WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

Olsztyn, 27 czerwca 2019 r.

FK-IV.431.14.2019

Szanowny Pan
Dawid Kopaczewski
Burmistrz Miasta Iławy
ul. Niepodległości 13
14-200 Iława

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 Iławy ul. Niepodległości 13, 14 – 200 Iława, NIP: 744-000-30-93, REGON: 000524370

W okresie objętym kontrolą oraz w okresie prowadzenia kontroli stanowiska pełnili:
1. **Pan Dawid Kopaczewski** - Burmistrz, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 19 listopada 2018 roku (*kierownik jednostki kontrolowanej, nadzorujący bezpośrednio pracownika realizującego zadania objęte kontrolą*),
2. **Pan Arkadiusz Kasiułajtis** - Podinspektor, zatrudniony na podstawie umowy o pracę od dnia 1 maja 2016 roku (*realizujący zadania objęte kontrolą*).

[akta kontroli str. 50]

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 upoważnienia do kontroli nr FK-IV.0030.401.2019 z 30 kwietnia 2019 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 49]

Kontrolę przeprowadzono w dniach 16-17 maja 2019 r., co zostało odnotowane w książce kontroli Urzędu Miasta Iławy pod pozycją Nr 3/2019.

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 16 maja br. (dzień rozpoczęcia czynności kontrolnych).

[akta kontroli str. 1, 30, 49]

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, 30, 49]

W czasie trwania czynności kontrolnych informacji i wyjaśnień udzielał pracownik upoważniony przez Burmistrza Miasta Iławy, tj. Podinspektor Urzędu Miasta Iławy - Informatyk.

[akta kontroli str. 51]

Na podstawie ustaleń kontroli, realizację zadań z zakresu działania systemów teleinformatycznych używanych przez Urząd Miasta Iławy do realizacji zadań zleconych z zakresu administracji rządowej ocenia się **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 Iławy przed rozpoczęciem czynności kontrolnych oraz uzyskanych w trakcie prowadzenia kontroli wynika, że w UM do realizacji zadań zleconych z zakresu administracji rządowej wykorzystywane są **4** systemy teleinformatyczne oraz prowadzony jest **1** rejestr publiczny.

Systemy teleinformatyczne wykorzystywane w Urzędzie Miasta Iławy:

1) **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).

2) **SELWIN -** obsługa z zakresu ewidencji ludności oraz wyborów. SYSTEM EWIDENCJI LUDNOŚCI na platformie systemowej windows (SELWIN) przeznaczony do obsługi procedur administracyjnych związanych z ewidencją ludności wykonywanych w Referatach Ewidencji Ludności podstawowych jednostek podziału administracyjnego kraju. Realizacja funkcji związanych z obsługą procedur administracyjnych jest zgodna z obowiązującą ustawą o ewidencji ludności i dowodach osobistych z dn. 10 kwietnia 1974 r. wraz z późniejszymi zmianami oraz z obowiązującymi wytycznymi MSWiA sformułowanymi w dokumencie „LOKALNY BANK DANYCH PESEL SYSTEM EWIDENCJI LUDNOŚCI" – Wytyczne dla projektanta – programisty. SELWIN dedykowany jest do pracy jedno lub wielostanowiskowej pod kontrolą systemu operacyjnego Windows. Dane ewidencyjne o mieszkańcach w postaci kartotek: stałych mieszkańców, czasowych mieszkańców, byłych mieszkańców oraz kartoteka przejściowa utrzymywane są w relacyjnej bazie danych MS SQL Serwer.

3) **POMOST** - oprogramowanie do obsługi Zespołów Interdyscyplinarnych (ZI) wydane przez Firmę Sygnity S.A z siedzibą w Warszawie, ul. F. Klimczaka 1. Oprogramowanie służy do obsługi niebieskich kart (rodzin dotkniętych przemocą). Dostęp do oprogramowania ma 3 użytkowników obsługujących program i 1 administrator.

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.

Rejestry publiczne prowadzone w Urzędzie Miasta Iławy:

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. 28-29, 53-62]

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 Iławy posiada (strona BIP oraz www Urzędu) aktywną Elektroniczną Skrzynkę Podawczą **/UMILAWA/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, pdf, doc, xls, csv, gif, jpg, zip.

Zgodnie z § 5 ust. 2 pkt 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.

Urząd Miasta Iławy w związku z posiadaniem aktywnej Elektronicznej Skrzynki Podawczej udostępniał oraz świadczył usługi elektroniczne, z wykorzystaniem ePUAP, tj. „Pismo ogólne do podmiotu publicznego" oraz „Skargi, wnioski, zapytania do urzędu". Usługi te umożliwiają złożenie do wybranego organu administracji publicznej pisma (podania) lub skargi w sprawie. W zakresie publikacji procedur spraw realizowanych przez Urząd należy stwierdzić, iż Urząd nie świadczył usług związanych z załatwianiem spraw od początku do końca w formie elektronicznej. Na stronie BIP Urzędu istnieje zakładka „Procedury załatwiania spraw" w której powinny zostać opisane obowiązujące procedury stosowane przez Urząd przy załatwianiu poszczególnych spraw będących w kompetencjach danego wydziału. Kontrolujący stwierdził, że lista opublikowanych w zakładce procedur obejmuje jedynie 2 jednostki tj.: Stanowisko ds. ochrony środowiska oraz Miejski Zespół Obsługi Szkół i Przedszkoli. Opublikowane procedury zawierał dane dotyczące: właściciela usługi

(komórka organizacyjna), podstawy prawnej, wymaganych dokumentów, wysokości opłaty, terminu i sposobu realizacji, trybu odwoławczego oraz dodatkowych informacji. Brak jest publikacji procedur realizacji zadań dotyczących pozostałych wydziałów Urzędu, co stanowi uchybienie. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki. Jednocześnie należy wspomnieć, że w BIP Urzędu podany jest zakres spraw realizowanych przez poszczególne wydział (będących w ich kompetencji).
W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami.

[akta kontroli str. 63-68]

1.2. Centralne repozytorium wzorów dokumentów elektronicznych (CRWDE)

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

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

W trakcie kontroli ustalono, że Urząd Miasta Iławy w badanym okresie nie przekazywał wzorów dokumentów elektronicznych do centralnego repozytorium wzorów dokumentów prowadzonego przez Ministerstwo Cyfryzacji, ze względu na fakt, iż nie uruchamiał nowej usługi, dla której nie ma wzorów dokumentów w CRWDE. Jednocześnie należy zaznaczyć, iż na stronie BIP kontrolowanego Urzędu w zakładce Menu Przedmiotowe – Druki i wzory dokumentów, opublikowano w wersji „do pobrania" formularze wzorów dokumentów niezbędnych do załatwienia poszczególnych spraw w Urzędzie.
Jednocześnie Urząd Miasta Iławy udostępniał oraz świadczył usługi elektroniczne, z wykorzystaniem ePUAP, na podstawie ogólnego wzoru: „Pismo ogólne do podmiotu publicznego" oraz „Skargi, wnioski, zapytania do urzędu".
W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 69, 75]

1.3. Model usługowy

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

Strona internetowa Urzędu działa pod adresem http://www.ilawa.pl/, a strona internetowa BIP Urzędu – pod adresem http://bip.umilawa.pl/.
Na stronie internetowej Urzędu zamieszczono link do strony BIP Urzędu w prawej górnej części panelu strony. Na stronie głównej Urzędu w zakładce Samorząd, Administracja - Urząd Miasta zamieszczono link do skrzynki podawczej ESP na platformie ePUAP.
Na stronie głównej BIP Urzędu, zamieszczono również link do skrzynki podawczej ESP na platformie ePUAP.
Ponadto na stronie internetowej UM i BIP UM, znajduje się link do najważniejszego serwisu internetowego ułatwiającego odbiorcy internetowemu załatwienie podstawowych spraw urzędowych, tj.:

– OBYWATEL.GOV.PL, który powstał jako część programu pl.ID, realizowanego w ramach Programu Operacyjnego Innowacyjna Gospodarka (7. Oś priorytetowa – Społeczeństwo informacyjne – budowa elektronicznej administracji) i współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego. Znajduje się tu kilkaset najpopularniejszych usług świadczonych przez administrację publiczną.

W Urzędzie brak jest formalnych procedur opisujących obsługę oraz monitorowanie usług elektronicznych, ze względu na fakt, iż instytucja ta 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. 76-77]

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 systemy teleinformatyczne zainstalowane i użytkowane w Urzędzie Miasta Iławy współpracują z systemami zewnętrznymi w następujących zakresach, cyt.: *„Program SELWIN współpracuje z systemem ŹRÓDŁO (SRP). Dane meldunkowe (PESEL) dane z zakresu stanu cywilnego (BUSC) oraz dane z Dowodów osobistych (RDO) są importowane do programu SELWIN w wydzielonej sieci ŹRÓDŁO. Współpraca jest możliwa jedynie dzięki odpowiedniemu sprzętowi oraz oprogramowaniu umożliwiającym wymianę danych z systemem ŹRÓDŁO”*

Jednocześnie należy wspomnieć, iż Źródło jest to system zarządzany przez Ministerstwo Cyfryzacji o charakterze ogólnopolskim, umożliwia współpracę z wcześniej opisywanym systemem teleinformatycznym. Stacje robocze na których zainstalowany jest system Źródło pracują w odizolowanej sieci. Dostęp do systemu uprawnieni użytkownicy uzyskują uwierzytelniając się poprzez logowanie do systemu Windows oraz przy pomocy kart kryptograficznych z zainstalowanymi certyfikatami dedykowanymi dla użytkownika aplikacji. W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 69]

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.*

Zgodnie z Zarządzeniem Nr 120-22/2014 Burmistrza Miasta Iławy z dnia 12 grudnia 2014 r. w sprawie zasad i trybu wykonywania czynności kancelaryjnych w Urzędzie Miasta Iławy, czynności kancelaryjne wykonywane są w systemie tradycyjnym, który jest podstawowym sposobem dokumentowania przebiegu spraw. Wspomagająco w stosunku do systemu tradycyjnego w Urzędzie wdrożono elektroniczny system zarzadzania dokumentacją (EZD).

Jednocześnie, w okazanej dokumentacji Urzędu brak jest procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby szczegółowe zasady obiegu dokumentów wpływających drogą elektroniczną oraz zakres stosowania elektronicznego obiegu dokumentów (skrzynka podawcza na platformie ePUAP e-mail, oraz EZD), co zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI, umożliwiłoby realizację i egzekwowanie, m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. Powyższe stanowi uchybienie.

Z wyjaśnienia pracownika odpowiedzialnego za realizacje zadania wynika, że cyt.: „*W UM nie ma regulacji wewnętrznych opisujących sposób zarządzania obiegiem dokumentów, w tym zakres stosowania elektronicznego obiegu dokumentów, w celu zapewnienia zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie. Urząd posiada tradycyjny obieg dokumentów oraz wspomagający system EZD. Wszystkie pisma elektroniczne są pobierane do EZD i przekazywane zgodnie z właściwością do odpowiedniego wydziału. Odpowiedzi elektroniczne są również realizowane tylko przez system EZD. Brak regulacji wewnętrznych spowodowane jest tym, iż w tym roku jest planowane wdrożenie projektu Przyjazny Cyfrowy Urząd w Iławie i w ramach projektu udostępniony będzie portal mieszkańca i spięty razem z EZD”*.

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

[akta kontroli str. 69-70, 78-92]

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 trakcie kontroli wynika, że cyt.*: „Dane z systemów są udostępniane w powszechnie dostępnych formatach plików (zał. nr 2 do KRI) np. podf, xls, xml, odt, html. Wymiana odbywa się za pomocą standardu kodowania znaków Unicode UTF-8. Systemy posiadają możliwość importu dokumentów elektronicznych."*

Systemy teleinformatyczne użytkowane w UM Iławy umożliwiają przyjmowanie dokumentów w wybranych formatach plików o których mowa w załączniku 2 rozporządzenia KRI w zakresie niezbędnym do prawidłowego załatwienia sprawy. Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 69]

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 0050-5/2013 Burmistrza Miasta Iławy z dnia 15 stycznia 2013 r. (zmienionym Zarządzeniem Nr 0120-11/2013 Burmistrza Miasta Iławy z dnia 7 maja 2013 r.) wprowadzono do stosowania w UM Iławy Instrukcję zarzadzania systemem informatycznym służącym do przetwarzania danych osobowych oraz Politykę bezpieczeństwa danych osobowych, zgodnie z obowiązującymi w tym okresie przepisami prawa, tj. ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. 2002 r., Nr 101, poz. 926 ze zm.) oraz rozporządzeniem 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 dokumenty, a w szczególności instrukcja zarządzania systemem informatycznym w Urzędzie, stanowiły dokumentację przetwarzania danych osobowych w rozumieniu §1 pkt 1 rozporządzenia MSWiA z 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych (…). Służyły one zapewnieniu poufności, integralności i rozliczalności przetwarzanych danych.

[akta kontroli str. 222-250]

– Zarządzeniem Nr 120-14/2018 Burmistrza Miasta Iławy z dnia 10 sierpnia 2018 r. w sprawie wprowadzenia Polityki Ochrony Danych przyjęto dokument stanowiący Politykę Ochrony Danych Osobowych w jednostce. Politykę Ochrony Danych Osobowych sporządzono na podstawie obowiązujących przepisów prawa, tj. RODO. Dokumentacja w zakresie ochrony danych dotyczyła danych przetwarzanych w Urzędzie i służyła zapewnieniu poufności, integralności przetwarzania danych, jak również monitorowania zdarzeń naruszających ochronę danych (w tym osobowych), zawierała także opis postępowania w przypadku naruszenia zasad bezpieczeństwa danych osobowych.

[akta kontroli str. 98-164]

Jednocześnie należy zaznaczyć, że zgodnie z punktem 21 (*Aktualizacje Polityki Ochrony Danych*) przyjętej w UM Iławy Polityki Ochrony Danych, powinna ona podlegać regularnym (nie rzadziej niż raz na rok) przeglądom dokonywanym przez Inspektora Ochrony Danych. W zależności od potrzeb mogą zostać przeprowadzone przez niego także dodatkowe przeglądy po stwierdzeniu istotnego naruszenia bezpieczeństwa, pojawieniu się zasadniczych zmian w jednostce, jego strukturze lub jego otoczeniu (nowe zagrożenia, technologie). Celem przeglądów polityki powinno być zapewnienie jej rozliczalności w stosunku do realizowanych zadań oraz możliwości obsługi interesantów w każdych warunkach niezależnie od okoliczności i zmian.
Do dnia kontroli tj. 16 maja 2019 r. IOD UM Iławy nie przeprowadził (brak dokumentacji w powyższym zakresie) takiego przeglądu. Powyższego zagadnienia nie poddano ocenie ze względu na istniejącą jeszcze możliwość przeprowadzenia przeglądu zgodnie z przyjętym w Polityce okresem czasowym - *nie rzadziej niż raz na rok*.

Zgodnie z pkt 18.1 Polityki, Informatyk przeprowadził okresową kontrolę uprawnień i kont użytkowników, w celu weryfikacji czy użytkownicy posiadają uprawnienia adekwatne do wykonywanej pracy w systemach informatycznych.

[akta kontroli str. 21, 23, 625]

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 przyjęta w UM Polityką Ochrony Danych pkt 19 - *Przeprowadzanie okresowych analiz ryzyka w zakresie bezpieczeństwa informacji,* głównym celem analizy ryzyka bezpieczeństwa informacji jest wyznaczenie właściwych kierunków działania kierownictwa oraz określenie priorytetów dla zarządzania ryzykami i zabezpieczeniami. Wyniki analizy ryzyka prowadzą do opracowania planu postępowania z ryzykiem obejmującego wprowadzenie rozwiązań umożliwiających odpowiednio: unikanie tych ryzyk, ograniczanie ich do akceptowanego poziomu, przeniesienie lub świadomą ich akceptację. Zaleca się, by zarządzanie ryzykiem w bezpieczeństwie informacji zapewniało:

1) zidentyfikowanie ryzyka,
2) oszacowanie ryzyka z punktu widzenia następstw dla działalności oraz prawdopodobieństwa wystąpienia,
3) informowanie o prawdopodobieństwie i następstwach ryzyka oraz zrozumienie tych informacji,
4) ustanowienie priorytetów postępowania z ryzykiem,
5) określenie priorytetów dla działań podjętych w celu zredukowania ryzyka,
6) regularne monitorowanie i przegląd różnych typów ryzyka oraz procesu zarządzania ryzykiem,
7) zbieranie informacji w celu doskonalenia podejścia do zarządzania ryzykiem,
8) szkolenie kierownictwa w zakresie ryzyka oraz działań podejmowanych w celu postępowania z ryzykiem.

Zgodnie z wymogiem wynikającym z § 20 ust. 2 pkt 3 rozporządzenia KRI, jak również przyjętej w UM Iławy Polityki Ochrony Danych w dniu 17 kwietnia 2019 roku Inspektor Ochrony Danych przeprowadził analizę ryzyka w zakresie bezpieczeństwa informacji

w Urzędzie Miasta Iławy i dokonał analizy zagrożeń przy przetwarzaniu danych osobowych w której określono źródła ryzyka, dokonano ich oceny (oszacowano % ryzyka i wagę dla IOD) oraz określono działania jakie należy podjąć w celu redukcji wykazanych zagrożeń (wydane zalecenia).

[akta kontroli str. 252-280]

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

[akta kontroli str. 281-297]

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.*

Kontrolującemu przedstawiono aktualną inwentaryzację sprzętu komputerowego użytkowanego w UM Iławy sporządzoną na potrzeby spisu inwentarzowego. Przedmiotowy spis zawierał dane dotyczące opisu sprzętu, numeru inwentarzowego, umiejscowienia i osoby odpowiedzialnej. Bardziej szczegółowa inwentaryzacja sprzętu i oprogramowania sporządzona zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI, prowadzona jest w formie elektronicznej przy pomocy oprogramowania LOG System. Przedmiotowa inwentaryzacja zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI obejmowała miedzy innymi rodzaj i konfigurację sprzętu. Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 183-196]

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 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 systemie informatycznym określone zostały w Zarządzeniu Nr 120-14/2018 Burmistrza Miasta Iławy z dnia 10 sierpnia 2018 r. w sprawie wprowadzenia Polityki Ochrony Danych. Zgodnie z procedurą opisaną w punkcie 12.1 Polityki:

1) Informatyk nadaje uprawnienia użytkownikom do pracy w systemach informatycznych na podstawie upoważnienia zatwierdzonego przez Administratora - *wzór wniosku stanowi załącznik nr 10 do* Polityki ochrony danych.
2) Informatyk dokonuje modyfikacji, zmiany lub wyrejestrowania uprawnień użytkowników systemów informatycznych na podstawie informacji otrzymanej od kierowników wydziału.
3) Wyrejestrowanie następuje poprzez:
   a) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
   b) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).
4) Wyrejestrowanie, może mieć charakter czasowy lub trwały.

Każdy z pracowników przetwarzających dane osobowe jak również pracujący w danym systemie teleinformatycznym otrzymał, zgodnie ze wzorem stanowiącym załącznik nr 10 do Polityki stosowne imienne upoważnienie do przetwarzania danych osobowych oraz do dostępu do danego systemu teleinformatycznego przetwarzającego dane osobowe.
Wszyscy pracownicy potwierdzili stosownym podpisem fakt zapoznania się z Polityką Ochrony Danych. W Urzędzie prowadzona była ewidencja osób upoważnionych do przetwarzania danych osobowych zgodnie z zał. nr 12 do Polityki, w tym ewidencja osób uprawnionych do pracy w systemach, zawierająca: imię i nazwisko, stanowisko, datę nadania, datę ustania oraz zakres upoważnienia. Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 197-217]

2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Z § 20 ust. 2 pkt 6 rozporządzenia KRI wynika, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: a) zagrożenia bezpieczeństwa informacji, b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.*

W okresie objętym kontrolą pracownicy UM uczestniczący w procesie przetwarzania danych brali udział w szkoleniach, w zakresie zdobycia wiedzy i umiejętności dotyczących ochrony

danych osobowych:

- w dniu 18 września 2018 r. – szkolenie z ochrony danych osobowych RODO,
- w dniu 22 stycznia 2019 r. – szkolenie z ochrony danych osobowych RODO,
- w dniu 18 marca 2019 r. – szkolenie z ochrony danych osobowych RODO,
- w dniu 17 kwietnia 2019 r. – szkolenie z ochrony danych osobowych RODO.

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 94-97]

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 informacji uzyskanych w UM Iławy wynika że cyt.: *„Wszystkie komputery przenośne mają możliwość pracy tylko w Urzędzie Miasta. Pracownicy nie zabierają ze sobą komputerów do domu. Prowadzona jest inwentaryzacja laptopów. Informatyk posiada laptop poza miejscem pracy. Laptop jest zaszyfrowany programem TrueCrypt oraz posiada zabezpieczenie w postaci loginu i hasła do systemu windows. Połączenie z UM odbywa się za pomocą dedykowanego oprogramowania z UTM poprzez połączenie VPN, (komputer oraz użytkownik jest zautoryzowany w UTM - Nie ma możliwości połączenia z zewnątrz z innego komputera).”*

Ponadto wprowadzona w UM Iławy Polityka Ochrony Danych w przypadku urządzeń przenośnych stanowi, że:

- Zakazuje się podłączania nośników pamięci flash na służbowych komputerach. Zakaz dotyczy wszelkich nośników jak pendrive, telefon, karty SD itp.
- Pamięci flash wynoszone poza obszar przetwarzania jakim jest Urząd muszą być szyfrowane, zabezpieczone hasłem co najmniej 8 - znakowym zawierającym: małe, wielkie litery, znaki specjalne lub cyfry
- Transportu i użytkowanie komputera przenośnego musi się odbywać w sposób minimalizujący ryzyko kradzieży lub zniszczenia, zdecydowanego i skutecznego uniemożliwienia korzystania z komputera osobom nieuprawnionym (np. rodzinie, dzieciom, znajomym).

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

[akta kontroli str. 70, 111]

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 Iławy użytkowane są 2 systemy teleinformatyczne do realizacji zadań publicznych zakupione u zewnętrznego dostawcy, tj.: SELWIN oraz Pomost. W związku z zakupem ww. systemów podpisane zostały umowy licencyjne z firmami: Sygnity SA (Pomost - oprogramowanie do obsługi Zespołów Interdyscyplinarnych ZI) oraz ARAM Software Sp. z o.o. (SELWIN).
Wraz z umowami licencyjnymi (asysta techniczna) z każdą firmą dostarczającą dany system informatyczny powinna zostać podpisana właściwa umowa powierzenia danych, gwarantująca poprzez zawarcie w niej określonych zapisów właściwe zabezpieczenie danych w przypadku awarii systemu oraz gwarantująca bezpieczeństwo informacji uzyskanych przez wykonawców w związku z realizacją umowy. W wyniku prowadzonych czynności kontrolnych nie stwierdzono w przedstawionej dokumentacji przedmiotowych umów powierzenia – co stanowi uchybienie. Zapisy zawarte w umowach licencyjnych gwarantują pewien poziom bezpieczeństwa, jednak podpisanie właściwych umów powierzenia danych gwarantuje odpowiedni wysoki poziom bezpieczeństwa przetwarzanych informacji. Na zadane przez kontrolującego pytanie dotyczące przyczyny braku podpisanych umów powierzenia danych osobowych, zgodnie ze wzorem stanowiącym zał. nr 16 do wprowadzonej Polityki Ochrony Danych Osobowych, Podinspektor (Informatyk) UM Iławy wyjaśnił, że brak podpisanych umów powierzenia danych wynika z niedopatrzenia i zostanie uzupełniony w najbliższym czasie.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami. Osoba odpowiedzialna jest Podinspektor (Informatyk) UM Iławy.

[akta kontroli str. 70, 152, 168-182]

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 ochrony danych osobowych w przypadku Urzędu

Miasta Iławy został uregulowany Zarządzeniem Nr 120-14/2018 Burmistrza Miasta Iławy z dnia 10 sierpnia 2018 r. w sprawie wprowadzenia Polityki Ochrony Danych, zał. nr 18 – Procedura zgłaszania naruszeń ochrony danych osobowych.
Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 159-165]

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.*

Zgodnie z Zarządzeniem Nr 120-14/2018 Burmistrza Miasta Iławy z dnia 10 sierpnia 2018 r. w sprawie wprowadzenia Polityki Ochrony Danych pkt 20 – *Audyt wewnętrzny w zakresie bezpieczeństwa informacji* podmioty realizujące zadania publiczne zobowiązane są do przeprowadzenia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok, bowiem utrzymywanie wysokiego poziomu bezpieczeństwa informacji, wymaga stałego monitorowania i okresowego badania stanu zabezpieczenia wszystkich elementów tego systemu.
W okresie objętym kontrolą obejmującym okres od 1 stycznia 2018 rok do dnia rozpoczęcia czynności kontrolnych (16 maja 2019 r.) przeprowadzono jedno zadanie audytowe. W dniach od 14.06.2018 r. do 30.07.2018 r. został przeprowadzony w Urzędzie Miasta Iławy przez firmę: Centrum Bezpieczeństwa Informatycznego audyt bezpieczeństwa informacji. W ramach przeprowadzonego audytu dokonano również analizy wykorzystania sprzętu oraz przeprowadzono audyt zainstalowanego oprogramowania. Celem audytu było przedstawienie zaobserwowanego przez audytorów stanu bezpieczeństwa informacji w jednostce oraz wskazanie ewentualnych podatności mających wpływ na przetwarzane dane. Audyt został przeprowadzony pod kątem zgodności z obowiązującymi przepisami prawa w zakresie przetwarzania informacji oraz dobrych praktyk i standardów bezpieczeństwa. Audyt został zrealizowany na podstawie udostępnionej przez Urząd dokumentacji (procedur) oraz sprzętu.

[akta kontroli str. 298-613]

W zakresie realizacji rekomendacji poaudytowych pracownik Urzędu wyjaśnił, że cyt: *„W UM zostały zabezpieczone drzwi w serwerowni, czujnik dymu, wymieniony zasilacz UPS z kartą sieciową, została wyłączona ogólnodostępna sieć WI-FI, aktualizacje systemu są przeprowadzane na bieżąco z poziomu konsoli oprogramowania antywirusowego. Wprowadzono rejestr osób pobierających klucze zapasowe, zmieniono domyślne hasła administratora w urządzeniach, sporządzono ewidencję haseł i zdeponowano ją w sejfie. Domena Active Directory na systemie Samba 4."*

[akta kontroli str. 70]

W związku z dopełnieniem w 2018 roku obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI oraz Polityki Ochrony Danych, 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 - przedmiotowe cząstkowe zagadnienie w zakresie 2018 roku ocenia się pozytywnie. W przypadku 2019 roku zaznaczyć należy, że do dnia kontroli (16.05.2019) wymagany roczny audyt bezpieczeństwa informacji nie został jeszcze przeprowadzony. Wobec powyższego dopełnienie obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI, w przypadku roku 2019 nie podlegało ocenie, ze względu na istniejącą możliwość przeprowadzenia przez jednostkę audytu bezpieczeństwa informacji do końca 2019 roku.

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.

Procedura tworzenia kopii zapasowych w przypadku Urzędu Miasta Iławy określona została w Polityce Ochrony Danych przyjętej Zarządzeniem Nr 120-14/2018 Burmistrza Miasta Iławy z dnia 10 sierpnia 2018 r. Zgodnie z wytycznymi zawartymi w Polityce dane osobowe przetwarzane w formie elektronicznej w systemach teleinformatycznych podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada informatyk zatrudniony w jednostce. Częstotliwość tworzenia kopii zapasowych danych przetwarzanych w Urzędzie zgodnie z przyjętą Polityką określono jako cykl codzienny.
Z wyjaśnienia pracownika odpowiedzialnego za wykonywanie kopii zapasowych (Informatyk UM Iławy) wynika, że cyt.: *„Kopie zapasowe są tworzone w harmonogramie: codziennie 60 kopii rotacyjnych i 5 pełnych kopii każdego użytkownika, które są trzymane na serwerze w UM. O prawidłowości wykonania kopii zapasowej administrator powiadamiany jest codziennie raportem mailowym (...).”* Powyższe potwierdza pobrana w toku kontroli dokumentacja.
Jednocześnie kontrolujący stwierdził, że w UM Iławy nie są wykonywane jakiekolwiek testy w celu sprawdzenia poprawności wykonywania kopii zapasowych oraz sprawdzenie przydatności utworzonych kopii podczas próby symulowanego przywrócenia i uruchomienia

oprogramowania dziedzinowego po przywróceniu. Powyższy stan potwierdził również pracownik odpowiedzialny za realizację zadania. Brak przeprowadzanych testów w celu sprawdzenia poprawności wykonywania kopii zapasowych stanowi uchybienie.
Jednocześnie należy zaznaczyć, iż problem dotyczący braku testowania kopii zapasowych sygnalizowany był również w przeprowadzonej w Urzędzie analizie ryzyka przy przetwarzaniu danych osobowych, gdzie ryzyko wpływu na proces przetwarzania danych osobowych oszacowano jak jedno z większych.

Odnoszą się do powyższego należy stwierdzić, iż regularne testowanie jakości kopii zapasowych poprzez odtworzenie systemu informatycznego z kopii zwykle na niezależnym od środowiska produkcyjnego sprzętowym środowisku testowym oraz testowaniu pracy użytkowej odtworzonego systemu jest kluczowym działaniem w celu minimalizowania ryzyka utraty informacji w wyniku awarii. Wskazane jest przechowywanie kopii zapasowych w innej lokalizacji niż miejsce ich tworzenia, w odległości niezbędnej do uniknięcia uszkodzeń spowodowanych przez katastrofę, która dotknęłaby ośrodek podstawowy przetwarzania danych.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami. Osoba odpowiedzialna jest Podinspektor (Informatyk) UM Iławy.

[akta kontroli str. 70, 147-148, 274, 277, 614-616]

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.*

Wykorzystywane w Urzędzie systemy teleinformatyczne wspomagające realizację zadań z zakresu administracji rządowej dzieliły się na systemy centralne tj. ŹRÓDŁO i CEiDG oraz 2 systemy wspierające zakupione u dostawców zewnętrznych SELWIN oraz Pomost. Na obsługę aktualnie zainstalowanego oprogramowania z każdą firmą dostarczającą dany system informatyczny zawarto stosowne umowy licencyjne (asysta techniczna), gwarantujące rozwój systemu i dostosowanie do obowiązujących przepisów prawa. Systemy teleinformatyczne, w razie awarii podlegają ekspertyzie technicznej zlecanej firmie zewnętrznej. Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 28, 168-175, 179-180]

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.
Z wyjaśnień uzyskanych w UM Iławy wynika, że w celu zabezpieczenia danych będących w posiadaniu w UM oraz uzyskania maksymalnego poziomu bezpieczeństwa ich przetwarzania zastosowano:

- Monitoring wizyjny - rejestrator znajduje się w pomieszczeniu Serwerowni.
- System alarmowy - instalacja alarmowa obejmuje IV strefy: - Księgowość/Kasę, I kondygnację, II kondygnację oraz pomieszczenia Urzędu Stanu Cywilnego. Każda strefa posiada wydzielony alarm. Czujki zlokalizowane są na korytarzach oraz w większości pomieszczeń. Instalacja uruchamiana jest za pomocą kodów, do których dostęp mają upoważnieni pracownicy.
- Po zakończeniu pracy - każdy pracownik zamyka pomieszczenie i deponuje klucz w wyznaczonym punkcie. Klucze do pomieszczeń biurowych pracownicy deponują w punkcie obsługi interesanta w gablocie zamykanej na klucz. Klucz do gabloty znajduje się w dyspozycji pracownika, a po godzinach urzędowania - w dyspozycji pracownika ochrony.
- Klucze zapasowe zdeponowane są: w oddzielnym pomieszczeniu w gablocie zamykanej na klucz będący w dyspozycji upoważnionej osoby. Prowadzony jest rejestr osób pobierających klucze zapasowe.
- Monitoring stacji roboczych oraz ruchu sieciowego odbywa się za pomocą oprogramowania LOGSystem.
- Dostęp do stron zabronionych, gier online, gier hazardowych i innych niepożądanych treści blokowane z poziomu UTM (wielofunkcyjne zapory sieciowe).
- UTM na końcówce INTERNET.

- Na każdym komputerze jest możliwość zalogowania się na wydzielone konto administratora domeny oraz na konto lokalnego administratora – użytkownicy nie posiadają praw administratora.
- Urząd posiada licencję na oprogramowanie antywirusowe COMODO na 100 licencji z zaporą sieciową, automatyczna piaskownicą oraz możliwością aktualizacji oprogramowania WINDOWS.

[akta kontroli str. 70-71, 621-624, 626-627]

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 jednostka kontrolowana zastosowała 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: CEIDG, POMOST, SelWIN 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. Zastosowano urządzenia typu UPS chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania,

Podczas kontroli dokonano także oględzin pomieszczenia serwerowni Urzędu Miasta

Iławy. W wyniku oględzin stwierdzono, że drzwi wejściowe do serwerowni są to specjalistyczne drzwi wzmocnione zabezpieczone zamkiem szyfrowym odblokowywanym kartą kodową, pinem lub kluczem. W serwerowni zamontowano czujnik wejścia i wyjścia z powiadomieniem (sms) na telefon informatyka. W pomieszczeniu zainstalowano urządzenie klimatyzujące, UPS oraz czujki monitorujące zadymienie i temperaturę. W przypadku nagłego wzrostu temperatury w pomieszczeniu urządzenie wysyła powiadomienie (sms) na telefon informatyka. Stwierdzone uchybienia to: brak czujki monitorującej wilgotność, brak czujki monitorującej zalanie pomieszczenia (w pomieszczeniu znajduje się sieć CO). W pomieszczeniu ponadto przechowywany był stary sprzęt przeznaczony do utylizacji.
Powyższe potwierdza dokumentacja z przeprowadzonych oględzin.

[akta kontroli str. 70, 644-654]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami.

2.14. Rozliczalność działań w systemach informatycznych

Stosownie do:

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

Z wyjaśnienia pracownika odpowiedzialnego za realizacje zadania wynika, że cyt.: *„Urząd gromadzi logi systemowe w bazach posiadanych programów. Logi przechowywane są w programie SELWIN od co najmniej 2016 r.”* Z przekazanej dokumentacji wynika że logi w zakresie systemu POMOST przechowywane są również od 2016 r.
Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 71, 617-620]

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 Miasta Iławy, ze względu na brak interakcji z klientami zewnętrznymi za pośrednictwem publicznej sieci Internet nie są objęte wymogami WCAG 2.0.

Zarówno strona internetowa BIP jaki i 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 w przypadku BIP oraz ikony dla niedowidzących - w przypadku strony www., a także (A+ A-) umieszczonej w przypadku obydwu stron w górnej części panelu strony. 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.

Powyższe zagadnienie oceniono pozytywnie.

[akta kontroli str. 655-656]

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny wnoszę o:

1. Uzupełnienie strony BIP Urzędu (zakładka „Procedury załatwiania spraw"), poprzez opisanie wszystkich 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 zasady obiegu dokumentów wpływających do Urzędu drogą elektroniczną.
3. Podpisanie z każdą firmą zewnętrzną dostarczającą dany system informatyczny

wykorzystywany do realizacji zadań zleconych z zakresu administracji rządowej, właściwej umowa powierzenia danych, gwarantującej odpowiednie zabezpieczenie danych w przypadku awarii systemu oraz bezpieczeństwo informacji uzyskanych przez wykonawców w związku z realizacją umowy.

4. Przeprowadzanie testów poprawności wykonywanych kopii zapasowych, w celu zminimalizowania ryzyka utraty danych.
5. Doposażenie pomieszczenia serwerowni o czujkę monitorującą wilgotność oraz czujkę sygnalizującą zalanie pomieszczenia, jak również usunięcie z pomieszczenia serwerowni zużytego sprzętu elektronicznego przeznaczonego do utylizacji.

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