WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

Olsztyn, 12 kwietnia 2021 r.

FK-IV.431.6.2021

Szanowny Pan
Mirosław Stegienko
Burmistrz Olsztynka
ul. Ratusz 1
11-015 Olsztynek

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 Olsztynku[1], ul. Ratusz 1, 11-015 Olsztynek, NIP: 7390512325, REGON: 000529338

W okresie objętym kontrolą oraz w czasie prowadzonych czynności kontrolnych kierownikiem kontrolowanej jednostki był Pan Mirosław Stegienko – Burmistrz, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 4 listopada 2018 roku.

W dniu rozpoczęcia czynności kontrolnych odpowiedzialnym za realizację zadania objętego kontrolą w Urzędzie był Pan [redacted], zatrudniony na podstawie umowy o pracę od dnia 21 lutego 2011 roku. Osobą bezpośrednio nadzorującą pracownika odpowiedzialnego za realizację zadania była Pani [redacted], zatrudniona na podstawie umowy o pracę od dnia 1 października 1986 roku.

[akta kontroli str. 62]

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.0030.50.2021 z 17 lutego 2021 r., wydanego przez

[1] Zwanym dalej: Urzędem

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.0030.51.2021 z 17 lutego 2021 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 17-18]

Kontrolę przeprowadzono w dniach 25 lutego 2021 r. – 18 marca 2021 r., co zostało odnotowane w książce kontroli Urzędu pod pozycją, Nr 2/2021.

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

Przedmiotem kontroli była ocena działania systemów teleinformatycznych używanych przez jednostki samorządu terytorialnego do realizacji zadań zleconych z zakresu administracji rządowej, na podstawie art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2020 r., poz. 346 ze zm.). Okres objęty kontrolą: od dnia 1 stycznia 2019 r. do dnia 31 grudnia 2020 r.

[akta kontroli str. 1-2, 45-56]

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, 45-56]

Burmistrz Olsztynka upoważnił podinspektora w Referacie Organizacyjnym i Kadr Urzędu Miejskiego w Olsztynku do udzielania informacji w okresie trwania czynności kontrolnych.

[akta kontroli str. 71]

Na podstawie ustaleń kontroli, realizację zadań z zakresu działania systemów teleinformatycznych używanych przez Urząd do realizacji zadań zleconych z zakresu administracji rządowej ocenia się **pozytywnie 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),
3. AA_USC (akty stanu cywilnego),
4. CEIDG (działalność gospodarcza).

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.
3) **Komputerowy system AA_USC** – moduł wspomagający w zakresie kompleksowej obsługi stanu cywilnego. Migracja aktów stanu cywilnego do ŹRÓDŁA. Producent Technika IT Sp. z o.o. Autoryzowanym dystrybutorem oprogramowania jest firma NanoCom Białystok.

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.

[akta kontroli str. 43-44, 153-154]

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 /811gd6wpjb/skrytka, znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie i odbieranie pism w formie dokumentów elektronicznych. Ścieżkę bezpośredniego przejścia na główną stronę e-PUAP, zawarto na stronie internetowej BIP Urzędu – Strona główna. 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.

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

W związku z powyższym w Urzędzie powinna być stosowana praktyka zamieszczania na stronach internetowych urzędu w BIP procedur postępowania określających sposób

przyjmowania i załatwiania poszczególnych spraw w Urzędzie, w tym załatwianych przy pomocy wniosku elektronicznego zgodnie z § 5 ust. 2 pkt 1 i 4 KRI. Brak publikacji procedur realizacji zadań dotyczących poszczególnych wydziałów Urzędu, należy zatem uznać za uchybienie. Obywatel ma prawo wiedzieć o wszystkich okolicznościach, które mogą wpłynąć na ustalenie jego praw i obowiązków w prowadzonym postępowaniu.
Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki. Zgodnie z wyjaśnieniem Burmistrza, cyt.: *„(...) Rozważamy jednak w najbliższym czasie opracowanie i zamieszczenie w Biuletynie Informacji Publicznej Urzędu opisów obowiązujących procedur przy załatwianiu spraw."*

Należy wskazać ponadto, że na stronie BIP opublikowane są wzory wniosków i formularzy, będących w zakresie poszczególnych referatów w Urzędzie. Urząd udostępniał oraz świadczył również usługi elektroniczne, z wykorzystaniem ePUAP, tj. „Skargi, wnioski, zapytania do urzędu". Usługa te umożliwiają złożenie do wybranego organu administracji publicznej skargi lub wniosku w sprawie.

W ramach prowadzonych czynności kontrolnych ustalono, iż na stronie głównej Urzędu znajduje się odnośnik do Elektronicznego Biura Obsługi Klienta Urzędu Miejskiego w Olsztynku. EBOK w założeniu miał umożliwić m.in. złożenie wniosku w wybranych sprawach, sprawdzić ewentualne należności zalogowanego kontrahenta na rzecz jednostki oraz umożliwić ich płatność. Kontrolujący w ramach prowadzonych czynności stwierdzili, że w okresie prowadzonych czynności kontrolnych nie było możliwości zalogowania się do sytemu za pomocą profilu zaufanego.
Burmistrz Olsztynka wyjaśnił, że cyt.: *„Brak możliwości korzystania z EBOK spowodowany jest brakiem aktualnego certyfikatu nadawanego przez Ministerstwo Cyfryzacji. W dniu 12 listopada 2020 roku, za pośrednictwem platformy EPUAP wystąpiliśmy z wnioskiem o wydanie stosownego certyfikatu (wniosek12112020.pdf), a w dniu 13 listopada ub. roku otrzymaliśmy potwierdzenie wygenerowania certyfikatu (email13112020.pdf). W związku z utratą klucza prywatnego zmuszeni byliśmy do wnioskowania o unieważnienie tego certyfikatu, co uczyniliśmy dnia 16 listopada 2020 roku (wniosek16112020.pdf). Dnia 25 stycznia 2021 roku wysłaliśmy zgłoszenie dotyczące wniosku z 16 listopada 2020 roku (email25012021.pdf). Do tej pory nie otrzymaliśmy odpowiedzi na wniosek i na zgłoszenie. Nie możemy wystąpić o nowy certyfikat dopóki obecny nie zostanie unieważniony".*

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

[akta kontroli str. 347-348, 431-435, 438-441]

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. Jednocześnie należy nadmienić, że wcześniej przekazywał takie dokumenty – zgodnie z wyjaśnieniem uzyskanym z Urzędu cyt.:

- 2015/11/10/2859; 0.11.2015; URZĄD MIEJSKI W OLSZTYNKU; DR-1 DEKLARACJA NA PODATEK ROLNY;
- 2015/02/18/2082; 18.02.2015; URZĄD MIEJSKI W OLSZTYNKU; Wniosek o rozłożenie należności na raty, odroczenie terminu, umorzenie zaległości, umorzenie odsetek;
- 2015/02/18/2080; 18.02.2015; URZĄD MIEJSKI W OLSZTYNKU; DN-1 Deklaracja na podatek od nieruchomości;
- 2014/12/03/1870; 03.12.2014; URZĄD MIEJSKI W OLSZTYNKU; DL-1 DEKLARACJA NA PODATEK LEŚNY.

Wskazane wzory dokumentów faktycznie znajdują się w zasobach CRWDE.

Jednocześnie należy zaznaczyć, iż na stronie BIP Urzędu oraz na portalu eUsługi, 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. 431-435, 442-445]

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://olsztynek.pl/, a strona internetowa BIP Urzędu – pod adresem http://bip.olsztynek.pl/.
Na stronie internetowej Urzędu zamieszczono bezpośredni link do strony BIP Urzędu, w prawej części panelu strony. Na stronie głównej BIP Urzędu zamieszczono ścieżkę do skrzynki podawczej ESP na platformie ePUAP.

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]

[redacted]

[akta kontroli str. 431-435]

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.*

W Urzędzie w celu zarządzania obiegiem dokumentów i dokumentacją stosowane są procedury i zasady postępowania z dokumentami wpływającymi do Urzędu zawarte w Instrukcji Kancelaryjnej, stanowiącej załącznik do rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych. W Urzędzie zgodnie z §41 ust. 1 Regulaminu Organizacyjnego (przyjętego zarządzeniem Nr k/22/17 Burmistrza Olsztynka z 7 kwietnia 2017 r.), obowiązuje tradycyjny (papierowy) system wykonywania czynności kancelaryjnych, wspomagany przez system elektronicznego obiegu dokumentów umożliwiający w szczególności: prowadzenie rejestrów przesyłek wpływających, udostępnianie i rozpowszechnianie pism wewnątrz podmiotu, przesyłanie przesyłek i ich dekretacje.

Z uzyskanego w ramach prowadzonych czynności kontrolnych wyjaśnienia wynika, że cyt.: *„W Urzędzie Miejskim w Olsztynku nie opracowano i nie przyjęto odrębnego zarządzenia regulującego ogólny obieg dokumentów w Urzędzie, w tym dokumentów wpływających i wypływających w formie elektronicznej. Zasady określające obieg dokumentów w Urzędzie, w tym wpływających i wypływających w formie elektronicznej reguluje załącznik Nr 1 do rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych opublikowanego w Dzienniku Ustaw Nr 14 pod poz. 67) oraz instrukcja do Systemu PROTON wspomagającego tradycyjny obieg dokumentacji w Urzędzie."*

System EZD PROTON firmy Sputnik Software Sp. z o.o. ul. Klinkierowa 7 60-104 Poznań pozwala na zarządzanie pełnym cyklem obiegu dokumentów i spraw w instytucji publicznej, począwszy od przyjęcia korespondencji, aż do wydania decyzji administracyjnej. Proton

może pracować w trybie EZD lub jako system wspomagający obieg tradycyjny, zgodnie z właściwą instrukcją kancelaryjną. W Urzędzie system działa jako wsparcie papierowego obiegu dokumentów (§41 ust. 1 Regulaminu Organizacyjnego). Do systemu wprowadzany jest skan pierwszej strony korespondencji przychodzącej i rejestrowana jest w nim dekretacja, dodatkowo pracownicy prowadzą sprawy w odpowiednich teczkach i rejestrują w systemie odpowiedzi. Cały proces ma na celu ułatwienie kontroli nad dokumentami, pismami, sprawami i teczkami oraz pomaga w odnajdywaniu poszczególnych elementów obiegu korespondencji. Pomaga pracownikom w utrzymaniu odpowiedniej kolejności spraw i wspiera w terminowości. Dzięki niemu można również wygenerować spis spraw.

Jednocześnie, 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 oraz Elektroniczne Biuro Obsługi Klienta), 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 pozwalają właściwie dbać o jej bezpieczeństwo.
W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie uchybieniami. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki.

[akta kontroli str. 431-435]

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. 431-435]

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.

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 K/70/2018 Burmistrza Olsztynka z dnia 17 września 2018 roku wprowadzono do stosowania w Urzędzie Miejskim w Olsztynku Politykę Ochrony Danych.

[akta kontroli str. 73-129]

Przedmiotową dokumentację sporządzono na podstawie obowiązujących przepisów prawa, tj. „RODO", ustawy dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000), w brzmieniu obowiązującym w tym okresie. 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.

Burmistrz Olsztynka wyznaczył Administratora Systemu Informatycznego w Urzędzie (ASI) oraz powołał w jednostce Inspektora Ochrony Danych (IOD) – umowa z firmą zewnętrzną.

[akta kontroli str. 130-152, 340-346]

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 przeglądu SZBI funkcjonującego w Urzędzie. Z przeprowadzanych czynności sporządzano raporty, które obejmowały również rekomendacje wydane w celu doskonalenia SZBI w jednostce.

[akta kontroli str. 155-175]

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.
Zgodnie z przekazaną dokumentacją wymagane oszacowanie i analiza ryzyka utraty integralności, dostępności lub poufności informacji w jednostce, przeprowadzona została w lutym 2020 roku. Jednocześnie należy zaznaczyć, iż kontrolującym nie przedstawiono dokumentacji świadczącej o przeprowadzeniu okresowej analiz ryzyka utraty integralności, dostępności lub poufności informacji w 2019 roku.

Z przekazanego w powyższej sprawie wyjaśnienia wynika, że: *„(...) Analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych przyjęta została na początku 2020 roku (luty) i poprzedzona została żmudnymi pracami nad aktualizacją Rejestru czynności przetwarzania danych. Kolejnej Analizy zagrożeń i ryzyka przy przetwarzaniu danych osobowych dokonano w marcu bieżącego roku, po dokonaniu aktualizacji obowiązujących dokumentów dotyczących ochrony danych."*

[akta kontroli str. 431-435]

Kontrolujący uwzględniają przedstawione wyjaśnienia. Jednocześnie zwraca się uwagę na to, iż w przyjętej Polityce Ochrony Danych należałoby wprowadzić zapisy ustalające minimalny okres do przeprowadzenia okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji.
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.

Jednocześnie należy wskazać, iż w jednostce jest opracowany i prowadzony rejestr czynności przetwarzania danych osobowych.

[akta kontroli str. 376-377]

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. 176-335]

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 K/70/2018 Burmistrza Olsztynka z dnia 17 września 2018 roku wprowadzającym do stosowania w Urzędzie Miejskim w Olsztynku Politykę Ochrony Danych.

[akta kontroli str. 73-129]

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. 378-382]

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 jednym szkoleniu (zorganizowanych przez IOD), dotyczącym ochrony danych osobowych.
Szkolenie przeprowadzone w 2020 roku obejmowało:

- zasady przetwarzania danych osobowych według RODO oraz w praktyce;
- rodzaje danych osobowych w świetle zapisów RODO;
- sposoby przetwarzania danych osobowych w świetle zapisów RODO;
- środki techniczne i organizacyjne stosowane do ochrony danych osobowych w praktyce; Praktyczne aspekty ochrony danych osobowych w świetle zapisów Polityki Ochrony Danych Osobowych;
- naruszenia danych osobowych w świetle zapisów RODO oraz ustawodawstwa krajowego;
- naruszenia danych osobowych w praktyce;
- zagrożenia związane z umyślnym naruszeniem danych osobowych (tj. kradzież lub wyłudzanie danych osobowych);
- zagrożenia związane z nieumyślnym naruszeniem danych osobowych;
- kradzież tożsamości w praktyce;
- zagrożenia związane z wykorzystaniem działań socjotechnicznych;
- sposoby ochrony urządzeń (telefony, komputery) przed utratą danych;
- odpowiedzialność pracodawcy (administratora) i pracownika (użytkownika) z tytułu naruszenia danych osobowych w kontekście ustawodawstwa krajowego.

W załączeniu przedstawiono listy obecności pracowników uczestniczących w szkoleniu.

[akta kontroli str. 383-387]

Na zadane przez kontrolujących pytanie dotyczące podania przyczyny braku przeprowadzonych szkoleń pracowników Urzędu w zakresie dotyczącym ochrony danych osobowych w 2019 r., Urząd wyjaśnił, że cyt.: *„W 2019 nie prowadzono zbiorczych szkoleń*

wszystkich pracowników Urzędu jedynie przeszkolono, na jednym posiedzeniu wszystkich piętnastu radnych Rady Miejskiej w Olsztynku. W 2019 roku – w dniach: 20 stycznia, 30 kwietnia, 16 czerwca, 12 września i 6 grudnia - wyznaczony inspektor ochrony danych osobowych prowadził szkolenia indywidualne dla pracowników będąc do ich dyspozycji w wyznaczonych dniach i godzinach w siedzibie Urzędu. Dodatkowo, na przestrzeni całego roku drogą e-mailową udzielał informacji i rozwiązywał bieżące problemy dotyczące ochrony danych osobowych. Z czynności przeprowadzanych w Urzędzie sporządzał stosowne raporty zawierające rekomendacje dla kierownictwa Urzędu.

[akta kontroli str. 431-435]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.6. Praca na odległość i mobilne przetwarzanie danych

Zgodnie z § 20 ust. 2 pkt 8 rozporządzenia KRI *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.*

Zasady pracy na komputerach przenośnych w uproszczonym zakresie określone zostały zarządzeniem Nr K/70/2018 Burmistrza Olsztynka z dnia 17 września 2018 roku wprowadzającym do stosowania w Urzędzie Miejskim w Olsztynku Politykę Ochrony Danych. W rozdziale 10 przedmiotowej polityki ujęto zasady wynoszenia przenośnego sprzętu informatycznego poza siedzibę Urzędu. Ponadto z wyjaśnienia Burmistrza Olsztynka wynika, że cyt.: „[redacted]".

[akta kontroli str. 73-129, 431-435]

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.

Zgodnie z zarządzeniem Nr K/70/2018 Burmistrza Olsztynka z dnia 17 września 2018 roku wprowadzającym do stosowania w Urzędzie Miejskim w Olsztynku Politykę Ochrony Danych rozdział 12.4 pracownik zajmujący się obsługą informatyczną Urzędu Miejskiego w Olsztynku jest odpowiedzialny za dokonywanie przeglądu i konserwacji systemów oraz nośników służących do przetwarzania danych.

W Urzędzie użytkowane są dwa systemy teleinformatyczny przeznaczone do realizacji zadań zleconych z zakresu administracji rządowej zakupione u zewnętrznego dostawcy, tj.: PUMA oraz AA_USC ([redacted]).

W związku z zakupem ww. systemów podpisane zostały z firmami [redacted] umowy licencyjne umożliwiające prawidłową eksploatację i rozwój systemu poprzez możliwość zgłaszania błędów pytań i roszczeń dotyczących użytkowanego systemu.
Zarówno z jedną jak i drugą firmą zawarte zostały również stosowne umowy powierzenia danych gwarantujące właściwe zabezpieczenie danych w przypadku awarii systemu oraz gwarantujące bezpieczeństwo informacji uzyskanych przez wykonawcę w związku z realizacją umowy.

[akta kontroli str. 388-423]

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 K/70/2018 Burmistrza Olsztynka z dnia 17 września 2018 roku wprowadzającym do stosowania w Urzędzie Miejskim w Olsztynku Politykę Ochrony Danych (zał. 18).

[akta kontroli str. 97-104]

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 2019 r. do dnia 31 grudnia 2020 r., w jednostce przeprowadzono 2 zadania audytowe w zakresie bezpieczeństwa informacji, tj.:

- w marcu 2019 r. dokument – raport z audytu RAP/2019/ŁS/03/07
- w kwietniu 2020 r. dokument – raport z audytu RAP/2019/KJ/04/37

Przeprowadzone zadania audytowe obejmowały m.in. następujące zagadnienia:

- Inwentaryzacja sprzętu i oprogramowania,
- Ochrona przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami,
- Urządzenia mobilne i praca na odległość,
- Zabezpieczenia informacji w sposób uniemożliwiający nieuprawnione jej ujawnienie, modyfikacje, usunięcie lub zniszczenie,
- Zasady postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych,
- Poziom bezpieczeństwa w systemach teleinformatycznych,
- Okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji,
- Analiza podatności systemu informatycznego,
- Skanowanie sieci lokalnej,
- Skanowanie od strony sieci Internet,
- Analiza podatności strony internetowej,
- Identyfikacja zasobów ogólnodostępnych sieci lokalnej.

[akta kontroli str. 336-339]

Na podstawie przekazanej dokumentacji kontrolujący stwierdzili, że w okresie objętym kontrolą 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 - został zrealizowany.

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 kopii zapasowych w okresie objętym kontrolą uregulowane zostały zarządzeniem Nr K/70/2018 Burmistrza Olsztynka z dnia 17 września 2018 roku wprowadzającym do stosowania w Urzędzie Miejskim w Olsztynku Politykę Ochrony Danych. W załączniku nr 13 do obowiązującej (w okresie objętym kontrolą) Polityki określono m.in. częstotliwość tworzenia kopii zapasowych, nośnik na jakim wykonywano kopię, sposób wykonywania oraz miejsce przechowywania kopii zapasowych.

Urząd w powyższej sprawie wyjaśnił, że cyt.: „[redacted]”

[akta kontroli str. 424-426, 431-436]

Mając powyższe na uwadze należy stwierdzić, że kopie zapasowe wykonywane były zgodnie z założeniami przyjętej w Urzędzie Polityki Ochrony Danych.

W przypadku wykonywania testów w celu sprawdzenia poprawności wykonywania kopii zapasowych oraz sprawdzenia przydatności utworzonych kopii podczas próby symulowanego przywrócenia i uruchomienia oprogramowania dziedzinowego po przywróceniu Urząd wyjaśnił, że cyt.: „[redacted]”

Jednocześnie należy zaznaczyć, iż brak potwierdzenia w dokumentacji czynności w zakresie wykonywania testów w celu sprawdzenia poprawności kopii zapasowych oraz sprawdzenia przydatności utworzonych kopii podczas próby symulowanego przywrócenia i uruchomienia, nie pozwala kontrolującemu jednoznacznie stwierdzić, że sprawdzenia poprawności tworzonych kopii zapasowych były faktycznie wykonywane. W dokumentacji SZBI przyjętej w Urzędzie brak jest opracowanych procedur regulujących proces testowania wytworzonych kopii zapasowych. Powyższe należy zakwalifikować jako uchybienie.
Osobami odpowiedzialnymi za powstanie uchybienie są: pracownik realizujący zadanie oraz osoba bezpośrednio go nadzorująca.

[akta kontroli str. 431-436]

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.

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

2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

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

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 oraz AA_USC. Na obsługę aktualnie zainstalowanego oprogramowania z firmami dostarczającymi dany system informatyczny zawarte zostały stosowne umowy licencyjne (opieka autorska), gwarantująca rozwój systemu i dostosowanie do obowiązujących przepisów prawa. Zakupione systemy teleinformatyczne, w razie awarii podlegają ekspertyzie technicznej zlecanej firmie dostarczającej.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 388-423]

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 wyjaśnieniem uzyskanym w trakcie kontroli, cyt.: „[redacted]

[redacted]

[akta kontroli str. 431-435]

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:

[redacted]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.14. Rozliczalność działań w systemach informatycznych

Stosownie do:

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

Zgodnie z § 21 ust. 1 KRI, rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach).

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

Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 431-435, 437, 446-447]

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. Na stronie BIP w zakładce *ułatwienia dla osób niesłyszących* widnieje informacja, że Urząd zapewnia wszystkim zainteresowanym przy załatwieniu spraw urzędowych bezpłatną pomoc:
- pośrednictwa tłumacza PJM – polskiego języka migowego,
- pośrednictwa tłumacza SJM – systemu językowo – migowego,
- tłumacza przewodnika, nazwanego w ustawie tłumaczem SKOGN.

Ponadto zawarto informację, iż aby skorzystać z pośrednictwa tłumacza należy powiadomić Urząd (np. e-mailem lub faksem) trzy dni przed planowanym terminem załatwienia sprawy, z wyłączeniem sytuacji nagłych. Formularz powiadomienia o chęci skorzystania ze świadczenia usług tłumacza PJM, SJM, SKOGN znajduje się w załączniku na stronie. Usługa jest bezpłatna dla osoby uprawnionej, będącej osobą niepełnosprawną w rozumieniu ustawy z dnia 27 sierpnia 1997 roku o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych.

Zgodnie z załącznikiem nr 4 do rozporządzenia KRI, strony BIP i www. spełniają 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.

Walidacja za pomocą narzędzia http://wave.webaim.org tj. walidatora WAVE-WCAG 2.0 dla strony BIP i strony www. wykazała błędy, które nie mają wpływu na przedmiot kontroli.

Powyższe zagadnienie oceniono pozytywnie.

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny wnoszę o:

1. Uzupełnienie strony BIP Urzędu poprzez opisanie i zawarcie obowiązujących procedur stosowanych przez Urząd przy załatwianiu poszczególnych spraw będących w kompetencjach danego wydziału.

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

3. Zgodnie z § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI regularne testowanie jakości wytworzonych kopii zapasowych poprzez odtworzenie danych systemu informatycznego z wytworzonej kopii. Ponadto każdorazowe dokumentowanie wykonywanych testów poprawności wytworzonych kopii zapasowych oraz uzupełnienie Polityki Ochrony Danych, w zakresie procedur regulujących proces przeprowadzania testów wytworzonych kopii zapasowych.

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

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

WOJEWODA
WARMIŃSKO-MAZURSKI

Artur Chojecki