WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

Olsztyn, 25 listopada 2022 r

Wydział Finansów i Kontroli
FK-IV.431.15.2022

Szanowny Pan
Józef Blank
Burmistrz
Nowego Miasta Lubawskiego
Rynek 1
13-300 Nowe Miasto Lubawskie

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 Nowym Mieście Lubawskim[1], Rynek 1, 13-300 Nowe Miasto Lubawskie, NIP jednostki: 877-10-01-987, REGON jednostki: 000525688.

- W okresie objętym kontrolą oraz w czasie prowadzonych czynności kontrolnych kierownikiem kontrolowanej jednostki był Pan **Józef Blank** - Burmistrz Nowego Miasta Lubawskiego, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 4 listopada 2018 r.

- W dniu rozpoczęcia czynności kontrolnych odpowiedzialnym za realizację zadania objętego kontrolą był [redacted] Zatrudniony w Urzędzie od dnia 15 września 2005 r.

- Osobą bezpośrednio nadzorującą pracownika odpowiedzialnego za realizację zadania [redacted] zatrudniona na podstawie umowy o pracę od dnia 1 marca 1987 r.

[akta kontroli str. 34]

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.0030.698.2022 z 12 września 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.0030.697.2022 z 12 września 2022 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 19-24]

Kontrolę przeprowadzono w dniach 22 września – 14 października 2022 r., co zostało odnotowane w książce kontroli Urzędu pod pozycją, Nr 8/2022.

[akta kontroli str. 35]

Kontrola prowadzona była w trybie hybrydowym, tj. w dniu 22 września – rozpoczęcie czynności kontrolnych w Urzędzie oraz oględziny serwerowni na miejscu w jednostce. Pozostałe dni (23 września – 14 października br.) kontrola prowadzona była zdalnie, bez osobistej obecności kontrolerów w Urzędzie, z wykorzystaniem narzędzi informatycznych do zgromadzenia materiału dowodowego, w celu ustalenia stanu faktycznego, a następnie dokonania oceny działalności jednostki kontrolowanej, a także sformułowanie ewentualnych zaleceń pokontrolnych. W dniu rozpoczęcia czynności kontrolnych okazano legitymację oraz upoważnienia do kontroli, poinformowano o zasadach kontroli w trybie hybrydowym, wymaganych dokumentach do kontroli oraz formach i terminie ich przekazywania.

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

[akta kontroli str. 1-2, 25-27]

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, 25-27]

Zastępca Burmistrza wyznaczył [redacted], do udzielania informacji w okresie trwania czynności kontrolnych.

---

[2] Zwanej dalej: ustawą

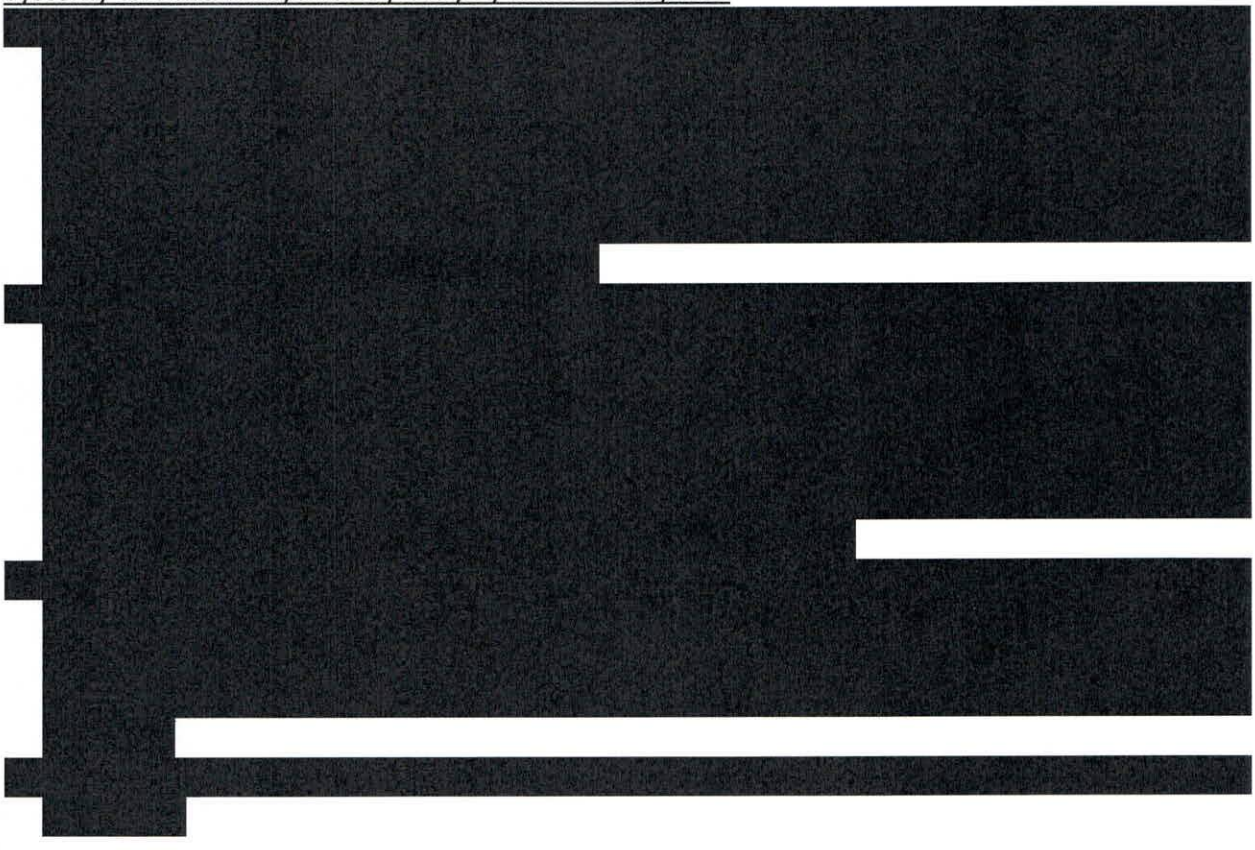
[3] Zwanego dalej: rozporządzeniem KRI

[akta kontroli str. 36]

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 4 niżej wymienione systemy teleinformatyczne.

Systemy teleinformatyczne wykorzystywane w Urzędzie:



[akta kontroli str. 29]

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 **/urzad-nml/SkrytkaESP**, znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie i odbieranie pism w formie dokumentów elektronicznych. Na stronie głównej BIP Urzędu podano adres Elektronicznej Skrzynki Podawczej, a na portalu internetowym Urzędu zamieszczono bezpośredni odnośnik do ePUAP. Formaty danych przyjmowane za pośrednictwem Elektronicznej Skrzynki Podawczej to m.in.: DOC, RTF, XLS, CSV, TXT, GIF, TIF, BMP, JPG, PDF, ZIP.

Na stronie głównej BIP Urzędu, w zakładce „e-usługi" zawarto odnośniki do portali:
- **https://obywatel.gov.pl** - Serwis powstał jako część programu pl.ID, który jest realizowany w ramach Programu Operacyjnego Innowacyjna Gospodarka (7. Oś priorytetowa – Społeczeństwo informacyjne – budowa elektronicznej administracji) i współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego. Obecnie znajduje się na portalu kilkaset najpopularniejszych usług świadczonych przez administrację publiczną.
- **www.podatki.umnowemiasto.pl** - Serwis internetowy ePodatki adresowany jest do osób fizycznych, które chcą przeglądać swoje zobowiązania podatkowe wobec gminy. Usługa ePodatki stanowi dodatkową formę wglądu podatnika do swoich zobowiązań wobec gminy. Dzięki usłudze użytkownik ma zawsze dostęp do aktualnych informacji z każdego komputera podłączonego do sieci Internet. Prezentowane informacje dotyczą podatku od nieruchomości, podatku rolnego i leśnego, opłat z tytułu użytkowania wieczystego. Ponadto, usługa wyświetla informacje dotyczące bieżących rozliczeń księgowych podatków i opłat.

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 „Poradnik interesanta (jak załatwić sprawę)", opublikowany jest przydatny dla petentów wykaz usług, które realizowane są przez poszczególne wydziału Urzędu.
Ponadto na stronie BIP w zakładce „Poradnik interesanta (jak załatwić sprawę)", 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.:

Sprawy ogólne:
1. Pismo ogólne do podmiotu publicznego.
2. Skargi, wnioski, zapytania do urzędu.
3. Wniosek Rodzina 500+.

Sprawy z zakresu Ewidencji Ludności i USC:

1. Wnioskowanie o wydanie dowodu osobistego.
2. Zgłoszenie utraty lub uszkodzenia dowodu osobistego.
3. Wnioskowanie o wydanie odpisu aktu stanu cywilnego.
4. Dopisanie do spisu wyborców.
5. Wydanie zaświadczenia o prawie do głosowania w miejscu pobytu w dniu wyborów.
6. Zawiadomienie o wpisaniu lub dopisaniu wyborcy do spisu wyborców w innym obwodzie głosowania.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 37-41]

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 ale wykorzystywał wzory dokumentów zawarte w CRWDE. Ponadto na stronie BIP w zakładce „Poradnik interesanta (jak załatwić sprawę)", 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. 28, 39, 41]

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.umnowemiasto.pl/, a strona internetowa BIP Urzędu – pod adresem https://bip.umnowemiasto.pl/
Na stronie internetowej Urzędu zamieszczono bezpośredni link do strony BIP Urzędu, w prawej części panelu strony. Na portalu znajdują się również odnośniki do przydatnych dla mieszkańca stron i informacji (np. ePUAP, ePODATKI,).
Na stronie BIP w zakładce „Poradnik interesanta (jak załatwić sprawę)", opublikowane są wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych wydziałów w Urzędzie.

[akta kontroli str. 37-41]

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. 313-321]

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 13/2011 Burmistrza Miasta w Nowym Mieście Lubawskim z dnia 31 stycznia 2011 r. w sprawie wskazania systemu wykonywania czynności kancelaryjnych w Urzędzie Miejskim w Nowym Mieście Lubawskim, (zmienionym zarządzeniami Nr1/2014, Nr 212/2020), podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw w Urzędzie jest tradycyjny system wykonywania czynności kancelaryjnych.

[akta kontroli str. 42-47]

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

[akta kontroli str. 313-331]

W ramach zarządzania obiegiem dokumentacji Urząd stosuje system Elektronicznego Zarządzania Dokumentacją (EZD), za pomocą aplikacji eDOKweb.
W zbiorze okazanej dokumentacji Urzędu zawarte są procedury (w odrębnych dokumentach) dotyczące wykonywania czynności kancelaryjnych, w których określone są zasady obiegu dokumentów wpływających i wypływających drogą elektroniczną, co zgodnie z § 20 ust. 2 pkt 9

rozporządzenia KRI, umożliwia realizację i egzekwowanie, m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie.
Jednocześnie kontrolujący zwracają uwagę, aby w celu zebrania i ujednolicenia zasad postępowania z dokumentacją w formie elektronicznej wpływającą i wychodzącą z Urzędu, powinien zostać opracowany właściwy jednolity dokument np. w formie zarządzenia, regulujący przedmiotową tematykę.

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

1.6. Formaty danych udostępniane przez systemy teleinformatyczne

Stosownie do:

- § 17 ust. 1 rozporządzenia KRI kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków, odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz ze zmianami lub normę ją zastępującą;
- § 18 ust. 1 rozporządzenia KRI systemy teleinformatyczne podmiotów realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia;
- § 18 ust. 2 rozporządzenia KRI jeżeli z przepisów szczegółowych albo opublikowanych w repozytorium interoperacyjności schematów XML lub innych wzorów nie wynika inaczej, podmioty realizujące zadania publiczne umożliwiają przyjmowanie dokumentów elektronicznych służących do załatwiania spraw należących do zakresu ich działania w formatach danych określonych w załącznikach nr 2 i 3 do rozporządzenia.

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

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

[akta kontroli str. 313-321]

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", przyjęto następującą dokumentację:

[redacted]

[akta kontroli str. 126-291]

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

- Polityka bezpieczeństwa teleinformatycznego;
- Polityka bezpieczeństwa fizycznego;
- Polityka bezpieczeństwa danych osobowych.
- Procedura zarzadzania ryzykiem;
- Regulamin korzystania z zasobów informatycznych;
- Procedura zarządzania sprzętem i oprogramowaniem;
- Procedura zarządzania konfiguracją;
- Procedura zarządzania uprawnieniami do pracy w systemach teleinformatycznych;
- Procedura monitorowania poziomu świadczenia usług;
- Procedura bezpiecznej utylizacji sprzętu elektronicznego;

- Procedura zarządzania zmianami i wykonywaniem testów;
- Procedura stosowania środków kryptograficznych;
- Procedura określania specyfikacji technicznych wymagań odbioru systemów IT;
- Procedura zgłaszania i obsługi incydentów naruszenia bezpieczeństwa informacji;
- Procedura wykonywania i testowania kopii bezpieczeństwa;
- Procedura monitoringu i kontroli dostępu do zasobów teleinformatycznych, prowadzenia logów systemowych.

Dokumentację SZBI stanowią także:

- Dokumentacja z przeglądów SZBI;
- Dokumentacja z szacowania ryzyka BI;
- Dokumentacja postępowania z ryzykiem;
- Dokumentacja akceptacji ryzyka;
- Dokumentacja audytów z zakresu BI;
- Dokumentacja incydentów naruszenia BI;
- Dokumentacja zarządzania uprawnieniami do pracy w systemach teleinformatycznych;
- Dokumentacja zarządzania sprzętem i oprogramowaniem teleinformatycznym;
- Dokumentacja szkolenia pracowników zaangażowanych w proces przetwarzania informacji.

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

Z wyjaśnienia uzyskanego z Urzędu w powyższej sprawie wynika, że, cyt.: „[redacted]

[akta kontroli str. 126-290, 313-321]

Odnosząc się do udzielonego wyjaśnienia, należy stwierdzić, że opracowana i wdrożona w 2018 r. Polityka Ochrony Danych Osobowych w Urzędzie Miejskim w Nowym Mieście Lubawskim -

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

W myśl § 20 ust. 1 rozporządzenia KRI podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji.
Rola podmiotu nie kończy się tylko i wyłącznie na opracowaniu i wdrożeniu do eksploatacji systemu zarządzania bezpieczeństwem informacji. Obowiązkiem podmiotu jest także monitorować, przeglądać i utrzymywać jak również doskonalić ten system tak, aby zapewniać poufność, dostępność i integralność informacji. Powyższe oznacza, iż realizacja obowiązku wynikającego z § 20 ust. 1 KRI nie kończy się z momentem wdrożenia do stosowania SZBI, lecz wymaga ona nieustannej uwagi.

W przekazanej dokumentacji, w ramach prowadzonych czynności kontrolnych nie stwierdzono dowodów świadczących o podejmowaniu dodatkowych działań w zakresie prowadzenia monitoringu i przeglądów przyjętego systemu zarządzania bezpieczeństwem informacji.
Z informacji uzyskanych z Urzędu wynika, że, cyt.: „

Z powyższych wyjaśnień oraz dokumentacji stanowiącej dowody kontroli wynika, że w okresie objętym kontrolą nie były prowadzone dodatkowe działania w postaci sprawdzeń

dokonywanych 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.

[akta kontroli str. 313-321]

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

2.2. Analiza zagrożeń związanych z przetwarzaniem informacji

Z § 20 ust. 2 pkt 3 rozporządzenia KRI wynika, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.

Wymogiem skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Kluczowa rola analizy ryzyka wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny i jest zależny od ważności aktywów informatycznych danego podmiotu. Analiza ryzyka jest ważnym wymaganiem nałożonym na administratorów i podmioty przetwarzające. Proces szacowania ryzyka powinien być przeprowadzony i udokumentowany w celu wykazania, że ryzyko zostało oszacowane i wprowadzono odpowiednie środki obrony. Szacowanie ryzyka pozwala na aktywne zarządzanie bezpieczeństwem informacji, w tym na przeciwdziałanie zagrożeniom oraz ograniczanie skutków zmaterializowanych ryzyk, a także wpływa na racjonalne zarządzanie środkami finansowymi poprzez stosowanie zabezpieczeń adekwatnych do oszacowanego poziomu ryzyka. Jednocześnie należy zaznaczyć, że prawidłowo przebiegająca analiza ryzyka nie jest jednorazowym działaniem, lecz regularnie i ciągle monitorowanym procesem.

Zgodnie z wymogiem wynikającym z § 20 ust. 2 pkt 3 rozporządzenia KRI analiza ryzyka utraty integralności, dostępności lub poufności informacji powinna być przeprowadzana okresowo, a w przypadku stwierdzenia podwyższonego ryzyka w przedmiotowym zakresie, powinny zostać wprowadzone działania minimalizujące to ryzyko. Zgodnie z przyjętą Polityką Ochrony Danych Osobowych pkt 5 (str. 15), analizę ryzyka przeprowadza się nie rzadziej niż raz na rok.

Na zadane przez kontrolujących pytanie: czy w 2021 r. przeprowadzono okresową analizę ryzyka, zgodnie z § 20 ust. 2 pkt 3 rozporządzenia KRI oraz pkt 5 przyjętej PODO. Jakiego okresu dotyczy przekazana kontrolującym analiza ryzyka przeprowadzona w Urzędzie?, kontrolujący uzyskali odpowiedź, cyt.: „[redacted]

Należy wspomnieć, że kontrolującym przedstawiono dokumentację (stanowiącą akta kontroli) świadczącą o przeprowadzeniu analizy ryzyka utraty integralności, dostępności lub poufności informacji w Urzędzie. Z wyjaśnień uzyskanych z Urzędu nie wynika jednak, że przedmiotowa analiza dotyczy okresu objętego kontrolą - zgodnie z przyjętą PODO. Brak analizy ryzyka utraty integralności, dostępności lub poufności informacji (w okresie objętym kontrolą) **należy traktować jako nieprawidłowość** skutkującą naruszeniem § 20 ust. 2 pkt 3 rozporządzenia KRI. Osobą odpowiedzialną jest pracownik pełniący obowiązki IOD w tym okresie.
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.

[akta kontroli str. 48-59, 313-321]

W toku prowadzonych czynności kontrolnych stwierdzono, że w jednostce zgodnie z art. 30 RODO oraz załącznikiem Nr 2 do przyjętej PODO, prowadzony jest rejestr czynności przetwarzania danych osobowych.

[akta kontroli str. 60-66]

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

2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego

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

Kontrolującym nie przedstawiono dokumentacji w zakresie spełnienia obowiązku wynikającego z § 20 ust. 2 pkt 2 rozporządzenia KRI, tj. prowadzenia inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

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

Zgodnie z przyjętym Programem kontroli nie sporządzanie bieżącej i aktualnej informacji nt. sprzętu i oprogramowania wykorzystywanego do przetwarzania informacji obejmującej ich

rodzaj i konfigurację **stanowi uchybienie**, skutkujące naruszeniem z § 20 ust. 2 pkt 2 rozporządzenia KRI. Powyższe skutkuje również brakiem możliwości sprawnego odtworzenia infrastruktury informatycznej, w przypadku wystąpienia katastrofy lub innego zdarzenia losowego. Osobami odpowiedzialnymi za powstanie uchybienia są: ASI (Informatyk) oraz Kierownik kontrolowanej jednostki.

[akta kontroli str. 67-75]

Mając powyższe na uwadze, brak realizacji przedmiotowego cząstkowego zagadnienia stanowi uchybienie.

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Stosownie do:

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

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

Zasady nadawania uprawnień do przetwarzania danych osobowych oraz do pracy w określonym zbiorze danych (systemie informatycznym), oraz wzór upoważnienia, określone zostały [redacted] – str. 8.

[akta kontroli str. 126-291]

Osoby posiadające dostęp do danych osobowych posiadały pisemne upoważnienia do ich przetwarzania. Jednocześnie należy nadmienić, że w upoważnieniach do przetwarzania danych osobowych przekazanych kontrolującym wraz z dokumentacją do kontroli, zawarto możliwość wskazania zbiorów (systemu teleinformatycznego) do pracy w którym dany pracownik jest upoważniony. Prowadzona była też ewidencja osób upoważnionych do przetwarzania danych osobowych.

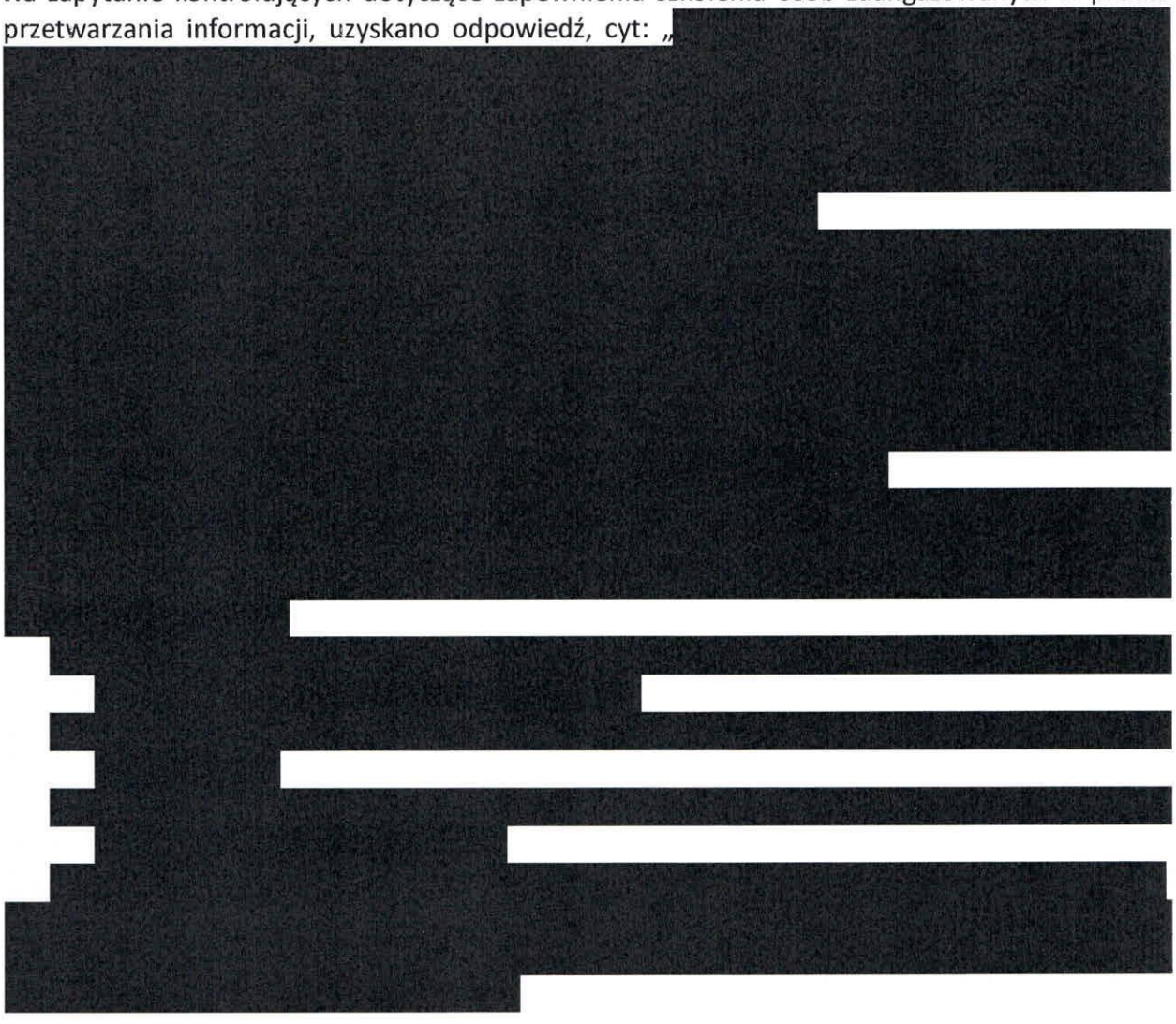
[akta kontroli str. 300-312]

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.

Na zapytanie kontrolujących dotyczące zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji, uzyskano odpowiedź, cyt: „



Odnosząc się do przekazanych wyjaśnień należy wskazać, że zgodnie z § 20 ust. 2 pkt 6 rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji. Ponieważ rozporządzenie KRI nie zawiera definicji pojęcia szkolenia, zatem należy odwołać się do językowego znaczenia tego pojęcia. Zgodnie z definicją językową zawartą w Słowniku PWN (www.sjp.pwn.pl) szkoleniem jest *cykl wykładów z jakiegoś przedmiotu, zorganizowanych w celu uzupełnienia czyjegoś wykształcenia lub czyichś wiadomości z jakiejś dziedziny. Wykład z kolei, to dłuższa zaplanowana wypowiedź służąca przekazaniu słuchaczom wiedzy na jakiś temat.*

Niewątpliwie, na podnoszonych w odpowiedzi Urzędu spotkaniach organizacyjnych można przekazać część wiedzy dotyczącej bezpieczeństwa informacji i przeciwdziałania skutkom jego

naruszenia, jednak takich spotkań organizacyjno-technicznych nie należy utożsamiać do końca ze szkoleniem, a tym samym ze spełnieniem obowiązku wynikającego z rozporządzenia KRI, gdyż wiedza specjalistyczna przekazywana jest na nich w ograniczonym zakresie. Kontrolujący nie mają możliwości weryfikacji faktycznego przekazania specjalistycznej wiedzy w zakresie bezpieczeństwa informacji na spotkaniach organizacyjnych, ze względu na brak list obecności oraz tematyki spotkań (rozliczalność działań). Ponadto wszystkie dowody świadczące o przeprowadzonych szkoleniach-spotkaniach (np. szkolenie z RODO z 2018 r., spotkanie z 25 maja 2018 r. z jednostkami podległymi itd.), przekazane kontrolującym, stanowiły dokumentacje spoza okresu objętego kontrolą i nie mogą być uwzględnione w bieżącej kontroli jako dowody świadczące o zapewnieniu szkolenia osób zaangażowanych w proces przetwarzania informacji w okresie objętym kontrolą.

Brak przeprowadzonych szkoleń dla osób zaangażowanych w proces przetwarzania informacji zgodnie z programem kontroli stanowi nieprawidłowość, jednakże ze względu na odbywające się - zgodnie z oświadczeniem uzyskanym z Urzędu - spotkania organizacyjne na których omawiane są wybrane zagadnienia dotyczące bezpieczeństwa informacji (których przeprowadzenie nie zostało udokumentowane w okresie objętym kontrolą), przedmiotowe zagadnienie ocenia się **pozytywnie z uchybieniami**, ze względu na fakt braku możliwości ich rozliczalności. Skutkiem uchybienia jest częściowe naruszenie § 20 ust. 2 pkt 6 rozporządzenia KRI. Osobą odpowiedzialną jest IOD.

[akta kontroli str. 313-321, 332-395]

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

2.6. Praca na odległość i mobilne przetwarzanie danych

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

Zasady udzielania zdalnego dostępu do systemów informatycznych, a także zasady pracy zdalnej, opracowane zostały w przyjętej [redacted]

[akta kontroli str. 126-143, 313-321]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.7. Serwis sprzętu informatycznego i oprogramowania

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

W przypadku systemów informatycznych niezbędne jest objęcie tych systemów (w zakresie oprogramowania użytkowego i systemowego, sprzętu oraz rozwiązań telekomunikacyjnych)

stosownymi umowami serwisowymi, gwarantującymi odpowiednio szybkie uruchomienie pracy systemu w przypadku awarii oraz gwarantującymi bezpieczeństwo informacji (BI) dla informacji uzyskanych przez wykonawców w związku z ich realizacją.

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

[redacted]

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

[redacted]

[akta kontroli str. 114-143, 292-297]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.8. Procedury zgłaszania incydentów naruszenia BI

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

Instrukcja postępowania w przypadku stwierdzenia zagrożenia w postaci naruszenia ochrony danych oraz informacji w systemach teleinformatycznych, jak również podejmowanych działań korygujących została uregulowana [redacted]

[akta kontroli str. 126-291]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

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

Audyt bezpieczeństwa informacji jest procesem przeprowadzanym w celu zidentyfikowania zagrożeń mogących skutkować utratą poufności, integralności lub dostępności informacji. Celem

audytu wewnętrznego bezpieczeństwa informacji jest ocena zakresu zgodności Systemu Zarządzania Bezpieczeństwem Informacji jednostki z kryteriami audytu.
Na podstawie okazanej dokumentacji kontrolujący stwierdzili, że w okresie objętym kontrolą w jednostce przeprowadzono zadanie sprawdzające pod nazwą Audyt bezpieczeństwa sieci informatycznej zrealizowany dla Urzędu Miejskiego w Nowym Mieście Lubawskim. [redacted] co eliminuje niebezpieczeństwo braku zapewnienia obiektywności i bezstronności procesu audytowego. Audyt bezpieczeństwa sieci IT jest jednym z elementów składowych (wycinkiem) Systemu Zarządzania Bezpieczeństwem Informacji jednostki. Dokument stanowiący raport z audytu zawierał zalecenia i wskazówki dotyczące konfiguracji urządzeń sieciowych modyfikacji architektury sieci komputerowej oraz wdrożenia rozwiązań organizacyjnych które pozwolą w przyszłości na poprawienie bezpieczeństwa i zwiększenie niezawodności działania infrastruktury teleinformatycznej w Urzędzie.
Mając powyższe na uwadze, należy stwierdzić, że obowiązek wynikający z § 20 ust. 2 pkt 14 rozporządzenia KRI – w 2021 r. został zrealizowany.

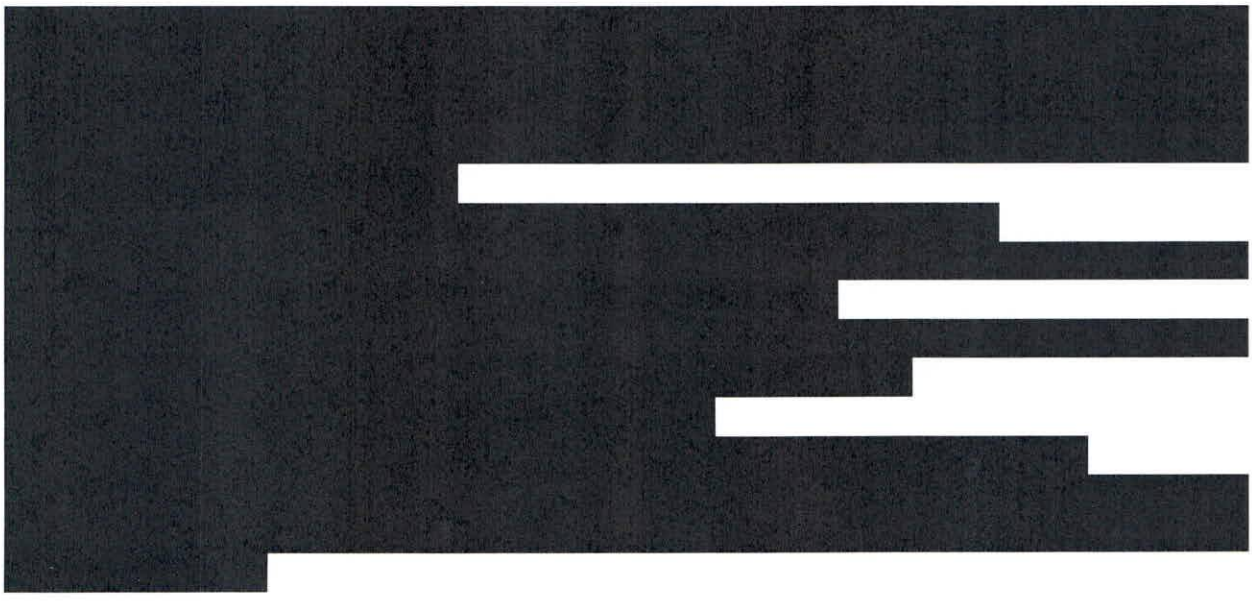
[akta kontroli str. 76-103]

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.



[redacted]

[redacted]

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

W przypadku wykonywania testów w celu sprawdzenia poprawności wykonywania kopii zapasowych oraz przydatności utworzonych kopii podczas próby symulowanego przywrócenia i uruchomienia oprogramowania, [redacted]

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 dokumentacji przekazanej kontrolującym oraz udzielonej odpowiedzi na pytania do kontrolowanego zakresu, brak jest dowodów świadczących o przeprowadzaniu prób odtworzenia systemów informatycznych z wykonanych kopii bezpieczeństwa.

[redacted] Przyczyną powstania uchybienia jest niestosowanie przepisów prawa oraz przyjętych norm w tym zakresie. Osobą odpowiedzialną jest Informatyk urzędu.

[akta kontroli str. 313-321, 396]

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.

[akta kontroli str. 114-125, 292-297]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

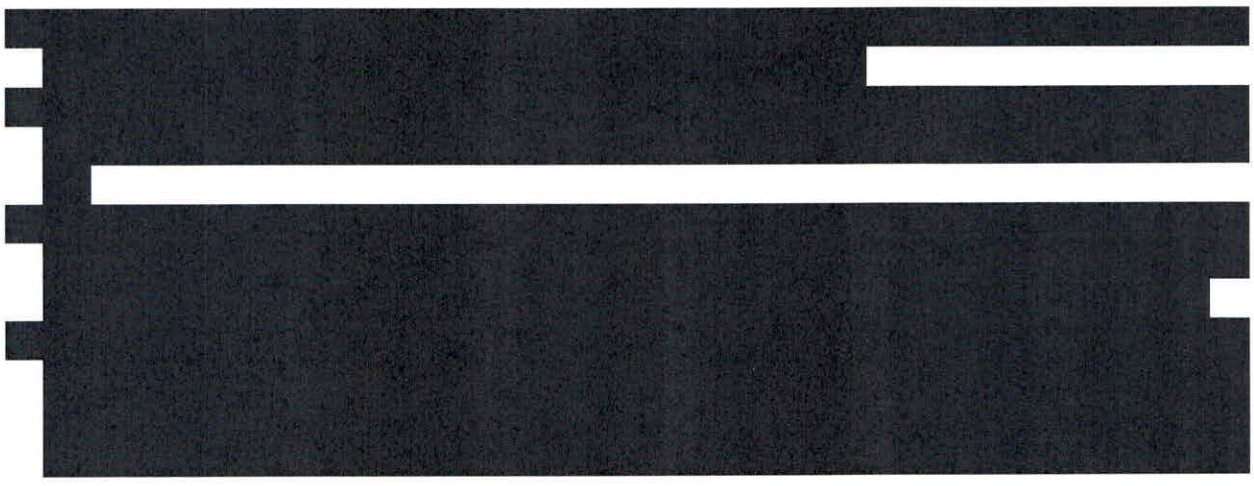
2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji

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

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

W celu uzyskania odpowiedniego poziomu BI, przy jednoczesnym zapewnieniu właściwego bieżącego dostępu uprawnionym użytkownikom, stosowany jest szereg zabezpieczeń technicznych. Celem zabezpieczeń jest uzyskanie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także np. kradzieżą środków przetwarzania informacji.

Z informacji uzyskanych podczas kontroli wynika, że w Urzędzie stosowane są następujące zabezpieczenia cyt.:



[redacted]

[akta kontroli str. 313-321]

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.

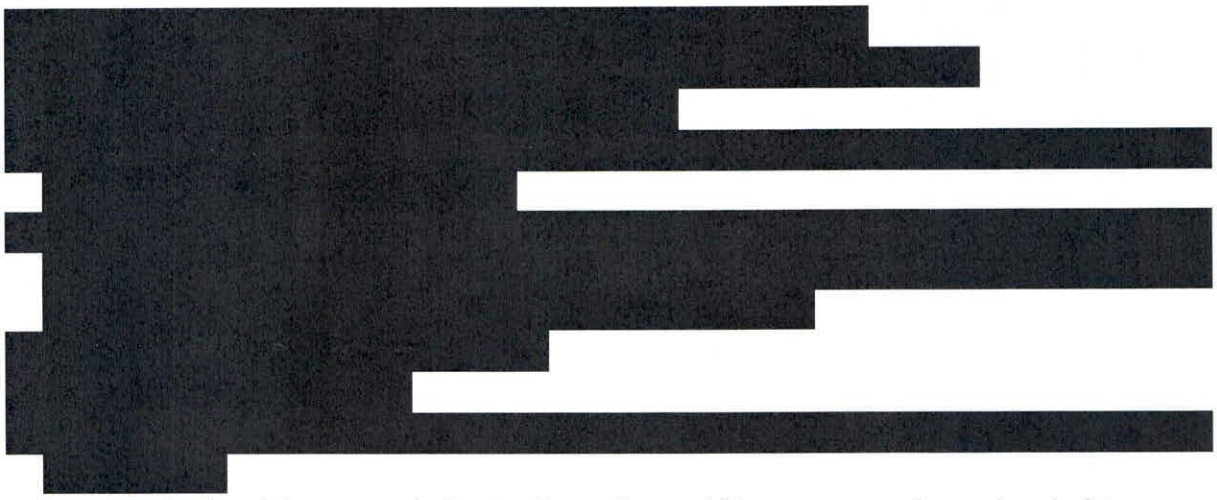
W punkcie 2.12 wykazano mechanizmy jakie jednostka kontrolowana zastosowała w celu zapewnienia ochrony przetwarzanych informacji, w ramach badanych systemów teleinformatycznych przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.

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

[redacted]

Podczas kontroli dokonano oględzin pomieszczenia serwerowni w Urzędzie. Oględzin dokonano w obecności Pana [redacted]. W toku oględzin dokonano ustalenia stanu faktycznego i stwierdzono:

[redacted]



Powyższe potwierdza dokumentacja fotograficzna i protokół z przeprowadzonych oględzin.

[akta kontroli str. 32-33]

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). Zgodnie z przyjętą Polityką Bezpieczeństwa Danych Osobowych w Środowisku IT:

- Każdy system operacyjny oraz baza danych musi mieć włączone audytowanie - włączony dziennik logów bezpieczeństwa.
- Jeżeli aplikacja umożliwia włączenie logów bezpieczeństwa, to musi mieć te logi włączone.
- Administrator danego systemu jest odpowiedzialny za systematyczne przeglądanie logów bezpieczeństwa.
- Wszystkie stwierdzone anomalie i incydenty bezpieczeństwa muszą być udokumentowane i rozpoznane przez administratora systemu.
- Jeżeli podczas analizy logów został stwierdzony prawdopodobny wyciek informacji a w szczególności danych osobowych, o tym fakcie należy niezwłocznie powiadomić IOD,

który powinien postępować zgodnie z opisanymi zasadami w sytuacji naruszenia ochrony danych osobowych opisanych w Polityce Ochrony Danych Osobowych.
- Zaleca się chronić aktualne logi oraz logi które zostały zarchiwizowane powinny zostać zabezpieczone przed manipulacją i nieuprawnionym dostępem.

Z informacji uzyskanych w trakcie kontroli wynika, że cyt.: „[redacted]

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

[akta kontroli str. 313-321]

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

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

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

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

WAVE-WCAG jest narzędziem do automatycznego testowania dostępności serwisów internetowych. Pomaga projektantom i administratorom tworzyć bardziej dostępne strony internetowe. W wyniku automatycznej analizy wskazuje ewentualne miejsca, które mogą powodować problemy z dostępnością.

[akta kontroli str. 298-299]

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

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny, wnoszę o:

[redacted]

2) Dokonywanie cyklicznych okresowych przeglądów i monitoringu SZBI w jednostce zgodnie z § 20 ust. 1 rozporządzenia KRI.
3) Zgodnie z § 20 ust. 2 pkt 3 rozporządzenia KRI oraz przyjętą Polityką Ochrony Danych Osobowych pkt 5, nie rzadziej niż raz na rok przeprowadzanie analizy ryzyka utraty integralności, dostępności lub poufności informacji, a w przypadku stwierdzenia podwyższonego ryzyka w przedmiotowym zakresie, wprowadzanie działań minimalizujących to ryzyko.
4) Prowadzenie inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji (obejmującej ich rodzaj i konfigurację) zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI.
5) W celu spełnienia wymogu rozliczalności - właściwe dokumentowanie przeprowadzonych szkoleń osób zaangażowanych w proces przetwarzania informacji, zgodnie z § 20 ust. 2 pkt 6 rozporządzenia KRI.

[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/