WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

Olsztyn, 24 kwietnia 2019 r.

FK-IV.431.4.2019

Szanowny Pan
Piotr Petrykowski
Burmistrz Bartoszyc
ul. Boh. Monte Cassino 1
11-200 Bartoszyce

Stosownie do art. 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. Nr 185, poz. 1092), zwanej dalej „ustawą o kontroli w administracji rządowej", przekazuję Panu treść wystąpienia pokontrolnego.

Wystąpienie pokontrolne

Kontrolę przeprowadzono w Urzędzie Miasta Bartoszyce ul. Boh. Monte Cassino 1, 11-200 Bartoszyce, NIP: 7430007729, REGON: 000524329 oraz Miejskim Ośrodku Pomocy Społecznej w Bartoszycach ul. Pieniężnego 10a, 11-200 Bartoszyce, NIP: 7431232374, REGON: 510518050.

W okresie objętym kontrolą oraz w okresie prowadzenia kontroli stanowiska pełnili:
Pracownicy Urzędu Miasta w Bartoszycach:

1. **Pan Piotr Petrykowski** - Burmistrz, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 4 listopada 2018 roku (*kierownik jednostki kontrolowanej*),
2. **Pan Robert Pająk** - Sekretarz Miasta, zatrudniony na podstawie umowy o pracę od dnia 16 stycznia 2015 roku,
3. **Pani Edyta Orpik** - Kierownik Wydziału Organizacyjno-Administracyjnego, zatrudniona na podstawie umowy o pracę od dnia 6 października 2003 roku (*nadzorująca bezpośrednio pracownika realizującego zadania objęte kontrolą*).
4. **Pan Karol Puszkiewicz** - Kierownik Referatu ds. Informatyzacji Urzędu, zatrudniony na podstawie umowy o pracę od dnia 1 września 2009 roku (*realizujący zadania objęte kontrolą*),

Pracownicy Miejskiego Ośrodka Pomocy Społecznej w Bartoszycach:

1. **Pani Stefania Michalik-Rosa** - Dyrektor Miejskiego Ośrodka Pomocy Społecznej w Bartoszycach (*kierownik jednostki kontrolowanej, nadzorujący bezpośrednio pracownika realizującego zadania objęte kontrolą*),
2. **Pan Rafał Matyjasek** - Informatyk Miejskiego Ośrodka Pomocy Społecznej

w Bartoszycach, Inspektor Ochrony Danych Osobowych (*realizujący zadania objęte kontrolą*),

[akta kontroli str. 51]

Kontrolę przeprowadził pracownik Wydziału Finansów i Kontroli Warmińsko- Mazurskiego Urzędu Wojewódzkiego w Olsztynie, Radosław Gazda – inspektor wojewódzki; legitymacja służbowa nr 9/2019, wydana przez Dyrektora Generalnego Warmińsko - Mazurskiego Urzędu Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienie do kontroli nr FK-IV.0030.123.2019 z 21 lutego 2019 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 50]

Kontrolę przeprowadzono w dniach 25-27 lutego 2019 r., co zostało odnotowane w książce kontroli Urzędu Miasta w Bartoszycach pod pozycją Nr 1/2019, w książce kontroli Miejskiego Ośrodka Pomocy Społecznej w Bartoszycach pod pozycją Nr 1/2019.

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 2017 r. poz. 570 ze zm.). Okres objęty kontrolą: od dnia 1 stycznia 2018 r. do dnia 25 lutego 2019 r. (dzień rozpoczęcia czynności kontrolnych).

[akta kontroli str. 1-4, 37-46]

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. Nr 185, poz. 1092) oraz art. 28 ust. 1 pkt 2 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (t.j. Dz. U. z 2017 r., poz. 2234) 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 (t.j. Dz.U. z 2017 r. poz. 570 ze zm.) zwanej dalej „ustawą" oraz 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 j.t.) zwanego dalej „rozporządzeniem KRI", 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. 1-4, 37-46]

W czasie trwania czynności kontrolnych informacji i wyjaśnień udzielali pracownicy upoważnieni przez Burmistrza Bartoszyc, tj.: Kierownik Referatu ds. Informatyzacji Urzędu oraz Audytor Wewnętrzny zatrudniony w UM Bartoszyce. Bieżąca kontrola była pierwszą

kontrolą zewnętrzną z tego zakresu przeprowadzaną w Urzędzie Miasta i MOPS w Bartoszycach.

[akta kontroli str. 52,55]

Na podstawie ustaleń kontroli, realizację zadań z zakresu wykorzystania systemów teleinformatycznych używanych przez jednostki samorządu terytorialnego do realizacji zadań zleconych z zakresu administracji rządowej w przypadku Urzędu Miasta w Bartoszycach ocenia się pozytywnie z nieprawidłowościami, w przypadku Miejskiego Ośrodka Pomocy Społecznej w Bartoszycach - pozytywnie z uchybieniami.

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

Z informacji przekazanych przez UM oraz MOPS w Bartoszycach przed rozpoczęciem czynności kontrolnych oraz uzyskanych w trakcie prowadzenia kontroli wynika, że w kontrolowanych jednostkach do realizacji zadań zleconych z zakresu administracji rządowej wykorzystywanych jest **7** systemów teleinformatycznych oraz prowadzony jest **1** rejestr publiczny.

Systemy teleinformatyczne wykorzystywane w Urzędzie Miasta Bartoszyce:

1) **PUMA SOJST- Moduł Ewidencja Ludności** posiada homologację MSW, a jego zadaniem jest kompleksowa obsługa komórki ewidencji ludności. Aplikacja umożliwia między innymi: gromadzenie, wyszukiwanie, uzupełnianie oraz zmianę w bazie danych wszystkich informacji znajdujących się na Karcie Osobowej Mieszkańca. Program automatyzuje pracę i drukuje zawiadomienia w zakresie: meldowania, wymeldowania, rejestracji urodzeń, zgonów, zmian stanu cywilnego, gromadzenia i dostępu do danych historycznych mieszkańców.
   Moduł Wyborcy – kompleksowa obsługa wyborów. Moduł Wyborcy umożliwia prowadzenie i aktualizację rejestru wyborców, sporządzanie spisów wyborców uprawnionych do udziału w wyborach i referendum, pozwala na generowanie kwartalnych meldunków dla KBW (Krajowego Biura Wyborczego) o stanie wyborców mieście na podstawie bazy danych ewidencyjnych.

2) **ŹRÓDŁO** - bezpłatna aplikacja, która obsługuje wszystkie wymagane polskim prawem działania w zakresie rejestru PESEL, dowodów osobistych i stanu cywilnego. 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 Rejestru Sprzeciwów (CRS).

3) **PB_USC** - moduł wspomagający w zakresie kompleksowej obsługi stanu cywilnego.

Migracja aktów stanu cywilnego do Bazy Usług Stanu Cywilnego (BUSC). Producent Technika IT Sp. z o.o.

4) **CEIDG** - 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.

<u>Systemy teleinformatyczne wykorzystywane w MOPS w Bartoszycach:</u>

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

2) **POMOST Std. -** jest systemem informatycznym przeznaczonym dla jednostek organizacyjnych pomocy społecznej i wspomagającym je w realizacji zadań gminy i powiatu, wynikających z ustawy o pomocy społecznej i towarzyszących jej aktów prawnych. Podstawowym zadaniem oprogramowania jest wsparcie procesu decyzyjnego w ośrodku oraz procesu realizacji świadczeń wynikających z decyzji.

3) **PUMA (dodatek energetyczny)** – obsługa procesów wydawania decyzji administracyjnych oraz realizacji świadczeń.

Rejestry publiczne prowadzone w Urzędzie Miasta Bartoszyce:

Rejestr działalności regulowanej w zakresie odbierania odpadów komunalnych od właścicieli nieruchomości (podstawa prawna - art. 9b ust. 2-3 ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach, t. j. Dz. U. z 2017 r., poz. 1289 ze zm.),

[akta kontroli str. 20-36]

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 Miasta w Bartoszycach posiada aktywną Elektroniczną Skrzynkę Podawczą (urzadmiastabartoszyce/SkrytkaESP) znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie pism w formie dokumentów elektronicznych. Szczegółowe informacje dotyczące funkcjonowania oraz możliwość bezpośredniego przejścia na główną stronę e-PUAP, zawarto na stronie internetowej BIP Urzędu, w lewym panelu ekranu w zakładce → MENU PRZEDMIOTOWE → Elektroniczna Skrzynka Podawcza. Formaty danych przyjmowane za pośrednictwem Elektronicznej Skrzynki Podawczej to: txt, rtf, pdf, odt, ods, odp, doc, docx, xls, xlsx, ppt, pptx, jpg, png, zip, 7z, XAdES.

MOPS w Bartoszycach posiada również aktywną Elektroniczną Skrzynkę Podawczą znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie pism w formie dokumentów elektronicznych. Adres skrytki Miejskiego Ośrodka Pomocy Społecznej to: /b34v79vxpe/SkrytkaESP/. Szczegółowe informacje dotyczące funkcjonowania oraz możliwość bezpośredniego przejścia na główną stronę e-PUAP, zawarto na stronie internetowej MOPS w lewym górnym panelu ekranu w zakładce: O nas – Kontakt.

W wyniku prowadzonej kontroli stwierdzono, iż w ramach funkcjonującej strony internetowej Urzędu Miasta w Bartoszycach działa Elektroniczne Biuro Obsługi Interesanta

(eBOI). Jest to platforma internetowa dla mieszkańców i kontrahentów Urzędu Miasta Bartoszyce umożliwiająca: uzyskanie kompleksowej informacji o procedurach załatwiania spraw w Urzędzie Miasta Bartoszyce, prowadzenie rozliczeń finansowych z Urzędem za pośrednictwem przelewów online, prezentację stanów indywidualnych kont kontrahentów, wysyłanie powiadomień za pośrednictwem poczty elektronicznej lub usługi sms o zbliżających się terminach płatności należności, wysyłanie powiadomień o aktualnych wydarzeniach. W ramach systemu udostępnione zostały:

- ***KARTY USŁUG*** – zawierające szczegółowe informacje o procedurach załatwiania spraw w Urzędzie,
- ***AKTYWNE FORMULARZE*** – czyli usługi elektroniczne realizowane za pośrednictwem Elektronicznej Skrzynki Podawczej Urzędu na platformie ePUAP,
- ***EPŁATNOŚCI*** – moduł umożliwiający zarządzanie zobowiązaniami wobec Urzędu poprzez podgląd bieżących należności i przeglądanie historycznych rozliczeń oraz dokonywanie płatności za pomocą przelewów on-line.

Treść publikowanych w systemie eBOI kart usług/procedur realizowanych przez Urząd Miasta Bartoszyce opracowywana jest przez komórki organizacyjne oraz jednostki podległe Urzędu, zgodnie z realizowanym zakresem zadań. Informacja jest przygotowywana w oparciu o wzór karty usługi, a opublikowana karta usługi zawiera:

- odnośnik do formularza aktywnego opublikowanego w ePUAP, umożliwiającego realizację procedury w sposób elektroniczny,
- odnośniki do wzorów dokumentów do pobrania,
- odnośnik do klauzuli informacyjnej.

Za opublikowanie treść w systemie eBOI odpowiada Referat ds. Informatyzacji Urzędu. Pracownicy referatu publikują karty usług, które otrzymują za pośrednictwem poczty elektronicznej, na specjalnie w tym celu przygotowany adres eboitgum.bartoszyce.pl.

Zarówno Urząd Miasta jaki i MOPS w Bartoszycach udostępniały oraz świadczyły usługę elektroniczną, z wykorzystaniem ePUAP, tj. „Pismo ogólne do urzędu". Usługa ta umożliwia złożenie do wybranego organu administracji publicznej pisma (podania) w sprawie, co do której nie mają zastosowania inne formularze.
W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 56-85]

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 ramach prowadzonych czynności kontrolnych ustalono, iż w okresie objętym kontrolą Urząd Miasta w Bartoszycach, w związku z uruchomioną platformą internetową dla mieszkańców i kontrahentów (eBOI), której działanie opisano w pkt 1.1, zwracał się do Ministerstwa Cyfryzacji o opublikowanie w CRWDE 17 wzorów dokumentów. Do dnia zakończenia kontroli przedmiotowe wzory nie zostały opublikowane w CRWDE. Jedynym aktualnym dokumentem widniejącym w CRWDE udostępnionym przez Urząd Miasta w Bartoszycach jest: *wzór deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi*, opublikowany w dniu 24 stycznia 2007 r. (ID wzoru: 3877, Nr wzoru: 2017/01/24/3877).
W trakcie kontroli ustalono, że MOPS w Bartoszycach w badanym okresie nie przekazywał wzorów dokumentów elektronicznych do centralnego repozytorium wzorów dokumentów prowadzonego przez Ministerstwo Cyfryzacji, ze względu na fakt, iż nie uruchamiał nowej usługi, dla której nie ma wzorów dokumentów w CRWDE.
W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 86-120]

1.3. Model usługowy

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

Strona internetowa Urzędu działa pod adresem http://bartoszyce.pl/, a strona internetowa BIP Urzędu – pod adresem http://bip.bartoszyce.pl/.
Strona internetowa MOPS w Bartoszycach działa pod adresem http://www.mopsbartoszyce.pl/, a strona internetowa BIP - MOPS w Bartoszycach pod adresem http://bip.bartoszyce.pl/128/Miejski_Osrodek_Pomocy_Spolecznej/.

Na stronie internetowej Urzędu zamieszczono link do strony BIP Urzędu w zakładce „Na

skróty". Na stronie głównej BIP UM Bartoszyce, w podanych danych kontaktowych zamieszczono link do skrzynki podawczej ESP na platformie ePUAP.
MOPS w Bartoszycach posiada również aktywną Elektroniczną Skrzynkę Podawczą, której adres podany jest w lewym panelu wyświetlanej strony, w zakładce – „O nas" – podzakładka „Kontakt". Zarówno Urząd Miasta jaki i MOPS wykorzystywały platformę ePUAP, jako pomocnicze narzędzie do świadczenia usług elektronicznych poprzez automatyczną integrację ePUAP z usługą „Pismo ogólne do urzędu" umożliwiającą złożenie do wybranego organu administracji publicznej pisma (podania) w sprawie.
Na stronie internetowej UM w Bartoszycach w prawej dolnej części panelu strony, znajduje się link publikujący procedurę tworzenia bezpłatnego profilu zaufanego, dzięki któremu bez wychodzenia z domu bądź z dowolnego miejsca, 24 godziny na dobę, można zrealizować wiele spraw urzędowych. Pisma podpisane bezpłatnym profilem zaufanym i wysłane na elektroniczną skrzynkę podawczą urzędu, mają taką samą ważność jak dokumenty złożone do urzędu w postaci papierowej. W podanych informacjach opublikowane są adresy punktów (na terenie miasta), w których można potwierdzić utworzony profil zaufany.
W ramach Projektu „Rozwój e-usług publicznych w Gminie Miejskiej Bartoszyce", Oś priorytetowa 3 – "Cyfrowy Region", Działanie 03.01.00 – "Cyfrowa dostępność informacji sektora publicznego oraz wysoka jakość e-usług publicznych" Regionalnego Programu Operacyjnego Województwa Warmińsko-Mazurskiego na lata 2014-2020, zgodnie z informacją umieszczoną na stronie internetowej Urzędu, w dniu 5 lutego 2019 r. rozpoczęło funkcjonowanie Elektroniczne Biuro Obsługi Interesanta (euslugi.bartoszyce.pl). Jest to (zgodnie z inf. z pkt 1.1) platforma internetowa dla mieszkańców i kontrahentów Urzędu Miasta Bartoszyce umożliwiająca: uzyskanie kompleksowej informacji o procedurach załatwiania spraw w Urzędzie Miasta Bartoszyce, prowadzenie rozliczeń finansowych z Urzędem za pośrednictwem przelewów online, prezentację stanów indywidualnych kont kontrahentów, wysyłanie powiadomień za pośrednictwem poczty elektronicznej lub usługi sms o zbliżających się terminach płatności należności, wysyłanie powiadomień o aktualnych wydarzeniach.
W Urzędzie Miasta oraz w MOPS w Bartoszycach brak jest formalnych procedur opisujących obsługę oraz monitorowanie usług elektronicznych, ze względu na fakt, że instytucje te nie świadczyły usług elektronicznych na zewnątrz za pomocą systemów teleinformatycznych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej, w związku z powyższym przedmiotowe cząstkowe zagadnienie nie podlegało ocenie.

[akta kontroli str. 121-131]

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 w wyniku kontroli wynika, że kontrolowane systemy Urzędu Miasta współpracują z innymi systemami publicznymi. Moduł Ewidencja Ludności systemu SOJST PUMA, jako aplikacja wspierająca, w zakresie aktualizacji danych mieszkańców miasta Bartoszyce pobiera dane z Systemu Rejestrów Państwowych (SRP). W tym celu firma ZETO Software sp. z o.o. świadcząca usługę opieki autorskiej na ww. system dostarczyła aplikację o nazwie import PESEL, która pobiera dane z Systemu Rejestrów Państwowych, a następnie na ich podstawie dokonuje aktualizacji danych zawartych w bazie danych systemu SOJST PUMA. Komunikacja pomiędzy systemami odbywa się z wykorzystanie połączenia szyfrowanego za pomocą protokołu https. Dodatkowo komunikacja jest uwierzytelniona przy pomocy indywidualnego certyfikatu Urzędu Miasta Bartoszyce zabezpieczonego hasłem wydanego przez Ministerstwo Spraw Wewnętrznych i Administracji.

System PUMA wykorzystywany w MOPS Bartoszyce nie współpracuje z zewnętrznymi systemami. Jedynym wyjątkiem jest udostępnienie do Urzędu Miasta połączeniem VPN danych księgowych (dane związane z VAT, nr faktury, kwota). Programy SYGNITY (POMOST/ŚWIADCZENIA) dokonują tzw. „zasilenia" służącego do komunikacji OPS-PUP.

Współpraca pomiędzy systemami była możliwa dzięki wyposażeniu w odpowiednie składniki sprzętowe oraz oprogramowanie umożliwiające wymianę danych z innymi systemami telekomunikacyjnymi, za pomocą protokołów komunikacyjnych i szyfrujących. Systemy informatyczne spełniały minimalne wymogi interoperacyjności w zakresie współpracy z innymi systemami Urzędu, jak również systemami innych jednostek administracji publicznej.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 132, 134, 140, 142]

1.5. Obieg dokumentów w podmiocie publicznym

Z § 20 ust. 2 pkt 9 rozporządzenia KRI wynika, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególność 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 Miasta w Bartoszycach zgodnie z § 41 pkt 1 Regulaminu Organizacyjnego wprowadzonego zarządzeniem Nr 19/2019 Burmistrza Miasta Bartoszyce z dnia 1 lutego 2019 r. 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 roku w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. Nr 14, poz. 67). Zgodnie z przyjętym regulaminem korespondencję przyjmuje sekretariat, którego pracownicy uprawnieni są do przyjmowania lub wysyłania przesyłek. Korespondencja rejestrowana jest w elektronicznym dzienniku korespondencji. Kierownicy komórek organizacyjnych po zapoznaniu się z treścią korespondencji wpływającej do komórki, przekazują ja na właściwe merytorycznie stanowisko pracy. W komórkach organizacyjnych obowiązuje system oparty na jednolitym rzeczowym wykazie akt.

Jednocześnie w trakcie kontroli nie przedstawiono kontrolującemu wewnętrznych procedur Urzędu dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby zasady obiegu dokumentów wpływających drogą elektroniczną oraz zakres stosowania elektronicznego obiegu dokumentów (skrzynka podawcza na platformie ePUAP oraz Elektroniczne Biuro Obsługi Interesanta), 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.
W związku z powyższym przedmiotowe cząstkowe zagadnienie w przypadku UM należy ocenić pozytywnie uchybieniami. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki – Burmistrz UM w Bartoszycach.

W przypadku MOPS w Bartoszycach, zgodnie załącznikiem nr 1 do zarządzenia Nr 14/2011 Dyrektora MOPS w Bartoszycach z dnia 19 grudnia 2011 r. w sprawie wprowadzenia normatywów kancelaryjno-archiwalnych w MOPS w Bartoszycach, zmienionego zarządzeniem Nr SO.0120.6.2017 Dyrektora MOPS w Bartoszycach z dnia 13 lipca 2017 r., czynności kancelaryjne w jednostce są wykonywane w sposób tradycyjny, oparty na jednolitym rzeczowym wykazie akt. Załącznik Nr 1 zawiera całą procedurę w zakresie postępowania z dokumentacją prowadzoną w sposób tradycyjny (papierowy) w celu zabezpieczenia informacji przed nieuprawnionym jej ujawnieniem, modyfikacją, usunięciem lub zniszczeniem. W przypadku dokumentacji wpływającej drogą elektroniczną (poczta e-mail lub ESP) procedura postępowania zawarta jest w paragrafach od 9 do 12 załącznika Nr 1 do zarządzenia Nr 14/2011 Dyrektora MOPS. Przedstawione procedury zgodnie z § 20 ust. 2

pkt 9 rozporządzenia KRI, zapobiegają narażeniu dokumentów elektronicznych na utratę autentyczności, integralności oraz poufności informacji w nich zawartych. W przypadku MOPS przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 151-215]

1.6. Formaty danych udostępniane przez systemy teleinformatyczne

Stosownie do:

- § 17 ust. 1 rozporządzenia KRI k*odowanie 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 w wyniku kontroli w UM wynika, że w związku z udostępnieniem przez administratora systemu Źródło funkcji migracji aktów stanu cywilnego z lokalnych baz danych Urzędów Stanu Cywilnego do Systemu Rejestrów Państwowych, Urząd Stanu Cywilnego w Bartoszycach zasila danymi SRP w zakresie BUSC poprzez migrację aktów stanu cywilnego z aplikacji wspierającej o nazwie Komputerowy System Rejestracji Stanu Cywilnego PB_USC. W tym celu firma Technika IT sp. z o.o. świadcząca usługę opieki autorskiej na ww. system dostarczyła aplikację o nazwie Eksport USC, która umożliwia eksport wybranego aktu stanu cywilnego z lokalnej bazy danych do pliku w formacie xml, zgodnego ze schematem ustalonym przez administratora systemu Źródło i kodowanego w standardzie unicode UTF-8.

W przypadku systemów użytkowanych w MOPS, to oprogramowanie do obsługi świadczeń oraz POMOST Std komunikują się z wieloma centralnymi systemami (np. ZUS, CBB, MF, baza PESEL) za pośrednictwem CSIZS Empatia. Ponadto istnieje także komunikacja z SEPI,

obsługiwanym przez Powiatowe Urzędy Pracy oraz komunikacja z Biurami Informacji Gospodarczej. Dane przesyłane, jak i importowane są w formacie XML. Standard kodowania znaków to unicode UTF-8.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 132, 135, 140, 142]

II. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych

2.1. Dokumenty z zakresu bezpieczeństwa informacji

Zgodnie z:

- § 20 ust. 1 rozporządzenia KRI p*odmiot 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 z*arządzanie 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 z*arządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.*

Podmiot publiczny 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. Wymaga to 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 możliwości 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.

- Zarządzeniem Nr 243/2015 Burmistrza Miasta Bartoszyce z dnia 4 grudnia 2015 r. wprowadzono Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta w Bartoszycach, stanowiącą załącznik nr 1 oraz Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta w Bartoszycach, stanowiącą załącznik nr 2 do zarządzenia.

[akta kontroli str. 220-245]

Stwierdzono, że obowiązująca w dniu rozpoczęcia czynności kontrolnych w UM w Bartoszycach Polityka Bezpieczeństwa przetwarzania danych osobowych mająca służyć zapewnieniu poufności, integralności rozliczalności przetwarzanych w Urzędzie danych, opracowana została na podstawie nieobowiązujących w dniu kontroli przepisów prawa, tj. ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. 2014, poz. 1182 ze zm.) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 roku, w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).
Powyższe stanowi nieprawidłowość. Przyczyną stwierdzonej nieprawidłowości jest niestosowanie obowiązujących przepisów prawa w zakresie systemu zarządzania bezpieczeństwem informacji. Skutkiem stwierdzonej nieprawidłowości jest brak wymaganej aktualizacji Polityki zgodnie z § 20 ust. 1 i ust. 2 pkt 1 rozporządzenia KRI, jak również art. 24 ust. 1 i 2 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) – RODO.

– Zarządzeniem Nr 132/2018 Burmistrza Miasta Bartoszyce z dnia 30 sierpnia 2018 r. w sprawie wyznaczenia Inspektora ochrony danych i Administratora Systemu Informatycznego, ustanowiono osoby do pełnienia obowiązków IOD oraz ASI, w Urzędzie Miasta w Bartoszycach.

[akta kontroli str. 246-247]

W toku prowadzonej kontroli stwierdzono, iż Zarządzeniem Nr 174/2018 Burmistrza Miasta Bartoszyce z dnia 20 listopada 2018 r. w sprawie odwołania Inspektora Ochrony Danych, odwołano osobę pełniącą do tej pory funkcję IOD w UM Bartoszyce. W okresie od dnia 20 listopada 2018 r. do dnia zakończenia czynności kontrolnych (27 lutego 2018 r.), w kontrolowanej jednostce brak było osoby wyznaczonej do pełnienia funkcji IOD.

[akta kontroli str. 248]

Zgodnie z art. 37 ust. 1 RODO, administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy:
a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
b) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele

wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę;

c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

Niewyznaczenie nowego IOD w jednostce stanowi uchybienie skutkujące: brakiem możliwości informowania administratora oraz pracowników jednostki, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów prawa o ochronie danych osobowych, brakiem monitorowania przestrzegania obowiązujących przepisów prawa o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych.

Jednocześnie należy nadmienić, iż funkcję IOD można powierzyć zarówno pracownikowi administratora (lub podmiotu przetwarzającego), jak i podmiotowi trzeciemu na podstawie umowy o świadczenie usług.

Mając na uwadze powyższe ustalenia, przedmiotowe cząstkowe zagadnienie w przypadku UM w Bartoszycach ocenia się pozytywnie z nieprawidłowościami. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki – Burmistrz UM w Bartoszycach.

– Zarządzeniem Nr SO.0120.4.2018 Dyrektora Miejskiego Ośrodka Pomocy Społecznej w Bartoszycach z dnia 2 maja 2018 r. przyjęto dokument stanowiący Politykę Bezpieczeństwa Danych Osobowych w jednostce. W skład dokumentu wchodzą Instrukcja ochrony danych osobowych, Instrukcja zarzadzania systemami informatycznymi służącymi do przetwarzania danych osobowych oraz Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych. Politykę Bezpieczeństwa Danych Osobowych sporządzono na podstawie obowiązujących przepisów, tj. RODO.

Przedmiotowy dokument zawiera również informacje o wyznaczeniu Inspektora Ochrony Danych Osobowych oraz Administratora Systemu Informatycznego. Dokumentacja w zakresie bezpieczeństwa informacji dotyczyła danych przetwarzanych w MOPS i służyła zapewnieniu poufności, integralności przetwarzania danych, jak również monitorowania zdarzeń naruszających ochronę danych osobowych, zawierała także opis postępowania w przypadku naruszenia zasad bezpieczeństwa danych.

[akta kontroli str. 249-277]

W przypadku MOPS w Bartoszycach 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 Zarządzeniem Nr 190/2017 Burmistrza Miasta Bartoszyce z dnia 28.11.2017 r. w sprawie zasad funkcjonowania kontroli zarządczej w Urzędzie Miasta Bartoszyce, raz w roku opracowywany jest roczny rejestr ryzyk Urzędu jako dokument zbiorczy wytworzony na podstawie wydziałowych rejestrów ryzyk, stanowiący podstawę zarzadzania ryzykiem w Urzędzie. Postępowanie przy identyfikowaniu i analizie ryzyka polegało na wykonaniu następujących czynności:
- ustaleniu listy celów / zadań do realizacji w każdej komórce Urzędu,
- określeniu ryzyk do każdego istotnego zadania określonego dla komórki organizacyjnej,
- określeniu przyczyn i skutków zidentyfikowanego ryzyka wg. określonej skali,
- dokonaniu punktowej oceny zidentyfikowanego ryzyka,
- określeniu występujących mechanizmów kontrolnych dla zidentyfikowanych ryzyk,
- określeniu koniecznych do wprowadzenia mechanizmów kontrolnych w celu zminimalizowania zidentyfikowanych ryzyk.

W przypadku MOPS w Bartoszycach zgodnie z Zarządzeniem Nr SO.0120.4.2018 Dyrektora Miejskiego Ośrodka Pomocy Społecznej w Bartoszycach z dnia 2 maja 2018 r. w sprawie przyjęcia Polityki Bezpieczeństwa Danych Osobowych (§8), IOD sporządza arkusz identyfikacji, oceny oraz określenia metod przeciwdziałania ryzyku w zakresie bezpieczeństwa danych osobowych przetwarzanych w MOPS w Bartoszycach. Zgodnie z przekazaną dokumentacją z kontroli przedmiotowy arkusz oceny został wykonany. Zgodnie z procedurą zarządzania ryzykiem w MOPS Bartoszyce (zał. 5) sporządzone zostało zbiorcze zestawienie ryzyk i działań podejmowanych w MOPS w 2018 i 2019 roku obejmujące również swym zakresem działanie systemów teleinformatycznych wykorzystywanych w MOPS. Na podstawie zidentyfikowanych ryzyk każdy z działów MOPS przeprowadził w 2018 r. ocenę zidentyfikowanych ryzyk.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 249-304, 305-334]

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.*

Z wyjaśnienia Zastępcy Burmistrza Miasta Bartoszyce wynika, że: *„Za inwentaryzację sprzętu i oprogramowania odpowiada Referat ds. Informatyzacji Urzędu. W tym celu zostało zakupione i wdrożone oprogramowanie wspierające Total Network Inventory (TNI). Ww. system zawiera kompletny wykaz sprzętu teleinformatycznego wykorzystywanego w Urzędzie oraz wydzieloną bazę do zarządzania licencjami na zakupione oprogramowanie. System TNI udostępnia dane o sprzęcie i jego konfiguracji zgodnie z §20 ust.2 pkt. 2 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. W tym celu w cyklu dobowym odbywa się skanowanie konfiguracji sprzętowej i zainstalowanego oprogramowania na stacjach roboczych Urzędu. W oparciu o gromadzone dane system umożliwia generowanie dowolnych raportów dotyczących konfiguracji sprzętowej, zainstalowanego oprogramowania, osób odpowiedzialnych za sprzęt, itp. Inwentaryzacja sprzętu i oprogramowania z wykorzystanie systemu TNI w zakresie konfiguracji realizowana jest automatycznie i aktualizowana w cyklu dobowym, natomiast pozostałe zmiany dotyczące np. lokalizacji, osoby odpowiedzialnej za sprzęt wprowadzone są do systemu przez pracowników Referatu ds. Informatyzacji Urzędu.”*

Z wyjaśnienia Dyrektora MOPS w Bartoszycach wynika, że: *„Miejski Ośrodek Pomocy Społecznej w Bartoszycach w ramach zarządzania infrastrukturą informatyczną prowadzi ewidencję sprzętu komputerowego. Każdorazowo, przy zakupie lub likwidacji sprzętu, jest ona aktualizowana. Z kolei, inwentaryzacja sprzętu komputerowego jest przeprowadzana zgodnie z Zarządzeniem nr SO.0120.27.6.2017 Dyrektora MOPS w Bartoszycach z dnia 29 grudnia 2017 roku w sprawie: wprowadzenia Instrukcji Inwentaryzacyjnej w Miejskim Ośrodku Pomocy Społecznej w Bartoszycach - kopia w załączeniu - Zał. nr 1. Inwentaryzacja dokonywana jest raz w ciągu 4 lat zgodnie z w/w instrukcją.”*

Kontrolującemu przedstawiono aktualną inwentaryzację oprogramowania oraz sprzętu komputerowego. Inwentaryzacja sporządzona została zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI. Przedmiotowa inwentaryzacja obejmowała rodzaj i konfigurację sprzętu oraz dodatkowo informację dotyczącą użytkownika i miejsce użytkowania (MOPS).
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 136, 142-143, 335-344]

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Stosownie do:

- § 20 ust. 2 pkt 4 rozporządzenia KRI z*arządzanie 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 bezpieczeństwa informacji (BI) 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 zmiany i cofania upoważnień do przetwarzania danych osobowych oraz prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych w Urzędzie Miasta w Bartoszycach określone są w obowiązującej na dzień kontroli przyjętej Zarządzeniem Nr 243/2015 Burmistrza Miasta Bartoszyce z dnia 4 grudnia 2015 r. Polityce bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta. W Urzędzie prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych wg. załącznika nr 7 do Zarządzenia wprowadzającego Politykę bezpieczeństwa przetwarzania danych osobowych. Każdy z pracowników, który pracował w systemach teleinformatycznych posiadał stosowne upoważnienie do przetwarzania danych osobowych, jak również w zależności od użytkowanego systemu teleinformatycznego, stosowne pisemne upoważnienie do danego systemu teleinformatycznego.
W związku z faktem, że zasady nadawania, zmiany i cofania upoważnień do przetwarzania danych osobowych oraz prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych w Urzędzie Miasta w Bartoszycach określone zostały w Polityce bezpieczeństwa przetwarzania danych osobowych opracowanej na podstawie nieobowiązujących w dniu kontroli przepisów prawa (o czym szczegółowo w pkt II. 2.1), przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki – Burmistrz UM w Bartoszycach.

Zasady nadawania zmiany i cofania upoważnień do przetwarzania danych osobowych oraz prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych w MOPS w Bartoszycach określone zostały w Polityce Bezpieczeństwa Danych Osobowych przyjętej Zarządzeniem z dnia 2 maja 2018 r. Nr SO.0120.4.2018 Dyrektora Miejskiego Ośrodka Pomocy Społecznej w Bartoszycach.
W MOPS w Bartoszycach zgodnie z załącznikiem 11 do Polityki Bezpieczeństwa Danych Osobowych prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych, ponadto każdy z pracowników, który pracował w systemie teleinformatycznym posiadał stosowne upoważnienie do przetwarzania danych osobowych, jak również upoważnienie do danego systemu teleinformatycznego.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie w MOPS ocenia się pozytywnie.

[akta kontroli str. 345-349, 350-360]

2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Z § 20 ust. 2 pkt 6 rozporządzenia KRI wynika, że z*arządzanie 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 wyjaśnienia Zastępcy Burmistrza Miasta Bartoszyce w zakresie szkoleń pracowników zaangażowanych w proces przetwarzania informacji wynika, że: „*W 2018 roku miało miejsce szkolenie prowadzone przez pracownika ABW zatytułowane (dość myląco) „Postępowanie w przypadku zagrożenia terrorystycznego". W treści szkolenia były zawarte informacje dot. bezpieczeństwa informacji m.in. fakt, iż cenne mogą być różne dane, którymi pracownicy dysponują, nawet te, które z pozoru wydają się nie chronione i mało znaczące. Bardzo ciekawe spotkanie zmieniające spojrzenie na informacje do jakich mają dostęp pracownicy i jakie mogą np. w trakcie prywatnych spotkań niekoniecznie świadomie przekazywać – szkolenie zwiększało świadomość istniejących zagrożeń."*
Ponadto w 2014 roku pracownicy UM uczestniczący w procesie przetwarzania danych brali udział w szkoleniu organizowanym przez zewnętrzną firmę, w zakresie zdobycia wiedzy i umiejętności dotyczących ochrony danych osobowych.

W badanym okresie pracownicy MOPS w Bartoszycach zaangażowani w proces przetwarzania informacji brali udział w szkoleniach w przedmiotowej tematyce. Zakres odbytych szkoleń obejmował obszary dotyczące podstawowych zasad przetwarzania danych osobowych, prawidłowego gromadzenia i przetwarzania danych osobowych, obowiązków pracownika, w zakresie zasad bezpiecznego przetwarzania danych, zastosowania środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych, postępowania w przypadku naruszenia bezpieczeństwa informacji oraz zgłaszania naruszeń bezpieczeństwa informacji. Ponadto pracownik pełniący funkcję IOD oraz ASI w MOPS w Bartoszycach przeprowadził 5 szkoleń dla pracowników MOPS w zakresie zapoznania z dokumentacją stanowiącą Politykę Bezpieczeństwa Danych Osobowych w jednostce, w skład której weszły Instrukcja ochrony danych osobowych, Instrukcja zarzadzania systemami informatycznymi służącymi do przetwarzania danych osobowych oraz Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych. Z każdego szkolenia sporządzona została notatka oraz lista obecności. Informatyk MOPS przeprowadził również 5 szkoleń pracowników w zakresie bezpiecznego korzystania z poczty e-mail, zabezpieczenia skrzynki tzw. „silnymi" hasłami, szyfrowania wiadomości oraz bezpiecznego kończenia pracy w systemie.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 361-397, 398-411]

2.6. Praca na odległość i mobilne przetwarzanie danych

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

Z wyjaśnienia Zastępcy Burmistrza Miasta Bartoszyce w powyższym zakresie wynika, że: „*Praca na odległość jest możliwa w przypadku pracowników wyposażonych w komputery przenośne (notebook). Pracę na odległość w Urzędzie Miasta Bartoszyce dzielimy na:*

a) pracę z wykorzystaniem jedynie zasobów dostępnych na komputerze mobilnym,
b) pracę zdalną na zasobach dostępnych na serwerach Urzędu (wyłącznie pracownicy Referatu ds. Informatyzacji Urzędu).

Komputery wykorzystywane do pracy na odległość, poza objęciem ich standardowymi politykami bezpieczeństwa Urzędu, zabezpieczone są dodatkowo poprzez:

a) zabezpieczenie dostępu do dysku twardego hasłem,
b) komunikację z sieci zewnętrznej z serwerem systemu zabezpieczającego Urzędu (antywirus, firewall, itp.), co pozwala otrzymywać na bieżąco powiadomienia o zidentyfikowanych zagrożeniach oraz przesyłanie zaktualizowanych polityk zabezpieczeń,
c) realizowanie pracy zdalnej na zasobach Urzędu z wykorzystanie bezpiecznego, szyfrowanego połączenia VPN.

Systemy teleinformatyczne używane do realizacji zadań publicznych nie są obsługiwane z wykorzystaniem komputerów umożliwiających pracę na odległość."

Z wyjaśnienia Dyrektora MOPS w Bartoszycach wynika, że: *Przetwarzanie informacji na odległość przez pracowników MOPS nie ma miejsca. Jedynie prace serwisowe, prowadzone przez dostawców oprogramowania dzięki narzędziu o nazwie ZetoPomoc, wykorzystują połączenie zdalne (program TeamViewer) za pomocą jednorazowego loginu i hasła tylko w celach serwisowych. Osoba korzystająca z pozwolenia na użytkowanie komputera przenośnego poza siedzibę Ośrodka, zgodnie z zapisem w Polityce Bezpieczeństwa Danych Osobowych MOPS, bierze na siebie odpowiedzialność za bezpieczeństwo informacji przetwarzanych na odległość.*

Zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość zostały ustanowione w Instrukcji zarzadzania systemami informatycznymi, stanowiącej załącznik do Polityki Bezpieczeństwa Danych Osobowych w MOPS w Bartoszycach.

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

[akta kontroli str. 136, 143, 260, 262, 264]

2.7. Serwis sprzętu informatycznego i oprogramowania

Stosownie do § 20 ust. 2 pkt 10 rozporządzenia KRI z*arządzanie 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 Miasta oraz MOPS w Bartoszycach użytkowane są 4 systemy teleinformatyczne do realizacji zadań publicznych zakupione u zewnętrznego dostawcy, tj.: SOJST Puma (UM i MOPS), PB_USC oraz SYGNITY.
W związku z zakupem ww. systemów podpisane zostały umowy licencyjne z firmami: Technika IT Sp. z o.o., ZETO SOFTWARE Sp. z o.o. oraz SYGNITY S.A. Wraz z umowami licencyjnymi (asysta techniczna) z każdą firmą dostarczającą dany system informatyczny podpisana została właściwa umowa powierzenia danych, gwarantująca poprzez zawarcie określonych zapisów właściwe zabezpieczenie danych w przypadku awarii systemu oraz gwarantująca bezpieczeństwo informacji uzyskanych przez wykonawców w związku z realizacją umowy.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 412-457]

2.8. Procedury zgłaszania incydentów naruszenia BI

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

Sposób zgłaszania incydentów naruszenia bezpieczeństwa informacji w przypadku Urzędu Miasta w Bartoszycach został uregulowany Zarządzeniem Nr 243/2015 Burmistrza Miasta Bartoszyce z dnia 4 grudnia 2015 r. wprowadzającym Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie, oraz Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
W związku z faktem, że sposób zgłaszania incydentów naruszenia bezpieczeństwa informacji w przypadku Urzędu Miasta w Bartoszycach określony zostały w Polityce bezpieczeństwa przetwarzania danych osobowych opracowanej na podstawie nieobowiązujących w dniu kontroli przepisów prawa, przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki – Burmistrz UM w Bartoszycach.

Sposób zgłaszania incydentów naruszenia bezpieczeństwa informacji w przypadku MOPS w Bartoszycach został uregulowany Zarządzeniem Nr SO.0120.4.2018 Dyrektora Miejskiego Ośrodka Pomocy Społecznej w Bartoszycach z dnia 2 maja 2018 r. którym przyjęto Politykę Bezpieczeństwa Danych Osobowych w jednostce. W skład dokumentu weszły również Instrukcja ochrony danych osobowych, Instrukcja zarzadzania systemami informatycznymi służącymi do przetwarzania danych osobowych oraz Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych.

W badanym okresie nie stwierdzono incydentów naruszenia BI. Przedmiotowe cząstkowe zagadnienie w przypadku MOPS ocenia się pozytywnie.

[akta kontroli str. 244-245, 265-266]

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

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

Z wyjaśnienia Zastępcy Burmistrza Miasta Bartoszyce w powyższym zakresie wynika, że: *W Urzędzie Miasta Bartoszyce prowadzony jest audyt wewnętrzny. Audyty wewnętrzne poszczególnych elementów całego systemu zarządzania bezpieczeństwem informacji są planowane co roku. Element systemu jaki jest audytowany wynika każdorazowo z analizy ryzyka wykonywanej na etapie początkowym zadania. Wynika to m.in. z faktu, iż audytor dysponuje ograniczonym budżetem czasowym i skupia się na największych ryzykach obszaru wynikających z analizy. Audyt wewnętrzny o szerokim zakresie – m.in. ocena organizacji całego systemu bezpieczeństwa informacji przeprowadzony był w 2014 roku (zadanie 4/2013). W następnych latach były monitorowania i czynności sprawdzające oraz zadania zapewniające obszarów największego ryzyka z tego zakresu.*

Z dokumentacji audytowej udostępnionej kontrolującemu wynika, że na przełomie 2017/2018 roku przeprowadzony został audyt wewnętrzny bezpieczeństwa informacji, którego celem było sprawdzenie zapewnienia rozliczalności pracy w wybranych systemach informatycznych. Audyt przeprowadził Audytor wewnętrzny (CGAP) zatrudniony w UM Bartoszyce. W wyniku przeprowadzonych czynności audytowych zalecono:

1) dokonanie okresowego przeglądu ustanowionych pracownikom dostępów i ustalenie dostępu do systemu zgodnie z zastępstwami na stanowiskach,
2) zapewnienie rozliczalności pracy w systemach poprzez dokonywanie czynności w danym systemie tylko i wyłącznie na podstawie własnego loginu i hasła (nie udostępnianie loginów i haseł innym pracownikom),
3) podjęcie starań o dodatkową funkcjonalność szczególnie wrażliwych modułów systemu PUMA i zapewnienie rozliczalności pracy obsługujących go pracowników.

[akta kontroli str. 469-474]

W dniu 24 października 2018 r. (po upływie wskazanych terminów realizacji zaleceń) audytor wewnętrzny przeprowadził czynności sprawdzające w zakresie wykonania zaleceń. Czynności sprawdzające miały na celu, czy i w jakim stopniu kierownik komórki audytowanej podjął kroki zmierzające do wprowadzenia w życie zaleceń wynikających z przeprowadzonego zadania audytowego. W wyniku zastosowanych technik audytorskich, Audytor wewnętrzny stwierdził, że zrealizowane zostały zalecenia nr 2-3, natomiast zalecenie nr 1 nie zostało zrealizowane (trwały prace nad jego realizacją polegające na aktualizacji Polityki bezpieczeństwa Informacji oraz Instrukcji zarzadzania systemem informatycznym).

[akta kontroli str. 475-476]

Jednocześnie należy nadmienić, że w Planie audytu wewnętrznego Gminy Miejskiej Bartoszyce na rok 2019 zawarte zostało zadanie audytowe w zakresie bezpieczeństwa informacji – jako zadanie zapewniające.

[akta kontroli str. 486-493]

Przedmiotowe cząstkowe zagadnienie w przypadku UM Bartoszyce ocenia się pozytywnie.

W przypadku MOPS w Bartoszycach, z wyjaśnień Dyrektora wynika, że nie przeprowadzono w okresie objętym kontrolą audytów w zakresie bezpieczeństwa informacji w systemach informatycznych (§ 20 ust. 2 pkt 14 rozporządzenia KRI). Zgodnie natomiast z okazaną dokumentacją jednostka w okresie objętym kontrolą przeprowadziła sprawdzenie (wewnętrzne) w zakresie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. W ramach dokonanego sprawdzenia wewnętrznego przeprowadzono oględziny pomieszczeń biurowych, ocenę kontroli dostępu do pomieszczeń oraz stanowisk, w których przetwarzane są dane osobowe, legalność przetwarzania danych i realizację obowiązku informacyjnego. Łącznie kontroli poddano 46 stanowisk komputerowych. Z przeprowadzonego sprawdzenia sporządzane było sprawozdanie, które obejmowało przedmiot i zakres sprawdzenia, opis stanu faktycznego stwierdzonego w toku dokonywanych czynności, ewentualne przypadki naruszenia przepisów o ochronie danych osobowych wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem. W wyniku przeprowadzonego sprawdzenia stwierdzono: uchybienie w zakresie umiejscowienia monitora komputerowego umożliwiające wgląd osobom nieuprawnionym, brak aktualizacji oprogramowania antywirusowego na 7 stanowiskach, w 10 przypadkach nie została zastosowana zasada złożoności hasła dostępowego. Wszystkie uchybienia zostały skorygowane.

[akta kontroli str. 528-531]

Zgodnie z przyjętym programem kontroli, nieprzeprowadzenie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji zgodnie z § 20 ust. 2 pkt 14

rozporządzenia KRI, stanowi nieprawidłowość. Jednakże, ze względu na przeprowadzenie w MOPS sprawdzenia wewnętrznego w zakresie bezpieczeństwa informacji będącego narzędziem nadzoru nad BI, brak przeprowadzonego audytu uznaje się za uchybienie.
Skutkiem było naruszenie § 20 ust. 2 pkt 14 rozporządzenia KRI. Intencją ustawodawcy było zobowiązanie podmiotów realizujących zadania publiczne do realizowania okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, bez szczegółowego wskazywania na rodzaj audytu oraz tryb jego przeprowadzania. Osobą odpowiedzialną jest Dyrektor MOPS. Przedmiotowe cząstkowe zagadnienie w przypadku MOPS ocenia się pozytywnie z uchybieniami.

2.10. Kopie zapasowe

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

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

Z wyjaśnienia Zastępcy Burmistrza Miasta Bartoszyce w powyższym zakresie wynika, że w celu zapewnienia ciągłości działania systemów teleinformatycznych Urzędu stosuje się następujące środki i metody:

a) jednostka posiada dwa pomieszczenia serwerowni, podstawowe zlokalizowane na parterze oraz zapasowe na II piętrze budynku Urzędu,
b) jednostka posiada w zapasowej serwerowni redundantną infrastrukturę serwerową w postaci serwera współpracującego z macierzą dyskową oraz dodatkowej, wydzielonej macierzy dyskowej przechowującej kopie zapasowe,
c) w celu zminimalizowania ryzyka przerw w pracy najważniejszych systemów Urzędu wdrożono rozwiązanie programowe w postaci wirtualnej infrastruktury serwerowej pozwalające, w przypadku wystąpienia awarii jednego z elementów infrastruktury (fizycznego serwera lub macierzy dyskowej), w krótkim czasie uruchomić systemy na pozostałych dostępnych zasobach,
d) infrastruktura sprzętowa, w ramach umów gwarancyjnych, serwisowych, objęta jest wsparciem producenta lub innego podmiotu realizującego usługi serwisowe,
e) w cyklu dobowym wykonywane są kopie zapasowe konfiguracji serwerów, systemu zarządzającego wirtualną infrastrukturą serwerową VMware vCenter Server,

f) każdorazowo w przypadku zmiany konfiguracji wykonywana jest kopia zapasowa konfiguracji urządzeń wchodzących w skład infrastruktury sieciowej: przełączniki sieciowe, router,
g) w cyklu dobowym wykonywane są kopie zapasowe maszyn wirtualnych serwerów bazodanowych i aplikacyjnych. Kopie zapasowe wykonywane są przy pomocy systemu Veeam Backup & Replication. Kopie zapasowe przechowywane są na macierzy dyskowej zlokalizowanej w pomieszczeniu zapasowej serwerowni Urzędu,.

Ponadto w UM wykonywane są kopie zapasowe baz danych systemów informatycznych Urzędu wg. poniższej procedury:

a) kopie wykonywane są automatycznie, w wyznaczonych porach, przy użyciu systemu Bacula oraz skryptów powłoki systemu,
b) kopie zapasowe wykonywane przez system Bacula przechowywane są na wydzielonej partycji zapasowego serwera ww. systemu oraz na przeznaczonej do tego celu macierzy dyskowej (urządzenia zlokalizowane w pomieszczeniu zapasowej serwerowni Urzędu),
c) kopie zapasowe wykonywane przez system Bacula wykonywane są w cyklu dobowym i przechowywane są przez okres 30 dni,
d) kopie zapasowe wykonywane w cyklu miesięcznym wykonywane są przy użyciu skryptów powłoki systemu wykonywanych z poziomu poszczególnych serwerów, (przechowywane są przez okres co najmniej 2 lat),
e) z uwagi na wartość danych zawartych w bazie danych systemu SOJST PUMA, codziennie o godzinie 9:00, 13:00, 17:00, 20:00 wykonywana jest dodatkowa kopia zapasowa systemu pozwalająca, w przypadku wystąpienia awarii, na odtworzenie możliwie najnowszej wersji bazy danych.

Procedura tworzenia kopii zapasowych określona została w rozdziale nr 7 Instrukcji zarzadzania systemem informatycznym służącym do przetwarzania danych osobowych, będącej załącznikiem do Polityki bezpieczeństwa przetwarzania danych osobowych.

Procedura tworzenia kopii zapasowych w MOPS Bartoszyce określona została w Instrukcji zarzadzania systemami informatycznymi służącymi do przetwarzania danych osobowych będącej załącznikiem do Polityki Bezpieczeństwa Danych Osobowych w jednostce przyjętej Zarządzeniem Nr SO.0120.4.2018 Dyrektora Miejskiego Ośrodka Pomocy Społecznej w Bartoszycach z dnia 2 maja 2018 r. Systemy teleinformatyczne w MOPS działają całą dobę, z małymi przerwami serwisowymi (aktualizacja oprogramowania, konserwacja sprzętu). Kopie tworzone są w cyklu dobowym - każdy z systemów o różnych godzinach, poza godzinami pracy MOPS. Przechowywane są w siedzibie Ośrodka. Kopia bazy systemu tworzona jest na serwerze, dodatkowo na nośniku danych zewnętrznych (przenośny Hdd) oraz na komputerze w pomieszczeniu kasowym MOPS (pomieszczenie zamknięte i okratowane). Kopie bazy danych przetrzymywane są 30 dni.

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 137, 143, 242, 262]

2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

Stosownie do § 15 ust. 1 rozporządzenia KRI s*ystemy 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.*

W okresie objętym kontrolą nie zidentyfikowano w Urzędzie Miasta oraz MOPS w Bartoszycach systemów będących na etapie projektowania oraz wdrażania, w związku z czym przedmiotowe cząstkowe zagadnienie nie podlegało ocenie.

[akta kontroli str. 15]

2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji

Z § 20 ust. 2 rozporządzenia KRI wynika, że z*arządzanie 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.

W przypadku UM stwierdzono, iż pracę w systemach wykonuje się z wykorzystaniem kont użytkowników nie posiadających uprawnień administracyjnych. Router brzegowy ze zintegrowanym urządzeniem UTM posiada wbudowaną zaporę ogniową (tzw. firewall) do filtrowania przepływu informacji pomiędzy siecią lokalną Urzędu a siecią Internet. Na każdej stacji roboczej oraz serwerach zainstalowane jest oprogramowanie antywirusowe pracujące w tle, którego baza wirusów aktualizowana jest automatycznie w cyklu dobowym, a użytkownik nie ma możliwości wyłączenia ochrony antywirusowej. Serwer, macierze dyskowe, urządzenia wchodzące w skład infrastruktury sieci komputerowej Urzędu oraz stacje robocze, gdzie odbywa się przetwarzanie danych wyposażone są w zasilacze awaryjne

(tzw. UPS) na wypadek zaniku napięcia lub awarii sieci zasilającej. Sieć lokalna Urzędu podłączona jest do sieci Internet za pomocą router zintegrowanego z urządzeniem typu UTM Fortigate 200B, urządzenie to zabezpiecza infrastrukturę Urzędu poprzez filtrowanie/kontrolę ruchu pomiędzy siecią lokalną a siecią Internet. Uwierzytelnienie w systemie operacyjnym komputera oraz scentralizowanej usłudze kontrolera domeny w celu uzyskania dostęp do danych osobowych, wymaga podania identyfikatora użytkownika oraz hasła. Każda aplikacja, w której przetwarzane są dane osobowe zabezpieczona jest hasłem oraz loginem autoryzującym do niej dostęp.

W przypadku MOPS stanowiska komputerowe oraz serwerowe zabezpieczone są programem antywirusowym firmy ESET z konsolą zarządzającą. W programie antywirusowym zastosowana jest funkcja blokady dostępu do potencjalnie niebezpiecznych stron internetowych. Logowanie pracownika do systemu przebiega dwuetapowo. Pierwszy etap to logowanie za pomocą loginu i hasła do komputera. Hasło to zmieniane jest raz na 30 dni i powinno składać się min. z 8 znaków oraz małych, dużych liter oraz cyfr. W celu dalszej pracy przy stanowisku komputerowym, aby uruchomić system komputerowy również należy podać login oraz wymagane hasło. Każdemu użytkownikowi nadane zostało odrębne konto. W systemie ustawiony jest wysoki poziom hasła - min. 8 znaków. Hasło składa się z trzech grup znaków, zmiana hasła następuje co 30 dni. Liczba błędnych logowań – 3 (później następuje blokada konta). Po upływie 15 min. bezczynności systemu, stacja robocza ulega samoczynnej blokadzie , aby kontynuować prace w systemie użytkownik musi uwierzytelnić się do systemu poprzez podanie hasła.

[akta kontroli str. 16-17, 138, 143-144, 494-495]

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 stosowane mechanizmy jakie jednostki kontrolowane zastosowały w celu zapewnienia ochrony przetwarzanych informacji, w ramach badanych systemów teleinformatycznych przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. Odbywa się to również poprzez działania związane z zapewnieniem środków uniemożliwiających nieautoryzowany dostęp oraz kontrolę dostępu do systemów teleinformatycznych służących do realizacji zadań zleconych z zakresu administracji rządowej. W systemach: PUMA, SYGNITY, CEIDG, PB_USC logowanie odbywa się za pomocą przyznanego loginu i hasła, które wymaga okresowej wymiany. W systemie Źródło logowanie odbywa się poprzez imienną kartę dostępową i indywidualne hasło dostępowe.

Oprócz zabezpieczeń systemów teleinformatycznych wykazanych w punkcie 2.12, zarówno UM jak i MOPS w Bartoszycach stosują fizyczne zabezpieczenia na wypadek próby dostępu do danych przetwarzanych przez systemy.
Urząd Miasta zapewnia fizyczne bezpieczeństwo przetwarzanych informacji, m.in. poprzez:
- dostęp do budynku oraz pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych chroniony jest poprzez podłączenie lokalnego systemu alarmowego w obiekcie do centrum operacyjnego firmy GROM S.C. Biuro Ochrony Mienia i Osób, z którą Urząd posiada podpisaną umowę o ochronę,
- zaopatrzenie pomieszczenia obszaru, w którym przetwarzane są dane osobowe w drzwi zamykane na zamek,
- zabezpieczenie wejścia pomieszczenia, w którym znajdują się serwery baz danych i aplikacji zlokalizowanych w serwerowni Urzędu na parterze, drzwiami antywłamaniowymi zaopatrzonymi w dwa zamki,

MOPS zapewnia fizyczne bezpieczeństwo przetwarzanych informacji, m.in. poprzez:
- zainstalowanie zabezpieczenia alarmowego -– podpisano stosowne umowy na obsługę systemu alarmowego i jego konserwację,
- zamykanie na klucz pokoi, w których przetwarzane są informacje, każdorazowo przy opuszczeniu przez pracownika stanowiska pracy,
- kontrolę dysponowania kluczami do pomieszczeń.

Bezpieczeństwo działania systemów teleinformatycznych realizowane jest również poprzez okresową aktualizację oprogramowania w zakresie działania poszczególnych systemów do najnowszych wersji.

Podczas kontroli dokonano także oględzin pomieszczenia serwerowni Urzędu Miasta i MOPS w Bartoszycach. W wyniku oględzin stwierdzono, że pomieszczenie serwerowni UM posiada zainstalowane urządzenie klimatyzujące oraz urządzenia monitorujące parametry środowiskowe (temperatura i wilgotność). Przed wejściem do pomieszczenia zainstalowano

wyłącznik główny odcinający zasilanie serwerowni poprzez wyłączenie zasilacza awaryjnego UPS. Drzwi wejściowe zabezpieczone zostały płaszczem stalowym oraz zamkiem konwencjonalnym i szyfrowym z pulpitem numerycznym. Podłoga serwerowni w celu zabezpieczenia przez zalaniem została podwyższona.

W przypadku MOPS w pomieszczeniu serwerowni znajduje się czujka alarmowa (reagująca na ruch wewnątrz). Pomieszczenie pełniące role serwerowni ze względu na ograniczona ilość pomieszczeń w budynku jest jednocześnie pokojem pracy informatyka MOPS. W pomieszczeniu zainstalowano urządzenie klimatyzujące, jak również sprzęt gaśniczy przeznaczony go gaszenia urządzeń pod napięciem. Główny budynek urzędu posiada monitoring oraz zabezpieczenie alarmowe.
Powyższe potwierdza dokumentacja z przeprowadzonych oględzin. Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 497-504, 505-523]

2.14. Rozliczalność działań w systemach informatycznych

Stosownie do:

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

Z informacji przekazanych przez Zastępcę Burmistrza Miasta Bartoszyce wynika, że w systemach teleinformatycznych stanowiących własność Urzędu Miasta Bartoszyce, używanych do realizacji zadań publicznych gromadzone są dane w postaci logów pracy poszczególnych użytkowników systemu. Dane te umożliwiają dokładną weryfikację wykonanych operacji na bazie danych. Dzienniki logów tych systemów przechowywane są przez okres co najmniej 36 miesięcy. W systemach teleinformatycznych używanych do realizacji zadań publicznych w zakresie obsługi Systemu Rejestrów Państwowych lokalny administrator systemu posiada możliwość zamówienia raportu z pracy wybranego użytkownika w zadanym okresie czasu.

Z informacji przekazanych przez Dyrektora MOPS wynika, że w przypadku systemów teleinformatycznych użytkowanych w MOPS, każdy z nich zapewnia rozliczalność wykonywanych w nim działań. Dane te są gromadzone w bazie połączonej z danym systemem. Dzięki temu wiadomo, kto i kiedy się do systemu logował, wiadomo o próbach ewentualnego nieautoryzowanego logowania do systemu, czy innych działaniach związanych z pracą w systemie (np. kto jaką zatwierdził decyzję, itp.). W systemie PUMA logi przetrzymywane są od lipca 2018r. Zawierają listę udanych/nieudanych dostępów do systemu, a także posiada możliwość odfiltrowania konkretnych modyfikacji przez konkretnego użytkownika. System ŚWIADCZENIA, pierwsze zapisy logów przypadają na rok 2005. Rejestrowane są operacje związane z dostępem do systemu oraz operacji wykonywanych przez danego użytkownika w systemie. W przypadku systemu POMOST Pierwsze logi przypadają na czerwiec roku 2018. Analogicznie rejestrowane są wszelkiego rodzaju operacje związane z pracą osób w systemie (np. udane, nieudane logowanie w systemie, blokada konta, wydruki, zatwierdzenia decyzji, itp.).
Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 138, 144-150, 458-468]

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 zarówno w Urzędzie Miasta jak i w MOPS Bartoszyce, ze względu na brak interakcji z klientami zewnętrznymi za pośrednictwem publicznej sieci Internet nie są objęte wymogami WCAG 2.0.

W toku kontroli dokonano weryfikacji zgodności ze standardem WCAG 2.0 strony internetowej Urzędu oraz BIP Urzędu. Zgodnie z załącznikiem nr 4 do rozporządzenia KRI, strona internetowa Urzędu oraz BIP Urzędu spełniały 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.

Strony internetowe BIP UM oraz www Urzędu zawierały elementy umożliwiające zmianę kontrastu oraz wielkości czcionki. Dostosowanie to zostało wykonane z możliwością zmiany kontrastu oraz kilku rozmiarów czcionki, za pomocą ikony (wersja wysokokontrastowa) oraz (A+ A-) umieszczonej w przypadku strony www, w prawym górnym rogu oraz w przypadku strony BIP lewym górnym rogu.
Powyższe zagadnienie w przypadku UM w Bartoszycach oceniono pozytywnie.

W przypadku strony internetowej BIP MOPS w Bartoszycach (zgodnie z załącznikiem nr 4 do rozporządzenia KRI), strona ta spełniała 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.

Strona BIP zawierała ponadto elementy umożliwiające zmianę kontrastu oraz wielkości czcionki. Dostosowanie to zostało wykonane z możliwością zmiany kontrastu oraz kilku rozmiarów czcionki, za pomocą ikony (wersja wysokokontrastowa) oraz (A+ A-) umieszczonej w lewym górnym rogu.
W przypadku strony www MOPS, stwierdzono, że nie zawiera ona elementów umożliwiających zmianę kontrastu oraz wielkości czcionki. Powyższe stanowi uchybienie ograniczające możliwość korzystania z treści zawartych na stronie przez osoby niedowidzące. Osobą odpowiedzialną za powstanie uchybienia jest Dyrektor MOPS.

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny w przypadku UM w Bartoszycach wnoszę o:
1. Opracowanie wewnętrznych procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby zasady obiegu dokumentów wpływających do Urzędu drogą elektroniczną.
2. Opracowanie Polityki Bezpieczeństwa przetwarzania danych osobowych mającej służyć zapewnieniu poufności, dostępności i integralności przetwarzanych w Urzędzie danych, na podstawie obowiązujących przepisów prawa, tj. § 20 ust. 1 i ust. 2 pkt 1 rozporządzenia KRI, jak również art. 24 ust. 1 i 2 RODO.
3. Wyznaczenie Inspektora Ochrony Danych zgodnie z art. 37 ust. 1 RODO.
4. Dokonanie aktualizacji upoważnień pracowników do przetwarzania danych osobowych, jak również w zależności od użytkowanego przez nich systemu teleinformatycznego - do danego systemu teleinformatycznego, na podstawie opracowanej aktualnej Polityki Bezpieczeństwa przetwarzania danych osobowych.

5. Dokonanie aktualizacji zasad zgłaszania incydentów naruszenia bezpieczeństwa informacji, na podstawie opracowanej aktualnej Polityki Bezpieczeństwa przetwarzania danych osobowych.

W przypadku MOPS w Bartoszycach wnoszę o:
1. Zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI.
2. Dostosowanie strony Internetowej jednostki, w celu umożliwienia korzystania z treści na niej zawartych osobom niedowidzącym.

Proszę Pana Burmistrza oraz Panią Dyrektor MOPS 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

Otrzymuje:
Stefania Michalik-Rosa
Dyrektor MOPS
w Bartoszycach.