WOJEWODA
WARMIŃSKO-MAZURSKI

Olsztyn, 10 lutego 2022 r.

Wydział Finansów i Kontroli
FK-IV.431.19.2021

Szanowny Pan
Tadeusz Zbigniew Sobierajski
Burmistrz Morąga
ul. 11 Listopada 9
14-300 Morąg

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 Morągu[1], ulica 11 Listopada 9, 14-300 Morąg, NIP: 7411979704, REGON: 510743580.

W okresie objętym kontrolą oraz w czasie prowadzonych czynności kontrolnych kierownikiem kontrolowanej jednostki był Pan **Tadeusz Zbigniew Sobierajski** – Burmistrz, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 21 października 2018 roku.

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

- [redacted] Urzędu Miejskiego w Morągu, zatrudniony na podstawie umowy o pracę od dnia 2 kwietnia 2001 r.
- [redacted], zatrudniony na podstawie umowy o pracę od dnia 2 kwietnia 2001 r.
- [redacted], zatrudniona na podstawie umowy o pracę od dnia 11 lutego 2009 r. Na stanowisku Inspektora ds. Niejawnych od 16 marca 2020 r.
- [redacted], zatrudniona na podstawie umowy o pracę od 10 lutego 2019 r.

[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

Osobą bezpośrednio nadzorującą pracowników odpowiedzialnych za realizację zadania była Pani Katarzyna Zarachowicz - Sekretarz Gminy, zatrudniona na podstawie umowy o pracę od dnia 1 stycznia 2019 r.

[akta kontroli str. 43]

Kontrolę przeprowadzili pracownicy Wydziału Finansów i Kontroli Warmińsko- Mazurskiego Urzędu Wojewódzkiego w Olsztynie:
Radosław Gazda – inspektor wojewódzki; przewodniczący zespołu kontrolnego, legitymacja służbowa nr 9/2019, wydana przez Dyrektora Generalnego Warmińsko - Mazurskiego Urzędu Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr FK-IV.0030.913.2021 z 23 listopada 2021 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.
Michał Wasilewski – inspektor wojewódzki; członek zespołu kontrolnego, legitymacja służbowa nr 23/2020, wydana przez Dyrektora Generalnego Warmińsko - Mazurskiego Urzędu Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr FK-IV.0030.914.2021 z 23 listopada 2021 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 15-16]

Kontrolę przeprowadzono w dniach 8-31 grudnia 2021 r., co zostało odnotowane w książce kontroli Urzędu pod pozycją, Nr 11/2021.

Kontrola prowadzona była w trybie zdalnym, tj. bez osobistej obecności kontrolerów, z wykorzystaniem narzędzi informatycznych do zgromadzenia materiału dowodowego, w celu ustalenia stanu faktycznego, a następnie dokonania oceny działalności jednostki kontrolowanej, a także sformułowanie ewentualnych zaleceń pokontrolnych. Rozpoczęcie kontroli nastąpiło podczas wideokonferencji, w trakcie której okazano legitymacje służbowe kontrolerów, poinformowano o zasadach kontroli w trybie zdalnym, wymaganych dokumentach do kontroli oraz formach i terminie ich przekazywania. Upoważnienia kontrolerów do kontroli zostały przekazane do kontrolowanej jednostki za pośrednictwem platformy e-PUAP.

Przedmiotem kontroli była ocena działania systemów teleinformatycznych używanych przez jednostki samorządu terytorialnego do realizacji zadań zleconych z zakresu administracji rządowej, na podstawie art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2021 r., poz. 2070). Okres objęty kontrolą: od dnia 1 stycznia 2019 r. do dnia 31 grudnia 2020 r.

[akta kontroli str. 1-2, 32-42]

Kontrola została przeprowadzona na podstawie art. 2 pkt 1 i art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U. 2020 poz. 224), art. 28 ust. 1 pkt 2 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz. U. z 2019 r., poz. 1464), w związku z art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 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

[2] Zwanej dalej: ustawą

teleinformatycznych (Dz.U. z 2017 r. poz. 2247 ze zm.)[3], jak również Wytycznych dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych, zatwierdzonych przez Ministra Cyfryzacji w dniu 15 grudnia 2015 r.

[akta kontroli str. 1-2, 32-42]

Burmistrz Morąga upoważnił Informatyka Urzędu Miejskiego w Morągu, do udzielania informacji w okresie trwania czynności kontrolnych.
[akta kontroli str. 60]

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

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

[redacted]

Systemy teleinformatyczne wykorzystywane w Urzędzie:

[redacted]

[3] Zwanego dalej: rozporządzeniem KRI

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

Zgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI interoperacyjność na poziomie organizacyjnym osiągana jest przez publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.
W zakresie publikacji procedur załatwiania spraw realizowanych przez Urząd należy stwierdzić, że na stronie BIP w zakładce e-Urząd, opublikowany jest wykaz usług przydatnych dla mieszkańców, które można zrealizować w Urzędzie Miejskim w Morągu drogą elektroniczną korzystając
z platformy ePUAP. Zakładka podzielona jest na dwie podzakładki, tj. strefa mieszkańca i strefa przedsiębiorcy, gdzie po wyborze konkretnej usługi i zalogowaniu do e-PUAP, udostępniona zostaje procedura załatwienia danej sprawy.

Ponadto na stronie BIP w zakładce Poradnik interesanta opublikowane są wzory wniosków i formularzy niezbędnych do załatwienia wybranej sprawy, 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.
Ponadto Urząd udostępniał oraz świadczył również usługi elektroniczne, z wykorzystaniem ePUAP, tj. „Pismo ogólne do podmiotu publicznego". Usługa te umożliwiają złożenie do wybranego organu administracji publicznej pisma w sprawie.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 61-65]

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 w okresie objętym kontrolą Urząd nie przekazywał wzorów dokumentów elektronicznych do centralnego repozytorium wzorów dokumentów prowadzonego przez Ministerstwo Cyfryzacji, ze względu na fakt nie uruchomienia nowej usług dla których nie ma wzorów dokumentów w CRWDE. Z informacji uzyskanej podczas kontroli wynika, że cyt.: „Urząd w latach objętych kontrolą (2019-2020) nie przekazywał do CRWD wzorów dokumentów. Wzory dokumentów do CRWD były przekazywane przez nasz Urząd w latach 2014-2015. Były to deklaracje na podatek leśny, rolny i od nieruchomości oraz wniosek o rozłożenie należności na raty, odroczenie terminu, umorzenie zaległości, umorzenie odsetek. Urząd nie korzystał ze wzorów dokumentów zamieszczonych w CRWDE."

Jednocześnie należy zaznaczyć, że na stronie BIP Urzędu opublikowano w zakładce Poradnik interesanta wersje „do pobrania" formularzy oraz wzorów dokumentów niezbędnych do załatwienia poszczególnych spraw w Urzędzie.
W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 45-53, 179-188]

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 http://www.morag.pl/, a strona internetowa BIP Urzędu – pod adresem https://bip.morag.pl/#.
Na stronie internetowej Urzędu zamieszczono bezpośredni link do strony BIP Urzędu, w prawej części panelu strony. Na stronie głównej BIP Urzędu w zakładce e-Urząd, zamieszczono bezpośredni link do platformy ePUAP oraz adres skrytki ESP.

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.: „[redacted]

[akta kontroli str. 179-188]

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.

Z uzyskanego w ramach prowadzonych czynności kontrolnych wyjaśnienia wynika, że cyt.: „W Urzędzie Miejskim w Morągu Zarządzeniem nr 31/2011 Burmistrza Morąga z dnia 24 stycznia 2011 roku w sprawie: określenia sposobu wykonywania czynności kancelaryjnych i wyznaczenia koordynatora czynności kancelaryjnych, został ustalony system tradycyjny jako podstawowy sposób dokumentowania przebiegu załatwiania i rozstrzygania spraw. W związku z tym, regulacje w zakresie obiegu dokumentów wpływających i wypływających w formie elektronicznej reguluje Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych."

W Urzędzie w celu zarządzania obiegiem dokumentów i dokumentacją stosowane są procedury i zasady postępowania z dokumentami wpływającymi do Urzędu zawarte w Instrukcji Kancelaryjnej, stanowiącej załącznik do rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych. Zgodnie z zarządzeniem nr 31/2011 Burmistrza Morąga z dnia 24 stycznia 2011 roku w sprawie: określenia sposobu wykonywania czynności kancelaryjnych i wyznaczenia koordynatora czynności kancelaryjnych - podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw w Urzędzie jest tradycyjny system wykonywania czynności kancelaryjnych. Jednocześnie, w okazanej dokumentacji Urzędu brak jest procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby szczegółowe zasady obiegu dokumentów wpływających i wypływających drogą elektroniczną oraz zakres stosowania elektronicznego obiegu dokumentów (skrzynka podawcza na platformie ePUAP), co zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI, umożliwiłoby realizację i egzekwowanie, m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. 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 przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki.

[akta kontroli str. 179-188]

1.6. Formaty danych udostępniane przez systemy teleinformatyczne

Stosownie do:

- § 17 ust. 1 rozporządzenia KRI kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków, odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz ze zmianami lub normę ją zastępującą;
- § 18 ust. 1 rozporządzenia KRI systemy teleinformatyczne podmiotów realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia;
- § 18 ust. 2 rozporządzenia KRI jeżeli z przepisów szczegółowych albo opublikowanych w repozytorium interoperacyjności schematów XML lub innych wzorów nie wynika inaczej, podmioty realizujące zadania publiczne umożliwiają przyjmowanie dokumentów

elektronicznych służących do załatwiania spraw należących do zakresu ich działania w formatach danych określonych w załącznikach nr 2 i 3 do rozporządzenia.

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

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

[akta kontroli str. 179-188]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie nie podlegało ocenie.

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", zarządzeniem Nr 769/18 Burmistrza Morąga z dnia 22 maja 2018 roku, w sprawie wprowadzenia dokumentacji zasad przetwarzania i bezpieczeństwa danych osobowych w Urzędzie Miejskim w Morągu, wprowadzono zasady przetwarzania danych osobowych oraz stosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych i przyjęto następującą dokumentację:

[redacted]

[akta kontroli str. 232-251]

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 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. 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 zarządzania 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.

Na podstawie przekazanej dokumentacji kontrolujący stwierdzili, że w okresie objętym kontrolą w Urzędzie nie została opracowana pełna dokumentacja ustanawiająca System Zarządzania Bezpieczeństwem Informacji, wymagana zgodnie z § 20 ust. 1 rozporządzenia KRI zapewniająca poufność, dostępność i integralność informacji.

Opracowane i wdrożone w 2018 r. w Urzędzie Miejskim w Morągu zarządzenie Burmistrza Miasta Morąga w sprawie wprowadzenia dokumentacji zasad przetwarzania i bezpieczeństwa danych osobowych, nie obejmowało wszystkich informacji jakie są przetwarzane w Urzędzie, lecz tylko dane osobowe. Polityka ochrony danych osobowych stanowi tylko jedną ze składowych dokumentacji ustanawiającej SZBI w jednostce i nie dopełnia obowiązku wynikającego z cytowanych powyżej przepisów.
Z wyjaśnienia Burmistrza w powyższej sprawie wynika, że, cyt.: „

[akta kontroli str. 179-188]

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.
Z wyjaśnienia Burmistrza wynika, że, cyt.:

Mając na względzie okres objęty kontrolą, na podstawie udostępnionej dokumentacji stwierdzono, że w 2020 r. w Urzędzie były podejmowane pewne działania dotyczące utrzymania oraz zarządzania bezpieczeństwem informacji w zakresie jego monitoringu oraz przeglądu.
Z wyjaśnienia Burmistrza wynika, że, cyt.:

[akta kontroli str. 179-188, 206-222]

Odnosząc się do powyższych wyjaśnień należy stwierdzić, że wskazanej w wyjaśnieniach kontroli w zakresie zabezpieczenia komputerów hasłami osobistymi oraz legalności zainstalowanego oprogramowania, z dnia 18. 02. 2019 r. zgodnie z dokumentacją przedłożoną kontrolującym nie przeprowadzono w 2019 r. a w roku 2020. Ponadto część wskazanych w wyjaśnieniach sprawdzeń dokonano poza okresem objętym kontrolą. Mając powyższe na uwadze na podstawie udostępnionej do kontroli dokumentacji kontrolujący stwierdzili, że oprócz działań automatycznych wykonywanych zdalnie przez system [redacted], w Urzędzie w 2019 r. nie były prowadzone dodatkowe działania w postaci kontroli i sprawdzeń, w zakresie utrzymania oraz zarządzania bezpieczeństwem informacji obejmujące jego monitoring i przegląd, co stanowi uchybienie.
Brak okresowych przeglądów i monitoringu SZBI w jednostce skutkuje naruszeniem § 20 ust. 1 rozporządzenia KRI. Osobą odpowiedzialną jest IOD jednostki pełniący funkcję w okresie objętym kontrolą.

Burmistrz zarządzeniem Nr 115/15 z dnia 16 czerwca 2015 r. wyznaczył Administratora Systemu Informatycznego w Urzędzie (ASI). Zarządzeniem Nr 768/18 Burmistrza Morąga z dnia 22 maja 2018 roku wyznaczony został w jednostce Inspektora Ochrony Danych (IOD).

[akta kontroli str. 228-231]

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.

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 w okresie objętym kontrolą analizy ryzyka utraty integralności, dostępności lub poufności informacji.
[akta kontroli str. 67-71]

W toku prowadzonych czynności kontrolnych stwierdzono również, że w jednostce prowadzono rejestr czynności przetwarzania danych osobowych. Przedmiotowy rejestr został opracowany i jest prowadzony przez IOD,

[akta kontroli str. 72-99]

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.

Z wyjaśnienia Burmistrza przedstawionego w powyższej sprawie wynika, że cyt.: [redacted]

Przedstawiona kontrolującym w formie elektronicznej inwentaryzacja sprzętu komputerowego użytkowanego w Urzędzie zawierała: nazwę sprzętu, ilość sztuk, numer inwentarzowy oraz imię i nazwisko pracownika użytkującego dany sprzęt. Przedmiotowa inwentaryzacja nie została sporządzona zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI, gdyż nie obejmowała między innymi rodzaju i konfiguracji sprzętu komputerowego. Na podstawie tak prowadzonej inwentaryzacji nie byłoby możliwe sprawne odtworzenie infrastruktury informatycznej, w przypadku wystąpienia katastrofy lub innego zdarzenia losowego.
Zgodnie z wyjaśnieniem oprócz wykazu sprzętu komputerowego w formie elektronicznej (nie obejmującego danych określonych w §20 ust. 2 pkt 2 rozporządzenia KRI), prowadzona jest również inwentaryzacja za pomocą [redacted]. Zgodnie z przekazanymi zrzutami ekranu zestawienie obejmuje parametry określone w §20 ust. 2 pkt 2 rozporządzenia KRI. Na podstawie tak prowadzonej inwentaryzacji byłoby możliwe sprawne odtworzenie infrastruktury informatycznej Urzędu.

[akta kontroli str. 100-101, 223-226]

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.

Uproszczone zasady nadawania uprawnień do przetwarzania danych osobowych oraz do pracy w określonym zbiorze danych (systemie informatycznym) określone zostały Zarządzeniem nr 769/18 Burmistrza Morąga z dnia 22 maja 2018 roku w sprawie wprowadzenia dokumentacji zasad przetwarzania i bezpieczeństwa danych osobowych w Urzędzie Miejskim w Morągu – Rozdział IV pkt 2 lit d oraz w Instrukcji określającej sposób zarządzania systemem informatycznym - Rozdział III pkt 2.

[akta kontroli str. 232-260]

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

[akta kontroli str. 102-121, 189-194]

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 2 szkoleniach, dotyczących m.in. ochrony danych osobowych:

1) Szkolenie w zakresie cyberbezpieczeństwa w samorządach, przeprowadził Informatyk Urzędu w dniu 19.12.2019 r.
2) Szkolenie w zakresie bezpiecznego łączenia się z siecią wewnętrzną Urzędu Miejskiego w Morągu oraz zasad pracy zdalnej, przeprowadził Informatyk Urzędu w dniu 10.09.2020 r. Przedmiotowe szkolenie zgodnie z uzyskaną informacją, obejmowały swym zakresem następujące zagadnienia:
   a) Warunki podjęcia pracy zdalnej - obowiązki pracownicze podczas pracy zdalnej, zasady świadczenia pracy zdalnej.
   b) Warunki jakie musi spełniać miejsce świadczenia pracy zdalnej - organizacja pracy oraz przygotowanie stanowiska pracy przed rozpoczęciem i w trakcie pracy zdalnej.
   c) Bezpieczeństwo pracy zdalnej:
      - Internet - techniczne aspekty pracy zdalnej, właściwe wykorzystanie sieci internetowej podczas pracy zdalnej, bezpieczeństwo i właściwe zabezpieczenie sieci internetowej podczas pracy zdalnej.
      - Urządzenia służące do pracy zdalnej - zabezpieczenie urządzeń do: pracy zdalnej, aktualizacje oprogramowania, programy antywirusowe.

- Zabezpieczanie przekazywanych informacji - bezpieczeństwo przekazywanych danych, logowania i hasła, bezpieczne korzystanie z poczty mailowej.

d) Zasady korzystania z dokumentów w formie papierowej - kopiowanie dokumentów, zabezpieczenie i bezpieczeństwo dokumentów, zasady rozliczania się z pobranej dokumentacji.
e) Szczególne sytuacje - Problemy techniczne, zagubienie sprzętu, kradzież sprzętu.
f) Przypomnienie ogólnych zasad przetwarzania i bezpieczeństwa danych osobowych w Urzędzie Miejskim w Morągu zawartych w Zarządzeniu Nr 769/18 Burmistrza Morąga z dnia 22 maja 2018 r.

W załączeniu przedstawiono listy obecności pracowników uczestniczących w szkoleniach.

[akta kontroli str. 122-165]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.6. Praca na odległość i mobilne przetwarzanie danych

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

Z wyjaśnienia Burmistrza wynika, że cyt.: [redacted]

Szkolenie pracowników Urzędu Miejskiego w Morągu z bezpiecznego łączenia się z siecią wewnętrzną Urzędu oraz zasad pracy zdalnej i bezpieczeństwa informacji w dniu 10 września 2020 r. przeprowadził informatyk Urzędu Miejskiego w Morągu (...)."

[akta kontroli str. 122-138, 179-188, 272-275]

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.

[redacted]

[redacted] stosowne umowy licencyjne umożliwiające prawidłową eksploatację i rozwój systemu poprzez możliwość zgłaszania błędów pytań i roszczeń dotyczących użytkowanego systemu. Zawarta została również stosowna umowa powierzenia danych gwarantująca właściwe zabezpieczenie danych w przypadku awarii systemu oraz gwarantująca bezpieczeństwo informacji uzyskanych przez wykonawcę w związku
z realizacją umowy.

[akta kontroli str. 166-173, 261-271]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.8. Procedury zgłaszania incydentów naruszenia BI

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

Instrukcja postępowania w przypadku stwierdzenia zagrożenia w postaci naruszenia ochrony danych osobowych oraz podejmowanych działań korygujących została uregulowana w załączniku nr 3 (Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych) do zarządzenia nr 769/18 Burmistrza Morąga z dnia 22 maja 2018 roku w sprawie wprowadzenia dokumentacji zasad przetwarzania i bezpieczeństwa danych osobowych w Urzędzie Miejskim w Morągu

[akta kontroli str. 232-260]

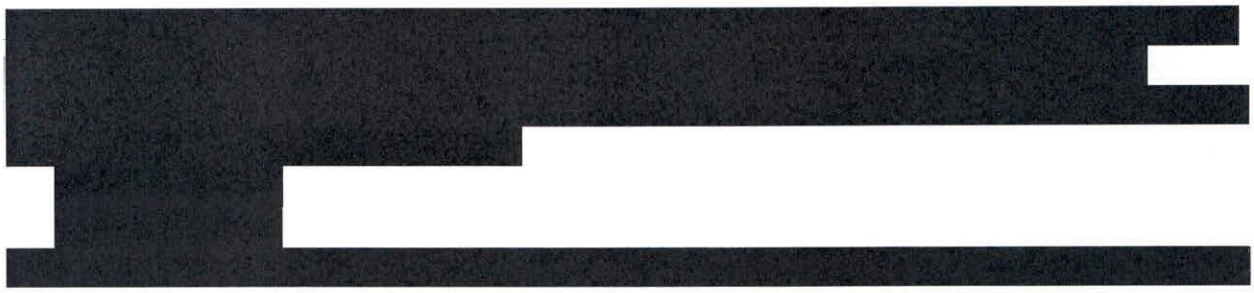
Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

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

Na podstawie okazanej dokumentacji kontrolujący stwierdzili, że w okresie objętym kontrolą tj. od 1 stycznia 2019 r. do dnia 31 grudnia 2020 r., w jednostce nie przeprowadzano audytów wewnętrznych w zakresie bezpieczeństwa informacji zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI

Z informacji uzyskanych z Urzędu w przedmiotowej sprawie wynika, że: „[redacted]



[akta kontroli str. 179-188]

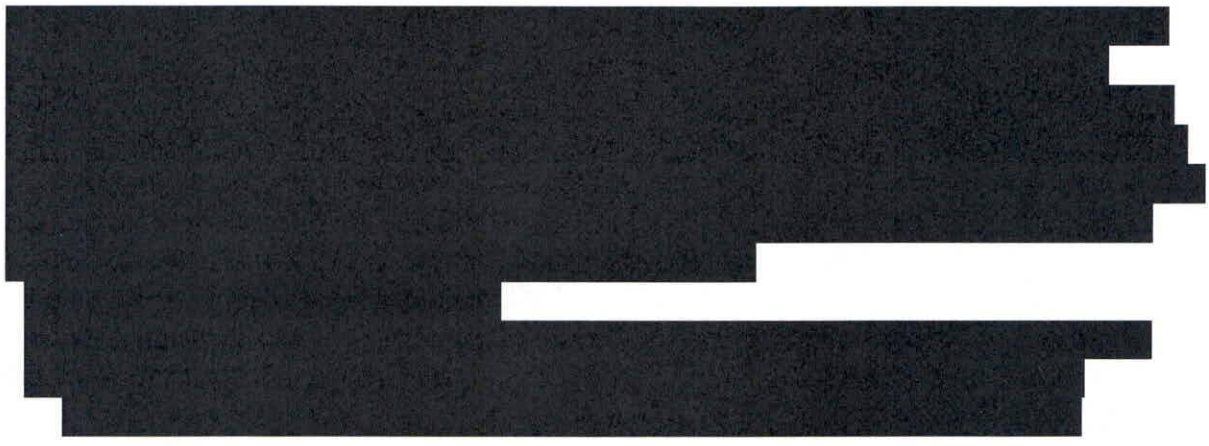
Odnosząc się do przekazanych wyjaśnień należy stwierdzić, że przedmiotowe kontrole o których mowa w wyjaśnieniach nie stanowią audytu bezpieczeństwa informacji zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI. Brak przeprowadzenia audytów wewnętrznych w zakresie bezpieczeństwa informacji w 2019 i 2020 r. skutkuje niedopełnieniem obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI. Osobą odpowiedzialną za powstanie nieprawidłowości jest IOD kontrolowanej jednostki.

Przedmiotowe cząstkowe zagadnienie ocenia się negatywnie.

2.10. Kopie zapasowe

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

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



Na podstawie udostępnionej dokumentacji kontrolujący stwierdzili, że w Urzędzie są wykonywane kopie zapasowe (zgodnie z założeniami Instrukcji) oraz testy w celu sprawdzenia poprawności wykonywania kopii zapasowych oraz przydatności utworzonych kopii podczas próby symulowanego przywrócenia i uruchomienia oprogramowania po przywróceniu.

[akta kontroli str. 174-175, 179-188, 227]

Należy wskazać, że regularne wykonywanie i testowanie jakości kopii zapasowych jest kluczowym działaniem w celu minimalizowania ryzyka utraty informacji w wyniku awarii. Wskazane jest przechowywanie kopii zapasowych w innej lokalizacji niż miejsce ich tworzenia.

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.

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 166-173, 261-271]

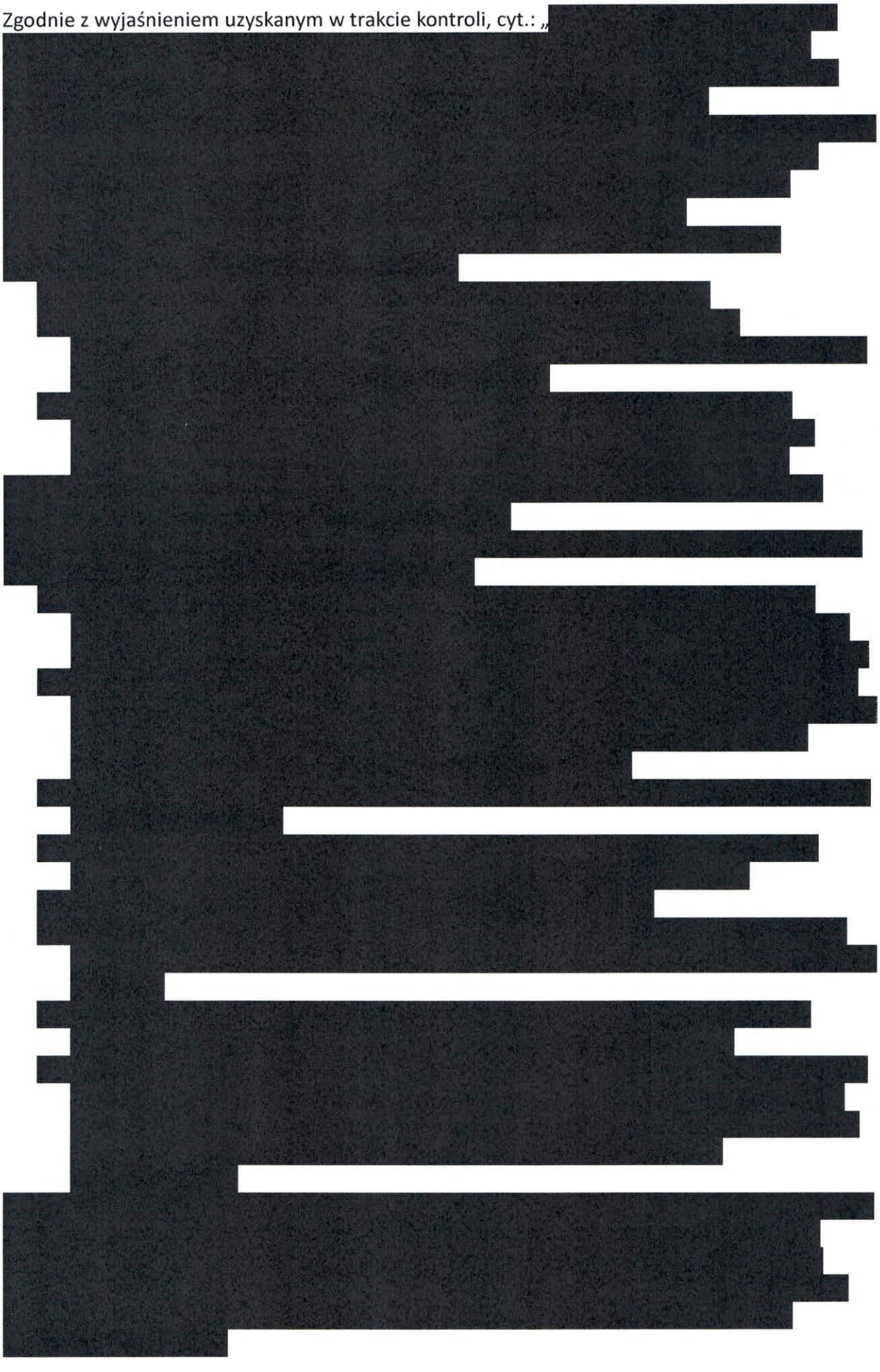
2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji

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.

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



[akta kontroli str. 179-188]

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.

[redacted]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.14. Rozliczalność działań w systemach informatycznych

Stosownie do:

- § 21 ust. 2 rozporządzenia KRI w dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do: 1) systemu z uprawnieniami administracyjnymi; 2) konfiguracji systemu, w tym konfiguracji zabezpieczeń; 3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa;
- § 21 ust. 3 rozporządzenia KRI poza informacjami wymienionymi w § 21 ust. 2 rozporządzenia KRI są odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci: 1) działań użytkowników

nieposiadających uprawnień administracyjnych, 2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu, 3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny – w zakresie wynikającym z analizy ryzyka;

- § 21 ust. 4 rozporządzenia KRI informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.

Zgodnie z § 21 ust. 1 KRI, rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach).

[redacted]

Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 179-188]

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

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

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

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

- możliwość doboru odpowiedniego kontrastu,
- możliwość powiększenia wielkości liter na stronie,
- moduł wyszukiwania.

[redacted]

[akta kontroli str. 276-277]

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny wnoszę o:

1. Opracowanie wewnętrznych procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby również zasady obiegu dokumentów wpływających i wypływających z Urzędu drogą elektroniczną.

[redacted]

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

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

WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki
/podpisano podpisem elektronicznym/