WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

Olsztyn, 9 maja 2022 r

Wydział Finansów i Kontroli
FK-IV.431.4.2022

Szanowny Pan
Wojciech Karol Iwaszkiewicz
Burmistrz Giżycka
al. 1 Maja 14
11-500 Giżycko

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 Giżycku[1], al. 1 Maja 14, 11-500 Giżycko, NIP jednostki 845-10-02-471, REGON jednostki: 000524364.

- W okresie objętym kontrolą oraz w czasie prowadzonych czynności kontrolnych kierownikiem kontrolowanej jednostki był Pan **Wojciech Karol Iwaszkiewicz** – Burmistrz, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 21 października 2018 roku.

- W dniu rozpoczęcia czynności kontrolnych odpowiedzialnym za realizację zadania objętego kontrolą w Urzędzie był Pan **Mirosław Domysławski** – główny specjalista, zatrudniony na podstawie umowy o pracę od dnia 14 czerwca 2006 r.

- Osobą bezpośrednio nadzorującą pracownika odpowiedzialnego za realizację zadania była Pan **Szymon Grabowski** – kierownik Biura Informatyki, zatrudniony na podstawie umowy o pracę od dnia 1 kwietnia 2007 r.

[akta kontroli str. 79]

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.0030.117.2022 z 25 lutego 2022 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

[1] Zwanym dalej: Urzędem

Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr FK-IV.0030.118.2022 z 25 lutego 2022 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 26-27]

Kontrolę przeprowadzono w dniach 11-31 marca 2022 r., co zostało odnotowane w książce kontroli Urzędu pod pozycją, Nr WO.1710.1.2022.

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

Przedmiotem kontroli była ocena działania systemów teleinformatycznych używanych przez jednostki samorządu terytorialnego do realizacji zadań zleconych z zakresu administracji rządowej, na podstawie art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2021 r., poz. 2070). Okres objęty kontrolą: od dnia 1 stycznia 2019 r. do dnia 31 grudnia 2020 r.

[akta kontroli str. 1-2, 52-62]

Kontrola została przeprowadzona na podstawie art. 2 pkt 1 i art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U. 2020 poz. 224), art. 28 ust. 1 pkt 2 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz. U. z 2022 r., poz. 135), w związku z art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2021 r., poz. 2070)[2], rozdziału III i IV Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247 ze zm.)[3], jak również Wytycznych dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych, zatwierdzonych przez Ministra Cyfryzacji w dniu 15 grudnia 2015 r.

[akta kontroli str. 1-2, 52-62]

Burmistrz Giżycka upoważnił kierownika Biura Informatyki oraz głównego specjalistę odpowiedzialnego za realizację zadania, do udzielania informacji w okresie trwania czynności kontrolnych.

[akta kontroli str. 80]

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

Na podstawie ustaleń kontroli, realizację zadań z zakresu działania systemów teleinformatycznych używanych przez Urząd do realizacji zadań zleconych z zakresu administracji rządowej ocenia się **pozytywnie z nieprawidłowościami.**
Ocena działalności jednostki kontrolowanej wynika z ustaleń i ocen dokonanych w poszczególnych obszarach (zagadnieniach) objętych kontrolą.

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

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** – Moduły: Ewidencja Ludności, Wyborcy. 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.
3) **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.

[akta kontroli str. 63-73]

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 /umgizycko/SkrytkaESP, znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie i odbieranie pism w formie dokumentów elektronicznych. Ścieżkę bezpośredniego przejścia na główną stronę e-PUAP, zawarto na stronie internetowej BIP Urzędu. Formaty danych przyjmowane za pośrednictwem Elektronicznej Skrzynki Podawczej to m.in.: DOC, RTF, XLS, CSV, TXT, GIF, TIF, BMP, JPG, PDF, ZIP.

Na stronie głównej Urzędu w zakładce „Załatw sprawę" – podzakładka „E-usługi" zawarto odnośnik do elektronicznego biura obsługi interesanta EBOI. Zgodnie z informacja zawartą na stronie portal Elektroniczne Biuro Obsługi Interesanta to skuteczne narzędzie umożliwiające obywatelom dostęp do informacji sektora publicznego. Portal umożliwia także komunikowanie się obywateli z sektorem publicznym przy wykorzystaniu systemów teleinformatycznych, a także zapewnia podniesienie efektywności działania administracji samorządowej.
Za pomocą systemu e-usług internetowych mieszkańcy mogą na bieżąco śledzić wydarzenia ze swojego miasta czy gminy, złożyć wniosek do swojego urzędu, a następnie na bieżąco monitorować status prowadzonej sprawy.

Zgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI interoperacyjność na poziomie organizacyjnym osiągana jest przez publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.
W zakresie publikacji procedur załatwiania spraw realizowanych przez Urząd należy stwierdzić, że na stronie BIP w zakładce „Menu przedmiotowe – wykaz spraw", opublikowany jest przydatny dla petentów wykaz usług, które realizowane są przez poszczególne wydziału Urzędu, w tym również te które możliwe są do zrealizowania drogą elektroniczną korzystając z platformy ePUAP.

Ponadto na stronie BIP w zakładce „Wykaz spraw", opublikowane są wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych wydziałów w Urzędzie.
Jednocześnie należy zaznaczyć, że Urząd nie świadczył usług związanych z załatwianiem spraw od początku do końca w formie elektronicznej, za pomocą systemów teleinformatycznych.
Ponadto Urząd udostępniał oraz świadczył również usługi elektroniczne, z wykorzystaniem ePUAP, tj. „Pismo ogólne do podmiotu publicznego". Usługa te umożliwiają złożenie do wybranego organu administracji publicznej pisma w sprawie.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 63-73, 81-120]

1.2. Centralne repozytorium wzorów dokumentów elektronicznych (CRWDE)

Stosownie do art. 19b ust. 3 ustawy, organy administracji publicznej przekazują do centralnego repozytorium oraz udostępniają w Biuletynie Informacji Publicznej wzory dokumentów elektronicznych. Przy sporządzaniu wzorów dokumentów elektronicznych stosuje się międzynarodowe standardy dotyczące sporządzania dokumentów elektronicznych przez organy

administracji publicznej, z uwzględnieniem konieczności podpisywania ich kwalifikowanym podpisem elektronicznym.

W celu ujednolicenia w skali kraju procedur usług świadczonych przez urzędy drogą elektroniczną, w tym ujednolicenia wzorów dokumentów elektronicznych w CRWDE przechowywane są wzory dokumentów, jakie zostały już opracowane i są używane. W przypadku uruchamiania przez dany podmiot publiczny usługi elektronicznej, która funkcjonuje już na koncie innego podmiotu, dany podmiot publiczny powinien skorzystać z procedury obsługi tej usługi oraz zastosować wzory dokumentów elektronicznych dotyczące tej procedury znajdujące się w CRWDE (nie dotyczy to sytuacji gdy usługa jest usługą centralną, tzn. jest udostępniania przez jeden podmiot, np. właściwego ministra, ale służy do świadczenia usług przez inne podmioty niż udostępniający, np. wszystkie gminy). W przypadku uruchamiania usługi, dla której nie ma wzorów dokumentów w CRWDE, podmiot publiczny jest zobowiązany przekazać do CRWDE procedurę obsługi usługi i wzory dokumentów elektronicznych z nią związanych.

W trakcie kontroli ustalono, że w okresie objętym kontrolą Urząd nie przekazywał wzorów dokumentów elektronicznych do centralnego repozytorium wzorów dokumentów prowadzonego przez Ministerstwo Cyfryzacji, ze względu na fakt nie uruchomienia nowej usług dla których nie ma wzorów dokumentów w CRWDE.

Z informacji uzyskanej podczas kontroli wynika, że w okresie 01.01. - 31.12.2021 r. nie przekazywano wzorów dokumentów elektronicznych do CRWD, ze względu na brak wdrożonych nowych usług oraz brak konieczności modyfikacji istniejących. Urząd w okresie objętym kontrola świadczył usługę „Pismo ogólne do urzędu" umożliwiająca złożenie dowolnego pisma w sprawie, która nie została ujęta w katalogu udostępnianych spraw / formularzy.
Jednocześnie należy zaznaczyć, że na stronie BIP - https://bip.gizycko.pl/sprawy, opublikowane są wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych wydziałów w Urzędzie.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 63-73]

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://gizycko.pl/, a strona internetowa BIP Urzędu – pod adresem https://bip.gizycko.pl/
Na stronie internetowej Urzędu zamieszczono bezpośredni link do strony BIP Urzędu, w prawej górnej części panelu strony. Na stronie głównej BIP Urzędu, zamieszczono bezpośredni link do platformy ePUAP , a w zakładce „Elektroniczna skrzynka podawcza ESP" - adres skrytki ESP. Na stronie BIP znajduje się równie odnośnik do strony OBYWATEL.GOV.PL

[akta kontroli str. 63-73, 82]

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

1.4. Współpraca systemów teleinformatycznych z innymi systemami

Stosownie do:

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

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

Z informacji uzyskanych z Urzędu wynika, że, cyt.: „Wymiana danych odbywa sią pomiędzy systemami SRP (platforma ŹRÓDŁO) a systemem lokalnym PUMA autorstwa ZETO Software. System PUMA jest zasilany bezpośrednio z systemu ŹRÓDŁO za pomocą aplikacji narzędziowej dostarczonej przez producenta (PUMA). Format przekazywanych danych to XML w kodowaniu Unicode UTF-8."

[akta kontroli str. 63-73]

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

1.5. Obieg dokumentów w podmiocie publicznym

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

Z uzyskanych w trakcie kontroli informacji wynika, że w Urzędzie nie wdrożono elektronicznego obiegu dokumentów. Obowiązuje tradycyjny model obiegu dokumentacji ze wsparciem

narządzi Informatycznych. Zarządzanie obiegiem dokumentów prowadzone jest zgodnie z zarządzeniem Burmistrza Nr 717 / 2021 z dnia 23.09.2021 r.

Ponadto z wyjaśnienia Burmistrza w powyższej sprawie wynika, że cyt.: „Obecnie w Urzędzie Miejskim w Giżycku trwają prace wdrożeniowe nad systemem EZD PUW (Elektronicznego Obiegu Dokumentów Podlaskiego Obiegu Dokumentów). Równocześnie z prowadzonymi pracami technicznymi, szkoleniami oraz przygotowaniem stanowisk roboczych opracowywana jest dokumentacja regulująca zasady obiegu dokumentów wpływających i wypływających oraz uprawnień związanych z procesem. W dotychczasowej pracy z dokumentami zastosowanie miało Zarządzenie Burmistrza Miasta Giżycka nr 32/2011 z dnia 4.04.2011 r. w sprawie instrukcji kancelaryjnej oraz archiwum zakładowego Urzędu Miejskiego w Giżycku (zm. Zarządzeniem nr 717/2021 Burmistrza miasta Giżycka z dnia 23 września 2021 r.)."

[akta kontroli str. 63-73, 121-220, 477-480]

W okazanej dokumentacji Urzędu 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 (skrzynka podawcza na platformie ePUAP), co zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI, umożliwiłoby realizację i egzekwowanie, m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. Opracowanie zasad postępowania z dokumentacją elektroniczną (wnioski elektroniczne, e-maile) oraz wymagań organizacyjno-technicznych dotyczących zarządzania tą dokumentacją pozwala właściwie dbać o jej bezpieczeństwo.

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

Zastosowanie w przyszłości systemu elektronicznego zarządzania dokumentami elektronicznymi EZD wpłynie na uporządkowanie i usprawnienie przepływu dokumentów w podmiocie publicznym, znacząco usprawni ich archiwizację oraz zapewni łatwy dostęp do dokumentów archiwalnych, co wpłynie na przyspieszenie załatwianych spraw w tym realizowanych przez podmiot publiczny usług oraz pozwoli na minimalizowanie nakładu pracy a także podniesie poziom Bezpieczeństwa Informacji. Celem wdrożenia systemu elektronicznego zarzadzania dokumentacją jest wyeliminowanie z obiegu wewnętrznego podmiotu publicznego dokumentów papierowych, co spowoduje dodatkowo obniżenie kosztów.

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami

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.: „System PUMA jest zasilany bezpośrednio z systemu ŹRÓDŁO za pomocą aplikacji narzędziowej dostarczonej przez producenta oprogramowania ZETO Software. Pobieranie danych - format przekazywanych danych - XML w kodowaniu Unicode UTF-8. Systemy informatyczne pozwalają na przyjmowanie i udostępnianie danych w ogólnie stosowanych formatach: XML, PDF, DOC, ODT, RTF."

[akta kontroli str. 63-73]

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

II. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych

2.1. Dokumenty z zakresu bezpieczeństwa informacji

Zgodnie z:

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

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", zarządzeniem Nr 503/2020 Burmistrza Miasta Giżycko z dnia 22 grudnia 2020 r. w sprawie wdrożenia polityki ochrony danych osobowych i instrukcji zarzadzania systemem informatycznym w Urzędzie Miejskim w Giżycku, wprowadzono zasady przetwarzania danych

osobowych oraz stosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych i przyjęto następującą dokumentację:

1. Politykę Ochrony Danych Osobowych w Urzędzie Miejskim w Giżycku (PBDO),
2. Instrukcję Zarządzania Systemem Informatycznym Urzędu Miejskiego w Giżycku (IZSI).

[akta kontroli str. 221-317]

Realizacja zadań w zakresie ochrony danych wymaga od podmiotu publicznego opracowania dokumentacji SZBI (system zarządzania bezpieczeństwem informacji), w tym szeregu regulacji wewnętrznych oraz zapewnienia aktualizacji tych regulacji w zakresie dotyczącym zmieniającego się otoczenia. Kompleksowa dokumentacja SZBI jest warunkiem niezbędnym, w celu skutecznego zarządzania bezpieczeństwem informacji w podmiocie.
Podstawowym dokumentem SZBI jest **Polityka Bezpieczeństwa Informacji**. Polityka zazwyczaj zawiera wyrażoną przez kierownictwo deklarację stosowania, opisuje organizację i ustala osoby odpowiedzialne oraz ich zakresy odpowiedzialności, wprowadza klasyfikację informacji, sposób postępowania z poszczególnymi rodzajami informacji. PBI może określać aktywa oraz ich właścicieli, oraz sposób szacowania ryzyka i postępowania z ryzykiem.
Zazwyczaj w ramach SZBI funkcjonują inne polityki, regulaminy i procedury np.:

- Polityka bezpieczeństwa teleinformatycznego;
- Polityka bezpieczeństwa fizycznego;
- Polityka bezpieczeństwa danych osobowych.
- Procedura zarzadzania ryzykiem;
- Regulamin korzystania z zasobów informatycznych;
- Procedura zarządzania sprzętem i oprogramowaniem;
- Procedura zarządzania konfiguracją;
- Procedura zarządzania uprawnieniami do pracy w systemach teleinformatycznych;
- Procedura monitorowania poziomu świadczenia usług;
- Procedura bezpiecznej utylizacji sprzętu elektronicznego;
- Procedura zarządzania zmianami i wykonywaniem testów;
- Procedura stosowania środków kryptograficznych;
- Procedura określania specyfikacji technicznych wymagań odbioru systemów IT;
- Procedura zgłaszania i obsługi incydentów naruszenia bezpieczeństwa informacji;
- Procedura wykonywania i testowania kopii bezpieczeństwa;
- Procedura monitoringu i kontroli dostępu do zasobów teleinformatycznych, prowadzenia logów systemowych.

Dokumentację SZBI stanowią także:

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

W Urzędzie nie opracowano i nie wdrożono całościowej SZBI, w szczególności nie wdrożono zaktualizowanej **polityki bezpieczeństwa informacji** - PBI.
Było to niezgodne z § 20 ust. 1 rozporządzenia KRI, w myśl którego 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.
Z § 20 ust. 3 rozporządzenia KRI wynika natomiast, że wymagania określone w ust. 1 tego paragrafu uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 270017 (*Polska Norma PN-EN ISO/IEC 27001:2017 Technika Informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania.*), a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą (*PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem, PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.*).
Jednocześnie w pkt 5.1 Polskiej Normy PN-EN ISO/IEC 27002, wskazano opracowanie i stosowanie dokumentu **polityki bezpieczeństwa informacji**.

Z wyjaśnienia Burmistrza w powyższej sprawie wynika, że, cyt.: „W Urzędzie Miejskim w Giżycku opracowano Politykę Bezpieczeństwa Danych Osobowych oraz instrukcję Zarządzania Systemami Informatycznymi, w których znajduje się m.in. uregulowania dotyczące zabezpieczeń fizycznych
i technicznych, nadawania/cofania uprawnień, zabezpieczenia systemu informatycznego, wykonywania przeglądów i konserwacji, postępowania z nośnikami i sprzętem poza urzędem, konfiguracji infrastruktury Informatycznej w tym serwerów, zarządzania hasłami dostępu do systemów IT, zasad bezpieczeństwa fizycznego w obiekcie, korespondencji służbowej czy stosowanych zabezpieczeń systemów informatycznych. Dokumentacja ta była opracowywana na podstawie norm ISO 27001".

Odnosząc się do udzielonego wyjaśnienia, należy stwierdzić, że opracowane i wdrożone w 2020 r. w Urzędzie zarządzenie Nr 503/2020 Burmistrza Miasta Giżycko z dnia 22 grudnia 2020 r. w sprawie wdrożenia polityki ochrony danych osobowych i instrukcji zarzadzania systemom informatycznym w Urzędzie Miejskim w Giżycku, nie obejmowało wszystkich informacji jakie są przetwarzane w Urzędzie, lecz przede wszystkim dane osobowe. Mając na względzie przepisy § 20 ust. 3 rozporządzenia KRI należy uznać, że przyjęta w Urzędzie polityka bezpieczeństwa danych osobowych stanowi tylko jedną ze składowych dokumentacji ustanawiającej SZBI w jednostce i nie dopełnia w całości obowiązku wynikającego z cytowanych powyżej przepisów.

[akta kontroli str. 221-316, 477-480]

Powyższe stanowi nieprawidłowość, skutkującą naruszeniem § 20 ust. 1 rozporządzenia KRI. Osobą odpowiedzialną za powstanie nieprawidłowości jest IOD pełniący funkcję w tym okresie.

W myśl § 20 ust. 1 rozporządzenia KRI podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji.
Rola podmiotu nie kończy się tylko i wyłącznie na opracowaniu i wdrożeniu do eksploatacji systemu zarządzania bezpieczeństwem informacji. Obowiązkiem podmiotu jest także

monitorować, przeglądać i utrzymywać jak również doskonalić ten system tak, aby zapewniać poufność, dostępność i integralność informacji. Powyższe oznacza, iż realizacja obowiązku wynikającego z § 20 ust. 1 KRI nie kończy się z momentem wdrożenia do stosowania SZBI, lecz wymaga ona nieustannej uwagi. Z dokumentacji przedstawionej kontrolującym wynika, że Administrator Systemu Informatycznego – Główny specjalista w Biurze Informatyki w okresie objętym kontrolą dokonywał przeglądów SZBI w jednostce poprzez przeprowadzenie kontroli podatności systemu informatycznego, w ramach których badano uprawnienia osób przetwarzających dane osobowe oraz zabezpieczenie stanowiska komputerowego.

[akta kontroli str. 320-336]

Burmistrz zarządzeniem Nr 512/2021 z dnia 4 stycznia 2021 r. powołał w jednostce Inspektora Ochrony Danych (IOD). Opracowano również zakres obowiązków IOD.

[akta kontroli str. 318-319]

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

2.2. Analiza zagrożeń związanych z przetwarzaniem informacji

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

Wymogiem skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Kluczowa rola analizy ryzyka wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny i jest zależny od ważności aktywów informatycznych danego podmiotu. Analiza ryzyka jest ważnym wymaganiem nałożonym na administratorów i podmioty przetwarzające. Proces szacowania ryzyka powinien być przeprowadzony i udokumentowany w celu wykazania, że ryzyko zostało oszacowane i wprowadzono odpowiednie środki obrony. Szacowanie ryzyka pozwala na aktywne zarządzanie bezpieczeństwem informacji, w tym na przeciwdziałanie zagrożeniom oraz ograniczanie skutków zmaterializowanych ryzyk, a także wpływa na racjonalne zarządzanie środkami finansowymi poprzez stosowanie zabezpieczeń adekwatnych do oszacowanego poziomu ryzyka. Jednocześnie należy zaznaczyć, że prawidłowo przebiegająca analiza ryzyka nie jest jednorazowym działaniem, lecz regularnie i ciągle monitorowanym procesem.
Zgodnie z wymogiem wynikającym z § 20 ust. 2 pkt 3 rozporządzenia KRI analiza ryzyka utraty integralności, dostępności lub poufności informacji powinna być przeprowadzana okresowo, a w przypadku stwierdzenia podwyższonego ryzyka w przedmiotowym zakresie, powinny zostać wprowadzone działania minimalizujące to ryzyko.
Kontrolującym przedstawiono dokumentację świadczącą o przeprowadzeniu okresowej analizy ryzyka utraty integralności, dostępności lub poufności informacji w Urzędzie, a także poza Urzędem, w zakresie pracy zdalnej.

[akta kontroli str. 337-347]

W toku prowadzonych czynności kontrolnych stwierdzono również, iż w jednostce zgodnie z art. 30 RODO oraz rozdziałem 6.5.3 przyjętej PBDO, prowadzony jest rejestr czynności

przetwarzania danych osobowych. Przedmiotowy rejestr został opracowany i jest prowadzony przez IOD.

[akta kontroli str. 348-349]

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 str. 350-362]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Stosownie do:

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

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

Zasady nadawania uprawnień do przetwarzania danych osobowych oraz do pracy w określonym zbiorze danych (systemie informatycznym), wzory wniosków (PBDO_27_1, PBDO_Z9, PBDO_Z10, PBDO_Z10_1) oraz wzór upoważnienia (PBDO_Z7) określone zostały zarządzeniem Nr 503/2020 Burmistrza Miasta Giżycko z dnia 22 grudnia 2020 r. w sprawie wdrożenia polityki ochrony danych osobowych i instrukcji zarzadzania systemom informatycznym w Urzędzie Miejskim w Giżycku – rozdział 6.6 PBDO oraz procedura nr 1 IZSI.

[akta kontroli str. 221-316]

Osoby posiadające dostęp do danych osobowych i pracujące w określonym systemie 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. 396-435, 481-498]

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 2 szkoleniach, dotyczących bezpieczeństwa informacji:

1) Szkolenie w zakresie ochrony danych osobowych oraz cyberbezpieczeństwa przeprowadzone w dniach 15-16.11.2021 r.
2) Szkolenie po przeprowadzonych testach socjotechnicznych (phishing), w dniu 18.06.2021 r.

Zakres szkolenia ochrona danych osobowych oraz cybrebezpieczeństwa:

- Podstawy prawne i pojęcia,
- Podstawy do przetwarzania danych osobowych,
- Klauzule informacyjne,
- Obowiązki Administratora,
- Naruszenia ochrony danych osobowych,
- Żądania realizacji praw osób, których dane dotyczą,
- Upoważnienia do przetwarzania danych osobowych,
- Zadania IOD,
- Przypomnienie zasad tzw. „cyberhigieny" (szyfrowanie, hasła),
- Phishing.

Ponadto zgodnie z wyjaśnieniem udzielonym kontrolującym, IOD przygotował materiały szkoleniowe - „Phishing - jak się przed nim bronić", które były przesłane do pracowników po kontrolowanym ataku phishingowym, zawierające takie zagadnienia jak:

- Co to jest phishing?
- Przykłady phishingu- jak to działa?
- Jaki jest cel ataku?
- Jak się bronić przed phishingiem?

W załączeniu przedstawiono listę pracowników uczestniczących w szkoleniach.

[akta kontroli str. 436-439, 477-480]

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.

W Urzędzie, wraz z zarządzeniem Nr 503/2020 Burmistrza Miasta Giżycko z dnia 22 grudnia 2020 r., w sprawie wdrożenia polityki ochrony danych osobowych i instrukcji zarzadzania systemom informatycznym w Urzędzie Miejskim w Giżycku, przyjęto Regulamin pracy zdalnej, stanowiących zbiór zasad do stosowania podczas wykorzystywania sprzętu przenośnego podczas świadczenia pracy na odległość.

[akta kontroli str. 221-279]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.7. Serwis sprzętu informatycznego i oprogramowania

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

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

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

- **PUMA** – Moduły: Ewidencja Ludności, Wyborcy, jego zadaniem jest kompleksowa obsługa komórki ewidencji ludności.

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 gwarantująca bezpieczeństwo informacji uzyskanych przez wykonawcę w związku z realizacją umowy.
Procedura w zakresie wykonywania przeglądów i konserwacji systemów informatycznych, zawarta jest w Instrukcji Zarządzania Systemem Informatycznym Urzędu Miejskiego w Giżycku - IZSI_P10.

[akta kontroli str. 280-316, 440-457]

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 zarządzeniem Nr 503/2020 Burmistrza Miasta Giżycka z dnia 22 grudnia 2020 r., w sprawie wdrożenia polityki ochrony danych osobowych i instrukcji zarzadzania systemom informatycznym w Urzędzie Miejskim w Giżycku – PBDO rozdział 6.12.

[akta kontroli str. 221-279]

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, że w okresie objętym kontrolą w jednostce przeprowadzono jedno zadanie audytowe w zakresie bezpieczeństwa informacji. Zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI, przeprowadzony został audyt bezpieczeństwa informacji. Przedmiotem audytu była ocena działania systemów teleinformatycznych pod względem zgodności z minimalnymi wymaganiami dla systemów teleinformatycznych lub rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz przestrzegania wymagań zawartych w KRI oraz RODO.

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

[akta kontroli str. 363-395]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.10. Kopie zapasowe

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

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

Zasady tworzenia, przechowywania i testowania kopii zapasowych zostały uregulowane zarządzeniem Nr 503/2020 Burmistrza Miasta Giżycko z dnia 22 grudnia 2020 r., w sprawie wdrożenia polityki ochrony danych osobowych i instrukcji zarzadzania systemom informatycznym w Urzędzie Miejskim w Giżycku – IZSI_P6 (IZSI_P6_Z1, IZSI_P6_Z2).
Zgodnie z przekazaną dokumentacją, kopie zapasowe wykonuje się w oparciu o harmonogram tworzenia kopii zapasowych - IZSI_P6_Z1.
Zgodnie natomiast z punktem 7 instrukcji tworzenia kopii zapasowych IZSI_P6, w celu zweryfikowania poprawności danych przechowywanych na kopiach zapasowych oraz możliwości przywrócenia za ich pomocą systemu do stanu sprzed awarii, Administrator Systemu Informatycznego zobowiązany jest do wykonywania okresowych testów odtworzenia kopii zapasowych. Testy powinny być wykonywane nie rzadziej niż raz na kwartał. Wyniki testów powinny zostać udokumentowane.
Przeprowadzanie testów odtworzeniowych dokumentowane jest w Urzędzie zgodnie z opracowaną instrukcją odzyskiwania kopii bezpieczeństwa IZSI_P6_Z2.

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

[akta kontroli str. 458-470]

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 dostawców zewnętrznych – PUMA. Na obsługę aktualnie zainstalowanego oprogramowania (system informatyczny) zawarte zostały stosowne umowy licencyjne (opieka autorska), gwarantujące rozwój systemu i dostosowanie do obowiązujących przepisów prawa. Zakupiony system teleinformatyczny, w razie awarii podlega ekspertyzie technicznej zlecanej firmie dostarczającej.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 63-73, 443-457]

2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji

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

- pkt 7 zapewnienie ochrony przetwarzania informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: a) monitorowanie dostępu do informacji; b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;

- pkt 9 zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie;
- pkt 11 ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.

W celu uzyskania odpowiedniego poziomu BI, przy jednoczesnym zapewnieniu właściwego bieżącego dostępu uprawnionym użytkownikom, stosowany jest szereg zabezpieczeń technicznych. Celem zabezpieczeń jest uzyskanie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także np. kradzieżą środków przetwarzania informacji. Z informacji uzyskanych podczas kontroli wynika, że w Urzędzie stosowane są następujące zabezpieczenia:

Zabezpieczenia sieci:

- Segmentacja sieci. Każda komórka organizacyjna urzędu ma odrębną, własną sieć, która ma dostęp tylko do zasobów (aplikacje sieciowe, udziały sieciowe) przypisanych tylko do danych komórek.
- Zapora sieciowa i wykrywanie zagrożeń. Realizowana przez urządzenie FortiGate 300E z aktualną subskrypcją sygnatur zagrożeń. Ruch z każdej podsieci jest ograniczony tylko do niezbędnych portów.
- Dodatkowo ruch poddawany jest wykrywaniu wirusów, sygnatur ataków sieciowych i weryfikacji warstwy aplikacji (blokowane są koparki krypto walut, torrent, sieci botnet, proxy, nieautoryzowane vpn).
- Użytkownicy mają ograniczony dostęp do stron www - blokowane są strony z kategorii: złośliwe strony, phishing, spam, strony do wymiany P2P, pornografia.
- Ograniczenia czasowe - dostęp do zasobów sieciowych jest ograniczony czasowo do godzin pracy urzędu. Wyjątkiem jest tu Straż Miejska (pracuje całą dobę) i zgłaszane wydarzenia typu zdalne posiedzenie Rady i Komisji Miejskiej.

Zabezpieczenia stacji roboczych:

- Na każdym stanowisku zainstalowane jest oprogramowanie Eset Endpoint Security zarządzane centralnie przez konsolę. Funkcje oprogramowania to wykrywanie wirusów i złośliwych programów, zapora sieciowa i blokowanie zagrożeń sieciowych, ochrona poczty email.
- Zarządzanie przez kontroler domeny. Dostęp do stacji dla użytkowników regulowany jest centralnie.
- Administratorzy posiadają oddzielne konta.
- Użytkownicy mają ograniczone prawa korzystania ze stacji roboczych. Użytkownicy nie mogą samodzielnie instalować programów.
- Zmiana haseł dla użytkowników i administratorów jest wymuszana co 40 dni.
- Stacje po 5 minutach bezczynności są blokowane hasłem. Po 3 błędnych próbach wpisania hasła konto użytkownika jest blokowane czasowo na 15 minut.
- Zawartość dokumentów i pulpitu jest synchronizowana z serwerem (zabezpieczenie przed awarią dysku stacji roboczej).
- Szyfrowanie dysku za pomocą funkcji bitlocker. Dotyczy tylko komputerów z TPM, starsze jednostki są sukcesywnie wymieniane.

[akta kontroli str. 477-480]

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 CEIDG logowanie odbywa się za pomocą certyfikatu kwalifikowanego i hasła,
- w systemie PUMA, logowanie odbywa się za pomocą przyznanego loginu i hasła.

Zabezpieczenie serwerów:

Zabezpieczenia serwerowni:

- Serwerownie posiadają drzwi przeciwpożarowe, gaśnice oraz monitoring wizyjny budynku urzędu oraz samych pomieszczeń.
- Obecnie trwa konfiguracja systemu kontroli parametrów fizycznych serwerowni tj. temperatury, wilgotności, detekcji ruchu, kontrola wejścia / wyjścia,
- Klucze do serwerowni są tylko w dyspozycji Biura Informatyki.

[akta kontroli str. 477-480]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.14. Rozliczalność działań w systemach informatycznych

Stosownie do:

- § 21 ust. 2 rozporządzenia KRI w dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do: 1) systemu z uprawnieniami administracyjnymi; 2) konfiguracji systemu, w tym konfiguracji zabezpieczeń;
  3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa;
- § 21 ust. 3 rozporządzenia KRI poza informacjami wymienionymi w § 21 ust. 2 rozporządzenia KRI są odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci: 1) działań użytkowników nieposiadających uprawnień administracyjnych, 2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu, 3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny – w zakresie wynikającym z analizy ryzyka;
- § 21 ust. 4 rozporządzenia KRI informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.

Zgodnie z § 21 ust. 1 KRI, rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach). Z informacji uzyskanych w trakcie kontroli wynika, że wszystkie systemy serwerowe (serwery aplikacji, plików, baz danych, ActiveDfrectory, Veem) posiadają mechanizmy rejestracji logów. Dodatkowo urządzenia typu UTM (Firewall) także gromadzą togi. Logi zawierają informacje o logowaniu i wylogowaniu użytkownika w systemie, ponadto zawierają dodatkowo informacje o zdarzeniach. Logi przechowywane są w zależności od rodzaju systemu od 14 dni do - bezterminowo.
Z dodatkowych wyjaśnień uzyskanych z Urzędu w powyższej sprawie wynika, że w plikach logów gromadzone są informacje, z jakim zasobem dana stacja robocza się łączyła (protokół i rozdaj aplikacji). Dane gromadzone są przez dwie oddzielne maszyny wirtualne FortiAnalyzer. Logi są nadpisywane gdy skończy się miejsce na dysku. Średni czas przechowywania logów - miesiąc.

Mając na względzie § 21 ust. 4 rozporządzenia KRI, który stanowi, że 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, kontrolujący zwracają uwagę na zachowanie minimalnego okresu przechowywania informacji, wskazanego w powyższym przepisie, w zakresie kontrolowanych systemów teleinformatycznych.

Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 63-73, 477-480]

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, jak i strona www. Urzędu zawierają elementy umożliwiające korzystanie z treści na niej zawartych przez osoby niedowidzące. Zastosowane ułatwienia to:

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

Walidacja za pomocą narzędzia http://wave.webaim.org tj. walidatora WAVE-WCAG 2.0 dla strony BIP i strony www. wykazała błędy (BIP-1 błąd, www.-31 błędów), które wskazują na brak pełnego spełniania standardów dostępności. Brak pełnej zgodności z ustawą o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, w tym niepełne dostosowanie portalu do standardów WCAG 2.0, należy ocenić jako uchybienie. Przyczyną uchybienia jest brak pełnej dostępności cyfrowej stron internetowych. Skutek uchybienia - brak zapewnienia maksymalnego wsparcia osobom niepełnosprawnym. Odpowiedzialnym za powstanie uchybienia jest Informatyk kontrolowanej jednostki.
Jednocześnie należy nadmienić, że na brak zgodności strony internetowej Urzędu ze standardami WCAG 2.0, wskazywały również ustalenia przeprowadzonego audytu bezpieczeństwa informacji (str. 9/32).

[akta kontroli str. 363-395, 499-500]

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia
Mając na uwadze powyższe ustalenia i oceny wnoszę o:

1. Opracowanie wewnętrznych procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby również zasady obiegu dokumentów wpływających i wypływających z Urzędu drogą elektroniczną.

2. Opracowanie i stosowanie w Urzędzie pełnej dokumentacji (w postaci regulacji wewnętrznych), ustanawiającej System Zarzadzania Bezpieczeństwem Informacji, wymaganej zgodnie z § 20 ust. 1 rozporządzenia KRI.

3. Podjęcie działań w celu dostosowania Portalu Internetowego oraz BIP Urzędu do standardów WCAG 2.0.

Proszę Pana Burmistrza o podjęcie działań mających na celu usunięcie stwierdzonych nieprawidłowości i uchybień oraz o poinformowanie Wojewody Warmińsko – Mazurskiego w terminie 14 dni od dnia otrzymania niniejszego wystąpienia, o sposobie wykorzystania uwag i wniosków oraz wykonania zaleceń, a także o podjętych działaniach lub przyczynach niepodjęcia działań.

Jednocześnie informuję, że stosownie do art. 48 ustawy o kontroli w administracji rządowej od wystąpienia pokontrolnego nie przysługują środki odwoławcze.

WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki
/podpisano podpisem elektronicznym/