WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

Olsztyn, 30 grudnia 2020 r.

FK-IV.431.20.2020

Szanowny Pan
Andrzej Jan Mazur
Wójt Gminy Lubomino
ul. Kopernika 7
11-135 Lubomino

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 Gminy w Lubominie[1], ul. Kopernika 7, 11-135 Lubomino, NIP: 7391163542, REGON: 000540920.

W okresie objętym kontrolą oraz w czasie prowadzonych czynności kontrolnych kierownikiem kontrolowanej jednostki był Pan Andrzej Mazur – Wójt Gminy, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 2l października 2018 roku.

Odpowiedzialnymi za realizację zadania objętego kontrolą byli:
1. Pan [redacted] – świadczący usługi informatyczne na podstawie umowy zawartej w dniu 31 grudnia 2019 r. (firma zewnętrzna).
2. Pani [redacted] – pełniąca funkcję Inspektora Ochrony Danych Osobowych, zatrudniona w Urzędzie od dnia 1 lutego 2018 r.

Nadzorującym bezpośrednio pracownika Urzędu realizującego zadania objęte kontrolą była Pani Krystyna Błażewicz - Sekretarz Gminy.

[akta kontroli str. 70, 216]

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

[1] Zwanego dalej: Urzędem

upoważnienia do kontroli nr FK-IV.0030.354.2020 z 5 listopada 2020 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.
Michał Wasilewski – inspektor wojewódzki; członek zespołu kontrolnego, legitymacja służbowa nr 23/2020, wydana przez Dyrektora Generalnego Warmińsko - Mazurskiego Urzędu Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr FK-IV.0030.355.2020 z 5 listopada 2020 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 15-20]

Kontrolę przeprowadzono w dniach 18 listopada – 11 grudnia 2020 r., co zostało odnotowane w książce kontroli Urzędu pod pozycją Nr 2/2020.
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 2020 r., poz. 346 ze zm.). Okres objęty kontrolą: od dnia 1 stycznia 2018 r. do dnia 18 listopada 2020 r. (dzień rozpoczęcia czynności kontrolnych).

[akta kontroli str. 1-2, 51-61]

Kontrola została przeprowadzona na podstawie art. 2 pkt 1 i art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U. 2020 poz. 224), art. 28 ust. 1 pkt 2 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz. U. z 2019 r., poz. 1464), w związku z art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2017 r. poz. 570 ze zm. - akt prawny obowiązujący do 02.04.2019 r., Dz.U. z 2019 r. poz. 700 ze zm. - akt prawny obowiązujący do 04.03.2020 r. oraz Dz.U. z 2020 r., poz. 346 ze zm.)[2], rozdziału III i IV Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247 ze zm.)[3], jak również Wytycznych

[2] Zwanej dalej: ustawą
[3] Zwanego dalej: rozporządzeniem KRI

dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych, zatwierdzonych przez Ministra Cyfryzacji w dniu 15 grudnia 2015 r.

[akta kontroli str. 1-2, 51-61]

Wójt Gminy Lubomino upoważnił Inspektora Ochrony Danych Osobowych do udzielania informacji i wyjaśnień w okresie trwania czynności kontrolnych.

[akta kontroli str. 69]

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 **4** systemy teleinformatyczne:

1. Źródło (Rejestr PESEL, Rejestr Stanu Cywilnego, Rejestr Dowodów Osobistych),
2. PUMA (ewidencja ludności, rejestr wyborców),
3. SYGNITY (świadczenia rodzinne, fundusz alimentacyjny, świadczenia wychowawcze, dobry start, dodatki mieszkaniowe i energetyczne),
4. CEIDG (działalność gospodarcza).

[akta kontroli str. 39-42]

Systemy teleinformatyczne wykorzystywane w Urzędzie:

1) **ŹRÓDŁO** – (Rejestr PESEL, Rejestr Stanu Cywilnego, Rejestr dowodów osobistych) bezpłatna aplikacja, która obsługuje wszystkie wymagane polskim prawem działania w zakresie rejestru PESEL, dowodów osobistych. Dodatkowo umożliwia również realizację zadań Systemu Odznaczeń Państwowych oraz Centralnego Rejestru Sprzeciwów. W efekcie ŹRÓDŁO to uniwersalne narzędzie obsługujące m.in.: Rejestr PESEL, Rejestr Bazy Usług Stanu Cywilnego (BUSC), Rejestr Dowodów Osobistych (RDO), System Odznaczeń Państwowych (SOP), Centralny Rejestr Sprzeciwów (CRS).

2) **PUMA - Moduł Ewidencja Ludności (rejestr mieszkańców)** posiada homologację Ministerstwa Spraw Wewnętrznych, a jego zadaniem jest kompleksowa obsługa komórki ewidencji ludności. Aplikacja umożliwia między innymi: gromadzenie, wyszukiwanie, uzupełnianie oraz zmianę w bazie danych wszystkich informacji znajdujących się na Karcie Osobowej Mieszkańca. Program automatyzuje pracę i drukuje zawiadomienia w zakresie: meldowania, wymeldowania, rejestracji urodzeń, zgonów, zmian stanu cywilnego - gromadzenia i dostępu do danych historycznych mieszkańców.
Moduł Wyborcy - kompleksowa obsługa wyborów. Moduł Wyborcy umożliwia prowadzenie i aktualizację rejestru wyborców, sporządzanie spisów wyborców uprawnionych

do udziału w wyborach i referendum, pozwala na generowanie kwartalnych meldunków dla KBW (Krajowego Biura Wyborczego) o stanie wyborców mieście na podstawie bazy danych ewidencyjnych.

3) **SYGNITY**, który dzieli się na moduły:
   - **Oprogramowanie do Obsługi Świadczeń Rodzinnych (SR)** ma na celu wspomaganie pracowników w realizacji zadań wynikających z ustawy o świadczeniach rodzinnych oraz towarzyszących ustawie aktów prawnych. Zadaniem oprogramowania SR jest obsługa rejestracji i przetwarzania danych związanych z procesem przyznawania i wypłaty świadczeń rodzinnych, windykacji świadczeń nienależnie pobranych oraz monitorowania stanu realizacji zadań. Zarejestrowane dane wykorzystywane są w obligatoryjnej sprawozdawczości statystycznej.
   - **Oprogramowanie do obsługi Funduszu Alimentacyjnego (FA)** ma na celu wspomaganie pracowników w realizacji zadań wynikających z ustawy o pomocy osobom uprawnionym do alimentów oraz towarzyszących ustawie aktów prawnych. Zadaniem oprogramowania FA jest obsługa rejestracji i przetwarzania danych związanych z procesem przyznawania i wypłaty świadczeń, obsługą świadczeń nienależnie pobranych, zadłużeń dłużników alimentacyjnych oraz monitorowania stanu realizacji zadań. Zarejestrowane dane wykorzystywane są w obligatoryjnej sprawozdawczości statystycznej.
   - **Oprogramowanie do Obsługi Świadczeń Wychowawczych (SW) + Dobry Start**, zapewnia pracownikom pomoc w realizacji podstawowych zadań wynikających z ustawy o pomocy państwa w wychowywaniu dzieci. Zadaniem Oprogramowania SW + Dobry Start jest obsługa rejestracji i przetwarzania danych związanych z procesem przyznawania i wypłaty świadczenia Dobry Start, windykacji świadczeń nienależnie pobranych, monitorowania stanu realizacji zadań oraz wykorzystaniu danych zarejestrowanych w systemie w obligatoryjnej sprawozdawczości statystycznej.
   - **Oprogramowanie do Obsługi Dodatków Mieszkaniowych i Energetycznych (DM/DE)** ma na celu wspomaganie pracowników w realizacji zadań wynikających z ustawy o dodatkach mieszkaniowych oraz towarzyszących tej ustawie aktów prawnych. Zadaniem Oprogramowania DM/DE jest obsługa rejestracji i przetwarzania danych związanych z procesem przyznawania i wypłaty dodatków mieszkaniowych i energetycznych, monitorowania stanu realizacji zadań oraz wykorzystaniu danych zarejestrowanych w systemie w obligatoryjnej sprawozdawczości statystycznej.

4) **CEIDG** jest to elektroniczny rejestr przedsiębiorców działających na terenie kraju. Portal ułatwia podatnikom prowadzenie działalności gospodarczej. Umożliwia on założenie firmy, aktualizację danych, jak również zamknięcie czy zawieszenie działalności gospodarczej. Służy również do przekazywania informacji o wydanych zezwoleniach, koncesjach oraz wpisach do rejestrów.

<u>Rejestry publiczne i ewidencje prowadzone w Urzędzie:</u>

- Rejestr działalności regulowanej w zakresie odbierania odpadów komunalnych od właścicieli nieruchomości (podstawa prawna - art. 9b ust. 2-3 ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach, Dz. U. z 2020 r., poz. 1439).
- Ewidencja udzielonych i cofniętych zezwoleń na opróżnianiem zbiorników bezodpływowych i transport nieczystości ciekłych na terenie Gminy (podstawa prawna - art. 7 ust. 6b ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach, Dz. U. z 2020 r., poz. 1439).
- Rejestr żłobków i klubów dziecięcych Gminy Lubomino
- Rejestr instytucji kultury, dla których organizatorem jest Gmina.

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

1.1. Usługi elektroniczne

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

Zgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI interoperacyjność na poziomie organizacyjnym osiągana jest przez:

a) informowanie przez podmioty realizujące zadania publiczne, w sposób umożliwiający skuteczne zapoznanie się, o sposobie dostępu oraz zakresie użytkowym serwisów dla usług realizowanych przez te podmioty;

b) publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.

Urząd posiada aktywną Elektroniczną Skrzynkę Podawczą (adres skrytki na ePUAP: /UGLUBOMINO/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.: ODF, ODS, DOC, RTF, XLS, CSV, TXT, PNG, GIF, TIF, BMP, JPG, PDF, ZIP, RAR, 7zip.

W zakresie publikacji procedur załatwiania spraw realizowanych przez Urząd należy stwierdzić, iż na stronie BIP w zakładce prawo lokalne – załatwianie spraw, opublikowane są wzory wniosków i formularzy, będących w zakresie poszczególnych referatów w Urzędzie.

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

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

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

[akta kontroli str. 309-314]

1.2. Centralne repozytorium wzorów dokumentów elektronicznych (CRWDE)

Stosownie do art. 19b ust. 3 ustawy, *organy administracji publicznej przekazują do centralnego repozytorium oraz udostępniają w Biuletynie Informacji Publicznej wzory dokumentów elektronicznych. Przy sporządzaniu wzorów dokumentów elektronicznych stosuje się międzynarodowe standardy dotyczące sporządzania dokumentów elektronicznych przez organy administracji publicznej, z uwzględnieniem konieczności podpisywania ich kwalifikowanym podpisem elektronicznym.*

W celu ujednolicenia w skali kraju procedur usług świadczonych przez urzędy drogą elektroniczną, w tym ujednolicenia wzorów dokumentów elektronicznych w CRWDE przechowywane są wzory dokumentów, jakie zostały już opracowane i są używane. W przypadku uruchamiania przez dany podmiot publiczny usługi elektronicznej, która funkcjonuje już na koncie innego podmiotu, dany podmiot publiczny powinien skorzystać z procedury obsługi tej usługi oraz zastosować wzory dokumentów elektronicznych dotyczące tej procedury znajdujące się w CRWDE (nie dotyczy to sytuacji gdy usługa jest usługą centralną, tzn. jest udostępniania przez jeden podmiot, np. właściwego ministra, ale służy do świadczenia usług przez inne podmioty niż udostępniający, np. wszystkie gminy). W przypadku uruchamiania usługi, dla której nie ma wzorów dokumentów w CRWDE, podmiot publiczny jest zobowiązany przekazać do CRWDE procedurę obsługi usługi i wzory dokumentów elektronicznych z nią związanych.
W trakcie kontroli ustalono, że Urząd w badanym okresie nie przekazywał wzorów dokumentów elektronicznych do centralnego repozytorium wzorów dokumentów prowadzonego przez Ministerstwo Cyfryzacji, ze względu na fakt, iż nie uruchamiał nowej usługi, dla której nie ma wzorów dokumentów w CRWDE.
Jednocześnie należy zaznaczyć, iż na stronie BIP kontrolowanego Urzędu, opublikowano w wersji „do pobrania" formularze wzorów dokumentów niezbędnych do załatwienia poszczególnych spraw w Urzędzie.
W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 25-38]

1.3. Model usługowy

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

Strona internetowa Urzędu działa pod adresem http://www.lubomino.ug.gov.pl, a strona internetowa BIP Urzędu – pod adresem ttps://bip.lubomino.tensoft.pl.

Na stronie internetowej Urzędu zamieszczono bezpośredni link do strony BIP Urzędu oraz adres do ESP (elektroniczna skrzynka podawcza), w zakładce dane kontaktowe. Na stronie głównej BIP Urzędu zamieszczono adres do ESP oraz bezpośredni link do platformy ePUAP.

[akta kontroli str. 309-314]

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

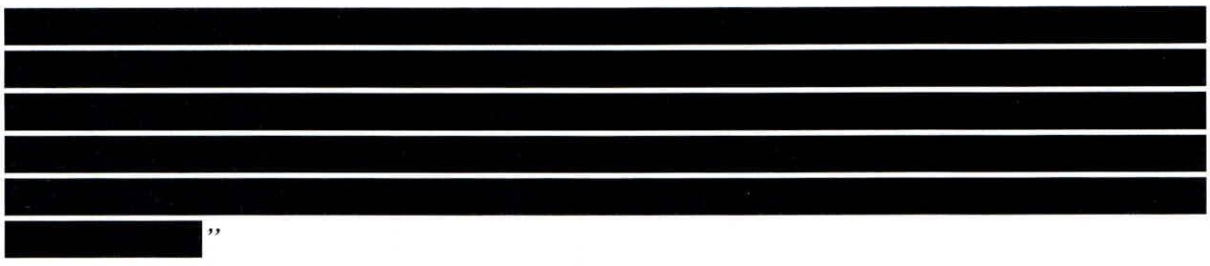
1.4. Współpraca systemów teleinformatycznych z innymi systemami

Stosownie do:

- § 5 ust. 3 pkt 3 rozporządzenia KRI *interoperacyjność na poziomie semantycznym osiągana jest przez: stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań;*
- § 16 ust. 1 rozporządzenia KRI *systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.*

Wiele rejestrów w urzędach administracji publicznej przechowuje i przetwarza identyczne informacje, np. o obywatelu/podmiocie, takie jak PESEL, REGON, NIP, dane adresowe itp. Ułatwieniem w załatwieniu spraw dla obywatela lub podmiotu będzie sytuacja, gdy podmiot publiczny nie będzie żądał od obywatela lub podmiotu informacji będących już w posiadaniu urzędów. Realizacja tego postulatu wymaga, aby system informatyczny, w którym prowadzony jest dany rejestr odwoływał się bezpośrednio do danych gromadzonych w innych rejestrach publicznych uznanych za referencyjne w zakresie niezbędnym do realizacji zadań.

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



[akta kontroli str. 322-325]

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

1.5. Obieg dokumentów w podmiocie publicznym

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

Zgodnie z zarządzeniem Nr Or.120.3.2011 Wójta Gminy Lubomino z dnia 1 lutego 2011 r. w sprawie wykonywania czynności kancelaryjnych w Urzędzie Gminy Lubomino, podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw w Urzędzie jest system tradycyjny (papierowy).
Jednocześnie, w okazanej dokumentacji brak jest procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby szczegółowe zasady obiegu dokumentów wpływających i wypływających drogą elektroniczną oraz zakres stosowania elektronicznego obiegu dokumentów (wpływ dokumentów na skrzynkę podawczą na platformie ePUAP), co zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI, umożliwiłoby realizację i egzekwowanie, m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. Powyższe stanowi uchybienie.

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie uchybieniami. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki.

[akta kontroli str. 215]

1.6. Formaty danych udostępniane przez systemy teleinformatyczne

Stosownie do:

- § 17 ust. 1 rozporządzenia KRI *kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków,*

odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz ze zmianami lub normę ją zastępującą;

- § 18 ust. 1 rozporządzenia KRI *systemy teleinformatyczne podmiotów realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia;*
- § 18 ust. 2 rozporządzenia *KRI jeżeli z przepisów szczegółowych albo opublikowanych w repozytorium interoperacyjności schematów XML lub innych wzorów nie wynika inaczej, podmioty realizujące zadania publiczne umożliwiają przyjmowanie dokumentów elektronicznych służących do załatwiania spraw należących do zakresu ich działania w formatach danych określonych w załącznikach nr 2 i 3 do rozporządzenia.*

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

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

[akta kontroli str. 322-325]

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

Zarządzeniem Nr 120.1./2016 Wójta Gminy Lubomino z dnia 26 stycznia 2016 r. wprowadzono w Urzędzie Politykę Bezpieczeństwa Informacji oraz Instrukcję Zarządzania Systemem Informatycznym.
Zarządzenie wprowadzono na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych /Dz.U. z 2015 r., poz. 2135/ oraz § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 923) w związku z art. 33 ust. 3 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz.U. z 2015 roku, poz. 1515 z późn. zm.)
Powyższe stanowiło dokumentację przetwarzania danych osobowych w rozumieniu §1 pkt 1 rozporządzenia MSWiA z 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych (...). Służyła ona zapewnieniu poufności, integralności i rozliczalności przetwarzanych danych.

[akta kontroli str. 244-268]

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 Urzędzie dokonano weryfikacji dokumentacji systemu zarządzania bezpieczeństwem informacji i przyjęto Zarządzenie Nr 120.8.2018 Wójta Gminy Lubomino z dnia 30 maja 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Lubomino oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Lubomino.

Przedmiotową dokumentację sporządzono na podstawie obowiązujących przepisów prawa, tj.

art. 24 ust.1.2 3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/WE w związku z art. 33 ust. 3 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz.U. z 2017 roku, poz. z późn.zm)

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

[akta kontroli str. 269-299, 300-302, 229-243]

Wójt Gminy Lubomino zarządzeniem Nr 120.9.2015 z dnia 30 czerwca 2015 r. wyznaczył Administratora Systemu Informatycznego w Urzędzie. Zgodnie z umową Nr Or 2/2019 z dnia 31 grudnia 2019 r. usługi informatyczne w Urzędzie prowadzi firma zewnętrzna.
Zarządzeniem Nr Or. 120.8a.2018 Wójta Gminy Lubomino z dnia 30 maja 2018 r. wyznaczony został w jednostce Inspektor Ochrony Danych Osobowych (IOD). Zawiadomienie o wyznaczeniu IOD przekazane zostało do Urzędu Ochrony Danych Osobowych.

[akta kontroli str. 303-306]

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.
W celu realizacji nałożonego przez KRI obowiązku, IOD powołany w jednostce dokonywał bieżących półrocznych przeglądów SZBI. Z przeprowadzanych czynności każdorazowo sporządzane były sprawozdania które obejmowały:

W 2018 r. (1 sprawozdanie):

- sprawdzenie zabezpieczeń technicznych w zakresie zabezpieczeń technicznych chroniących przed skórkami awarii zasilania – UPS,
- sprawdzenie „zasady czystego biurka",
- sprawdzenie zabezpieczenia fizycznego w zakresie przechowywania danych w pomieszczeniach zabezpieczonych przed skutkami pożaru za pomocą gaśnic wolnostojących
- sprawdzenie wygaszaczy ekranów.

W 2019 r. (2 sprawozdania):

- sprawdzenie zabezpieczeń technicznych w zakresie systematycznego tworzenia kopii zapasowych,
- sprawdzenie „zasady czystej drukarki",

- sprawdzenie zabezpieczenia fizycznego w zakresie przechowywania danych w szafach zamykanych na klucz,
- sprawdzenie zabezpieczeń technicznych w zakresie stosowania programów antywirusowych
- sprawdzenie zabezpieczeń fizycznego w zakresie przechowywania danych w pomieszczeniach zamykanych – drzwi zamykane na klucz,
- sprawdzenie czy zachodzi konieczność aktualizacji rejestru czynności przetwarzania danych osobowych,

w 2020 r. (do dnia kontroli 1 sprawozdanie):

- przegląd infrastruktury IT urzędu: komputerów i sprzętu peryferyjnego,
- sprawdzenie „zasady czystego biurka",
- sprawdzenie ustawień monitorów w zakresie ustawienia w sposób uniemożliwiający wgląd osobom postronnym.

Sprawozdania w przypadku konieczności podjęcia działań naprawczych zawierały wnioski i zalecenia.

[akta kontroli str. 71-98]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.2. Analiza zagrożeń związanych z przetwarzaniem informacji

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

Wymogiem skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Kluczowa rola analizy ryzyka wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny i jest zależny od ważności aktywów informatycznych danego podmiotu.
Zgodnie z wymogiem wynikającym z § 20 ust. 2 pkt 3 rozporządzenia KRI analiza ryzyka utraty integralności, dostępności lub poufności informacji powinna być przeprowadzana okresowo, a w przypadku stwierdzenia podwyższonego ryzyka w przedmiotowym zakresie, powinny zostać wprowadzone działania minimalizujące to ryzyko. Ponadto z zapisów Polityki Bezpieczeństwa Informacji przyjętej w Urzędzie - §18 wynika, że w celu zapewnienia bezpieczeństwa informacji w Urzędzie Gminy Lubomino minimum raz w roku przeprowadzana jest analiza ryzyka.
Z przedstawionej kontrolującym dokumentacji wynika, że IOD powołany w jednostce przeprowadził stosowne okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji w latach 2018-2019. W przypadku 2020 roku, do dnia kontroli przedmiotowa analiza ryzyka nie została przeprowadzona (brak potwierdzenia w

przedstawionej dokumentacji), jednakże ze względu na istniejącą jeszcze możliwość jej przeprowadzenia, powyższe nie podlegało ocenie.

[akta kontroli str. 71-98]

Jednocześnie należy wskazać, iż zgodnie z art. 30 ust. 1 RODO, w jednostce został opracowany i jest prowadzony rejestr czynności przetwarzania danych osobowych.

[akta kontroli str. 209-214]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego

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

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

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 206-208]

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Stosownie do:

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

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

uprawnień.

Zasady nadawania i odbierania uprawnień do przetwarzania danych osobowych oraz do pracy w określonym zbiorze danych (systemie informatycznym) określone zostały:

- Zarządzeniem Nr 120.1./2016 Wójta Gminy Lubomino z dnia 26 stycznia 2016 r. wprowadzającym w Urzędzie Politykę Bezpieczeństwa Informacji oraz Instrukcję Zarządzania Systemem Informatycznym – obowiązującym do 30 maja 2018 r.
- Zarządzeniem Nr 120.8.2018 Wójta Gminy Lubomino z dnia 30 maja 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Lubomino oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Lubomino.

[akta kontroli str. 229-302]

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

[akta kontroli str. 218-228]

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 szkoleniach (zorganizowanych przez IOD), dotyczących ochrony danych osobowych, tj.:

2018 rok

- przeprowadzono 2 szkolenia (dla 17 oraz dla 3 uczestników) w zakresie: „Ochrona danych osobowych w oparciu o RODO po 25 maja 2018 r.". Szkolenie obejmowało:
  - zapoznanie uczestników z funkcją RODO, jego uprawnieniami i obowiązkami,
  - zapoznanie uczestników z funkcją ABI, jego uprawnieniami i obowiązkami,
  - zapoznanie uczestników z Rozporządzeniem 2016/679,
  - omówienie podstawowych zasad przetwarzania danych osobowych,
  - omówienie upoważnień nadawanych do przetwarzania danych osobowych,
  - omówienie obowiązku informacyjnego,

- omówienie praw osób, których dane dotyczą,
- omówienie środków technicznych i organizacyjnych stosowanych przez ADO w celu bezpiecznego przetwarzania danych osobowych,
- omówienie sprawozdań wewnętrznych w zakresie bezpiecznej informacji,
- omówienie polityki bezpieczeństwa informacji w UG Lubomino.

2019 rok.

- przeprowadzono szkolenie dla wszystkich pracowników (19 uczestników) w temacie: „Wpływ regulacji RODO – Unijne Rozporządzenie o Ochronie Danych Osobowych i wynikające z niego zadania dla administratorów danych oraz dla osób przetwarzających dane osobowe w 2019 r.". Szkolenie obejmowało:
  - zapoznanie uczestników z funkcją ADO, jego uprawnieniami i obowiązkami,
  - zapoznanie uczestników z zadaniami IODO,
  - omówienie podstawowych pojęć: dane osobowe, przetwarzanie, profilowanie, zbiór danych, odbiorca danych, zgoda, dane szczególnej kategorii,
  - omówienie naruszeń przetwarzania danych osobowych, w tym w zakresie systemów informatycznych,
  - omówienie zasad korzystania z poczty służbowej, Internetu oraz sprzętu komputerowego, zasady czystej drukarki i czystego ekranu.

- przeprowadzono szkolenie dla 2 pracowników w temacie: „Omówienie zadań związanych z obsługą wyborów do Sejmu i Senatu Rzeczypospolitej Polskiej 2019 r. w zakresie bezpieczeństwa przetwarzanych danych osobowych". Szkolenie obejmowało:
  - omówienie zadań związanych z obsługą wyborów do Sejmu i Senatu – praca w systemie informatycznym, dostęp do danych osobowych,
  - omówienie naruszeń przetwarzania danych osobowych, w tym w zakresie systemów informatycznych,
  - omówienie zasad korzystania z poczty służbowej, Internetu oraz zasady czystej drukarki i czystego ekranu.

2020 rok.

- przeprowadzono szkolenie (20 uczestników) w temacie: „Planowane zmiany (projekt dotyczący e-usług publicznych) w zakresie bezpieczeństwa informacji Urzędzie Gminy Lubomino, usystematyzowanie wiedzy". Szkolenie obejmowało:
  - przypomnienie uczestnikom o obowiązkach nałożonych na osoby uprawnione do przetwarzania danych osobowych zawartych w Polityce Bezpieczeństwa Informacji oraz Instrukcji Zarządzania Systemem Informatycznym,
  - zapoznanie uczestników z organem nadzoru – Urzędem Ochrony Danych Osobowych,
  - omówienie umów powierzenia przetwarzania danych osobowych,
  - omówienie aktualizacji rejestru czynności przetwarzania danych osobowych w UG Lubomino,

- omówienie sprzętu informatycznego planowanego do zakupu w ramach projektu wdrożenia e-usług publicznych,
- omówienie elektronicznego obiegu dokumentów-program EDICTA.

– przeprowadzono szkolenie (3 uczestników) w temacie: „Unijne Rozporządzenie o Ochronie Danych Osobowych i wynikające z niego zadania dla osób przetwarzających dane osobowe w 2020 r. w zakresie dowozu uczniów do placówek oświatowych na terenie Gminy Lubomino". Szkolenie obejmowało:
  - zapoznanie uczestników z funkcją ADO, jego uprawnieniami i obowiązkami,
  - zapoznanie uczestników z zadaniami IODO,
  - omówienie podstawowych pojęć: dane osobowe, przetwarzanie, profilowanie, zbiór danych, odbiorca danych, zgoda, dane szczególnej kategorii,
  - warunki wyrażenia zgody na przetwarzanie danych osobowych,
  - omówienie naruszeń przetwarzania danych osobowych, w tym w zakresie systemów informatycznych,
  - omówienie zasad korzystania z telefonu służbowego.

[akta kontroli str. 191-205]

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.*

Z uzyskanych z Urzędu podczas kontroli informacji wynika, że cyt.: *„Ze względu na brak możliwości technicznych pracownicy urzędu przetwarzają dane osobowe stacjonarnie w siedzibie jednostki. Do dnia 2 grudnia br. nie przetwarzano danych osobowych poza siedzibą jednostki, do dnia 11 grudnia br. nie planuje się przetwarzania danych osobowych w inny sposób."*

[akta kontroli str. 322-325]

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

2.7. Serwis sprzętu informatycznego i oprogramowania

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

W przypadku systemów informatycznych niezbędne jest objęcie tych systemów (w zakresie

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

W Urzędzie użytkowane są 2 systemy teleinformatyczne przeznaczone do realizacji zadań zleconych z zakresu administracji rządowej zakupione u zewnętrznych dostawców, tj.:

- **SYGNITY** (świadczenia rodzinne, fundusz alimentacyjny, świadczenia wychowawcze, dobry start, dodatki mieszkaniowe i energetyczne) - autorem oprogramowania jest firma [redacted], z którą podpisane zostały stosowne umowy w zakresie asysty technicznej umożliwiająca prawidłową eksploatację i rozwój systemu. Urząd Gminy zawarł również z powyższą firmą umowę powierzenia danych gwarantującą bezpieczeństwo przetwarzanych w systemie danych, na wypadek awarii systemu oraz konieczności ingerencji firmy jako autora oprogramowania w bazy zawierające dane osobowe.
- **PUMA** (ewidencja ludności, rejestr wyborców) - związku z zakupem ww. systemu podpisane zostały z [redacted] stosowne umowy licencyjne, umożliwiające prawidłową eksploatację i rozwój systemu poprzez możliwość zgłaszania błędów pytań i roszczeń dotyczących użytkowanego systemu. Urząd Gminy zawarł również z powyższą firmą umowę powierzenia danych gwarantującą bezpieczeństwo przetwarzanych w systemie danych, na wypadek awarii systemu oraz konieczności ingerencji firmy jako autora oprogramowania w bazy zawierające dane osobowe.

[akta kontroli str. 107-190]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.8. Procedury zgłaszania incydentów naruszenia BI

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

Instrukcja postępowania w przypadku stwierdzenia zagrożenia w postaci naruszenia ochrony danych osobowych oraz podejmowanych działań korygujących została uregulowana zarządzeniami:

- Zarządzeniem Nr 120.1./2016 Wójta Gminy Lubomino z dnia 26 stycznia 2016 r. wprowadzającym w Urzędzie Politykę Bezpieczeństwa Informacji oraz Instrukcję Zarządzania Systemem Informatycznym – obowiązującym do 30 maja 2018 r. - §23.
- Zarządzeniem Nr 120.8.2018 Wójta Gminy Lubomino z dnia 30 maja 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Lubomino oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych

osobowych w Urzędzie Gminy Lubomino - §17.

[akta kontroli str. 229-302]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

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

Na podstawie okazanej dokumentacji kontrolujący stwierdzili, iż w okresie objętym kontrolą tj. od 1 stycznia 2018 r. do dnia rozpoczęcia czynności kontrolnych (18 listopada 2020 r.), w jednostce nie przeprowadzano audytu wewnętrznego w zakresie bezpieczeństwa informacji.

Z wyjaśnienia otrzymanego z Urzędu w powyższej sprawie wynika, że cyt.: *„Zarzadzanie bezpieczeństwem informacji zgodnie z §20 ust.2 rozporządzenia KRI polega w szczególności na zapewnieniu przez kierownictwo urzędu warunków umożliwiających realizację i egzekwowanie 14 działań, w tym wskazanego w pkt.14 okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok. We Wspólnym stanowisku Departamentu informatyzacji MAiC i Departamentu Audytu Sektora Finansów Publicznych MF odnośnie zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji obowiązek ten posiada doprecyzowanie zapisu w postaci: „Intencją projektodawcy było zobowiązanie podmiotów realizujących zadania publiczne do realizowania okresowego audytu wewnętrznego, bez szczegółowego wskazywania na rodzaj audytu oraz tryb jego przeprowadzenia". Nie określono sposobu, formy audytu. Jednak wspólne stanowisko określa 2 sposoby wykonania obowiązku: pierwszy z nich nie ma zastosowania w urzędzie, bowiem system zarządzania bezpieczeństwem informacji nie został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001 drugi sposób wskazuje, iż decyzja co do tego, komu zostanie powierzone prowadzenie omówionego audytu spoczywa no kierownictwie podmiotu". Wobec powyższego należy wnioskować, że decyzja w zakresie doboru rozwiązań organizacyjnych (obejmujących m.in. sposób, formę oraz wykonawcę) stosowanych w zakresie realizacji obowiązku podejmuje kierownictwo urzędu. Decyzja uwzględnia zasoby kadrowe, którymi dysponuje jednostka oraz zasoby finansowe (ewentualne zlecenie czynności na zewnątrz-outsourcing). Tym samym w urzędzie w okresie objętym kontrolą IODO przeprowadził niepełne audyty systemu zarządzania bezpieczeństwem informacji zgodnie z planem sprawdzeń (...) W 2020 r. w II półroczu IODO jest w trakcie prac nad audytem."*

[akta kontroli str. 322-325]

Odnosząc się do powyższego wyjaśnienia należy stwierdzić, że przeprowadzone w Urzędzie „sprawdzenia" zgodności przetwarzania danych osobowych z przyjętą Polityką bezpieczeństwa informacji, spełniają jedynie wymagania wynikające z § 20 ust. 1 KRI, który

stanowi, że *podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje,* ***monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji*** (...), nie spełniają jednak wymogów § 20 ust. 2 pkt 14 rozporządzenia KRI, które stanowi, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.*
Kryteriami, jakimi należy się kierować przy wyborze osób/komórek organizacyjnych prowadzących audyt w zakresie bezpieczeństwa informacji są: odpowiednie kwalifikacje, doświadczenie, znajomość metodyki audytu w zakresie bezpieczeństwa informacji, **a także niezależność od obszaru audytowanego,** aby uniknąć sytuacji „audytowania samego siebie". Audyt sytemu bezpieczeństwa informacji może być przeprowadzony w dwóch zakresach:

1) „wąskim" - sprawdzenie spełnienia wymagań zawartych w § 20 ust. 2 rozporządzenia (14 punktów);
2) „szerokim" sprawdzenie zgodności z normą PN-ISO/IEC 27001.

Niedopełnienie obowiązku wynikającego 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 – zgodnie z przyjętym programem kontroli klasyfikowane jest jako nieprawidłowość, jednak ze względu na przeprowadzone (zgodnie z przyjętym w jednostce planem) sprawdzenia bezpieczeństwa informacji będące narzędziem nadzoru nad BI, brak przeprowadzonego audytu uznaje się za uchybienie.
Skutkiem nieprzeprowadzenia zadań audytowych było naruszenie § 20 ust. 2 pkt 14 rozporządzenia KRI. Osobą odpowiedzialną jest IOD wyznaczony w jednostce.
Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami.

2.10. Kopie zapasowe

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

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

W okresie objętym kontrolą zasady tworzenia kopii zapasowych uregulowane zostały:

- Zarządzeniem Nr 120.1./2016 Wójta Gminy Lubomino z dnia 26 stycznia 2016 r. wprowadzającym w Urzędzie Politykę Bezpieczeństwa Informacji oraz Instrukcję Zarządzania Systemem Informatycznym – obowiązującym do 30 maja 2018 r. - §6 Instrukcji Zarządzania Systemem Informatycznym.
- Zarządzeniem Nr 120.8.2018 Wójta Gminy Lubomino z dnia 30 maja 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Lubomino oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Lubomino - §6 Instrukcji Zarządzania Systemem Informatycznym.

[akta kontroli str. 229-302]

Zgodnie z obowiązującymi w Urzędzie na dzień prowadzenia czynności kontrolnych zasadami wynikającymi z Instrukcji Zarządzania Systemem Informatycznym:

[redacted]

Z wyjaśnienia przekazanego z Urzędu w powyższej sprawie wynik, iż, cyt.: „[redacted]".

[akta kontroli str. 99-103, 229-243]

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

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

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. ŹRÓDŁO i CEiDG oraz systemy wspierające zakupione u dostawcy zewnętrznego – PUMA, SYGNITY. Na obsługę aktualnie zainstalowanego oprogramowania z firmami dostarczającymi dany 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. Systemy teleinformatyczne były każdorazowo aktualizowane do najnowszej wersji.

Jednocześnie należy wspomnieć, iż obsługę informatyczną Urzędu zapewnia firma zewnętrzna, z którą Wójt podpisał stosowne umowy zarówno na zapewnienie bieżącej i nieprzerwanej obsługi w zakresie funkcjonowania sprzętu i oprogramowania, jak również powierzenia danych w ramach świadczonej usługi.

[akta kontroli str. 107-190]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

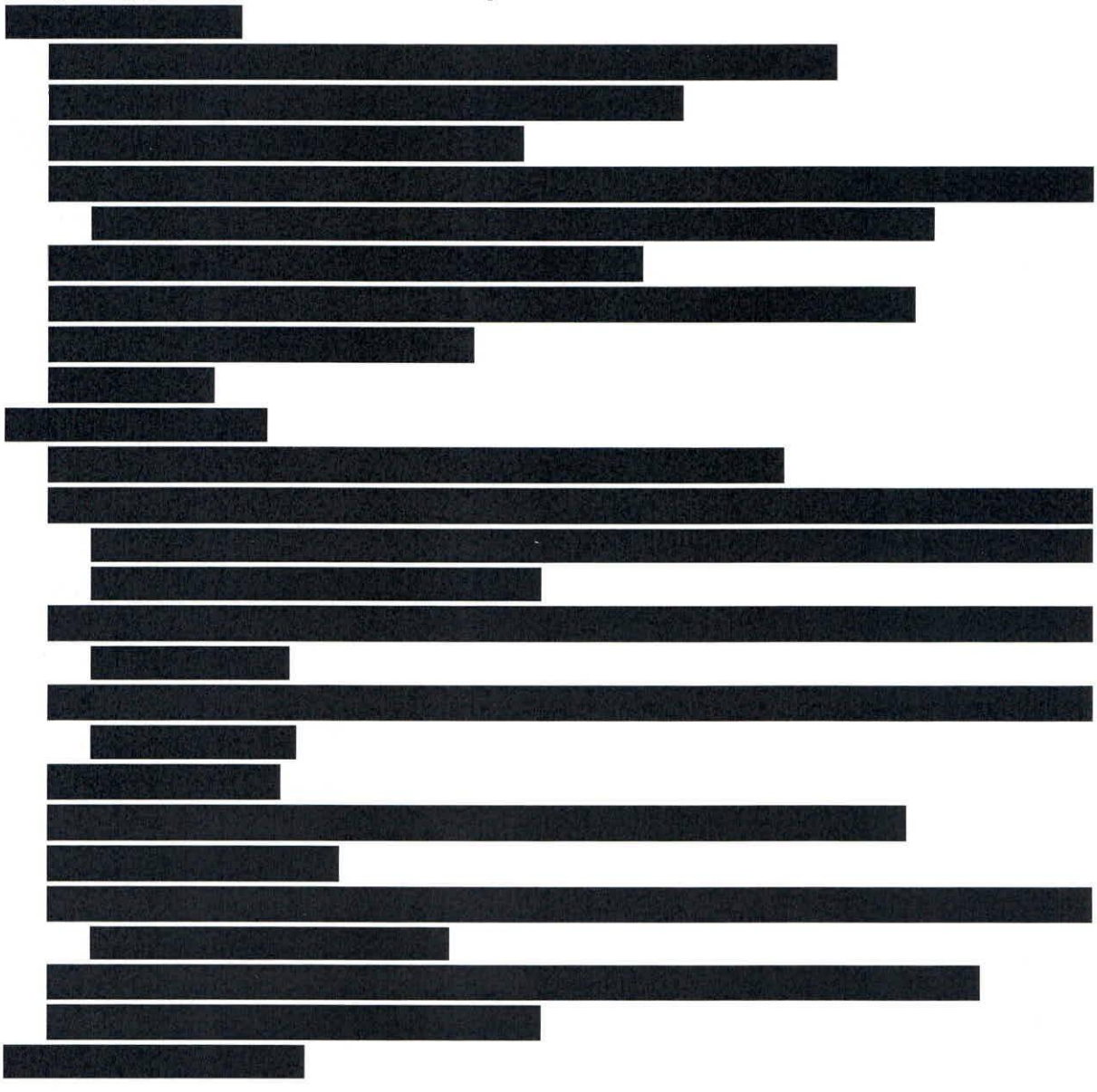
2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji

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

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

W celu uzyskania odpowiedniego poziomu BI, przy jednoczesnym zapewnieniu właściwego do nich dostępu przez uprawnionych użytkowników stosowany jest szereg zabezpieczeń informatycznych. Celem zabezpieczeń jest uzyskanie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także np. kradzieżą środków przetwarzania informacji.

Zgodnie z zarządzeniem Nr 120.8.2018 Wójta Gminy Lubomino z dnia 30 maja 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Lubomino oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Lubomino, w celu zapewnienia ochrony przetwarzania informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie wprowadzono:



[redacted]

[akta kontroli str. 229-243, 269-299]

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:

- w systemie Źródło logowanie odbywa się poprzez imienną kartę dostępową i indywidualne hasło dostępowe,
- w systemie: PUMA, logowanie odbywa się za pomocą przyznanego loginu i hasła, które wymaga okresowej wymiany,
- w systemie SYGNITY, logowanie indywidualnym loginem i hasłem,
- w systemie CEIDG logowanie odbywa się za pomocą certyfikatu kwalifikowanego i hasła.

Ponadto zgodnie z wyjaśnieniem uzyskanym w trakcie kontroli, cyt.: [redacted]

[akta kontroli str. 322-325]

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.*

Z wyjaśnień uzyskanych z Urzędu w powyższej sprawie wynika, że cyt.: „[redacted]”

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

[akta kontroli str. 104-106, 322-325]

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.

W wyniku przeglądu strony BIP Urzędu ustalono, iż strona zawiera narzędzia umożliwiające zmianę kontrastu w celu ułatwienia korzystania z treści na niej zawartych przez osoby niedowidzące. Zgodnie z załącznikiem nr 4 do rozporządzenia KRI, strona BIP spełnia poniższe zasady:

- postrzeganie – informacje oraz komponenty interfejsu strony były przedstawione użytkownikom w sposób dostępny dla jego zmysłów,
- funkcjonalność – komponenty interfejsu stron umożliwiały korzystanie z nich,
- zrozumiałość – informacje oraz obsługa interfejsu były zrozumiałe.

W wyniku przeglądu strony www. Urzędu stwierdzono, że nie zawiera ona wbudowanych narzędzi umożliwiających zmianę kontrastu lub wielkości czcionki, w celu ułatwienia korzystania z treści na niej zawartych przez osoby niedowidzące. Brak wbudowanych narzędzi umożliwiających zmianę kontrastu lub wielkości czcionki powoduje, że strona nie spełnia zasad postrzegania (dostępności), funkcjonalności oraz zrozumiałości tj., informacje oraz komponenty interfejsu strony nie są w pełni przedstawione użytkownikom w sposób dostępny dla jego zmysłów (w przypadku osób niedowidzących).

Z wyjaśnień uzyskanych z Urzędu w powyższej sprawie wynika, że cyt.: *„(...) urząd uwzględnia potrzeby osób niepełnosprawnych, umożliwiając tym osobom zapoznanie się z treści informacji zawartych na stronie internetowej urzędu i stronie BIP. Strona BIP urzędu zawiera w prawym górnym rogu odnośnik do wersji kontrastowej, w celu ułatwienia korzystania dla osób niedowidzących. Odniesienie do wytycznej 1.4, która mówi, że „Użytkownik powinien móc dobrze widzieć lub słyszeć treści", a tym samym spełnienie kryterium na poziomie podwójnego AA, gdzie rozmiar tekstu może zostać powiększony do 200% bez użycia technologii wspomagających oraz bez utraty treści lub funkcjonalności zawiera dwa wymagania: pierwsze to dostarczenie użytkownikowi mechanizmu, który umożliwi mu stopniowe zwiększenie rozmiaru tekstu i przywracanie wartości domyślnych, drugie to zapewnienie, że zastosowanie tego mechanizmu nie będzie powodowało utraty treści lub funkcjonalności strony. Wymóg pierwszy zostaje spełniony poprzez zaimplementowanie możliwości skalowania rozmiaru stron we wszystkich współczesnych przeglądarkach za pomocą skrótów klawiaturowych (w Windows CTRL i +, CTRL i - oraz CTRL i 0) wszyscy użytkownicy mają możliwość stopniowego zwiększania i zmniejszania obrazu na swoich wyświetlaczach, dotyczy to również stron BIP urzędu oraz strony internetowej urzędu. Również w urządzeniach z ekranami dotykowymi powiększenie rozmiaru obszaru widocznego w wyświetlaczu jest standardową funkcjonalnością. Zmiana rozmiaru tekstu w opisanym powyżej sposobie nie powoduje utraty treści lub funkcjonalności.*
W chwili obecnej trwają prace nad dostosowaniem strony internetowej urzędu i strony BIP urzędu do wymagań WCAG 2.1 w ramach projektu „informatyzacja usług publicznych i dostępu do informacji przestrzennej w Gminie Lubomino"."

Odnosząc się do powyższych wyjaśnień należy stwierdzić, że przez pełny dostęp do strony

należy rozumieć to, iż każda informacja i usługa na danej stronie będzie możliwa do odczytania i wykorzystania przez każdego użytkownika korzystającego z powszechnie stosowanych technologii. Samodzielny dostęp oznacza, iż informacje lub usługi mogą zostać wykorzystane przez każdego użytkownika bez potrzeby angażowania innych osób. Efektywny dostęp oznacza, że nie jest wymagany znacząco wyższy wydatek pracy lub czasu na osiągnięcie porównywalnego efektu. Wskazana w udzielonej odpowiedzi możliwość wykorzystania tzw. „skrótów klawiszowych" umożliwiających powiększenie obrazu strony, nie może być traktowana jako spełnienie zasady dostępności, gdyż nie każdy z użytkowników posiada wiedzę z zakresu stosowania „skrótów klawiszowych". Dlatego też interfejs strony internetowej powinien zawierać wbudowane na etapie projektowania narzędzia umożliwiające zmianę kontrastu oraz wielkości czcionki.
Brak możliwości skorzystania z treści udostępnionych na stronach internetowych urzędów ogranicza dostęp części obywateli do informacji i do elektronicznych usług publicznych, co może prowadzić do zarzutu nierównego traktowania osób niepełnosprawnych. Dostosowywanie stron internetowych do potrzeb osób z niepełnosprawnościami to nie zadanie jednorazowe, ale proces ciągły, który powinien być prowadzony nieprzerwanie - równolegle z rozbudową i prowadzeniem strony internetowej.
Zgodnie z wyjaśnieniem Urzędu trwają obecnie prace nad dostosowaniem strony internetowej i strony BIP do wymagań WCAG 2.1 w ramach realizowanego projektu, dlatego też powyższe braki oceniono w kategorii uchybienia. Skutkiem uchybienia jest ograniczenie możliwość korzystania z treści zawartych na stronie przez osoby niedowidzące. Osobą odpowiedzialną za powstanie uchybienia jest informatyk Urzędu.

Walidacja za pomocą narzędzia http://wave.webaim.org tj. walidatora WAVE-WCAG 2.0 dla strony BIP wykazała 7 błędów, dla strony www. Urzędu wykazała 18 błędów. Wave 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. 315-318, 322-325]

Powyższe zagadnienie oceniono pozytywnie z uchybieniami.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny wnoszę o:

1. Opracowanie wewnętrznych procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby zasady obiegu dokumentów wpływających i wypływających z Urzędu drogą elektroniczną.
2. Zapewnienie w jednostce nie rzadziej niż raz na rok okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI.

3. Dostosowanie strony internetowej jednostki, w celu umożliwienia korzystania z treści na niej zawartych osobom niepełnosprawnym.

Proszę Pana Wójta 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

Artur Chojecki