



Wydział Finansów i Kontroli  
FK-IV.431.16.2023

Szanowny Pan  
Jarosław Kowalski  
Burmistrz Dobrego Miasta  
ul. Warszawska 14  
11-040 Dobre Miasto

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

### Wystąpienie pokontrolne

Kontrolę przeprowadzono w Urzędzie Miejskim w Dobrym Mieście<sup>1</sup>, ul. Warszawska 14, 11-040 Dobre Miasto, NIP jednostki: 739-10-18-254, REGON jednostki: 000687770.

- W okresie objętym kontrolą oraz w czasie prowadzonych czynności kontrolnych kierownikiem kontrolowanej jednostki był Pan **Jarosław Kowalski** - Burmistrz, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 04.11.2018 r.

[akta kontroli poz. 32]

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

**Radosław Gazda** – inspektor wojewódzki; przewodniczący zespołu kontrolnego, legitymacja służbowa nr 9/2019, wydana przez Dyrektora Generalnego Warmińsko - Mazurskiego Urzędu Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr FK-IV.0030.1015.2023 z 24 listopada 2023 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

<sup>1</sup> Zwanym dalej: Urzędem

FK-IV.0030.1016.2023 z 24 listopada 2023 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli poz. 11-12]

Kontrolę przeprowadzono w dniach 8 grudnia 2023 r. - 3 stycznia 2024 r., co zostało odnotowane w książce kontroli Urzędu pod pozycją Nr 5/2023.

[akta kontroli poz. 22]

Kontrola prowadzona była w trybie hybrydowym, tj. w dniu 8 grudnia br. – rozpoczęto czynności kontrolne w Urzędzie oraz dokonano oględzin serwerowni na miejscu w jednostce. Pozostałe dni (11 grudnia 2023 – 3 stycznia 2024) kontrola była prowadzona zdalnie, bez osobistej obecności kontrolerów Urzędzie, z wykorzystaniem narzędzi informatycznych do zgromadzenia materiału dowodowego, w celu ustalenia stanu faktycznego, a następnie dokonania oceny działalności jednostki kontrolowanej, a także sformułowanie ewentualnych zaleceń pokontrolnych. W dniu rozpoczęcia czynności kontrolnych okazano legitymacje oraz upoważnienia do kontroli, poinformowano o zasadach kontroli w trybie hybrydowym, wymaganych dokumentach do kontroli oraz formach i terminie ich przekazywania.

Przedmiotem kontroli była ocena działania systemów teleinformatycznych używanych przez jednostki samorządu terytorialnego do realizacji zadań zleconych z zakresu administracji rządowej, na podstawie art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. Dz.U. z 2023 r., poz. 57 ze zm.). Okres objęty kontrolą: od 1 stycznia do 31 grudnia 2022 r.

[akta kontroli poz. 1, 18]

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 (tj. Dz. U. z 2023 r., poz. 190), 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 (tj. Dz.U. z 2023 r., poz. 57 ze zm.)<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.

[akta kontroli poz. 1, 18]

Burmistrz upoważnił podinspektora w Referacie Organizacyjnym Urzędu, do udzielania informacji w okresie trwania czynności kontrolnych.

---

<sup>2</sup> Zwanej dalej: ustawą

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

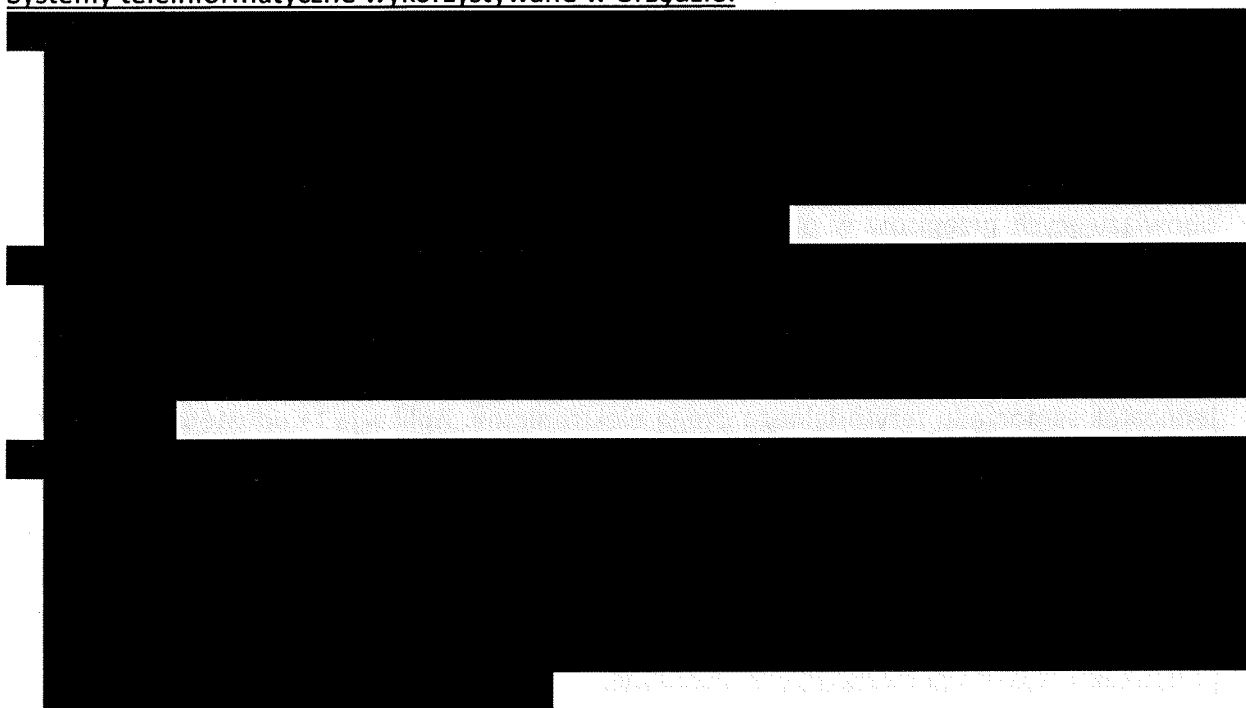
[akta kontroli poz. 33]

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 uchybieniami**.

Ocena działalności jednostki kontrolowanej wynika z ustaleń i ocen dokonanych w poszczególnych obszarach (zagadnieniach) objętych kontrolą.

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

Systemy teleinformatyczne wykorzystywane w Urzędzie:



[akta kontroli poz. 17]

**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 /urządmiestkodobreństwo/SkrytkaESP, znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie i odbieranie pism w formie dokumentów elektronicznych. Formaty danych przyjmowane za pośrednictwem Elektronicznej Skrzynki Podawczej to m.in.: DOC, RTF, XLS, CSV, TXT, GIF, TIF, BMP, JPG, PDF, ZIP.

Podczas kontroli ustalono, że Urząd dysponuje Elektroniczną Skrzynką Podawczą (ESP), która działa zgodnie z określonymi prawnie wymogami. Na stronie internetowej BIP Urzędu wprowadzono opublikowano informację o uruchomieniu ESP, jednakże nie opublikowano informacji o metodach dostarczania i wymaganiach dla dokumentów elektronicznych, wynikających z § 3 ust. 1 rozporządzenia Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (t.j. Dz.U. z 2018 poz.180). Brak spełnienia powyższych wymogów stanowi **uchybiecie** skutkujące niedoinformowaniem petentów o metodach dostarczania i wymaganiach dla dokumentów elektronicznych. Przyczyna uchybiecia jest niestosowanie obowiązujących przepisów w przedmiotowym zakresie. Osobą odpowiedzialną jest pracownik nadzorujący działanie ESP Urzędu.

Na stronie Portalu Urzędu istnieje zakładka „Elektroniczne Biuro Obsługi Interesanta”. Platforma e-Usług Publico 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 Publico daje możliwości interakcji interesantowi z wirtualnym biurem obsługi, gdzie uzyska on dostęp do usług realizowanych przez daną jednostkę z opcją umówienia się na spotkanie oraz złożenia dokumentów, zgodnych z dostępnymi i obsługiwanymi formularzami. Dodatkowo platforma jest połączona z systemami dziedzinowymi jednostek samorządowych, dzięki czemu umożliwia realizację płatności w ramach zobowiązań wynikających z podatków i innych opłat w zakresie oferowanych usług, a także dostęp do danych udostępnionych publicznie oraz danych ściśle powiązanych z zalogowanym interesantem.

[akta kontroli poz. 23, 28-29]

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. Jednocześnie należy zaznaczyć, że Urząd nie świadczył usług związanych z załatwianiem spraw od początku do końca w formie elektronicznej, za pomocą systemów teleinformatycznych. Istnieje jednak możliwość złożenia wniosku w formie elektronicznej (np. ePUAP), w przypadku wybranych spraw załatwianych w Urzędzie.

W zakresie publikacji procedur załatwiania spraw realizowanych przez Urząd należy stwierdzić, że zarówno na stronie BIP w zakładce „Procedury załatwiania spraw”, jak i na Portalu Urzędu w zakładce „Na skróty”, opublikowany jest przydatny dla petentów wykaz usług (w tym

elektronicznych) wraz ze sposobem postępowania, które realizowane są przez poszczególne referaty i samodzielne stanowiska Urzędu.

Jednocześnie na stronie BIP w zakładce „Druki do pobrania” opublikowane są wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych referatów oraz samodzielnych stanowisk w Urzędzie. Podobnie portal Internetowy Urzędu w zakładce „Na skróty” → „Dokumenty do pobrania”, zawiera wzory wniosków i dokumentów w zakresie działania poszczególnych referatów w Urzędzie.

Urząd świadczył za pomocą ePUAP usługę „Pismo ogólne do podmiotu publicznego. Usługa przeznaczona jest do tworzenia pism w postaci elektronicznej wnoszonych za pomocą elektronicznej skrzynki podawczej lub doręczanych przez podmioty publiczne za potwierdzeniem doręczenia, w przypadkach gdy łącznie spełnione są następujące warunki: organ administracji publicznej nie określił wzoru dokumentu elektronicznego umożliwiającego załatwienie danej sprawy, przepisy prawa nie wskazują jednoznacznie, że jedynym skutecznym sposobem przekazania informacji jest jej doręczenie w postaci papierowej.

[akta kontroli poz. 24-27]

W związku z powyższym przedmiotowe częściowe zagadnienie ocenia się **pozytywnie z uchybieniami**.

## **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 Urząd nie przekazywał wzorów dokumentów do CRWDE. Jednocześnie na stronie BIP w zakładce „Druki do pobrania” opublikowane są wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych referatów oraz samodzielnych stanowisk w Urzędzie. Podobnie portal Internetowy Urzędu w zakładce „Na skróty” → „Dokumenty do pobrania”, zawiera wzory wniosków i dokumentów w zakresie działania poszczególnych referatów w Urzędzie.

[akta kontroli poz. 14]

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 <https://www.dobremiasto.com.pl/>, a strona internetowa BIP Urzędu – pod adresem <https://bip.dobremiasto.com.pl/>

Na stronie głównej Portalu Urzędu, zawarto bezpośrednie odnośniki (linki) do przydatnych informacji oraz stron przeznaczonych dla mieszkańców Gminy.

Ponadto na Internetowej stronie głównej Urzędu - w zakładce „Elektroniczne Biuro Obsługi Interesanta”, zamieszczono link do platformy e-Uслуг Publico przeznaczonej dla mieszkańców, którzy chcą korzystać z usług jednostek samorządu terytorialnego drogą elektroniczną.

Na stronie BIP w zakładce „Druki do pobrania” opublikowane są wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych referatów oraz samodzielnych stanowisk w Urzędzie. Podobnie portal Internetowy Urzędu w zakładce „Na skróty” → „Dokumenty do pobrania”, zawiera wzory wniosków i dokumentów w zakresie działania poszczególnych referatów w Urzędzie.

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

### 1.4. Współpraca systemów teleinformatycznych z innymi systemami

Stosownie do:

- § 5 ust. 3 pkt 3 rozporządzenia KRI interoperacyjność na poziomie semantycznym 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.:

[akta kontroli poz. 54]

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

#### **1.5. Obieg dokumentów w podmiocie publicznym**

Z § 20 ust. 2 pkt 9 rozporządzenia KRI wynika, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie, m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie.

Zgodnie z zarządzeniem Nr Og.0050.245.2019.MG Burmistrza Dobrego Miasta z dnia 23 grudnia 2019 r. w sprawie wprowadzenia Systemu Elektronicznego Obiegu Dokumentów EDICTA w Urzędzie Miejskim w Dobrym Mieście - podstawowym sposobem dokumentowania przebiegu, załatwiania i rozstrzygania spraw w Urzędzie Miejskim w Dobrym Mieście, jest system tradycyjny. Funkcjonujący w urzędzie elektroniczny system obiegu dokumentów działa równoległe do obiegu dokumentacji prowadzonej w systemie tradycyjnym i jest systemem wspomagającym system tradycyjny.

EDICTA to elektroniczny system obsługi dokumentów. Umożliwia zarządzanie dokumentami, korespondencją, sprawami (projektami), poleceniami, terminami oraz czasem pracy pracowników, tworząc centralną, uporządkowaną bazę dokumentów i informacji. Umożliwia również sprawny dostęp do korespondencji, umów, procedur wewnętrznych itp., kontroluje drogę obiegu korespondencji oraz stan realizacji projektów, usprawnia obsługę klientów. Moduł zarządzania procesami pracy – wyposażony w graficzny edytor – pozwala na automatyzację procesów zachodzących w organizacji.

Opracowanie procedur dotyczących wykonywania czynności kancelaryjnych, w których określone są zasady obiegu dokumentów wpływających drogą elektroniczną oraz zakres stosowania elektronicznego obiegu dokumentów, zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI, umożliwia realizację i egzekwowanie, m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. Opracowanie zasad postępowania z dokumentacją elektroniczną (wnioski elektroniczne, e-maile) oraz wymagań organizacyjno-technicznych dotyczących zarządzania tą dokumentacją pozwala właściwie dbać o jej bezpieczeństwo.

[akta kontroli poz. 34]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

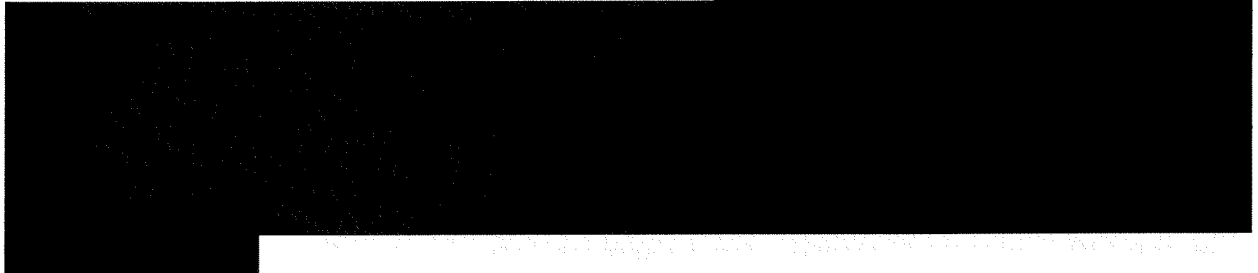
#### 1.6. Formaty danych udostępniane przez systemy teleinformatyczne

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 poz. 54]

W trakcie kontroli ustalono ponadto, że operacja synchronizacji *Respons* → *SRP ŹRÓDŁO* odbywa się na podstawie skryptu wymiany danych pomiędzy tymi systemami, na stanowisku służącym jedynie do celów komunikacji między wskazanymi systemami. Dane z systemu *Respons* mogą być udostępniane w formatach danych określonych w załącznikach nr 2 do rozporządzenia KRI.

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.



## II. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych

### 2.1. Dokumenty z zakresu bezpieczeństwa informacji

Zgodnie z:

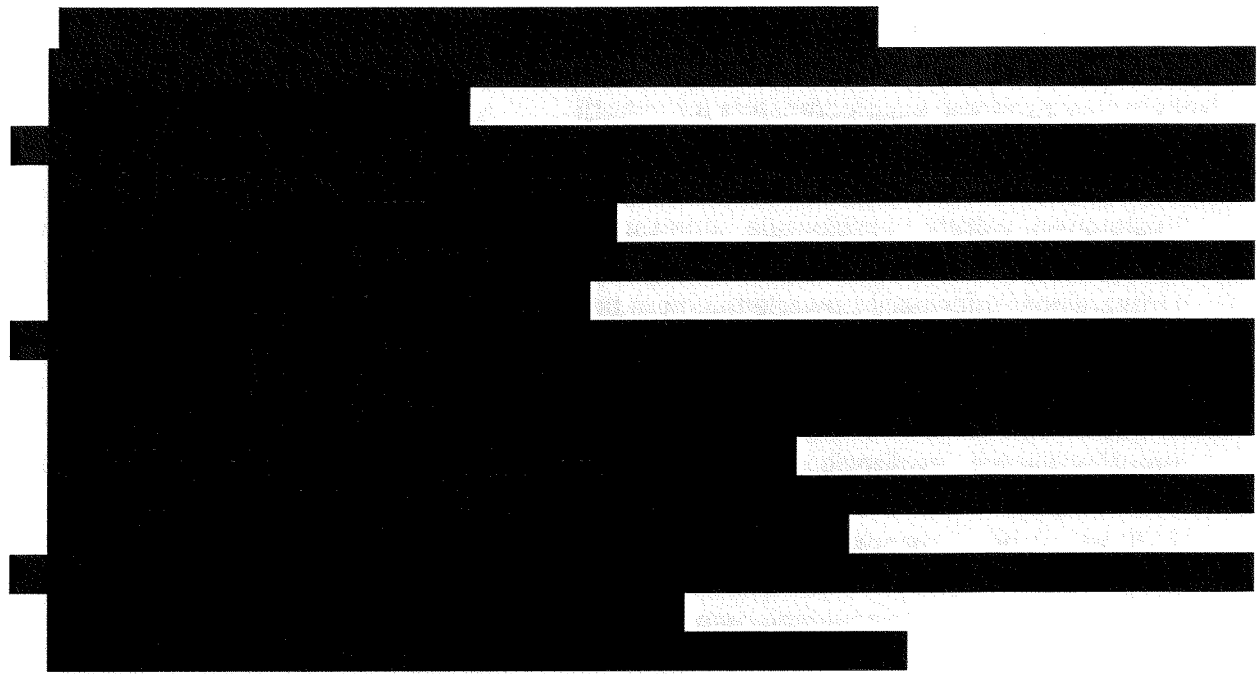
- § 20 ust. 1 rozporządzenia KRI podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, 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.

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 jednolitego i adekwatnego systemu zarządzania bezpieczeństwem informacji (SZBI) w Urzędzie, przyjęto

Przedmiotową dokumentację sporządzono na podstawie obowiązujących przepisów prawa w tym zakresie, tj. „RODO” oraz „KRI”. 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.

[akta kontroli poz. 42-44, 54]

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. Zgodnie z wyjaśnieniem uzyskanym z Urzędu, cyt.:



Jednocześnie, należy wskazać, że 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.

[akta kontroli poz. 54-61]

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

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

Kontrolującym przedstawiono dokumentację (stanowiącą akta kontroli) świadczącą o przeprowadzeniu okresowej analizy ryzyka utraty integralności, dostępności lub poufności informacji w Urzędzie w 2022 roku.

[akta kontroli poz. 35-36]

W toku prowadzonych czynności kontrolnych stwierdzono, że w jednostce zgodnie z art. 30 RODO, prowadzony jest rejestr czynności przetwarzania. W jednostce powołano również Inspektora Ochrony Danych.

[akta kontroli poz. 37, 54, 62-63]

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 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 poz. 38-39, 64]

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.

Osoby posiadające dostęp do danych osobowych posiadały pisemne upoważnienia do ich przetwarzania oraz do przetwarzania danych osobowych w określonym zbiorze danych wynikającym z zakresu czynności danego pracownika. W jednostce prowadzona była ewidencja osób upoważnionych do przetwarzania danych osobowych.

[akta kontroli poz. 40, 65-66]

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.

W okresie objętym kontrolą, zapewniono pracownikom zaangażowanym w proces przetwarzania informacji szkolenie, wynikające z § 20 ust. 2 pkt 6 rozporządzenia KRI. Zakres szkolenia obejmował następujące zagadnienia:

- Główne założenia i wymagania prawne cyberbezpieczeństwa w pracy urzędnika.
- Polityka bezpieczeństwa w organizacji.
- Definicja incydentu bezpieczeństwa i zasady postępowania z incydemem.
- Rodzaje ataków: ataki socjotechniczne, ataki komputerowe, ataki przez sieci.
- Bezprzewodowe, ataki przez pocztę e-mail (fałszywe e-maile), ataki przez strony WWW.
- Ataki przez telefon, phishing, spoofing, poparte rzeczywistymi przykładami.
- Zasady cyberhigieny.
- Bezpieczeństwo fizyczne - urządzenia, dokumenty, „czyste biurko”.
- Zdalny dostęp do zasobów jednostki i korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia.
- Polityka haseł, zarządzanie dostępem i tożsamością.

Szkolenie przeprowadziła Firma EDPO zajmująca się organizacją systemu bezpieczeństwa informacji i ochrony danych. Lista obecności na szkoleniu stanowi akta kontroli.

[akta kontroli poz. 41]

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.

Zasady pracy zdalnej z wykorzystaniem przez pracowników służbowego sprzętu, przyjęte zostały zarządzeniem [redacted]

[akta kontroli poz. 42-44]

Mając powyższe na uwadze przedmiotowe częściowe zagadnienie ocenia się pozytywnie.

## **2.7. Serwis sprzętu informatycznego i oprogramowania**

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

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

[redacted]

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

[redacted]

[akta kontroli poz. 45-46]

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, umożliwiający szybkie podjęcie działań korygujących.

[akta kontroli poz. 43-44]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

## **2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji**

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

Audyt bezpieczeństwa informacji jest procesem przeprowadzanym w celu zidentyfikowania zagrożeń mogących skutkować utratą poufności, integralności lub dostępności informacji. Celem audytu wewnętrznego bezpieczeństwa informacji jest ocena zakresu zgodności Systemu Zarządzania Bezpieczeństwem Informacji jednostki z kryteriami audytu.

Zgodnie z przekazanym wyjaśnieniem, w 2022 roku Urząd dokonał sprawdzenia zgodności ustanowionego systemu zarządzania bezpieczeństwem informacji z rozporządzeniem KRI oraz ustawą o krajowym systemie cyberbezpieczeństwa. Przedłożony w toku kontroli dokument, w rzeczywistości odpowiada kryteriom audytu wewnętrznego bezpieczeństwa informacji, gdyż w dokumencie tym poddano analizie zagadnienia wskazane w rozporządzeniu KRI. W określonych obszarach poddanych ocenie, nie dopatrzonego się braku ich spełnienia.

Mając powyższe na uwadze, należy stwierdzić, że obowiązek wynikający z § 20 ust. 2 pkt 14 rozporządzenia KRI – w 2022 r. został zrealizowany.

[akta kontroli poz. 47-48, 54]

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.

[REDAKTION]

Na podstawie udostępnionej dokumentacji oraz wyjaśnień kontrolujący stwierdzili, że w Urzędzie są wykonywane kopie zapasowe m.in. z systemów objętych kontrolą.

[REDAKTION]

[akta kontroli poz. 49-51, 54, 67]

W przypadku prowadzenia testów w celu sprawdzenia poprawności wykonywania kopii zapasowych oraz przydatności utworzonych kopii podczas próby symulowanego przywrócenia i uruchomienia oprogramowania, zgodnie z wyjaśnieniem w powyższej sprawie, cyt.:

[REDAKTION]

[akta kontroli poz. 51]

Mając na względzie wyjaśnienia uzyskane z Urzędu w tym zakresie, należy stwierdzić, że opisany sposób dokonywania sprawdzenia przydatności wytworzonej kopii bezpieczeństwa spełnia swoją funkcję, gdyż dane są odzyskiwane.

[REDAKTION]

Mając powyższe na uwadze należy stwierdzić, że w okresie objętym kontrolą nie wytworzono dokumentacji potwierdzającej wykonanie testów odtworzeniowych (np. notatki, wpisy w dzienniku systemowym). Brak dokumentacji świadczącej o wykonaniu testów odtworzeniowych, oraz brak stosownych zapisów w POD, w zakresie metodyki i harmonogramu wykonywania testów odtworzeniowych **należy uznać za uchybienie**, skutkujące naruszeniem § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI. Przyczyną powstania uchybienia jest niestosowanie przepisów prawa w tym zakresie. Osobą odpowiedzialną za uchybienie jest Informatyk jednostki oraz osoba dokonująca przeglądów POD.

Regularne tworzenie i testowanie jakości kopii zapasowych jest kluczowym działaniem w celu minimalizowania ryzyka utraty informacji w wyniku awarii. Prawidłowo zdefiniowana polityka kopii bezpieczeństwa oraz gruntownie przetestowane procesy odtwarzania systemów teleinformatycznych są istotnymi aspektami w każdej jednostce, której procesy opierają się na działaniu systemów informatycznych. Prawidłowo zdefiniowana i wykonana procedura pozwala mieć pewność, że w razie awarii systemu, wytworzone backupy spełnią swoje zadanie i nie odbije się to negatywnie na ciągłości działania jednostki.

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.



Na obsługę zainstalowanego w okresie objętym kontrolą 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.

[akta kontroli poz. 45]

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

### **2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji**

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

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

W celu uzyskania odpowiedniego poziomu BI, przy jednoczesnym zapewnieniu właściwego bieżącego dostępu uprawnionym użytkownikom, stosowany jest szereg zabezpieczeń technicznych. Celem zabezpieczeń jest uzyskanie ochrony przetwarzanych informacji przed ich



kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także np. kradzieżą środków przetwarzania informacji.

[akta kontroli poz. 68]

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:

Podczas kontroli dokonano oględzin pomieszczenia serwerowni w Urzędzie, w obecności Pana Arkadiusza Szymakowicza pracownika Referatu Organizacyjnego Urzędu Miejskiego w Dobrym Mieście - Informatyka Urzędu. W toku oględzin stwierdzono:

[akta kontroli poz. 20-21]

Stwierdzone uchybienie, skutkować może utratą przetwarzanych informacji w wyniku awarii sprzętu. Przyczyną powstania uchybienia jest niepełne dostosowanie pomieszczenia serwerowni do pracy jednostek centralnych, na których opiera się działanie poszczególnych systemów informatycznych w Urzędzie. Osobą odpowiedzialną jest pracownik kontrolowanej jednostki nadzorujący funkcjonowanie serwerowni.

Przedmiotowe częściowe zagadnienie ocenia się **pozytywnie z uchybieniami**.

#### **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 informacji uzyskanych w trakcie kontroli wynika, że logi systemowe gromadzone są wewnątrz kontrolowanych systemów przez okres dłuższy niż dwa lata.

[akta kontroli poz. 54, 70]

Mając na uwadze powyższe, przedmiotowe cząstkowe 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.

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

- możliwość doboru odpowiedniego kontrastu (ciemny-jasny),
- możliwość powiększenia wielkości liter na stronie,
- funkcja „Przeczytaj na głos”,
- podświetlanie linków,
- moduł wyszukiwania.

Ponadto na stronie internetowej Urzędu Miejskiego oraz BIP, można korzystać z następujących skrótów klawiaturowych:

- TAB - przejście do następnej pozycji,
- SHIFT + TAB - przejście do poprzedniej pozycji,
- ENTER - przejście do podrzędnej pozycji lub wybór pozycji,
- STRZAŁKA GÓRA/DÓŁ - nawigowanie po pozycjach w zakresie jednego poziomu.

Dostępność cyfrowa to cecha rozwiązań cyfrowych (np. stron, aplikacji, systemów), która umożliwia samodzielne korzystanie z nich przez osoby z niepełnosprawnościami. Jednocześnie wiele jej elementów jest uniwersalnych (np. kontrast, napisy), poprawiających użyteczność każdemu, a nie tylko osobom niepełnosprawnym.

Dostępne cyfrowo muszą być między innymi strony internetowe, aplikacje mobilne, systemy teleinformatyczne i wszystkie treści publikowane w Internecie przez podmioty publiczne. To wyzwanie wdrożeniowe, ale także szansa na dotarcie z informacjami i usługami do szerokiej grupy użytkowników, w tym osób z niepełnosprawnościami.

Jednocześnie należy zaznaczyć, że pomimo tego, że dana strona zawiera podstawowe elementy umożliwiające korzystanie z treści na niej zawartych przez osoby niepełnosprawne (np. kontrast, powiększenie czcionki, wyszukiwanie), to strona ta wcale nie musi z automatu spełniać kryteriów dostępności cyfrowej.

Walidacja za pomocą narzędzia <http://wave.webaim.org> tj. walidatora WAVE-WCAG 2.0 dla strony BIP wykazała 4 błędy, natomiast walidacja portalu internetowego Urzędu, nie wykazała błędów. WAVE-WCAG jest narzędziem do automatycznego testowania dostępności serwisów internetowych. Pomaga administratorom tworzyć bardziej dostępne strony internetowe. W wyniku automatycznej analizy wskazuje ewentualne miejsca, które mogą powodować problemy z dostępnością.

Brak pełnej zgodności z ustawą o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, **należy ocenić jako uchybienie**. Przyczyną uchybienia jest częściowe niedostosowanie stron internetowych do standardów dostępności, w tym WCAG 2.0. Skutek uchybienia - brak zapewnienia maksymalnego wsparcia osobom niepełnosprawnym. Odpowiedzialnym za powstanie uchybienia jest osoba nadzorująca BIP kontrolowanej jednostki.

[akta kontroli poz. 30-31]

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

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.


#### IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny, wnoszę o:

[Redacted text block]

[Redacted text block]

[Redacted text block]



Proszę Pana Burmistrza o podjęcie działań mających na celu usunięcie stwierdzonych 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  
***Radosław Król***

*/podpisano podpisem elektronicznym/*