



Olsztyn, 23 grudnia 2021 r.

WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

FK-IV.431.16.2021

**Szanowny Pan
Maciej Sitarek
Burmistrz Lidzbarka
ul. Sądowa 21
13-230 Lidzbark**

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 i Gminy Lidzbark¹, ul. Sądowa 21, 13-230 Lidzbark, NIP Gminy: 571-000-50-38, REGON Gminy: 000529290.

W okresie objętym kontrolą oraz w czasie prowadzonych czynności kontrolnych stanowiska pełnili:

- Pan **Maciej Sitarek** - Burmistrz Lidzbarka wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 21 października 2018 roku (kierownik kontrolowanej jednostki).
- Pani **Małgorzata Nawrocka** - Naczelnik Wydziału Organizacyjnego zatrudniona na podstawie umowy o pracę od dnia 1 stycznia 2009 roku (nadzorująca bezpośrednio pracowników realizujących zadania objęte kontrolą).

W dniu rozpoczęcia czynności kontrolnych odpowiedzialnym za realizację zadania objętego kontrolą w Urzędzie był Pan [REDAKTOWANE].

[akta kontroli str. 53]

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 -

¹ Zwany dalej: Urzędem

Mazurskiego Urzędu Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr FK-IV.0030.751.2021 z 11 października 2021 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

Michał Wasilewski – inspektor wojewódzki; członek zespołu kontrolnego, legitymacja służbowa nr 23/2020, wydana przez Dyrektora Generalnego Warmińsko - Mazurskiego Urzędu Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr FK-IV.0030.752.2021 z 11 października 2021 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 16-17]

Kontrolę przeprowadzono w dniach 25 października – 17 listopada 2021 r., co zostało odnotowane w książce kontroli Urzędu, pod pozycją, Nr 56/2021.

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

Przedmiotem kontroli była ocena działania systemów teleinformatycznych używanych przez jednostki samorządu terytorialnego do realizacji zadań zleconych z zakresu administracji rządowej, na podstawie art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2021 r., poz. 670 ze zm.). Okres objęty kontrolą: od dnia 1 stycznia 2019 r. do dnia 31 grudnia 2020 r.

[akta kontroli str. 1-2, 39-50]

Kontrola została przeprowadzona na podstawie art. 2 pkt 1 i art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U. 2020 poz. 224), art. 28 ust. 1 pkt 2 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz. U. z 2019 r., poz. 1464), w związku z art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne tekst jednolity (Dz.U. z 2017 r. poz. 570 ze zm. - akt prawny obowiązujący do 02.04.2019 r., Dz.U. z 2019 r. poz. 700 ze zm. - akt prawny obowiązujący do 04.03.2020 r., Dz.U. z 2020 r., poz. 346 ze zm. - akt prawny obowiązujący do 12.04.2021 r. oraz Dz.U. z 2021 r., poz. 670 ze zm.)², rozdziału III i IV Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów

² Zwanej dalej: ustawą

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, 39-50]

Burmistrz Miasta i Gminy Lidzbark, upoważnił Sekretarza Gminy, do udzielania informacji i wyjaśnień w okresie trwania czynności kontrolnych.

[akta kontroli str. 54]

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 12 systemów

[Redacted text block containing 12 system names]

³ Zwanego dalej: rozporządzeniem KRI

I. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.

1.1. Usługi elektroniczne

Z art. 16 ust. 1a ustawy wynika, że *podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę.*

Zgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI interoperacyjność na poziomie organizacyjnym osiągnana 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 /uradlidzbark/SkrytkaESP/, znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie i odbieranie pism w formie dokumentów elektronicznych. Ścieżkę bezpośredniego przejścia na główną stronę e-PUAP, zawarto na stronie internetowej BIP Urzędu. 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 osiągnana 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. Jednocześnie należy zaznaczyć, iż Urząd nie świadczył usług związanych z załatwianiem spraw od początku do końca w formie elektronicznej, za pomocą systemów teleinformatycznych. W przypadku wybranych spraw załatwianych w Urzędzie, istnieje jednak możliwość złożenia wniosku w formie elektronicznej (np. ePUAP),

W związku z powyższym w BIP Urzędu zamieszczone zostały procedury postępowania określające sposób przyjmowania i załatwiania poszczególnych spraw w Urzędzie, w tym załatwianych przy pomocy wniosku elektronicznego zgodnie z § 5 ust. 2 pkt 1 i 4 KRI.

Obywatel ma prawo wiedzieć o wszystkich okolicznościach, które mogą wpłynąć na ustalenie jego praw i obowiązków w prowadzonym postępowaniu.

Ponadto na stronie BIP opublikowane są wzory wniosków i formularzy, będących w zakresie poszczególnych referatów w Urzędzie. Urząd udostępniał oraz świadczył również usługi elektroniczne, z wykorzystaniem ePUAP, tj. „Pismo ogólne do urzędu”. Usługa te

umożliwiają złożenie do wybranego organu administracji publicznej pisma (podania) w sprawie.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 364-365]

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 ujednoczenia w skali kraju procedur usług świadczonych przez urzędy drogą elektroniczną, w tym ujednoczenia 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 udostępniana przez jeden podmiot, np. właściwego ministra, ale służy do świadczenia usług przez inne podmioty niż udostępniający, np. wszystkie gminy). W przypadku uruchamiania usługi, dla której nie ma wzorów dokumentów w CRWDE, podmiot publiczny jest zobowiązany przekazać do CRWDE procedurę obsługi usługi i wzory dokumentów elektronicznych z nią związanych.

W trakcie kontroli ustalono, że Urząd w badanym okresie nie korzystał i nie przekazywał wzorów dokumentów elektronicznych do centralnego repozytorium wzorów dokumentów prowadzonego przez Ministerstwo Cyfryzacji, ze względu na fakt, iż nie uruchamiał nowej usługi, dla której nie ma wzorów dokumentów w CRWDE.

Jednocześnie należy zaznaczyć, iż na stronie BIP Urzędu opublikowano w wersji „do pobrania” formularze wzorów dokumentów niezbędnych do załatwienia poszczególnych spraw w Urzędzie.

[akta kontroli str. 26-34, 367-369]

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

1.3. Model usługowy

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

Strona internetowa Urzędu działa pod adresem <http://www.lidzbark.pl/>, a strona internetowa BIP Urzędu – pod adresem <http://bip.umig.lidzbark.pl/>.

Na stronie internetowej Urzędu zamieszczono bezpośredni link do strony BIP Urzędu, w prawej dole części panelu strony. Na stronie głównej Urzędu, zamieszczono ścieżkę do platformy ePUAP.

Na stronie internetowej BIP, znajdują się linki do najważniejszych serwisów internetowych ułatwiających odbiorcy internetowemu załatwienie podstawowych spraw urzędowych, tj.:

- OBYWATEL.GOV.PL, który powstał jako część programu pl.ID, realizowanego w ramach Programu Operacyjnego Innowacyjna Gospodarka (7. Oś priorytetowa – Społeczeństwo informacyjne – budowa elektronicznej administracji) i współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego. Znajduje się tu kilkaset najpopularniejszych usług świadczonych przez administrację publiczną.
- CEiDG – portal umożliwiający założenie działalności gospodarczej.
- Dzienniki Urzędowe Województwa, Dzienniki Ustaw, Monitor Polski.

[akta kontroli str. 366]

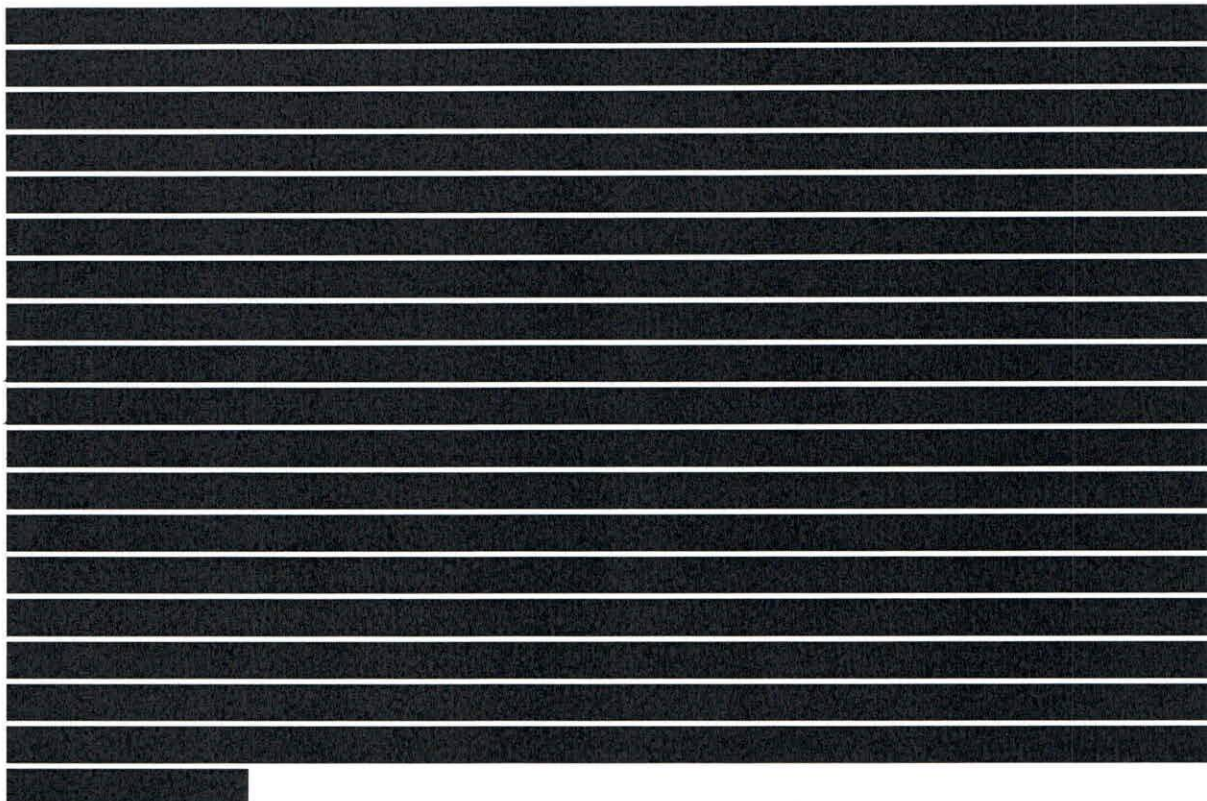
W Urzędzie brak jest formalnych procedur opisujących obsługę oraz monitorowanie usług elektronicznych realizowanych przez systemy teleinformatyczne wykorzystywane do realizacji zadań zleconych z zakresu administracji rządowej ze względu na fakt, iż jednostka nie świadczyła usług elektronicznych na zewnątrz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



[akta kontroli str. 367-369]

W związku z powyższym przedmiotowe częściowe 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, modyfikację, usunięcie lub zniszczenie.*

Zgodnie z zarządzeniem Nr 23/11 Burmistrza Lidzbarka z dnia 31 marca 2011 r. w sprawie wdrożenia instrukcji kancelaryjnej - podstawowym systemem czynności kancelaryjnych oraz ich dokumentowania w Urzędzie Miasta i Gminy Lidzbark jest system tradycyjny.

W sprawach nieuregulowanych, zarządzeniem zastosowanie mają przepisy Rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.

W okazanej dokumentacji Urzędu brak było regulacji wewnętrznych opisujących sposób zarządzania dokumentacją wpływającą drogą elektroniczną tj., procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby zasady obiegu dokumentów wpływających i wypływających drogą elektroniczną oraz zakres stosowania elektronicznego obiegu dokumentów (np. skrzynka podawcza na platformie ePUAP), co zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI, umożliwiłoby realizację i egzekwowanie, m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie.

Na zadane przez kontrolujących pytanie - czy w jednostce opracowano i przyjęto regulujące w zakresie obiegu dokumentów wpływających i wypływających w formie elektronicznej,

[REDAKTED]

Brak przedmiotowych regulacji stanowi uchybienie. Skutkiem stwierdzonego uchybienia jest naruszenie § 20 ust. 2 pkt 9 rozporządzenia KRI. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki.

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

[akta kontroli str. 367-369, 417]

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.



[akta kontroli str. 367-369]

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.*

Realizacja ww. zadań 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. Dokument ten 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 ramach dokumentacji wchodzącej w skład SZBI w Urzędzie przyjęto:

- Zarządzenie nr 7/18 Burmistrza Lidzbarka z dnia 24 sierpnia 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miasta i Gminy w Lidzbarku. Polityka bezpieczeństwa zawiera uregulowania dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

[REDACTED]

Przedmiotową dokumentację sporządzono na podstawie 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”, ustawy dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000).

Dokumentacja w zakresie ochrony danych dotyczyła danych przetwarzanych w Urzędzie i służyła zapewnieniu poufności, integralności przetwarzania danych, jak również monitorowania zdarzeń naruszających ochronę danych (w tym osobowych), zawierała także opis postępowania w przypadku naruszenia zasad bezpieczeństwa danych osobowych.

[akta kontroli str. 181-271]

Burmistrz Lidzbarka, zarządzeniem nr 6/18 z dnia 21 sierpnia 2018 r. powołał w jednostce Inspektora Ochrony Danych (IOD).

[akta kontroli str. 274-284]

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.

Z dokumentacji przedstawionej kontrolującym wynika, że IOD w okresie objętym kontrolą dokonywał przeglądu SZBI w jednostce poprzez przeprowadzenie corocznych sprawdzeń zgodności przetwarzania danych osobowych, w ramach których.

[akta kontroli str. 285-288]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.2. Analiza zagrożeń związanych z przetwarzaniem informacji

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

Wymogiem skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Kluczowa rola analizy ryzyka wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny i jest zależny od ważności aktywów informatycznych danego podmiotu.

Zgodnie z wymogiem wynikającym z § 20 ust. 2 pkt 3 rozporządzenia KRI analiza ryzyka utraty integralności, dostępności lub poufności informacji powinna być przeprowadzana okresowo, a w przypadku stwierdzenia podwyższonego ryzyka w przedmiotowym zakresie, powinny zostać wprowadzone działania minimalizujące to ryzyko.

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

[akta kontroli str. 58-180]

Jednocześnie należy wskazać, iż zgodnie z zarządzeniem nr 7/18 Burmistrza Lidzbarka z dnia 24 sierpnia 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych, rozdział – Rejestr czynności przetwarzania danych osobowych, w jednostce został opracowany i jest prowadzony powyższy rejestr.

[akta kontroli str. 181-272]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego

Z § 20 ust. 2 pkt 2 rozporządzenia KRI wynika, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: utrzymanie aktualności inwentaryzacji sprzętu*

i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

Kontrolującym przedstawiono aktualną 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. 273]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Stosownie do:

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

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

Zasady nadawania i odbierania uprawnień do przetwarzania danych osobowych oraz do pracy w określonym zbiorze danych (systemie informatycznym) określone zostały w zarządzeniu nr 7/18 Burmistrza Lidzbarka z dnia 24 sierpnia 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miasta i Gminy w Lidzbarku – Procedura dopuszczenia osób do przetwarzania danych osobowych.

[Redacted text block]

[akta kontroli str. 181-271, 332]

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

[akta kontroli str. 333-357]

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.*

Zgodnie z zarządzeniem nr 7/18 Burmistrza Lidzbarka z dnia 24 sierpnia 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych - Procedura szkoleń z zakresu danych osobowych Urzędu Miasta i Gminy w Lidzbarku (§5), szkolenia z zakresu przetwarzania danych osobowych dla pracowników wykonuje się przynajmniej raz do roku.

Z dokumentacji przedstawionej kontrolującym wynika, że pracownicy Urzędu zaangażowani w proces przetwarzania informacji, uczestniczyli w 2019 r. w szkoleniu (zorganizowanym przez firmę zewnętrzną – zgodnie z umową), dotyczącym ochrony danych osobowych.

Program szkolenia obejmował:

1. Przetwarzanie danych osobowych:
 - wpływ ROOO na strukturę i procesy w organizacji,
 - podstawowe pojęcia i obrazowe przykłady ich funkcjonowania,
 - zasady przetwarzania danych osobowych,
 - podstawy przetwarzania danych osobowych zwykłych oraz szczególnych kategorii tzw. danych wrażliwych).
2. Prawa przysługujące osobie, której dane dotyczą:
 - prawo do bycia zapomnianym,
 - prawo dostępu do danych,
 - prawo do przenoszenia danych,
 - prawo do niepodlegania profilowaniu, pojęcia profilowania i praw z nim związanych,
 - zasada przejrzystości i inne.
3. Klauzule informacyjne:
 - rola klauzuli w procesie przetwarzania danych osobowych,
 - rozszerzenie treści klauzuli informacyjnej,
 - omówienie wzoru nowych klauzul.

4. Obowiązki administratorów danych:
 - proaktywne, oparte na ryzyku podejście do ochrony danych,
 - realizacja żądań osób, których dane dotyczą,
 - konieczność zgłaszania naruszeń ochrony danych osobowych do organu nadzorczego.
5. RODO a obowiązki pracownicze:
 - jak reagować na żądania realizacji praw osób, których dane dotyczą,
 - gdzie szukać informacji na temat przetwarzania danych w organizacji
 - na jakiej podstawie pracownik może przetwarzać dane osobowe i skąd wynika ich zakres.
6. Inspektor ochrony danych (zmiana statusu administratora bezpieczeństwa informacji):
 - zadania i obowiązki,
 - współpraca pracowników z inspektorem ochrony danych.
7. Urząd Ochrony Danych Osobowych:
 - rola, status, zadania i uprawnienia,
 - sankcje za nieprzestrzeganie przepisów rozporządzenia, w tym administracyjne kary pieniężne - warunki ich nakładania i wysokość.
8. Przetwarzanie danych osobowych w praktyce:
 - zasady ochrony informacji,
 - źródła zagrożeń dla danych osobowych w organizacji,
 - incydent ochrony danych - czym jest, jak go rozpoznać i jak postępować w przypadku jego wystąpienia,
 - praktyczne wskazówki do zastosowania przy stanowisku pracy - bezpieczne korzystanie z komputera, tworzenie haseł, podstawowe zabezpieczenia i polityki związane z przetwarzaniem danych (w tym polityka czystego biurka, ekranu, retencji danych itp.).

W przypadku 2020 roku zgodnie z notatką służbową z dnia 2 grudnia 2020 r w związku z sytuacją epidemiologiczną panującą w tym okresie, prośbami pracowników w zakresie zorganizowania szkolenia stacjonarnego a nie zdalnego, znaczną rotacją pracowników spowodowaną kwarantanną w związku z COVID-19, podjęto decyzję o przeniesieniu przedmiotowego szkolenia na rok 2021.

[akta kontroli str. 55-57, 181-271]

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.*



[akta kontroli str. 367-369]

Przedmiotowe częściowe zagadnienie ze względu na wykorzystywanie sprzętu w zakresie systemów teleinformatycznych tylko w siedzibie jednostki (stacjonarny tryb pracy) nie podlegało ocenie.

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.

Zgodnie z Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Urzędu Miasta i Gminy w Lidzbarku, Administrator Systemu Informatycznego (ASI), jest zobowiązany do wykonywania czynności konserwacyjnych, naprawczych jak również sprawowania nadzoru nad tymi czynnościami w obszarze systemu.

W związku z zakupem systemów podpisane zostały z poszczególnymi firmami umowy licencyjne umożliwiające prawidłową eksploatację i rozwój systemu poprzez możliwość zgłaszania błędów pytań i roszczeń dotyczących użytkowanego systemu.

Zawarte zostały również stosowne umowy powierzenia danych gwarantujące właściwe zabezpieczenie danych w przypadku awarii systemu oraz gwarantujące bezpieczeństwo informacji uzyskanych przez wykonawcę w związku z realizacją umowy.

[akta kontroli str. 367-369, 370-371, 418-445]

Mając powyższe na uwadze przedmiotowe częściowe 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, umożliwiającą szybkie podjęcie działań korygujących.*

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych zawarta jest w zarządzeniu nr 7/18 Burmistrza Lidzbarka z dnia 24 sierpnia 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych.

[akta kontroli str. 181-271]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

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

Na podstawie okazanej dokumentacji kontrolujący stwierdzili, iż w 2020 r., w jednostce przeprowadzono jedno zadanie audytowe w zakresie bezpieczeństwa informacji. Zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI, w czerwcu 2020 r. przeprowadzony został audyt bezpieczeństwa informacji, który obejmowały następujące zagadnienia:

1. Bezpieczeństwo fizyczne i środowiskowe.
2. Zarządzanie systemami i sieciami.
3. Kontrola dostępu.

[akta kontroli str. 288-331]

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 2020 r. został zrealizowany.

W przypadku 2019 r. na podstawie okazanej dokumentacji kontrolujący stwierdzili, że obowiązek wynikający z § 20 ust. 2 pkt 14 rozporządzenia KRI nie został zrealizowany.

[Redacted content]

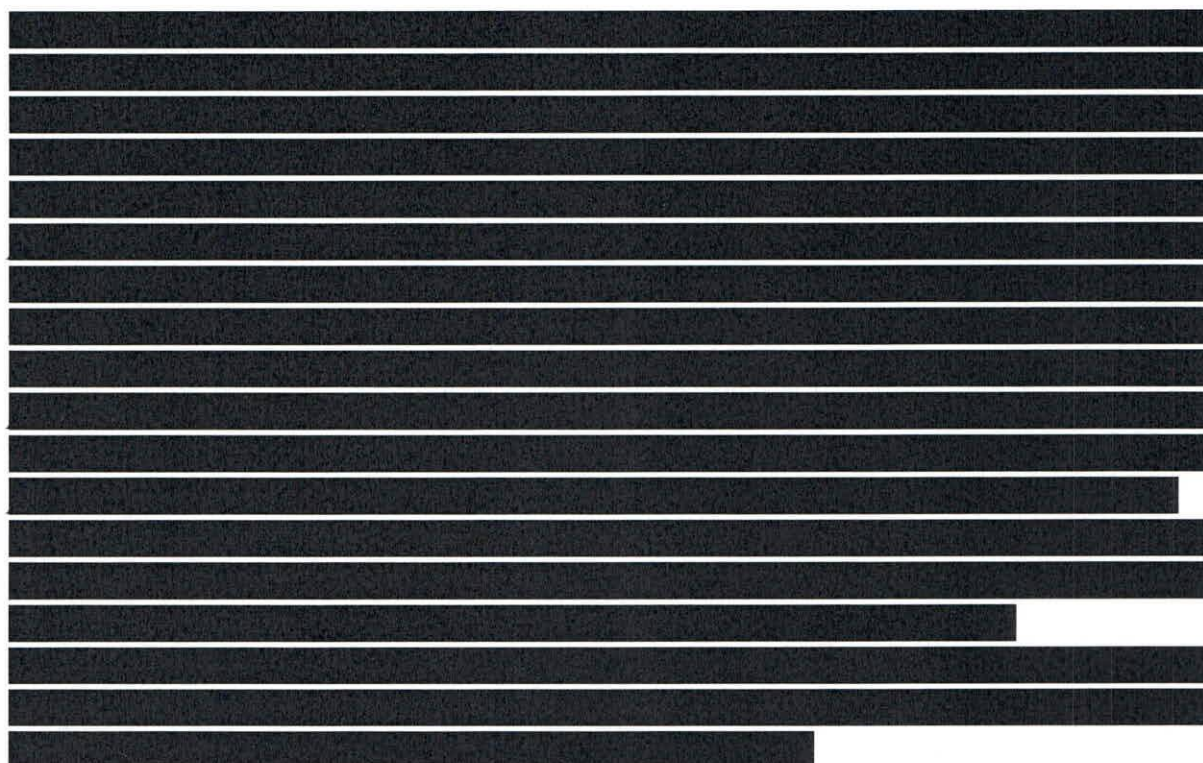
Brak przeprowadzenia audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok skutkuje niedopełnieniem obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI i stanowi nieprawidłowość. Osobą odpowiedzialną za powstanie nieprawidłowości jest Kierownik jednostki.

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z nieprawidłowościami.

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 kopii 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 text block]

[Redacted text block]

W związku z tym, że kopie zapasowe z systemów teleinformatycznych są tworzone i testowane w Urzędzie, brak opracowanych regulacji w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, w zakresie testowania, należy uznać za uchybienie. Przyczyną powstania uchybienia jest brak minimalizowania ryzyka utraty informacji, a skutkiem, naruszenie § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI. Osobą odpowiedzialną jest ASI jednostki.

[akta kontroli str. 359, 367-369]

Regularne tworzenie i testowanie jakości kopii zapasowych jest kluczowym działaniem w celu minimalizowania ryzyka utraty informacji w wyniku awarii. Wskazane jest przechowywanie kopii zapasowych w innej lokalizacji niż miejsce ich tworzenia, w odległości niezbędnej do uniknięcia uszkodzeń spowodowanych przez katastrofę, która dotknęłaby podstawowy ośrodek przetwarzania danych.

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.

[REDACTED]

Na obsługę aktualnie zainstalowanego oprogramowania z firmami zewnętrznymi dostarczającymi dany system informatyczny zawarte zostały stosowne umowy licencyjne (opieka autorska), gwarantujące rozwój systemu i dostosowanie do obowiązujących przepisów prawa. Zakupione systemy teleinformatyczne, w razie awarii podlegają ekspertyzie technicznej zlecanej firmie dostarczającej.

[akta kontroli str. 367-369, 370-371, 418-445]

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 do nich dostępu przez uprawnionych użytkowników stosowany jest szereg zabezpieczeń informatycznych. Celem zabezpieczeń jest uzyskanie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także np. kradzieżą środków przetwarzania informacji.

[REDACTED]

[Redacted text block]

[akta kontroli str. 367-369]

Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Stosownie do:

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

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

[Redacted text block]

[REDACTED]

[akta kontroli str. 367-369]

Przedmiotowe częściowe 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.*

Z wyjaśnień uzyskanych z Urzędu w powyższej sprawie wynika, że [REDACTED]

[REDACTED]

[akta kontroli str. 367-369]

Mając na uwadze powyższe przedmiotowe częściowe zagadnienie ocenia się pozytywnie.

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

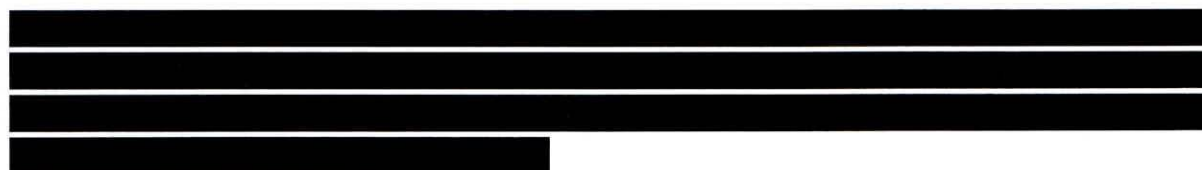
Uwzględniając potrzeby osób niepełnosprawnych podmiot publiczny powinien zastosować w eksploatowanych systemach teleinformatycznych rozwiązania techniczne umożliwiające osobom niedosłyszącym, niedowidzącym lub niewidomym zapoznanie się z treścią informacji, m.in. poprzez powiększenie czcionki, obrazu,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

Systemy informatyczne wspomagające realizację zadań zleconych z zakresu administracji rządowej w Urzędzie, ze względu na brak interakcji z klientami zewnętrznymi za pośrednictwem publicznej sieci Internet nie są objęte wymogami WCAG 2.0. W toku kontroli dokonano jednak weryfikacji zgodności ze standardem WCAG 2.0 strony internetowej Urzędu oraz BIP Urzędu.

Dostępność strony internetowej oznacza, że może z niej skutecznie korzystać każdy na dowolnej aplikacji klienckiej, na dowolnym urządzeniu, z dowolnego rodzaju połączenia, w każdych warunkach, bez względu na sprawność swoich zmysłów. Podmioty publiczne zobowiązane są do zapewnienia dostępności cyfrowej swoich stron. Zapewnienie dostępności cyfrowej stron internetowych oznacza spełnienie wielu kryteriów sukcesu zdefiniowanych w Web Content Accessibility Guidelines (WCAG 2.0). Wytyczne wymagają spełnienia czterech głównych zasadami, którymi są:

1. postrzegalność,
2. funkcjonalność,
3. zrozumiałość,
4. kompatybilność.

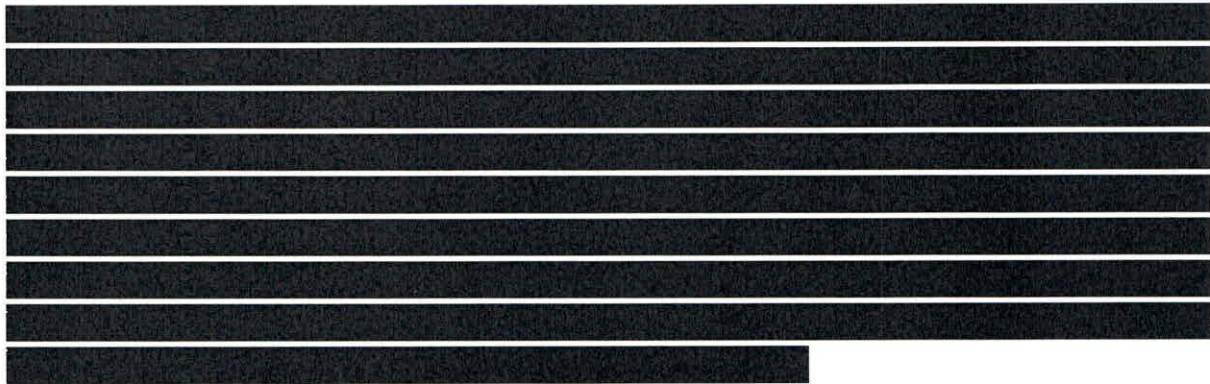
Każda strona dostępna w Internecie powinna zapewniać maksymalne wsparcie wszystkim grupom wiekowym jak i społecznym. Warunkiem dostępności strony jest dobry kontrast zapewniający swobodny odczyt przedstawionych informacji. Im wyższy jest kontrast, tym łatwiej odróżnić obiekt, zdjęcie czy tekst pierwszego 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.



WAVE-WCAG jest narzędziem do automatycznego testowania dostępności serwisów internetowych. Pomaga projektantom i administratorom tworzyć bardziej dostępne strony internetowe. Wprawdzie nie odpowiada do końca na pytanie, czy zawartość serwisu jest dostępna, bo to może uczynić tylko człowiek-użytkownik, ale poglądowo wskazuje miejsca, które mogą powodować problemy z dostępnością.



[akta kontroli str. 446-450]



Powyższe zagadnienie oceniono pozytywnie z uchybieniami.

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny wnoszę o

1. Opracowanie wewnętrznych procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby również zasady obiegu dokumentów wpływających i wypływających z Urzędu drogą elektroniczną.
2. Zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok, zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI.
3. W celu zachowania pełnej rozliczalności podejmowanych w Jednostce działań, należy uzupełnić zapisy *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Urzędu Miasta i Gminy w Lidzbarku*, o zasady testowania kopii zapasowych danych ze wszystkich systemów podmiotu kontrolowanego oraz zwrócić szczególną uwagę na właściwe udokumentowanie tych czynności (np. dzienniki testowania kopii lub protokoły z testów odtworzeniowych).
4. 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