



Wydział Finansów i Kontroli  
FK-IV.431.7.2022

Szanowny Pan  
**Tomasz Andrukiewicz**  
Prezydent Miasta Ełku  
ul. Marszałka Józefa Piłsudskiego 4  
19-300 Ełk

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 Ełku<sup>1</sup>, ul. Marszałka Józefa Piłsudskiego 4, 19-300 Ełk, NIP jednostki 848-00-07-927, REGON jednostki: 000523287.

W okresie objętym kontrolą oraz w czasie prowadzonych czynności kontrolnych kierownikiem kontrolowanej jednostki był Pan **Tomasz Andrukiewicz** – Prezydent Miasta Ełku, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 21 października 2018 r.

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



Osobą bezpośrednio nadzorującą pracowników odpowiedzialnych za realizację zadania była Pan **Marcin Radziłowicz** - Sekretarz Miasta Ełku zatrudniony na podstawie umowy o pracę od dnia 23 kwietnia 2007 r.

[akta kontroli str. 69]

<sup>1</sup> Zwany dalej: Urzędem  
Warmińsko-Mazurski Urząd Wojewódzki w Olsztynie  
Al. Marsz. J. Piłsudskiego 7/9  
10-575 Olsztyn

Kontrolę przeprowadzili pracownicy Wydziału Finansów i Kontroli Warmińsko- Mazurskiego Urzędu Wojewódzkiego w Olsztynie:

**Radosław Gazda** – starszy 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.0030.209.2022 z 1 kwietnia 2022 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

**Michał Wasilewski** – starszy 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.0030.210.2022 z 1 kwietnia 2022 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 16-21]

Kontrolę przeprowadzono w dniach 22 kwietnia - 16 maja 2022 r., co zostało odnotowane w książce kontroli Urzędu pod pozycją 6/2022.

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

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

[akta kontroli str. 1-2, 53-64]

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)<sup>2</sup>, 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.)<sup>3</sup>, jak również Wytycznych dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych, zatwierdzonych przez Ministra Cyfryzacji w dniu 15 grudnia 2015 r.

---

<sup>2</sup> Zwanej dalej: ustawą

<sup>3</sup> Zwanego dalej: rozporządzeniem KRI



[akta kontroli str. 1-2, 53-64]

Prezydent Ełku upoważnił pełnomocnika prezydenta ds. informatyzacji oraz kierownika referatu spraw obywatelskich, do udzielania informacji w okresie trwania czynności kontrolnych.

[akta kontroli str. 70-71]

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**.

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 5 niżej wymienionych systemów teleinformatycznych.

Systemy teleinformatyczne wykorzystywane w Urzędzie:

[akta kontroli str. 39-44]

**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 osiągnięta 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 **/umelk/skrytka**, znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie i odbieranie pism w formie dokumentów elektronicznych. Ścieżkę bezpośredniego przejścia na główną stronę e-PUAP, zawarto na stronie internetowej BIP Urzędu (e-urząd). 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 „Menu przedmiotowe” – podzakładka „e-Urząd” zawarto odnośnik do elektronicznego biura obsługi (eUsługi). Zgodnie z informacją zawartą na stronie portalu, platforma eUsług przeznaczona jest dla mieszkańców, którzy chcą korzystać z usług jednostek samorządu terytorialnego drogą elektroniczną. Aplikacja ta udostępnia obywatelom dane urzędowe oraz umożliwia sprawną komunikację pomiędzy interesantem i pracownikiem urzędu. Platforma eUsług składa się z następujących modułów:

- Obsługa interesanta i sprawy – wirtualne biuro obsługi interesanta wspiera proces załatwiania spraw w urzędzie. Udostępnia opisy usług świadczonych przez jednostkę samorządu terytorialnego. Dodatkowo umożliwia umówienie się na spotkanie z urzędnikiem.
- Płatności – moduł umożliwia realizację płatności w ramach zobowiązań wynikających z podatków i innych opłat w zakresie usług oferowanych przez urząd. Przykładowym zobowiązaniem jest opłata za podatek od nieruchomości. Platforma eUsług udostępnia przegląd analiz i zestawień danych o użytkowniku, które zostały zgromadzone w systemie. Aplikacji umożliwia również prezentacje aktualnych informacji na temat gminy oraz planowanych wydarzeń.

Zgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI interoperacyjność na poziomie organizacyjnym osiągnięta 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 „Menu przedmiotowe – Poradnik interesanta (jak załatwić sprawę)”, opublikowany jest przydatny dla petentów wykaz usług, które realizowane są przez poszczególne wydziały Urzędu, w tym również te które możliwe są do zrealizowania drogą elektroniczną korzystając z platformy ePUAP. Opublikowane tam są również wzory wniosków i formularzy niezbędnych do załatwienia poszczególnych spraw, będących w zakresie działania poszczególnych wydziałów w Urzędzie.

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

Ponadto Urząd udostępniał oraz świadczył również usługi elektroniczne, z wykorzystaniem ePUAP, tj. „Pismo ogólne do podmiotu publicznego”. Usługa ta umożliwia złożenie do wybranego organu administracji publicznej pisma w sprawie.



W związku z powyższym przedmiotowe częściowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 91-93]

### 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 w okresie objętym kontrolą (2021) Urząd nie przekazywał wzorów dokumentów elektronicznych do centralnego repozytorium wzorów dokumentów prowadzonego przez Ministerstwo Cyfryzacji, ze względu na fakt nie uruchomienia nowej usługi dla których nie ma wzorów dokumentów w CRWDE. Z rejestrów CRWDE wynika, że Urząd w latach 2015-2017 przekazywał do zasobu wzory dokumentów związane z realizowanymi zadaniami.

Z informacji uzyskanej podczas kontroli wynika ponadto, że: „



Jednocześnie należy zaznaczyć, że na stronie BIP, opublikowane są wzory wniosków i formularzy niezbędnych do załatwienia poszczególnych spraw, będących w zakresie działania wydziałów w Urzędzie.

W związku z powyższym przedmiotowe częściowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 25-38, 94-96]

### 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.elk.pl/>, a strona internetowa BIP Urzędu – pod adresem <https://bip.elk.warmia.mazury.pl/>

Na stronie internetowej Urzędu zamieszczono bezpośredni link do strony BIP Urzędu, w prawej górnej części panelu strony. Na stronie głównej BIP Urzędu w zakładce „Manu przedmiotowe” – podzakładka „e-Urząd” zawarto odnośnik do elektronicznego biura obsługi (eUsługi).

[akta kontroli str. 91-93]

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 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 osiągnięta 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 text block]

[akta kontroli str. 25-38]

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, modyfikacje, usunięcie lub zniszczenie.

Z uzyskanych w trakcie kontroli informacji wynika, że Urząd w ramach SZBI wdrożył procedury bezpieczeństwa teleinformatycznego oraz fizycznego w celu zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie. W celu zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie Urząd wdrożył system zarządzania użytkownikami systemu informatycznego poprzez kontroler domeny AD oraz politykę bezpieczeństwa fizycznego.

Zgodnie z zarządzeniem Nr 1349.2017 Prezydenta Miasta Ełku z dnia 27 grudnia 2017 r. w sprawie wskazania podstawowego systemu wykonywania czynności kancelaryjnych w Urzędzie Miasta Ełku oraz określenia wyjątków od systemu podstawowego, podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw oraz gromadzenia i tworzenia dokumentacji w Urzędzie jest



Umożliwia prowadzenie dowolnej sprawy w formie elektronicznej od momentu jej zarejestrowania przez pracownika do momentu jej zakończenia. Udostępnia informacje zawarte w pismach w formie dokumentów elektronicznych oraz zeskanowanych dokumentów papierowych.

[akta kontroli str. 25-28, 97-113]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

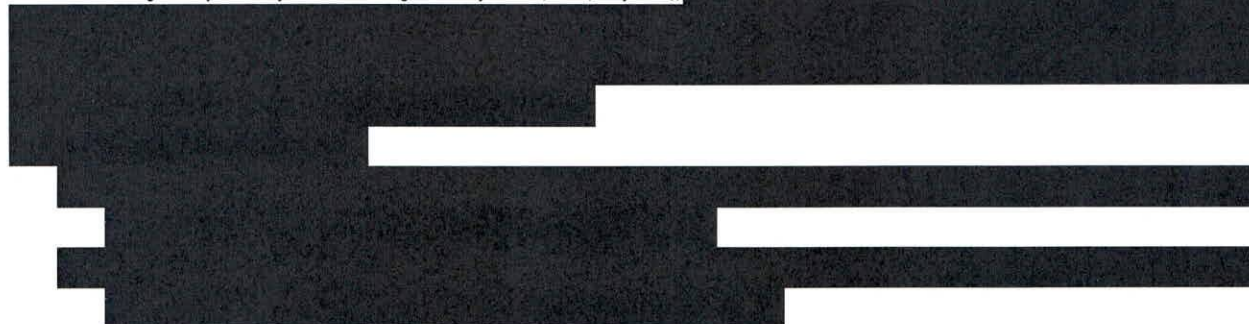
### 1.6. Formaty danych udostępniane przez systemy teleinformatyczne

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.: „



[akta kontroli str. 605-701]

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

## **II. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych**

### **2.1. Dokumenty z zakresu bezpieczeństwa informacji**

Zgodnie z:

- § 20 ust. 1 rozporządzenia KRI podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
- § 20 ust. 2 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań związanych z bezpieczeństwem informacji;
- § 20 ust. 2 pkt 1 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

Realizacja zadań w zakresie ochrony danych wymaga od podmiotu publicznego opracowania dokumentacji SZBI (system zarządzania bezpieczeństwem informacji), w tym szeregu regulacji wewnętrznych oraz zapewnienia aktualizacji tych regulacji w zakresie dotyczącym zmieniającego się otoczenia. Kompleksowa dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) jest warunkiem niezbędnym, w celu skutecznego zarządzania bezpieczeństwem informacji w podmiocie. Podstawowym dokumentem SZBI jest Polityka Bezpieczeństwa Informacji. Polityka zazwyczaj zawiera wyrażoną przez kierownictwo deklarację stosowania, opisuje organizację i ustala osoby odpowiedzialne oraz ich zakresy odpowiedzialności, wprowadza klasyfikację informacji, sposób postępowania z poszczególnymi rodzajami informacji.

W związku z wejściem w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 roku, w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych



osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s.1) – zwanego dalej „RODO”, w celu zapewnienia bezpiecznego przetwarzania informacji w Urzędzie Miasta Ełku wprowadzono System Zarządzania Bezpieczeństwem Informacji składający się z:

[Redacted text block]

[akta kontroli str. 314-385, 495-532]

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

W myśl § 20 ust. 1 rozporządzenia KRI podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji.

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, że realizacja obowiązku wynikającego z § 20 ust. 1 KRI nie kończy się z momentem wdrożenia do stosowania SZBI, lecz wymaga ona nieustannej uwagi.

Zgodnie z harmonogramem wewnętrznego przeglądu i audytu SZBI, przegląd SZBI zaplanowano w Urzędzie w miesiącu czerwcu, natomiast audyt SZBI planowany był w jednostce we wrześniu 2021 r. Ze sprawozdania dotyczącego wewnętrznego przeglądu i audytu SZBI w roku 2021 wynika, że obydwa zadania przeprowadzono łącznie w miesiącu wrześniu 2021 r.

Z wyjaśnień przekazanych w przedmiotowej sprawie wynika, że cyt.: „ [Redacted text block] ”

[akta kontroli str. 605-701]

Z dokumentacji przedstawionej kontrolującym wynika, że w okresie objętym kontrolą dokonano przeglądu SZBI w jednostce zgodnie z § 20 ust. 1 rozporządzenia KRI.

[akta kontroli str. 386-401]

Prezydent Ełku zarządzeniem wewnętrznym powołał w jednostce Inspektora Ochrony Danych (IOD) oraz Administratora Systemu Informatycznego (ASI).

[akta kontroli str. 402-405]

Mając powyższe na uwadze przedmiotowe częściowe 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. Analiza ryzyka jest ważnym wymogiem nałożonym na administratorów i podmioty przetwarzające. Proces szacowania ryzyka powinien być przeprowadzony i udokumentowany w celu wykazania, że ryzyko zostało oszacowane i wprowadzono odpowiednie środki obrony. Szacowanie ryzyka pozwala na aktywne zarządzanie bezpieczeństwem informacji, w tym na przeciwdziałanie zagrożeniom oraz ograniczanie skutków zmaterializowanych ryzyk, a także wpływa na racjonalne zarządzanie środkami finansowymi poprzez stosowanie zabezpieczeń adekwatnych do oszacowanego poziomu ryzyka. Jednocześnie należy zaznaczyć, że prawidłowo przebiegająca analiza ryzyka nie jest jednorazowym działaniem, lecz regularnie i ciągle monitorowanym procesem.

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

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

[akta kontroli str. 605-730]

W toku prowadzonych czynności kontrolnych stwierdzono również, że w jednostce zgodnie z art. 30 RODO, prowadzony jest rejestr czynności przetwarzania danych osobowych. Przedmiotowy rejestr został opracowany i jest prowadzony przez IOD wyznaczonego w Urzędzie.

[akta kontroli str. 406-423]

Mając powyższe na uwadze przedmiotowe częściowe zagadnienie ocenia się pozytywnie.



### **2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego**

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

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

[akta kontroli str. 424]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

### **2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych**

Stosownie do:

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

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

Zasady nadawania uprawnień do przetwarzania danych osobowych oraz do pracy w określonym zbiorze danych (systemie informatycznym), określone zostały w [REDACTED]

[akta kontroli str. 327-345, 473-532]

Osoby posiadające dostęp do danych osobowych i pracujące w określonym systemie posiadały pisemne upoważnienie. Prowadzona była też ewidencja osób upoważnionych do przetwarzania danych osobowych.

[akta kontroli str. 731-736]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

## 2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Z § 20 ust. 2 pkt 6 rozporządzenia KRI wynika, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: a) zagrożenia bezpieczeństwa informacji, b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

Z dokumentacji przedstawionej kontrolującym wynika, że pracownicy Urzędu zaangażowani w proces przetwarzania informacji, uczestniczyli w okresie objętym kontrolą w szkoleniu dotyczących bezpieczeństwa informacji oraz ochrony danych osobowych:

Zakres szkolenia:

- Wprowadzenie do bezpieczeństwa,
- Współczesne zagrożenia dla danych elektronicznych,
- Czym jest bezpieczeństwo informacji,
- Dlaczego należy chronić dane,
- Wybrane skutki utraty kontroli nad danymi,
- Pojęcie integralności, poufności i dostępności,
- Wymagania dotyczące przetwarzania danych,
- Wybrane ramy prawne związane z ochroną i zagrożeniami dla informacji i danych osobowych,
- Określanie poziomu bezpieczeństwa systemów informatycznych,
- Ataki socjotechniczne, podszywanie się, phishing,
- Programy antywirusowe, ochrona przed malware,
- Kopie zapasowe,
- Analiza i ocena ryzyka, zarządzanie ryzykiem,
- Cel procesu szacowania ryzyka,
- Identyfikacja i uwierzytelnienie,
- Pojęcie identyfikacji i uwierzytelnienia,
- Stosowanie haseł i fraz hasłowych,
- Incydenty bezpieczeństwa,
- Plan awaryjny,
- Pojęcie ciągłości działania.

W załączeniu przedstawiono listę pracowników uczestniczących w szkoleniach.

[akta kontroli str. 425-427]

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.

Zbiór podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość określono w [REDACTED]



[akta kontroli str. 327-345, 495-532, 605-701]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

## 2.7. Serwis sprzętu informatycznego i oprogramowania

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

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

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

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

Kontrolujący zwrócili uwagę, że z [redacted] podpisana została tylko umowa licencyjna. Z wyjaśnień przekazanych w przedmiotowej sprawie wynika, że cyt.: „ [redacted] ”

Kontrolujący przychylają się do wyjaśnień Urzędu w kwestii braku umowy powierzenia przetwarzania danych podpisanej z firmą [redacted]. Jednocześnie należy zauważyć, że brak aktualnej umowy powierzenia przetwarzania danych w sytuacji wystąpienia awarii danego systemu, znacznie wydłuży okres jego przywrócenia do prawidłowego działania, gdyż

w pierwszej kolejności należy podpisać stosowną umowę, a dopiero po jej podpisaniu możliwe jest przekazanie ewentualnych uszkodzonych baz danych do weryfikacji w ramach umów serwisowych.

Procedura w zakresie wykonywania przeglądów i konserwacji systemów informatycznych, zawarta jest w [REDAKTOWANE]

[akta kontroli str. 327-345, 495-603. 605-701]

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, umożliwiając szybkie podjęcie działań korygujących.

Instrukcja postępowania w przypadku stwierdzenia zagrożenia w postaci naruszenia bezpieczeństwa informacji oraz podejmowanych działań korygujących została uregulowana w [REDAKTOWANE]

[akta kontroli str. 315-326, 737-741]

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.

Zgodnie z przedstawionym Planem Audytu Jednostki na rok 2021, w obszarze bezpieczeństwo informacji zaplanowano jedno zadanie zapewniające.

Na podstawie okazanej dokumentacji kontrolujący stwierdzili, że w okresie objętym kontrolą przeprowadzono w Urzędzie jedno audytowe zadanie zapewniające w zakresie bezpieczeństwa informacji. Celem zadania zapewniającego było zbadanie i ocena obszaru związanego ze sposobem realizacji zadań z zakresu zapewnienia bezpieczeństwa informacji w Urzędzie Miasta Ełku oraz nadzorowania czynności w zakresie realizacji poszczególnych zadań. Ustalenie sposobu realizacji celów dla prowadzonych działań i sposobu postępowania ze zidentyfikowanymi w obszarach ryzykami. Ocena sposobu zarządzania i administrowania ryzykiem w obszarach objętych zadaniem.

Ponadto w dniach 12-13 lipca 2021 roku w Urzędzie przeprowadzony został zdalny audyt bezpieczeństwa sieci informatycznej. W wyniku przeprowadzonego audytu wykryto podatności o różnym stopniu zagrożenia.

Mając powyższe na uwadze, należy stwierdzić, że obowiązek wynikający z § 20 ust. 2 pkt 14 rozporządzenia KRI który stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok – w 2021 r. został zrealizowany.



[akta kontroli str. 428-472]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

## **2.10. Kopie zapasowe**

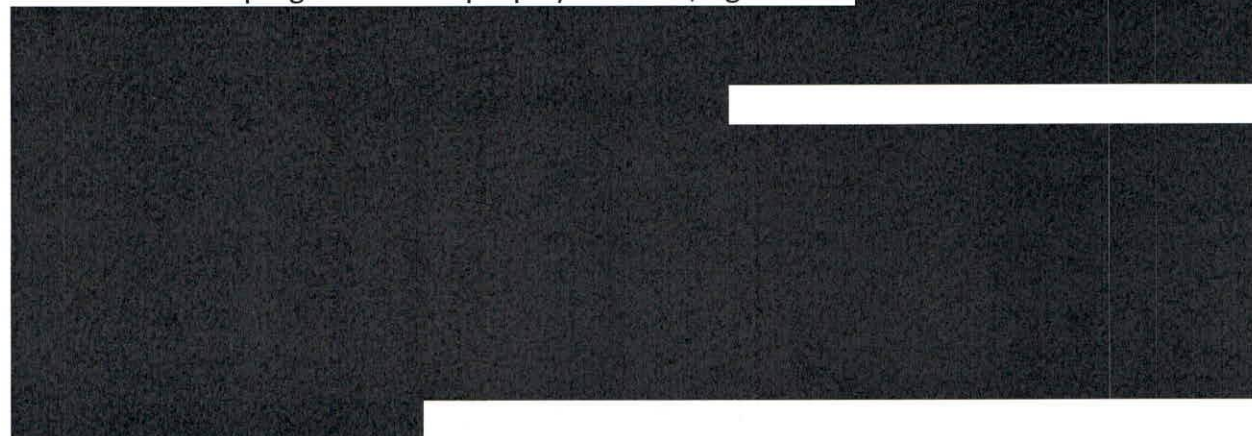
Z § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI wynika, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: minimalizowanie ryzyka utraty informacji w wyniku awarii.

Jednym z kluczowych sposobów zapobiegania utracie informacji w wyniku awarii jest wykonywanie kopii zapasowych. Tworzenie 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.

Zasady tworzenia i przechowywania kopii zapasowych zostały uregulowane w dokumencie –



W przypadku wykonywania testów w celu sprawdzenia poprawności wykonywania kopii zapasowych oraz przydatności utworzonych kopii podczas próby symulowanego przywrócenia i uruchomienia oprogramowania po przywróceniu, zgodnie z



Na podstawie udostępnionej dokumentacji kontrolujący stwierdzili, że w Urzędzie wykonywane są kopie zapasowe z poszczególnych systemów, jak również przeprowadzane są testy w celu sprawdzenia poprawności oraz przydatności wykonywanych kopii zapasowych.

[akta kontroli str. 347-358, 605-701]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

## **2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych**



Stosownie do § 15 ust. 1 rozporządzenia KRI systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.

Wykorzystywane w Urzędzie systemy teleinformatyczne wspomagające realizację zadań z zakresu administracji rządowej, dzieliły się na systemy centralne tj. [REDAKTOWANE] oraz systemy wspierające zakupione u dostawców zewnętrznych – [REDAKTOWANE]. Na obsługę aktualnie zainstalowanego oprogramowania (system informatyczny) zawarte zostały stosowne umowy licencyjne (opieka autorska), gwarantujące rozwój systemu i dostosowanie do obowiązujących przepisów prawa. Zakupiony system teleinformatyczny, w razie awarii podlega ekspertyzie technicznej zlecanej firmie dostarczającej.

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

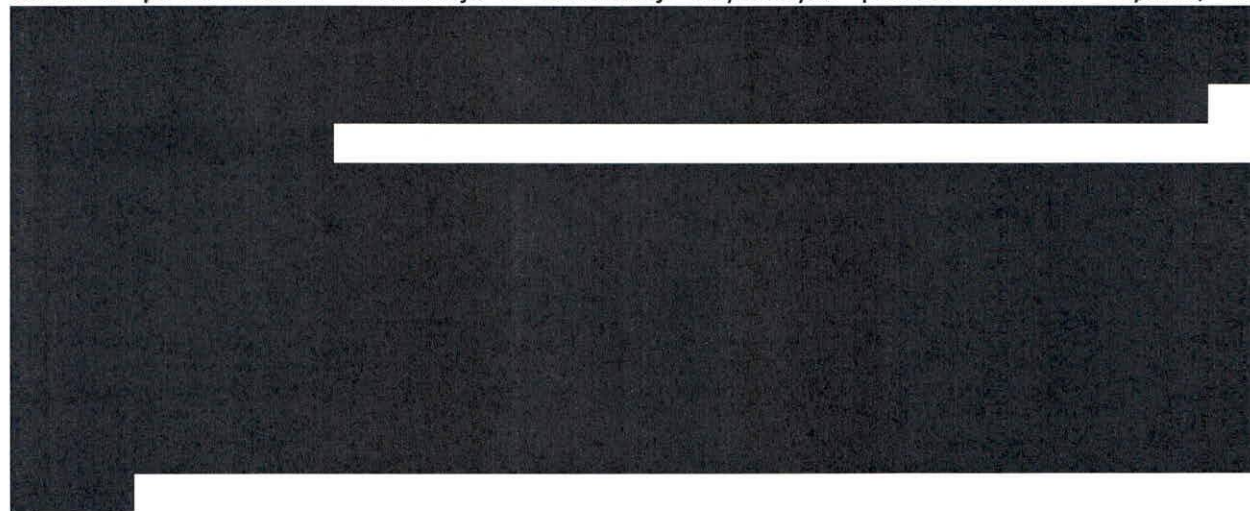
[akta kontroli str. 533-601]

## **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







[akta kontroli str. 379-385, 605-701]

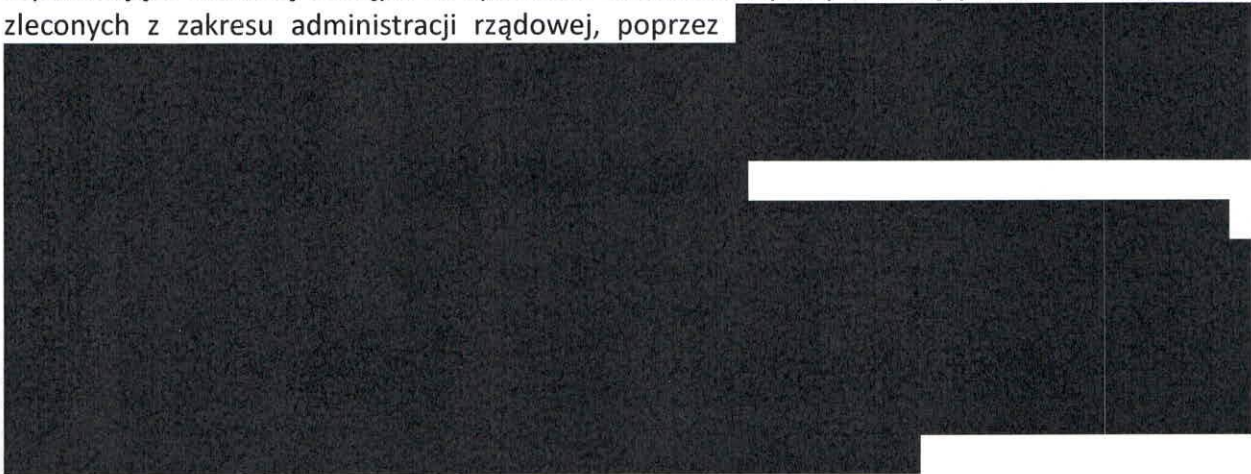
Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

### **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



[akta kontroli str. 605-701]

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).

Z wyjaśnień uzyskanych z Urzędu w powyższej sprawie wynika, że



Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 605-701]

## 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 niedostępszącym, niedowidzącym lub niewidomym zapoznanie się z treścią informacji, m.in. poprzez powiększenie czcionki, obrazu, zmianę kontrastu. Zgodnie z § 19 rozporządzenia KRI, w systemie teleinformatycznym podmiotu realizującego zadania publiczne służące prezentacji zasobów informacji należy zapewnić spełnienie przez ten system wymagań Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia KRI.



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

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

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

Walidacja za pomocą narzędzia <http://wave.webaim.org> tj. walidatora WAVE-WCAG 2.0 Portalu Internetowego Urzędu nie wykazała błędów, natomiast walidacja strony BIP wykazała 4 błędy które nie miały wpływu na realizację zadania.

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. 742-743]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

Do ustaleń kontroli nie wniesiono zastrzeżeń.

#### **IV. Zalecenia**

W związku z tym, iż nie stwierdzono istotnych nieprawidłowości i uchybień w kontrolowanym zakresie, odstępuje się od wydania zaleceń pokontrolnych.

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/*

