WOJEWODA
WARMIŃSKO-MAZURSKI

Olsztyn, 23 marca 2022 r.

Wydział Finansów i Kontroli
FK-IV.431.1.2022

Szanowny Pan
Ryszard Henryk Niedziółka
Burmistrz Miasta Kętrzyn
ul. Wojska Polskiego 11
11-400 Kętrzyn

Stosownie do art. 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U. 2020 poz. 224), przekazuję Panu treść wystąpienia pokontrolnego.

Wystąpienie pokontrolne

Kontrolę przeprowadzono w Urzędzie Miasta Kętrzyn[1], ul. Wojska Polskiego 11, 11-400 Kętrzyn, NIP jednostki 742-000-83-48, REGON jednostki: 000524387.

- W okresie objętym kontrolą oraz w czasie prowadzonych czynności kontrolnych kierownikiem kontrolowanej jednostki był Pan **Ryszard Henryk Niedziółka** – Burmistrz, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 4 listopada 2018 roku.

- W dniu rozpoczęcia czynności kontrolnych odpowiedzialnymi za realizację zadania objętego kontrolą w Urzędzie był [redacted]

- Osobą bezpośrednio nadzorującą pracownika odpowiedzialnego za realizację zadania była [redacted]

[akta kontroli str. 74]

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.0030.30.2022 z 19 stycznia 2022 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[1] Zwanym dalej: Urzędem

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.0030.31.2022 z 19 stycznia 2022 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 16-17]

Kontrolę przeprowadzono w dniach 28 stycznia – 18 lutego 2022 r., co zostało odnotowane w książce kontroli Urzędu pod pozycją, Nr 1/2022.

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, 47-51]

Kontrola została przeprowadzona na podstawie art. 2 pkt 1 i art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U. 2020 poz. 224), art. 28 ust. 1 pkt 2 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz. U. z 2022 r., poz. 135), w związku z art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2021 r., poz. 2070)[2], rozdziału III i IV Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247 ze zm.)[3], jak również Wytycznych dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych, zatwierdzonych przez Ministra Cyfryzacji w dniu 15 grudnia 2015 r.

[akta kontroli str. 1-2, 47-51]

Burmistrz Kętrzyna upoważnił Sekretarza Miasta oraz Inspektora Urzędu Miasta Kętrzyn odpowiedzialnego za realizację zadania, do udzielania informacji w okresie trwania czynności kontrolnych.

[akta kontroli str. 75-78]

---

[2] Zwanej dalej: ustawą

[3] Zwanego dalej: rozporządzeniem KRI

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

Z informacji przekazanych przez Urząd przed rozpoczęciem czynności kontrolnych oraz uzyskanych w trakcie prowadzenia kontroli wynika, że w Urzędzie do realizacji zadań zleconych z zakresu administracji rządowej wykorzystywanych jest 6 niżej wymienionych systemów teleinformatycznych.

Systemy teleinformatyczne wykorzystywane w Urzędzie:

[redacted]

[akta kontroli str. 44-46]

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 /280801/skrytka, znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie i odbieranie pism w formie dokumentów elektronicznych. Ścieżkę bezpośredniego przejścia na główną stronę e-PUAP, zawarto na stronie internetowej BIP Urzędu. Formaty danych przyjmowane za pośrednictwem Elektronicznej Skrzynki Podawczej to m.in.: DOC, RTF, XLS, CSV, TXT, GIF, TIF, BMP, JPG, PDF, ZIP.

Zgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI interoperacyjność na poziomie organizacyjnym osiągana jest przez publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.
W zakresie publikacji procedur załatwiania spraw realizowanych przez Urząd należy stwierdzić, że na stronie BIP w zakładce „Procedury załatwiania spraw", opublikowany jest przydatny dla petentów wykaz usług, które realizowane są przez poszczególne wydziału Urzędu, w tym również te które możliwe są do zrealizowania drogą elektroniczną korzystając z platformy ePUAP. Zakładka podzielona jest na dwie podzakładki, tj. „wydziały/stanowiska" oraz „sprawy".

Ponadto na stronie BIP w zakładce „Procedury załatwiania spraw", opublikowane są wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych wydziałów w Urzędzie.
Jednocześnie należy zaznaczyć, że Urząd nie świadczył usług związanych z załatwianiem spraw od początku do końca w formie elektronicznej, za pomocą systemów teleinformatycznych. 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. 23-31, 79-80]

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 Urząd nie przekazywał do CRWDE wzorów dokumentów oraz nie korzystał ze wzorów zamieszczonych w CRWDE.
Jednocześnie należy zaznaczyć, że na stronie BIP w zakładce „Procedury załatwiania spraw", opublikowane są wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych wydziałów w Urzędzie.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 23-31, 79-80, 211-214]

1.3. Model usługowy

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

Strona internetowa Urzędu działa pod adresem https://www.miastoketrzyn.pl/, a strona internetowa BIP Urzędu – pod adresem https://bip.miastoketrzyn.pl/
Na stronie internetowej Urzędu zamieszczono bezpośredni link do strony BIP Urzędu, w prawej górnej części panelu strony. Na stronie głównej BIP Urzędu w zakładce „witamy", zamieszczono bezpośredni link do platformy ePUAP oraz adres skrytki ESP. Strona internetowa Urzędu zawiera wiele zakładek (panel „na skróty") ułatwiających bezpośrednie przeniesienia zainteresowanych do strony z poszukiwanymi informacjami.

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. 211-214]

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 zarządzeniem Nr 166/2014 Burmistrza Miasta Kętrzyna z dnia 27 czerwca 2014 r. w sprawie wprowadzenia w Urzędzie Miasta Kętrzyn procedury elektronicznego obiegu dokumentów w ramach aplikacji Elektronicznego Obiegu Dokumentów PROTON, zmienionego zarządzeniem Nr 18/2014 Burmistrza Miasta Kętrzyna z dnia 31 grudnia 3014 r., podstawowym systemem wykonywania czynności kancelaryjnych w Urzędzie Miasta Kętrzyn jest system tradycyjny. Z dniem 1 lipca 2014 r. wprowadzono w Urzędzie procedurę obiegu dokumentów i spraw w aplikacji elektronicznego obiegu dokumentów. Opracowano podstawowe zasady elektronicznego obiegu dokumentów stanowiące załącznik do zarządzenia, obejmujące swym zakresem również dokumentację wpływającą do Urzędu poprzez skrzynkę ESP oraz pocztę elektroniczną. [redacted]. System opracowano zgodnie z instrukcją kancelaryjną oraz w oparciu o Jednolity Rzeczowy Wykaz Akt (JRWA).
Opracowanie procedur dotyczących wykonywania czynności kancelaryjnych, w których określone są szczegółowe zasady obiegu dokumentów wpływających i wypływających drogą elektroniczną oraz zakres stosowania elektronicznego obiegu dokumentów (skrzynka podawcza na platformie ePUAP oraz poczta elektroniczna), zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI, umożliwia realizację i egzekwowanie, m.in. zabezpieczenia informacji w sposób

uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. 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

[akta kontroli str. 81-91]

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. 211-214]

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

II. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych

2.1. Dokumenty z zakresu bezpieczeństwa informacji

Zgodnie z:

- § 20 ust. 1 rozporządzenia KRI podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system

zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;

- § 20 ust. 2 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań związanych z bezpieczeństwem informacji;
- § 20 ust. 2 pkt 1 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

Realizacja 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.

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 358/2020 Burmistrza Miasta Kętrzyn z dnia 30 listopada 2020 roku, w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Miasta Kętrzyn, przyjęto następującą dokumentację:

[redacted]

[akta kontroli str. 92-167]

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.

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

[redacted]".

Z powyższych wyjaśnień wynika, że w Urzędzie w 2021 r. nie były prowadzone dodatkowe działania w postaci kontroli oraz sprawdzeń, w zakresie utrzymania oraz zarządzania bezpieczeństwem informacji obejmujące jego monitoring i przegląd. Powyższe 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 oraz informatyk urzędu.

Burmistrz zarządzeniem Nr 82/2020 z dnia 31 marca 2020 r. powołał Administratora Systemu Informatycznego w Urzędzie (ASI). Zarządzeniem Nr 154/2018 Burmistrza Miasta Kętrzyn z dnia 24 maja 2018 roku powołany został w jednostce Inspektora Ochrony Danych (IOD). Podpisane zostały również stosowne umowy wyznaczające zakres obowiązków powołanego IOD.

[akta kontroli str. 168-183, 211-214]

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.

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 nie przedstawiono dokumentacji świadczącej o przeprowadzeniu w okresie objętym kontrolą analizy ryzyka utraty integralności, dostępności lub poufności informacji.
Z informacji uzyskanych z Urzędu wynika, że, cyt.: „[redacted]".

Odnosząc się do wyjaśnienia należy stwierdzić, że 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.
W związku z powyższym brak przeprowadzonej okresowej analizy ryzyka należy uznać za nieprawidłowość skutkującą naruszeniem § 20 ust. 2 pkt 3 rozporządzenia KRI. Osobą odpowiedzialną jest pracownik pełniący obowiązki IOD w tym okresie.

[akta kontroli str. 211-214]

[redacted]

Brak w 2021 r. rejestru czynności przetwarzania danych osobowych stanowi nieprawidłowość skutkującą naruszeniem art. 30 RODO oraz rozdziału I pkt 4 (załącznik Nr 1) przyjętej PBI. Przyczyna powstania nieprawidłowości był brak stosowania obowiązujących przepisów oraz przyjętej PBI. Osobą odpowiedzialną jest pracownik pełniący obowiązki IOD w tym okresie.

[akta kontroli str. 92-157, 211-214]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się negatywnie.

2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego

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

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

[akta kontroli str. 211-214, 215-223]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Stosownie do:

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

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

Zasady nadawania uprawnień do przetwarzania danych osobowych oraz do pracy w określonym zbiorze danych (systemie informatycznym), wzory wniosków oraz wzory upoważnień określone zostały zarządzeniem 358/2020 Burmistrza Miasta Kętrzyn z dnia 30 listopada 2020 roku, w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Miasta Kętrzyn – rozdział II-VI PBI oraz pkt 6 IZSI.

[akta kontroli str. 92-157]

Osoby posiadające dostęp do danych osobowych i pracujące w określonym systemie 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. 192-208, 224-232]

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 3 szkoleniach, dotyczących ochrony danych osobowych:

1) Szkolenie „Ochrona danych osobowych na gruncie RODO", przeprowadził IOD w dniu 04.02.2021 r.
2) Szkolenie „Naruszenia ochrony danych osobowych", przeprowadził IOD w dniu 16.09.2021 r.
3) Szkolenie „Ochrona danych osobowych", przeprowadził IOD w dniu 16.09.2021 r.

Zgodnie z przekazanymi materiałami program szkoleń obejmował:

- Definicje dot. Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.
- Definicje dot. Ustawy o ochronie danych osobowych z dnia 10 maja 2018 r.
- Legalność przetwarzania danych osobowych.
- Obowiązek informacyjny.
- Zasady ujawniania oraz powierzania danych osobowych.
- Prowadzenie rejestru czynności przetwarzania.
- Przepisy karne.
- Przegląd zbiorów danych osobowych oraz programów służących do ich przetwarzania.
- Przegląd treści Polityki Ochrony Danych Osobowych.

- Zabezpieczenia fizyczne obszarów przetwarzania.
- Zasady bezpiecznego użytkowania sprzętu IT.
- Zasady bezpiecznego korzystania z oprogramowania.
- Zasady bezpiecznego korzystania z Internetu.
- Zasady bezpiecznego korzystania z poczty elektronicznej.
- Nadawanie upoważnień do przetwarzania danych osobowych.
- instrukcja postępowania w przypadku wystąpienia incydentu.
- Postępowanie dyscyplinarne.

W załączeniu przedstawiono listy obecności pracowników uczestniczących w szkoleniach.

[akta kontroli str. 184-191, 233-234]

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 Urzędzie Miasta Kętrzyn wraz z zarządzeniem 358/2020 Burmistrza Miasta Kętrzyn z dnia 30 listopada 2020 roku, w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Miasta Kętrzyn, przyjęto Regulamin użytkowania komputerów przenośnych, stanowiących zbiór zasad do stosowania podczas wykorzystywania sprzętu przenośnego.
Zgodnie z informacją przekazaną z Urzędu, w okresie objętym kontrolą pracę zdalną świadczyło ok. czterdziestu pracowników.

[akta kontroli str. 92-157, 211-214]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.7. Serwis sprzętu informatycznego i oprogramowania

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

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

W Urzędzie użytkowane są dwa systemy teleinformatyczne przeznaczone do realizacji zadań zleconych z zakresu administracji rządowej zakupione u zewnętrznych dostawców, tj.:

- [redacted].

- [redacted]

W związku z zakupem ww. systemów 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 gwarantująca bezpieczeństwo informacji uzyskanych przez wykonawcę w związku z realizacją umowy.

Zgodnie z pkt 11 Instrukcji Zarządzania Systemem Informatycznym, będącej załącznikiem do zarządzeniem 358/2020 Burmistrza Miasta Kętrzyn z dnia 30 listopada 2020 roku, w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Miasta Kętrzyn:

[redacted]

[akta kontroli str. 158-167, 211-214, 235-351]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.8. Procedury zgłaszania incydentów naruszenia BI

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

Instrukcja postępowania w przypadku stwierdzenia zagrożenia w postaci naruszenia ochrony danych osobowych oraz podejmowanych działań korygujących została uregulowana zarządzeniem 358/2020 Burmistrza Miasta Kętrzyn z dnia 30 listopada 2020 roku, w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Miasta Kętrzyn – rozdział X.

[akta kontroli str. 92-157]

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.

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

Na podstawie okazanej dokumentacji kontrolujący stwierdzili, że w okresie objętym kontrolą tj. od 1 stycznia 2021 r. do dnia 31 grudnia 2021 r., badaniu audytowemu w ramach realizowanego zadania zapewniającego „Funkcjonowanie kontroli zarządczej w Urzędzie Miasta Kętrzyn" poddane zostały również wybrane zagadnienia z zakresu bezpieczeństwa informacji ujęte w KRI. 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 2021 r. został zrealizowany.

[akta kontroli str. 211-214, 254-266]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.10. Kopie zapasowe

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

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

Zasady w zakresie tworzenia i przechowywania kopii zapasowych zostały uregulowane zarządzeniem 358/2020 Burmistrza Miasta Kętrzyn z dnia 30 listopada 2020 roku, w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Miasta Kętrzyn.

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

.

[akta kontroli str. 158-167, 211-214, 252]

W przypadku wykonywania testów w celu sprawdzenia poprawności wykonywania kopii zapasowych oraz przydatności utworzonych kopii podczas próby symulowanego przywrócenia i uruchomienia oprogramowania po przywróceniu, z informacji uzyskanych z Urzędu wynika, że, cyt.: „

”.

Odnosząc się do przekazanych wyjaśnień należy stwierdzić, że regularne testowanie jakości kopii zapasowych jest kluczowym działaniem w celu minimalizowania ryzyka utraty informacji w wyniku awarii. Prawidłowo zdefiniowana polityka kopii bezpieczeństwa oraz gruntownie przetestowane procesy odtwarzania systemów teleinformatycznych są istotnymi aspektami w każdej jednostce, której procesy opierają się na działaniu systemów informatycznych. Prawidłowo zdefiniowana i wykonana procedura pozwala mieć pewność, że w razie awarii

systemu, wytworzone backupy spełnią swoje zadanie i nie odbije się to negatywnie na ciągłości działania jednostki.
W Instrukcji Zarządzania Systemem Informatycznym – pkt 8, brak jest jakichkolwiek procedur definiujących: wykonywanie testów, w celu sprawdzenia poprawności wytworzonych kopii zapasowych oraz sposób dokumentowania tych czynności.

W świetle powyższego, [redacted].

[akta kontroli str. 158-167, 211-214]

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. [redacted] oraz systemy wspierające zakupione u dostawców zewnętrznych – [redacted]. Na obsługę aktualnie zainstalowanego 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.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 32-33, 158-167, 211-214]

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.: „[redacted]".

[akta kontroli str. 92-157, 211-214]

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:

[redacted]

Ponadto zgodnie z zapisami przyjętej do stosowania Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych pkt. 10.2:

[redacted]

[akta kontroli str. 92-157]

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. 253]

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.

Walidacja za pomocą narzędzia http://wave.webaim.org tj. walidatora WAVE-WCAG 2.0 dla strony BIP i strony www. wykazała jednak błędy (BIP-4 błędy, www.-35 błędów), które wskazują

na brak pełnego spełniania standardów dostępności. Brak pełnej zgodności z ustawą o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, w tym niepełne dostosowanie portalu do standardów WCAG 2.0, należy ocenić jako uchybienie. Przyczyną uchybienia jest brak pełnej dostępności cyfrowej stron internetowych. Skutek uchybienia - brak zapewnienia maksymalnego wsparcia osobom niepełnosprawnym. Odpowiedzialnym za powstanie uchybienia jest Informatyk kontrolowanej jednostki.

[akta kontroli str. 267-270]

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny wnoszę o:

1. Dokonywanie cyklicznych okresowych przeglądów i monitoringu SZBI w jednostce zgodnie z § 20 ust. 1 rozporządzenia KRI.

2. Przeprowadzanie okresowej analiza ryzyka utraty integralności, dostępności lub poufności informacji, a w przypadku stwierdzenia podwyższonego ryzyka w przedmiotowym zakresie, wprowadzenie działań minimalizujących to ryzyko, zgodnie z wymogiem wynikającym z § 20 ust. 2 pkt 3 rozporządzenia KRI.

3. Prowadzenie rejestru czynności przetwarzania danych osobowych zgodnie z art. 30 RODO, na wzorze określonym w rozdziale I pkt 4 (załącznik Nr 1) przyjętej PBI.

[redacted]

5. Uzupełnienie zapisów Instrukcji Zarządzania Systemem Informatycznym, w zakresie procedur definiujących:
   - częstotliwość wykonywania kopii zapasowych - zgodnie z ich faktyczną realizacją,
   - wykonywanie testów, w celu sprawdzenia poprawności wytworzonych kopii zapasowych oraz sposób dokumentowania tych czynności.

6. Podjęcie działań w celu dostosowania Portalu Internetowego oraz BIP Urzędu do standardów WCAG 2.0.

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/