WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

Olsztyn, 22 września 2023 r

Wydział Finansów i Kontroli
FK-IV.431.9.2023

Szanowny Pan
Krzysztof Szulborski
Burmistrz Miłakowa
ul. Olsztyńska 16
14 - 310 Miłakowo

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 Miłakowie[1] ul. Olsztyńska 16, 14-310 Miłakowo, NIP jednostki: 7411001387, REGON jednostki: 000535557.

- W okresie objętym kontrolą oraz w czasie prowadzonych czynności kontrolnych kierownikiem kontrolowanej jednostki był Pan **Krzysztof Szulborski** – Burmistrz, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 04.11.2018 r.

- W okresie objętym kontrolą oraz w dniu rozpoczęcia czynności kontrolnych odpowiedzialnymi za realizację zadania objętego kontrolą byli:
  - Pan **Paweł Łapa** - Informatyk, zatrudniony na podstawie umowy o pracę od dnia 10.02.2014 r.,
  - Pan **Łukasz Bylica** - Informatyk, zatrudniony na podstawie umowy o pracę od dnia 01.05.2023 r.,

- Osobą bezpośrednio nadzorującą pracowników odpowiedzialnych za realizację zadania była Pani **Justyna Zabiełło-Alaameri –** Sekretarz Gminy, zatrudniona na podstawie umowy o pracę od dnia 01.07.2007 r.

[akta kontroli poz. 24]

Kontrolę przeprowadzili pracownicy Wydziału Finansów i Kontroli Warmińsko- Mazurskiego Urzędu Wojewódzkiego w Olsztynie:
Radosław Gazda – inspektor wojewódzki; przewodniczący zespołu kontrolnego, legitymacja służbowa nr 9/2019, wydana przez Dyrektora Generalnego Warmińsko - Mazurskiego Urzędu

[1] Zwanym dalej: Urzędem

Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr FK-IV.0030.635.2023 z 14 lipca 2023 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.
Michał Wasilewski – inspektor wojewódzki; członek zespołu kontrolnego, legitymacja służbowa nr 23/2020, wydana przez Dyrektora Generalnego Warmińsko - Mazurskiego Urzędu Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr FK-IV.0030.636.2023 z 14 lipca 2023 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli poz. 9-10]

Kontrolę przeprowadzono w dniach 28 lipca – 18 sierpnia 2023 r., co zostało odnotowane w książce kontroli Urzędu pod pozycją, Nr 1/2023.

[akta kontroli poz. 25]

Kontrola prowadzona była w trybie hybrydowym, tj. w dniu w dniu 28 lipca br. – rozpoczęto czynności kontrolne w Urzędzie oraz dokonano oględziny serwerowni na miejscu w jednostce. Pozostałe dni (31 lipca – 18 sierpnia br.) kontrola była prowadzona zdalnie, bez osobistej obecności kontrolerów Urzędzie, z wykorzystaniem narzędzi informatycznych do zgromadzenia materiału dowodowego, w celu ustalenia stanu faktycznego, a następnie dokonania oceny działalności jednostki kontrolowanej, a także sformułowanie ewentualnych zaleceń pokontrolnych. W dniu rozpoczęcia czynności kontrolnych okazano legitymacje oraz upoważnienia do kontroli, poinformowano o zasadach kontroli w trybie hybrydowym, wymaganych dokumentach do kontroli oraz formach i terminie ich przekazywania.

Przedmiotem kontroli była ocena działania systemów teleinformatycznych używanych przez jednostki samorządu terytorialnego do realizacji zadań zleconych z zakresu administracji rządowej, na podstawie art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. Dz.U. z 2023 r., poz. 57 ze zm.). Okres objęty kontrolą: od 1 stycznia do 31 grudnia 2022 r.

[akta kontroli poz. 1, 20]

Kontrola została przeprowadzona na podstawie art. 2 pkt 1 i art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U. 2020 poz. 224), art. 28 ust. 1 pkt 2 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (tj. Dz. U. z 2023 r., poz. 190), w związku z art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. Dz.U. z 2023 r., poz. 57 ze zm.)[2], rozdziału III i IV Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247 ze zm.)[3], jak również Wytycznych dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych, zatwierdzonych przez Ministra Cyfryzacji w dniu 15 grudnia 2015 r.

[akta kontroli poz. 1, 20]

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

Burmistrz upoważnił Informatyka urzędu, do udzielania informacji i wyjaśnień w okresie trwania czynności kontrolnych.

[akta kontroli poz. 26]

Na podstawie ustaleń kontroli, realizację zadań z zakresu działania systemów teleinformatycznych używanych przez Urząd do realizacji zadań zleconych z zakresu administracji rządowej ocenia się **pozytywnie z uchybieniami.**
Ocena działalności jednostki kontrolowanej wynika z ustaleń i ocen dokonanych w poszczególnych obszarach (zagadnieniach) objętych kontrolą.

Z informacji przekazanych przez Urząd przed rozpoczęciem czynności kontrolnych oraz uzyskanych w trakcie prowadzenia kontroli wynika, że w Urzędzie do realizacji zadań zleconych z zakresu administracji rządowej wykorzystywane są **3** niżej wymienione systemy teleinformatyczne.

Systemy teleinformatyczne wykorzystywane w Urzędzie:

1) **SRP ŹRÓDŁO** (dwa moduły) – (moduł: Rejestr PESEL oraz Rejestr Stanu Cywilnego, moduł: 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) **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,
3) **RESPONS** – jego zadaniem jest m.in. 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.

[akta kontroli poz. 11-12]

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.

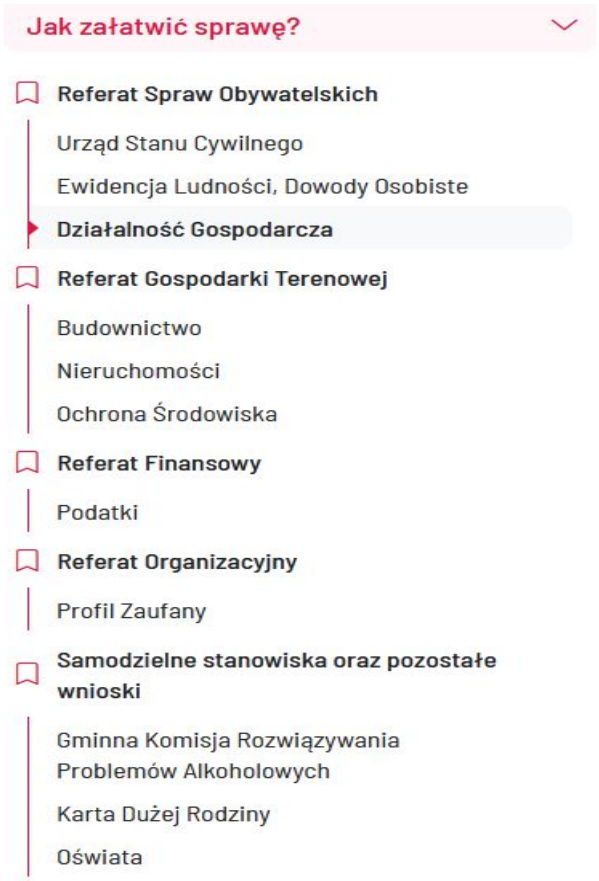
Zgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI interoperacyjność na poziomie organizacyjnym osiągana jest przez:

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 **/UMmilakowo/skrytka**, znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie i odbieranie pism w formie dokumentów elektronicznych. Na stronie BIP Urzędu, podano adres Elektronicznej Skrzynki Podawczej. Formaty danych przyjmowane za pośrednictwem Elektronicznej Skrzynki Podawczej to: DOC, RTF, DOCX, XLS, XLSX, CSV, TXT, GIF, TIF, BMP, JPG, PDF, ZIP

[akta kontroli poz. 27]

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 opublikowano zakładkę „*Jak załatwić sprawę*”



Opublikowany wykaz usług, które realizowane są przez poszczególne referaty Urzędu, z założenia miał ułatwić dostęp oraz przekazać petentom niezbędne informacje w tym zakresie. Jednocześnie należy stwierdzić, że spośród wskazanych w wykazie referatów aktywne zakładki kontrolujący stwierdzili w odniesieniu do Referatu Spraw Obywatelskich, Referatu Organizacyjnego oraz Karty Dużej Rodziny. Pozostałe zakładki w ww. wykazie nie działały. Informacje z tych zakresów można było odnaleźć dopiero w *Menu Podmiotowym* BIP. Powyższa sytuacja wymaga zmiany, tak aby petenci w jednym miejscu (zakładka - *Jak załatwić sprawę*) mogli uzyskać niezbędne informacje. Na stronie BIP opublikowane są wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych referatów w Urzędzie.

Jednocześnie kontrolujący nie stwierdzili, aby na stronie BIP zawarto opisy usług świadczonych przez Urząd drogą elektroniczną. Opisy takie powinny zawierać nazwę usługi, podstawę prawną, terminy realizacji, niezbędne dokumenty oraz komórki odpowiedzialne. Brak przedmiotowych informacji stanowi uchybienie. Przyczyna stwierdzonego uchybienia jest niestosowanie obowiązujących przepisów, tj.§ 5 ust. 2 pkt 1 i 4 rozporządzenia KRI, skutkiem – niedoinformowanie petenta o możliwości np. złożenie wniosku drogą elektroniczną. Osobą odpowiedzialna za stwierdzone uchybienie jest pracownik zarządzający stroną BIP Urzędu.

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

[akta kontroli poz. 27-33]

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się **pozytywnie z uchybieniami.**

1.2. Centralne repozytorium wzorów dokumentów elektronicznych (CRWDE)

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

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

W trakcie kontroli ustalono, że Urząd nie przekazywał do CRWDE wzorów dokumentów, jednakże. Wykorzystywał wzory dokumentów, które są obecnie dostępne na platformie ePUAP.

[akta kontroli poz. 42]

Jednocześnie, na stronie BIP w zakładkach „*Jak załatwić sprawę*" oraz Menu Podmiotowe opublikowany jest przydatny dla petentów wykaz usług, które realizowane są przez poszczególne referaty Urzędu.
Ponadto na stronie BIP opublikowane są wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych referatów w Urzędzie.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

1.3. Model usługowy

- Z § 15 ust. 2 rozporządzenia KRI wynika, że zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.

Strona internetowa Urzędu działa pod adresem https://milakowo.eu/, a strona internetowa BIP Urzędu – pod adresem https://bip.milakowo.eu/.
Na stronie głównej Portalu Urzędu, zawarto bezpośrednie odnośniki (linki) do przydatnych informacji oraz stron przeznaczonych dla mieszkańców Gminy.
Na stronie BIP w zakładkach „*Jak załatwić sprawę*" oraz *Menu Podmiotowe* opublikowany jest przydatny dla petentów wykaz usług, które realizowane są przez poszczególne referaty Urzędu.
Urząd świadczył również usługę w zakresie potwierdzenia profilu zaufanego, co daje możliwość skorzystania z usług online na wielu portalach urzędowych.

[akta kontroli poz. 34-36]

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

1.4. Współpraca systemów teleinformatycznych z innymi systemami

Stosownie do:

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

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

Z informacji uzyskanych z Urzędu wynika, że, cyt.: „*Kontrolowane systemy teleinformatyczne urzędu współpracują z publicznymi systemami teleinformatycznymi. SRP (Źródło) przekazuje za pomocą dedykowanej aplikacji ImportPesel, Rejestr Mieszkańców do aplikacji Respons. Aplikacja komunikuje się poprzez router Huawei z dedykowanym łączem na urzędowym UTM. Operacja dokonywana cyklicznie co godzinę. Szyfrowanie poprzez dedykowany certyfikat wydany przez COI.*"

[akta kontroli poz. 42]

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 wyjaśnieniem uzyskanym z Urzędy w przedmiotowej sprawie, cyt.: *„Zasady obiegu dokumentów w Urzędzie zawarte są w Regulaminie Organizacyjnym Urzędu Miejskiego w Miłakowie, Załącznik 2. Zasady obiegu elektronicznego zostaną wprowadzone wraz z realizacją projektu „E-administracja nowa jakość usług w Gminie Miłakowo", gdyż wtedy zostanie wdrożony elektroniczny obieg dokumentów. Obecnie wszystkie dokumenty przesłane w formie elektronicznej są dostosowywane do obiegu papierowego tj. drukowane."*

Odnosząc się do powyższych wyjaśnień, należy wskazać, że zapisy *Regulaminu Organizacyjnego Urzędu Miejskiego w Miłakowie* - Rozdział XI, regulują zasady obiegu, tylko i wyłącznie dokumentów papierowych. W przypadku wpływającej dokumentacji elektronicznej (e-mail, ePUAP), zasady jej obiegu nie są określone w Regulaminie.

W okazanej dokumentacji Urzędu, kontrolujący nie stwierdzili dodatkowych opracowanych procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby szczegółowe zasady obiegu dokumentów wpływających i wypływających drogą elektroniczną (w sytuacji UM Miłakowo – e-mail, ePUAP).
Zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI, opracowanie procedur umożliwia realizację i egzekwowanie, m.in. zabezpieczenia informacji, w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. Opracowanie zasad postępowania z dokumentacją elektroniczną (wnioski elektroniczne, e-maile) oraz wymagań organizacyjno-technicznych dotyczących zarządzania tą dokumentacją pozwala właściwie dbać o jej bezpieczeństwo.

W związku z powyższym brak procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby zasady obiegu dokumentów wpływających i wypływających drogą elektroniczną ocenia się jako uchybienie. Stwierdzone uchybienie skutkować może brakiem zabezpieczenia informacji, w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki.

Jednocześnie kontrolujący poddają pod rozważenie Kierownictwu kontrolowanej jednostki zastosowanie w Urzędzie elektronicznego systemu zarządzania dokumentami, który z pewnością wpłynie na usprawnienie przepływu dokumentów w podmiocie, znacząco usprawni ich archiwizację oraz zapewni łatwy dostęp do dokumentów archiwalnych, co z kolei wpłynie na przyspieszenie załatwianych spraw w tym realizowanych przez podmiot usług oraz pozwoli na minimalizowanie nakładu pracy a także podniesie poziom Bezpieczeństwa Informacji. Celem wdrożenia systemu elektronicznego zarzadzania dokumentacją jest wyeliminowanie z obiegu wewnętrznego podmiotu dokumentów papierowych, co spowodowałoby dodatkowo obniżenie kosztów.

[akta kontroli poz. 42]

Przedmiotowe cząstkowe zagadnienie ocenia się **pozytywnie z uchybieniami**.

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.: „*Wymiana danych pomiędzy SRP-Respons za pomocą dedykowanej aplikacji ImportPesel. Dane są udostępniane w powszechnych dostępnych formatach. Podpis elektroniczny Sigillum Sign-Xades; przesyłanie dokumentów do bazy aktów własnych (Prawo Miejscowe) poprzez Legislator format .zipx; przesyłanie dokumentów poprzez*

ePUAP formaty .zip, .pdf; udostępnianie dokumentów na BIP formaty .doc, .pdf .xls; Sprawozdania z jednostek podległych wysłanych poprzez ePUAP do Responsa .xml(UTF-8).”

[akta kontroli poz. 42]

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 zapewnienia jednolitego i adekwatnego systemu zarządzania bezpieczeństwem informacji (SZBI) w Urzędzie zaktualizowano i przyjęto Politykę Ochrony Danych, zarządzeniem Nr 25/2018 Burmistrza Miłakowa z dnia 25 maja 2018 r.(obowiązującą w okresie objętym kontrolą)

[akta kontroli poz. 45]

Realizacja zadań w zakresie ochrony danych wymaga od podmiotu publicznego opracowania dokumentacji SZBI (system zarządzania bezpieczeństwem informacji), w tym szeregu regulacji wewnętrznych oraz zapewnienia aktualizacji tych regulacji w zakresie dotyczącym zmieniającego się otoczenia. Kompleksowa dokumentacja Systemu Zarzadzania Bezpieczeństwem Informacji (SZBI) jest warunkiem niezbędnym, w celu skutecznego zarządzania bezpieczeństwem informacji w podmiocie. Podstawowym dokumentem SZBI jest Polityka Bezpieczeństwa Informacji. Polityka zazwyczaj zawiera wyrażoną przez kierownictwo deklarację stosowania, opisuje organizację i ustala osoby odpowiedzialne oraz ich zakresy odpowiedzialności, wprowadza klasyfikację informacji, sposób postępowania z poszczególnymi rodzajami informacji. Przyjęta w Urzędzie dokumentacja wprawdzie nie była Polityką Bezpieczeństwa Informacji, jednakże zawierała podstawowe niezbędne elementy. Kontrolujący sugerują zmianę nazwy obowiązującego dokumentu.

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

W myśl § 20 ust. 1 rozporządzenia KRI podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji.
Zgodnie z zapisami pkt 21 - przyjętej w Urzędzie POD – Polityka podlega regularnym przeglądom (nie rzadziej niż raz na rok), dokonywanym przez IOD Urzędu.
Kontrolującym przedstawiono dokumentację sporządzoną w okresie objętym kontrolą świadczącą o przeprowadzeniu oceny zgodności SZBI z rozporządzeniem KRI.
W przypadku obowiązku przyjętego zgodnie z zatwierdzoną POD, dotyczącego regularnych przeglądów przyjętej Polityki (nie rzadziej niż raz do roku), kontrolującym nie przedstawiono żadnej dokumentacji świadczącej o przeprowadzeniu przeglądu POD w okresie objętym kontrolą.
Zgodnie z wyjaśnieniem uzyskanym z Urzędu, cyt.: *„Przegląd Polityki ochrony danych wraz z sugerowanymi poprawkami, wykonany 08.07.2022 przez IOD."*
Wyniki przeglądów POD powinny być jasno udokumentowane, a odpowiednie zapisy należy przechowywać w celu ich ewentualnej weryfikacji. Brak dokumentacji świadczącej o dokonaniu koniecznego przeglądu, należy traktować jako uchybienie. Przyczyną powstania uchybienia jest brak zastosowania zasady rozliczalności wypełnienia zapisów przyjętej POD – pkt 21. Sutkiem uchybienia jest utrudniona weryfikacja i ocena wypełnienia przyjętego obowiązku, osobą odpowiedzialną jest IOD Urzędu.

[akta kontroli poz. 44, 45]

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

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

[akta kontroli poz. 46]

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

[akta kontroli poz. 47-49, 66]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego

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

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

[akta kontroli poz. 50-51]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Stosownie do:

- § 20 ust. 2 pkt 4 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
- § 20 ust. 2 pkt 5 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.

Istotnym elementem polityki BI (bezpieczeństwa informacji) jest zarządzanie dostępem do systemów teleinformatycznych przetwarzających informacje. Zarządzanie dostępem ma zapewnić, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków, a w przypadku zmiany zadań następuje również zmiana ich uprawnień.

Zasady nadawania i cofania uprawnień do przetwarzania danych osobowych oraz do pracy w określonym zbiorze danych (systemie informatycznym), określone zostały zarządzeniem Nr 25/2018 Burmistrza Miłakowa z dnia 25 maja 2018 r., w sprawie wprowadzenia Polityki Ochrony Danych – pkt 7.4 oraz 12 POD. Zgodnie z przyjętymi rozwiązaniami nowozatrudniony pracownik w chwili przystąpienia do pracy otrzymuje upoważnienie do przetwarzania danych osobowych oraz do pracy w określonych systemach informatycznych nadane przez Administratora Danych. Pracownik kadr prowadzi ewidencję nadanych upoważnień do przetwarzania danych osobowych oraz dokumentację związaną z udzielaniem upoważnień.
Osoby posiadające dostęp do danych osobowych posiadały pisemne upoważnienia do ich przetwarzania oraz do przetwarzania danych osobowych w określonym zbiorze danych wynikającym z zakresu czynności danego pracownika. Prowadzona była też ewidencja osób upoważnionych do przetwarzania danych osobowych i pracy w określonym zbiorze danych.

[akta kontroli poz. 38-39]

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.

W okresie objętym kontrolą w Urzędzie przeprowadzano szkolenia wynikające z § 20 ust. 2 pkt 6 rozporządzenia KRI, w szczególności dla osób zaangażowanych w proces przetwarzania informacji. Przeprowadzenie szkoleń dla pracowników w zakresie ochrony danych osobowych, potwierdzano lista osób uczestniczącego w szkoleniu.

[akta kontroli poz. 37]

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.

W okresie objętym kontrolą w dokumentacji przekazanej kontrolującym, nie stwierdzono opracowanych podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu

mobilnym i pracy na odległość. W przyjętej (w okresie objętym kontrolą) POD – pkt 10, opracowano wprawdzie szczątkowe zasady pracy z komputerami przenośnymi, jednakże nie obejmowały one wszystkich zasad i nie gwarantowały w pełni bezpiecznej pracy przy przetwarzaniu mobilnym świadczonym na odległość.
Zgodnie z wyjaśnieniem uzyskanym z Urzędu, cyt.: *Zasady gwarantujące bezpieczną pracę ww. przypadkach zostały zawarte w obowiązującej obecnie Polityce ochronnych danych osobowych Załącznik 7. W kontrolowanych okresie w Urzędzie nie było pracy zdalnej oraz nie były przetwarzane informacje w sposób mobilny.*

Należy jednocześnie nadmienić, że zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość opracowano podczas aktualizacji obowiązującej POD w 2023 roku, a więc poza okresem objętym kontrolą i jako takie nie mogły być uwzględnione w ramach prowadzonych czynności kontrolnych.
Brak opracowanych (w okresie objętym kontrolą) podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, stanowi uchybienie. Przyczyną powstania uchybienia jest niestosowanie przepisów § 20 ust. 2 pkt 8 rozporządzenia KRI. Skutkiem stwierdzonego uchybienia był brak adekwatnego zarządzania bezpieczeństwem informacji w okresie objętym kontrolą, osoba odpowiedzialna – IOD jednostki.

[akta kontroli poz. 42, 52]

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

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** w zakresie m.in. kompleksowej obsługi 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 poz. 53]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.8. Procedury zgłaszania incydentów naruszenia BI

Z § 20 ust. 2 pkt 13 rozporządzenia KRI wynika, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

Instrukcja postępowania w przypadku stwierdzenia zagrożenia w postaci naruszenia ochrony informacji, jak również podejmowanych działań korygujących uregulowana została zarządzeniem Nr 25/2018 Burmistrza Miłakowa z dnia 25 maja 2018 r., w sprawie wprowadzenia Polityki Ochrony Danych – Zał. nr 18 do POD.

[akta kontroli poz. 45]

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.

W dniu 18 maja 2022 r. został przeprowadzony w Urzędzie Miejskim w Miłakowie przez firmę: Centrum Bezpieczeństwa Informatycznego, audyt bezpieczeństwa informacji. Celem audytu było przedstawienie zaobserwowanego przez audytorów stanu bezpieczeństwa informacji w jednostce oraz wskazanie ewentualnych podatności mających wpływ na przetwarzane dane. Audyt został przeprowadzony pod kątem zgodności z obowiązującymi przepisami prawa w zakresie przetwarzania informacji oraz dobrych praktyk i standardów bezpieczeństwa. Audyt został zrealizowany na podstawie udostępnionej dokumentacji (procedur), sprzętu oraz w oparciu o obowiązujące przepisy prawne.
Mając powyższe na uwadze, należy stwierdzić, że obowiązek wynikający z § 20 ust. 2 pkt 14 rozporządzenia KRI który stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok – w 2022 r. został zrealizowany.

[akta kontroli poz. 54]

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.

Zgodnie z wyjaśnieniem w powyższej sprawie, cyt.: *„Procedura tworzenia kopii zapasowych zawarta w obecnej Polityce ochronnych danych osobowych - Załącznik 6. Kopie są sprawdzane 2 razy w roku. Procedura odtworzenia zawarta w obowiązującej obecnie Polityce ochronnych danych osobowych - Załącznik 6. Brak dokumentacji potwierdzającej za okres objęty kontrolą."*

Odnosząc się do powyższych wyjaśnień należy stwierdzić, że kontrolującym nie przedstawiono dokumentacji w zakresie opracowanych procedur tworzenia i testowania kopii zapasowych obowiązującej w okresie objętym kontrolą. Przedstawiona kontrolującym procedura tworzenia i testowania kopii zapasowych, stanowiąca załącznik nr 1 do Zarządzenia nr 11/2023 Burmistrza Miłakowa z dnia 06.02.2023 r. opracowana została podczas aktualizacji obowiązującej POD w 2023 roku, a więc poza okresem objętym kontrolą i jako taka nie może być uznana jako dowód i uwzględniona w ramach prowadzonych czynności kontrolnych.

Na podstawie przekazanej dokumentacji (zrzuty ekranowe), kontrolujący stwierdzili, że w Urzędzie są wykonywane kopie zapasowe z użytkowanych systemów.
W przypadku testów odtworzeniowych przydatności kopii zapasowych, podczas próby symulowanego przywrócenia i uruchomienia oprogramowania z kontrolowanych systemów, kontrolujący oparli się tylko i wyłącznie na wyjaśnieniach jednostki, gdyż w przekazanej dokumentacji nie odnaleziono dowodów świadczących o ich wykonaniu.
Mając powyższe na uwadze należy stwierdzić, że w okresie objętym kontrolą nie wytworzono dokumentacji potwierdzającej wykonanie testów odtworzeniowych oraz nie została opracowana procedura w zakresie tworzenia i testowania kopii zapasowych. Podobne wnioski w zakresie braku opracowanej procedury, zamieszczono w raporcie z audytu bezpieczeństwa informacji, za rok 2022. Brak dokumentacji świadczącej o wykonaniu testów odtworzeniowych i procedur dotyczących tworzenia i testowania kopii (w okresie objętym kontrolą), zgodnie z programem kontroli należy uznać za uchybienie, skutkujące naruszeniem § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI. Przyczyną powstania uchybienia jest niestosowanie przepisów prawa w tym zakresie. Osobami odpowiedzialnymi są IOD oraz Informatyk jednostki, pełniący funkcję w okresie objętym kontrolą.

[akta kontroli poz. 42, 55-56]

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

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się **pozytywnie 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. SRP ŹRÓDŁO, CEiDG, oraz systemy wspierające zakupione u dostawców zewnętrznych, tj. RESPONS. Na obsługę zainstalowanego w okresie objętym kontrolą oprogramowania (system informatyczny) zawarte zostały stosowne umowy licencyjne (opieka autorska), gwarantujące rozwój systemu i dostosowanie do obowiązujących przepisów prawa. Zakupiony system teleinformatyczny, w razie awarii podlega ekspertyzie technicznej zlecanej firmie dostarczającej.

[akta kontroli poz. 11-12, 53]

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 z Urzędu podczas kontroli wynika, że stosowane są następujące zabezpieczenia, cyt.: *„Urząd zabezpieczony jest alarmem. Wokół budynku zainstalowany jest monitoring. Sieć zabezpieczona przez urządzenie UTM. Konta użytkowników chronione hasłem wg. procedur ustalonych w obowiązującej obecnie Polityce ochrony danych osobowych. W Urzędzie dokonywane są regularne kopie zapasowe. Pracownicy mają ograniczony dostęp do*

stron www. Konto administratora jest wydzielone od konta użytkownika. Hasła do serwerów oraz konta admina przechowywane w wersji elektronicznej w zaszyfrowanym pliku aplikacji keepass, a wersji papierowej zdeponowane w zaplombowanej kopercie w kasie. Blokada nieautoryzowanego instalowania oprogramowania. Aktualizacje systemów dokonywane na bieżąco. Stosowanym oprogramowaniem antywirusowym jest Bitdefender."

[akta kontroli poz. 42]

Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Stosownie do:

- § 20 ust. 2 pkt 12 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: a) dbałości o aktualizację oprogramowania; b) minimalizowaniu ryzyka utraty informacji w wyniku awarii; c) ochronie przed błędami, nieuprawnioną modyfikacją; d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa; e) zapewnieniu bezpieczeństwa plików systemowych; f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych; g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa; h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
- § 20 ust. 4 rozporządzenia KRI niezależnie od zapewnienia działań, o których mowa w ust. 2, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.

W punkcie 2.12 wykazano mechanizmy jakie jednostka kontrolowana zastosowała w celu zapewnienia ochrony przetwarzanych informacji, w ramach badanych systemów teleinformatycznych przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.

Zapewniono również środki uniemożliwiające nieautoryzowany dostęp oraz zapewniające kontrolę dostępu do systemów teleinformatycznych służących do realizacji zadań zleconych z zakresu administracji rządowej, poprzez:

- w systemie SRP Źródło - logowanie odbywa się poprzez imienną kartę dostępową i indywidualne hasło dostępowe,
- w systemie CEIDG - logowanie odbywa się za pomocą certyfikatu kwalifikowanego i hasła,
- w systemie RESPONS - logowanie odbywa się za pomocą loginu i hasła.

Podczas kontroli dokonano oględzin pomieszczenia serwerowni w Urzędzie, w obecności Pana **Łukasza Bylicy** – Informatyka Urzędu. W toku oględzin stwierdzono:

- główny budynek urzędu zabezpieczony alarmem,
- okna – szyba i okucia antywłamaniowe,
- w pomieszczeniach serwerowni umieszczono przenośne urządzenie klimatyzujące,
- urządzenia serwerowe zabezpieczone za pomocą UPS-a,

- w pomieszczeniu przylegającym do serwerowni umieszczono gaśnice p-poż.

Ponadto, stwierdzono następujące **uchybienie**:

- drzwi wejściowe do serwerowni niespecjalistyczne zwykłe - wzmocnione blachą metalową oraz zabezpieczone dwoma zamkami marki Kobra,
- do pomieszczeń serwerowni dostęp ma dwóch pracowników, w tym jeden nie związany z realizacją kontrolowanego zadania - realizujący zadania obrony cywilnej,
- w pomieszczeniu serwerowni znajduje się czynna instalacja centralnego ogrzewania,
- urządzenia serwerowe nie są zainstalowane w specjalistycznych szafach lecz stoją luźno na biurku,
- w pomieszczeniu serwerowni nie stwierdzono zainstalowanych czujek monitorujących aktualną temperaturę, wilgotność oraz ewentualne zadymienie i zalanie.

Powyższe potwierdza dokumentacja fotograficzna i protokół z przeprowadzonych oględzin, stanowiące akta kontroli.

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

[akta kontroli poz. 22-23]

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 oraz przekazanej dokumentacji wynika, że w przypadku systemu RESPONS logi użytkowników są gromadzone w dzienniku systemowym i przechowywane przez okres min. 2 lat.

[akta kontroli poz. 42, 63-64]

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

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

Uwzględniając potrzeby osób niepełnosprawnych podmiot publiczny powinien zastosować w eksploatowanych systemach teleinformatycznych rozwiązania techniczne umożliwiające osobom niedosłyszącym, niedowidzącym lub niewidomym zapoznanie się z treścią informacji, m.in. poprzez powiększenie czcionki, obrazu, zmianę kontrastu. Zgodnie z § 19 rozporządzenia KRI, w systemie teleinformatycznym podmiotu realizującego zadania publiczne służące prezentacji zasobów informacji należy zapewnić spełnienie przez ten system wymagań Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia KRI.

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

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.
Strona internetowa BIP Urzędu, zawierała elementy ułatwiające korzystanie z treści na niej zawartych przez osoby niedowidzące. Zastosowane ułatwienia to:

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

Ponadto na stronie internetowej Urzędu Miejskiego w Miłakowie, można korzystać z następujących skrótów klawiaturowych:

- TAB - przejście do następnej pozycji,
- SHIFT + TAB - przejście do poprzedniej pozycji,
- ENTER - przejście do podrzędnej pozycji lub wybór pozycji,
- STRZAŁKA GÓRA/DÓŁ - nawigowanie po pozycjach w zakresie jednego poziomu,
- SPACJA - wybór pozycji,
- ESCAPE - powrót do nadrzędnej pozycji.

Dostępność cyfrowa to cecha rozwiązań cyfrowych (np. stron, aplikacji, systemów), która umożliwia samodzielne korzystanie z nich przez osoby z niepełnosprawnościami. Jednocześnie wiele jej elementów jest uniwersalnych (np. kontrast, napisy), poprawiających użyteczność każdemu, a nie tylko osobom niepełnosprawnym.
Dostępne cyfrowo muszą być między innymi strony internetowe, aplikacje mobilne, systemy teleinformatyczne i wszystkie treści publikowane w Internecie przez podmioty publiczne. To wyzwanie wdrożeniowe, ale także szansa na dotarcie z informacjami i usługami do szerokiej grupy użytkowników, w tym osób z niepełnosprawnościami.
Jednocześnie należy zaznaczyć, że pomimo tego, że dana strona zawiera podstawowe elementy umożliwiające korzystanie z treści na niej zawartych przez osoby niepełnosprawne (np. kontrast, powiększenie czcionki, wyszukiwanie), to strona ta wcale nie musi z automatu spełniać kryteriów dostępności cyfrowej.

Walidacja za pomocą narzędzia http://wave.webaim.org tj. walidatora WAVE-WCAG 2.0 dla strony BIP wykazała 1 błąd, natomiast walidacja portalu internetowego Urzędu, wykazała 8 błędów.
WAVE-WCAG jest narzędziem do automatycznego testowania dostępności serwisów internetowych. Pomaga administratorom tworzyć bardziej dostępne strony internetowe. W wyniku automatycznej analizy wskazuje ewentualne miejsca, które mogą powodować problemy z dostępnością.
Brak pełnej zgodności z ustawą o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, należy ocenić jako uchybienie. Przyczyną uchybienia jest częściowe niedostosowanie stron internetowych do standardów dostępności, w tym WCAG 2.0. Skutek uchybienia - brak zapewnienia maksymalnego wsparcia osobom niepełnosprawnym. Odpowiedzialnym za powstanie uchybienia jest osoba nadzorująca portal internetowy kontrolowanej jednostki.

[akta kontroli poz. 57-59]

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) Opublikowanie na stronie BIP opisów usług świadczonych przez Urząd drogą elektroniczną zawierających nazwę usługi, podstawę prawną, terminy realizacji, niezbędne dokumenty oraz komórki odpowiedzialne.
2) Opracowanie wewnętrznych procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby również zasady obiegu dokumentów wpływających i wypływających z Urzędu drogą elektroniczną (e-mail, ePUAP).
3) Przeprowadzanie przeglądów POD (pkt 21 POD), rzetelne ich dokumentowanie oraz przechowywanie odpowiednich zapisów, w celu ewentualnej weryfikacji.
4) Dokumentowanie wykonywania testów wytworzonych kopii zapasowych oraz

przechowywanie odpowiednich zapisów, w celu ewentualnej ich weryfikacji.

5) Dostosowanie pomieszczenia serwerowni do standardów przewidzianych w tym zakresie – w miarę możliwości finansowych Urzędu.
6) Podjęcie działań w celu dostosowania strony BIP oraz portalu internetowego Urzędu do wymogów dostępności, w tym standardów WCAG 2.0.

Jednocześnie należy wskazać, że zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, jak również procedura tworzenia kopii zapasowych oraz procedura wykonywania testów, zawarta została w obecnie obowiązującej zaktualizowanej Polityce przyjętej w 2023 roku, w związku z powyższym odstępuje się od wydania zaleceń pokontrolnych w powyższym zakresie.

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.

II WICEWOJEWODA
WARMIŃSKO-MAZURSKI
Piotr Opaczewski
/podpisano podpisem elektronicznym/