego loginu i hasła,
- Besti@, logowanie odbywa się za pomocą przyznanego loginu i hasła.

Podczas kontroli dokonano oględzin pomieszczenia serwerowni w Urzędzie. Oględzin dokonano w obecności Pana Andrzeja Doraczyńskiego - Starszego Informatyka Urzędu Miejskiego w Mrągowie. W toku oględzin dokonano ustalenia stanu faktycznego i stwierdzono:

- główny budynek urzędu posiada zabezpieczenie alarmowe,
- do pomieszczeń serwerowni dostęp ma tylko wyznaczony pracownik,
- urządzenia serwerowe umieszczony w specjalistycznych szafach,
- w pomieszczeniach serwerowni zainstalowano urządzenie klimatyzujące,
- urządzenia serwerowe podłączone są do UPS-a,
- w pomieszczeniu serwerowni zainstalowano czujkę monitorującą aktualną temperaturę,
- w pomieszczeniu serwerowni znajduje się gaśnica przeznaczone do gaszenia urządzeń elektrycznych.

**Ponadto, stwierdzono następujące uchybienia:**

- drzwi wejściowe zwykłe drewniane (bez wzmocnień) zabezpieczone pojedynczym zamkiem patentowym,
- podłoga – wykładzina dywanowa,
- w pomieszczeniu serwerowni znajduje się czynna instalacja grzewcza CO,
- w pomieszczeniu serwerowni zdeponowany jest sprzęt IT przeznaczony do kasacji,
- brak czujek ewentualnego zadymienie oraz wilgotności.

Powyższe potwierdza dokumentacja fotograficzna i protokół z przeprowadzonych oględzin.

Stwierdzone uchybienia, skutkować mogą utratą przetwarzanych informacji w wyniku awarii sprzętu lub nieautoryzowanego dostępu. Przyczyną powstania uchybień jest niepełne dostosowanie pomieszczenia pełniącego rolę serwerowni do pracy jednostek centralnych, na których opiera się działanie poszczególnych systemów informatycznych w Urzędzie. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki.

[akta kontroli str. 47-48, 51]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami.

**2.14. Rozliczalność działań w systemach informatycznych**

Stosownie do:

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

Zgodnie z § 21 ust. 1 KRI, rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach). Z informacji uzyskanych w trakcie kontroli wynika, że cyt.: „Na każdym komputerze jest zainstalowane oprogramowanie monitorujące pracę użytkownika łącznie z kopiowaniem danych do i z komputera, drukowaniem plików, otwieranymi stronami itd. Systemy dziedzinowe posiadają mechanizmy rejestracji logów wszystkich operacji w systemie. Logi są przechowywane bezterminowo. Dodatkowo logi gromadzone są w urządzeniu FortiAnalyzer które analizuje je i generuje raporty."

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

[akta kontroli str. 203-207, 242-244]

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

Uwzględniając potrzeby osób niepełnosprawnych podmiot publiczny powinien zastosować w eksploatowanych systemach teleinformatycznych rozwiązania techniczne umożliwiające osobom niedosłyszącym, niedowidzącym lub niewidomym zapoznanie się z treścią informacji,

m.in. poprzez powiększenie czcionki, obrazu, zmianę kontrastu. Zgodnie z § 19 rozporządzenia KRI, w systemie teleinformatycznym podmiotu realizującego zadania publiczne służące prezentacji zasobów informacji należy zapewnić spełnienie przez ten system wymagań Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia KRI.

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

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

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

Walidacja za pomocą narzędzia http://wave.webaim.org tj. walidatora WAVE-WCAG 2.0 dla strony BIP nie wykazała jakichkolwiek błędów, w przypadku portalu internetowego Urzędu – 11 błędów.
WAVE-WCAG jest narzędziem do automatycznego testowania dostępności serwisów internetowych. Pomaga projektantom i administratorom tworzyć bardziej dostępne strony internetowe. W wyniku automatycznej analizy wskazuje ewentualne miejsca, które mogą powodować problemy z dostępnością.
Brak pełnej zgodności z ustawą o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, w tym niepełne dostosowanie portalu do standardów WCAG 2.0, **należy ocenić jako uchybienie**. Przyczyną uchybienia jest brak pełnej dostępności cyfrowej stron internetowych. Skutek uchybienia - brak zapewnienia maksymalnego wsparcia osobom niepełnosprawnym. Odpowiedzialnym za powstanie uchybienia jest osoba nadzorująca stronę BIP oraz portal internetowy kontrolowanej jednostki.

[akta kontroli str. 197-198]

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

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

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

**IV. Zalecenia**

Mając na uwadze powyższe ustalenia i oceny, wnoszę o:

1) Opracowanie i stosowanie w Urzędzie pełnej dokumentacji (w postaci regulacji wewnętrznych), ustanawiającej System Zarzadzania Bezpieczeństwem Informacji, wymaganej zgodnie z § 20 ust. 1 i 3 rozporządzenia KRI.
2) Dostosowanie pomieszczenia serwerowni do standardów przewidzianych w tym zakresie - w miarę możliwości finansowych Urzędu.
3) Podjęcie działań w celu dostosowania strony BIP oraz portalu internetowego Urzędu do wymogów dostępności, w tym standardów WCAG 2.0.

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

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

WOJEWODA
WARMIŃSKO-MAZURSKI
***Artur Chojecki***
*/podpisano podpisem elektronicznym/*